ANKARA ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ ANABİLİM DALI

EĞİTİM TEKNOLOJİSİ DOKTORA PROGRAMI

YÜKSEKÖĞRETİM KURUMLARINDAKİ ÖĞRETİM ELEMANLARININ BİLGİ GÜVENLİĞİ FARKINDALIK DÜZEYLERİNİN DEĞERLENDİRİLMESİ

DOKTORA TEZİ

Can GÜLDÜREN

Danışman: Hafize KESER

Ankara, Temmuz, 2015

Eğitim Bilimleri Enstitüsü Müdürlüğü'ne,

Can GÜLDÜREN' in hazırladığı "Yükseköğretim Kurumlarındaki Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Düzeylerinin Değerlendirilmesi" başlıklı bu çalışma jürimiz tarafından Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı/Eğitim Teknolojisi Programı'nda Doktora Tezi olarak kabul edilmiştir.

İmza

Başkan ……. …….

Üye ……. …….

Üye ……. …….

Üye ……. …….

Üye ……. …….

ONAY

Bu tez Ankara Üniversitesi Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliği'nin ilgili maddeleri uyarınca yukarıdaki jüri üyeleri tarafından …../…../ 2015 tarihinde uygun görülmüş ve Enstitü Yönetim Kurulunca …../…../ 2015 tarihinde kabul edilmiştir.

Prof. Dr. İsmail GÜVEN

Eğitim Bilimleri Enstitüsü Müdürü

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

Can GÜLDÜREN

ÖZET

YÜKSEKÖĞRETİM KURUMLARINDAKİ ÖĞRETİM ELEMANLARININ BİLGİ GÜVENLİĞİ FARKINDALIK DÜZEYLERİNİN DEĞERLENDİRİLMESİ

Güldüren, Can
Doktora, Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı
Tez Danışmanı: Prof.Dr. Hafize Keser
Temmuz 2015, xvi + 149 sayfa

Bu araştırmanın temel amacı; yükseköğretim kurumlarında görev yapan öğretim elemanlarına bilgi güvenliği farkındalığı kazandırmaya yönelik, çoklu ortam materyallerini içeren bir web sitesi geliştirmek ve geliştirilen web sitesinin bilgi güvenliği farkındalığı kazandırmadaki etkisini belirlemektir. Bu kapsamda araştırma iki aşamadan oluşmaktadır.

Araştırmanın birinci aşamasında, yükseköğretim kurumlarında çalışan öğretim elamanlarının bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik bir ölçek geliştirilmiştir. Ölçek geliştirme çalışması, Eylül 2013 – Nisan 2014 tarihleri arasında Türkiye'de çeşitli yükseköğretim kurumunda görev yapan 363 öğretim elemanıyla gerçekleştirilmiştir. Açımlayıcı faktör analizi sonucunda, ölçeğin 34 madde ve 2 alt boyuttan ("saldırı ve tehditler" ile "kişisel verilerin korunması") oluştuğu belirlenmiştir. Katılımcılar arasından rastgele seçilen 200 kişilik grup üzerinde yapılan doğrulayıcı faktör analizi sonucunda 2 faktörlü yapı doğrulanmıştır. Ölçeğin tamamı için Cronbach Alfa güvenirlik katsayısı .97; her alt boyut için sırasıyla .97 ile .94'tür. Bu çalışma sonucunda yükseköğretim kurumlarındaki öğretim elemanlarının bilgi güvenliği farkındalık düzeylerini belirlemek için kullanılabilecek geçerli ve güvenilir bir ölçek geliştirilmiştir.

Araştırmanın ikinci aşamasında, yükseköğretim kurumlarında görev yapan öğretim elemanlarına bilgi güvenliği farkındalığı kazandırmaya yönelik çoklu ortam materyallerini içeren bir web sitesi geliştirmek ve bilgi güvenliği farkındalığı kazandırmadaki etkisini belirlemek amaçlanmıştır. Araştırmada 2x2'lik bir karışık desen (split-plot) kullanılmıştır. Desendeki iki düzeyden oluşan birinci faktör iki ayrı deneysel işlemi ("Bilgi Güvenliği ve Farkındalık" web sitesini kullanan deney grubunu,

“Bilgi Güvenliği ve Farkındalık” web sitesini kullanmayan kontrol grubunu); desendeki iki düzeyden oluşan ikinci faktör ise deneysel işlem öncesi ve sonrası ölçümleri (öntest, sontest) göstermektedir. Çalışma Haziran 2014 – Ocak 2015 tarihleri arasında bir üniversitenin eğitim bilimleri fakültesinde görev yapmakta olan 65 öğretim elemanı (Deney Grubu:31, Kontrol Grubu:34) üzerinde 12 hafta süresince yürütülmüştür. Öğretim elemanları iki farklı çalışma grubuna yansız olarak atanmışlardır. Araştırmanın verileri bilgi güvenliği farkındalık ölçeği ve web sitesi değerlendirme formundan elde edilmiştir. Araştırmada elde edilen veriler, t-testi, ANOVA ve ANCOVA ile incelenmiştir. Öğretim elemanlarının web sitesi değerlendirme formuna verdiği cevaplar ise frekans ve yüzde tabloları şeklinde ifade edilip, yorumlanmıştır.

Araştırma sonuçlarına göre “Bilgi Güvenliği ve Farkındalık” web sitesinin kullanılıp kullanılmamasına göre çalışma gruplarının son test bilgi güvenliği farkındalık düzeyi toplam puanları karşılaştırıldığında; Deney Grubu ile Kontrol Grubu'ndaki öğretim elemanları arasında anlamlı bir farklılık olduğu görülmüş ve geliştirilen çoklu ortam materyalleri ile web sitesinin son test bilgi güvenliği farkındalık düzeyi toplam puanlarını artırdığı belirlenmiştir. Açık uçlu sorulara yönelik veri analizi sonucuna göre, bilgi güvenliği farkındalığı konusunda genel bilgilendirme açısından yararlı ve iyi tasarlanmış olduğu; ayrıca detaylı ve önemli noktalara değinilerek hazırlanan videolar ile oldukça faydalı ve kullanımı kolay olarak değerlendirilmiştir.

Anahtar Kelimeler: Bilgi, güvenlik, farkındalık, bilinçlendirme, bilgi güvenliği, ölçek geliştirme.

SUMMARY

EVALUATION OF INFORMATION SECURITY AWARENESS LEVEL OF THE FACULT MEMBERS

GÜLDÜREN, Can

Doctor of Philosophy, Computer Education and Instructional Technologies Department

Thesis Supervisor: Prof. Dr. Hafize KESER

July 2015, xvi + 149 pages

The purpose of this study is to develop a web site for faculty members to determine the level of information security awareness and to learn about the effectiveness of the web site which includes developed multimedia materials in gaining information security awareness. In this context, the study consists of two phases.

In the first phase of the study, a scale has been developed to determine the level of information security awareness of faculty members. Scale development study was carried out with 363 faculty members working in various higher education institutions in Turkey in September 2013 – April 2014. As a result of exploratory factor analysis, it was determined that the scale consists of 34 items and 2 subscales (‘attacks and threats’ and ‘the protection of personal data’). Confirmatory factor analysis was conducted with randomly selected group of 200 academicians among participants. Two-factor structure was confirmed. Cronbach's alpha reliability coefficient is .97 for the entire scale; .94, .97, respectively, for each subscale. Consequently in this study, a valid and reliable instrument which can be used to determine the level of information security awareness of faculty members has been developed.

In the second phase of the study, a web site including developed multimedia materials has been developed to learn about the effectiveness of the web site in gaining information security awareness. 2x2 mixed design (split-plot) was used in the study. The first factor in the design, which was composed of two levels, consisted of two different experimental processes (Experimental Group which is used "Information Security and Awareness" web site, Control Group which is not used "Information Security and Awareness" web site); while the second factor, which was composed of two levels, consisted of pre and post-experiment measurements (pre-test and post-test).

The study was carried out twelve weeks with 65 faculty members (Experimental Group:31, Control Group:34) working in a faculty of educational science of a university in Turkey in June 2014 – January 2015. Faculty members were randomly assigned to one of the two study groups. The data of the study were obtained from the information security awareness scale and the web site evaluation form. The data were analyzed using t-test, ANOVA and ANCOVA. The faculty member' responses to the questions in the interview form were analyzed through frequency and percentage rates.

In accordance with the results of the study, when the post-test information security awareness scores of the study groups were compared based on whether using "Information Security and Awareness" web site including multimedia materials or not, it was found that there was a statistically significant difference between the faculty members in Experimental Group and Control Group; and that using "Information Security and Awareness" web site including multimedia materials increased the post-test scores. According to the results of the open-ended questions data analysis, it is considered as useful and well designed in terms of general information about information security awareness. It is also considered as very useful and easy to use web site with video prepared by reference to the detailed and important points.

Keywords: Information, security, awareness, awareness raising, information security, scale development.

ÖNSÖZ

Bilgi ve iletişim teknolojileri alanındaki hızlı değişme ve gelişmeler, İnternetin yaygın olarak kullanılması ve İnternet üzerinde kullanılan çevrimiçi uygulamalardaki artış, beraberinde güvenlik açıklarının artışına sebep olmaktadır. Bilgi güvenliği, bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişimini, kullanımını, değiştirilmesini, ifşa edilmesini, ortadan kaldırılmasını, el değiştirmesini ve hasar verilmesini önlemek olarak tanımlanabilir. Gizlilik, bütünlük ve erişilebilirlik olarak isimlendirilen üç temel unsurdan meydana gelir. Bu üç temel güvenlik öğesinden herhangi biri zarar görürse güvenlik zafiyeti oluşur. Bilgi güvenliği kurumlar ve bireyler için vazgeçilmez ve değerli bir varlık olan bilginin korunması için gerekmektedir. Bir diğer husus ise bilginin işlenmesi için kullanılan ve sürekli gelişim gösteren teknolojilerin de bilgi unsuru için riskler yarattığı gerçeğidir. Günümüzde, bilgi sistemlerinin küreselleşmesi sonucunda bu sistemlerle doğrudan veya dolaylı yönden ilişkili olan ve bu sistemleri kullanan tüm birey ve kurumların artık bilgi güvenliğine katkıda bulunması gerekmektedir.

Bilgi sistemleri bir zincir olarak düşünüldüğünde, bu zincirin en zayıf halkasının genelde sistemin kullanıcıları olduğu görülmektedir. Bilgi güvenliği seviyesi bu durumda kullanıcılara bağlı olduğundan, kullanıcı farkındalığı bilgi güvenliğinin sağlanmasında son derece kritik bir öneme sahiptir. Alanyazın incelemesiyle elde edilen sonuçlar bilgi güvenliği farkındalığı açısından yükseköğretim kurumlarının çok iyi durumda olmadığına işaret etmektedir. Bilginin üretiminden, öğretiminden, sunumundan ve dağıtımından sorumlu temel ve öncü kurumlardan olan üniversiteler ve öğretim elemanları bu görevlerini yerine getirirken bilgi güvenliği konusunu ön planda tutmak ve kendilerini bu konuda yetiştirmek zorundadırlar. Bu bağlamda, toplumu ve öğrencileri bilinçlendirme görevi üstlenecek olan öğretim elemanlarının bilgi güvenliği farkındalıklarının hangi düzeyde olduğu, bu konuda eksikliklerinin hangi alanlarda yoğunlaştığının belirlenmesi önem arz etmektedir. Ancak, yükseköğretim kurumlarındaki öğretim elemanlarına yönelik olarak yapılan çalışmalar oldukça az sayıdadır. Yükseköğretim kurumlarındaki öğretim elemanlarının bilgi güvenliği farkındalık düzeylerinin belirlenebilmesi ve bilgi güvenliği farkındalığının

arttırılabilmesi için gerekli önlemlerin alınabilmesi gibi nedenlerle, bu konularda yapılacak çalışmalara ihtiyaç duyulmaktadır.

Bu araştırmanın temel amacı; yükseköğretim kurumlarında görev yapan öğretim elemanlarına bilgi güvenliği farkındalığı kazandırmaya yönelik, çoklu ortam materyallerini içeren bir web sitesi geliştirmek ve geliştirilen web sitesinin bilgi güvenliği farkındalığı kazandırmadaki etkisini belirlemektir.

Araştırma beş bölümden oluşmaktadır. Birinci bölümde, araştırma kapsamındaki problem, amaç, alt amaçlar, önem, sınırlılıklar, tanımlar ve kısaltmalara ilişkin bilgilere yer verilmiştir. İkinci bölümde, kavramsal çerçeveye yer verilmiş; bilgi güvenliği farkındalığıyla ilgili ulusal ve uluslararası araştırmalar incelenmiştir. Üçüncü bölümde araştırmanın modeli, evren ve örneklem, veri toplama araç ve teknikleri ile verilerin toplanması ve verilerin analizine ilişkin bilgilere yer verilmiştir. Dördüncü bölümde, ölçek geliştirme çalışması, deneysel çalışma sonucu elde edilen veriler ile araştırma grubunun kişisel özelliklerine yönelik bulgu ve yorumlara ve bilgi güvenliği farkındalık ölçeğinden elde edilen puanlar ile deney ve kontrol grubu arasındaki ilişkiye yönelik bulgu ve yorumlara yer verilmiştir. Beşinci bölümde araştırma kapsamında elde edilen sonuçlara ve sonuçlar göz önünde bulundurularak yapılan önerilere yer verilmiştir.

TEŞEKKÜR

Yüksek lisans ve doktora eğitimim süresince emeği geçen, araştırmanın başından sonuna kadar devam eden süreçte her türlü desteğini ve yardımlarını esirgemeyen, her konudaki bilgi ve tecrübesine rahatlıkla başvurabildiğim, bana önemli katkılar sağlayan ve birlikte çalışmaktan onur duyduğum saygı değer tez danışmanım Prof. Dr. Hafize KESER' e,

Değerli fikirleri ve yönlendirmeleriyle araştırmaya önemli katkılar sağlayan ve tanımaktan onur duyduğum saygı değer hocalarım Prof. Dr. Ahmet MAHİROĞLU, Doç. Dr. Selçuk ÖZDEMİR, Doç. Dr. Tolga GÜYER ve Yrd. Doç. Dr. Necmettin TEKER' e,

Bu çalışmanın gerçekleştirilmesi sırasında yardımlarını esirgemeyen Arş. Grv. Melike KAVUK' a, ölçek geliştirme ve deneysel aşamaya katılan öğretim elemanları ile adlarını saymakla bitiremeyeceğim, araştırmaya katkı sağlayan desteklerini gördüğüm değerli hocalarıma, çalışma arkadaşlarıma,

Bana inanan, güvenen, sevgi ve desteklerini her zaman hissettiğim ve canımdan çok sevdiğim aileme ve arkadaşlarıma, eğitim çalışmalarım esnasında her türlü desteği veren eşim Kıymet GÜLDÜREN, oğlum İsmet Berke GÜLDÜREN ve kızım Cansu GÜLDÜREN' e sonsuz teşekkürler...

İÇİNDEKİLER

ÇİZELGELER DİZİNİ

ŞEKİLLER DİZİNİ

BÖLÜM 1

1.GİRİŞ

Bu bölümde araştırmanın problem durumundan, amacından, öneminden, sınırlılıklarından ve araştırmayla ilgili önemli kavramlardan işlevsel olarak bahsedilmiştir.

1.1.Problem

Günümüzde teknolojiyi temsil eden ve cisimsiz varlık olarak nitelendirilen bilgi (Gemci ve Bay, 2011), insanlık tarihi boyunca politik ve sosyal yaşamdan ekonomik olaylara kadar tüm hayatı kuşatmıştır (Çirasun, 2011). Yaşadığımız çağda bilgi, ekonomik, sosyal ve kültürel gelişmenin en önemli anahtarı konumundadır. Ülkelerin zenginliğinin belirlenmesinde, vazgeçilmez kilit bir kavramdır. Ayrıca, ekonomik faaliyetlerin temelinde de bilgi yatmakta ve bilginin etkin olarak kullanımı ülkelerin zenginliğinin alt yapısını ve itici gücünü oluşturmaktadır (Aslan, 2007; Berberoğlu, 2010).

Bilgi insanoğlunun yaşamını, düşüncesini, davranışını, iletişimini, gelişimini, üretmesini, tüketmesini belirleyen faktörlerin başındaki yerini her zaman korumuştur. İnsanoğlu varoluşundan bu yana daha nitelikli bir yaşam için bilgiye ulaşma, kullanma ve sahip olma gereksinimi duymuştur. Bu gereksinim bilgi ve iletişim teknolojilerinin hızlı bir şekilde gelişiminin en önemli nedeni olmuştur (Vardal, 2009).

Bilgi ve iletişim teknolojilerinin gelişimiyle birlikte zaman, mekân ve coğrafi uzaklık gibi faktörlerden kaynaklanan sınırlamalar ortadan kalkmıştır. Bilgiye erişimin kolaylaşması, bilgi ağlarının yoğunlaşması, buna bağlı olarak gelişen karşılıklı bağımlılık ilişkileri ve toplumların giderek daha çok birbirine benzeşmesi ile birlikte yaşanılan yüzyıl artık küresel köy, küresel bilgi toplumu, bilgi toplumu terimleriyle tanımlanmaktadır (Alaboodi, 2006). Tandoğan ve diğerleri (1998), ülkeler için bilgi toplumuna geçişte, teknolojinin temel teşkil etmekte olduğunu ve bilginin, toplum tarafından bir güç olarak görüldüğünü ifade etmektedir.

Friedman (2007), hizmet ve bilgi ve iletişim teknolojileri (BİT) alanlarında Amerika Birleşik Devletleri (ABD) ve diğer sanayileşmiş ülkelere taşeronluk yapan

Hindistan'ı göz önünde bulundurarak, bilgisayar ve internet teknolojisinin yuvarlak olan dünyayı düzleştirdiğini ifade etmektedir. Hindistan ile sembolize edilen yapı, aslında BİT 'in yaygınlaşmasıyla tüm dünyada ekonomik ve sosyal gelişmenin önemli itici güçlerinden "bilgi toplumu" nu ifade etmektedir (Civelek, 2011). Çeşitli ülkelerin resmi politika belgelerine bakıldığında bilgi toplumu; sosyo-ekonomik faaliyetlerin giderek etkileşimli sayısal iletişim ağlarının katılımıyla veya bu iletişim ağlarının yoğun kullanımıyla gerçekleştirilmesi yanında, bu amaçla kullanılan her türlü teknolojinin ve uygulamanın üretilmesi olarak tanımlanmaktadır (TÜBİTAK, 2002, s. 4; Berberoğlu, 2010).

Bilgi toplumunun temel özelliği, BİT sayesinde bilgi üretiminin önem kazanmasıdır (Aslan, 2007). Yaşanılan çağda ülkelerin en önemli serveti, sahip olunan para ya da doğal kaynak miktarı değil, bunların bilgi üretme yeteneği ve sahip olunan nitelikli insan kaynağıdır (Berberoğlu, 2010). Dolayısıyla bilgi toplumunda, birey merkezi bir konuma sahiptir ve bilgi, toplumun stratejik kaynağını oluşturmaktadır. Bilginin temel özelliği ise, sürekli üretilebilmesi ve artış göstermesi; iletişim ağları içinde taşınabilir; bölünebilir ve paylaşılabilir olmasıdır (Aslan, 2007)

Bilgi ve iletişim teknolojilerindeki hızlı yaygınlaşma; bilgi yönetimi, iş verimliliği, hızlı iş akışı, kolay ve hızlı iletişim kurabilme gibi insan yaşamına sunduğu yeteneklerle, üretilen ve tüketilen bilgide artışa sebep olmuştur. Bu hızlı yaygınlaşma, bilginin elektronik ortamlarda işlenmesine, taşınmasına, saklanmasına, zamandan ve mekândan bağımsız istenilen ortamlardan erişilebilmesine imkân sağlamıştır (Vural, 2007). Günlük yaşantıda yapılmakta olan birçok iş ve işlem kolay ve hızlıca yapılabilir hale gelmiştir. Devlet kurumlarından bilgi edinmek, bankacılık işlemleri yapmak, borç sorgulamak, fatura ödemek, pasaport ve vize başvurusunda bulunmak, rezervasyon yapmak, bilet almak, sınav sonuçlarını öğrenmek, kayıt yaptırmak, hastane tetkik sonuçlarına ulaşmak, uzaktan eğitim ilk akla gelen örnekler arasında sayılabilir.

Bilgi güvenliği, bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişimini, kullanımını, değiştirilmesini, ifşa edilmesini, ortadan kaldırılmasını, el değiştirmesini ve hasar verilmesini önlemek olarak tanımlanabilir; gizlilik, bütünlük ve erişilebilirlik olarak isimlendirilen üç temel unsurdan meydana gelir (Puhakainen, 2006). Bu üç temel güvenlik öğesinden herhangi biri zarar görürse güvenlik zafiyeti oluşur. Bilgi güvenliği kurumlar ve bireyler için vazgeçilmez ve değerli bir varlık olan bilginin korunması için gerekmektedir. Bir diğer husus ise bilginin işlenmesi için

kullanılan ve sürekli gelişim gösteren teknolojilerin de bilgi unsuru için riskler yarattığı gerçeğidir.

Bilgi ve iletişim teknolojisinin yaygınlaşması, Internet'in yaygın olarak kullanılması ve Internet üzerinde kullanılan çevrimiçi uygulamalardaki artış, beraberinde güvenlik açıklarının artışına sebep olur iken bilgi güvenliğini sağlamak toplumda sadece bilgi güvenliğinden sorumlu kişi ve kuruluşların işi olmaktan çıkmıştır (Acılar, 2009; Tsohou, Kokolakis, Karyda ve Kiountouzis, 2008; Vural ve Sağıroğlu, 2011). Günümüzde, bilgi sistemlerinin küreselleşmesi sonucunda bu sistemlerle doğrudan veya dolaylı yönden ilişkili olan ve bu sistemleri kullanan tüm birey ve kurumların artık bilgi güvenliğine katkıda bulunması gerekmektedir. Buna sebep olarak ilk akla gelenler;

a. günlük iş ve/veya özel yaşamın bir parçası haline gelen çevrimiçi uygulamaların artışı,
b. ihtiyaç olan bilgilerin yerel/geniş alan ağı(YAA/GAA) üzerinden paylaşımı,
c. bilgiye her noktadan ve ortamdan erişilebilirlik,
d. YAA/GAA meydana gelen açıkların büyük tehdit oluşturması,
e. BİT üzerinde meydana gelen organize suçların artışı ile buna bağlı olarak belki de en önemlisi kişisel ve kurumsal kayıplardaki artışlar

sayılabilir (Gülmüş, 2010; Civelek, 2011; Vural, 2007).

Yukarıda bahsedilen çerçevede, sonuçları insan yaşamının her alanında hissedilen teknolojik gelişmelerin sonucunda oluşabilecek güvenlik zafiyetlerini gidermek, ayrıca elektronik ortamdaki birey ve kurumların sahip olduğu bilgilerinin mahremiyetini korumak kaçınılmaz bir zorunluluk haline gelmiştir (Civelek, 2011; Özcan, 2009; Vardal, 2009; Vural ve Sağıroğlu, 2011).

Bilgi güvenliği risklerinden korunmanın en iyi yolu bilgi teknolojilerine çok para harcamak ve korunma amaçlı teknolojileri daha çok kullanmaktan önce, insanların bilinçlenmesi ve ihtiyaç duyulan güvenlik teknolojisini doğru yer ve zamanda kullanmakla mümkün olabilir (Puhakainen, 2006; Siponen, 2001; Şahinaslan, Kantürk, Şahinaslan ve Borandağ, 2009). İnsan faktörüne bağlı bilgi güvenlik risklerini tamamen ortadan kaldırmak hiçbir zaman mümkün olmasa da, iyi planlanmış bir farkındalık etkinliği ile güvenlik risklerinin kabul edilebilir bir seviyeye çekilmesi sağlanabilir (Acılar, 2009; Gülmüş, 2010; Kruger ve Kearney, 2006; Şahinaslan, Kandemir ve Şahinaslan, 2009; Vardal, 2009; Vural, 2007).

Bilgi ve iletişim teknolojileri ile birlikte geliştirilen elektronik uygulamalar bir yandan hayatın işleyişini kolaylaştırırken diğer yandan yeni güvenlik tehditlerini ve yeni suç tiplerini beraberinde getirmektedir (Gülmüş, 2010). Son 15-20 yılda bilgi güvenliğine olan ilgi, dünyada olduğu gibi ülkemizde de çok büyük bir artış göstermiş ve bununla birlikte bu alanda ülkemizde yapılan araştırmalarda artmıştır. Bilgi güvenliği konusundaki araştırmalar daha çok teknik bakış açısıyla problemleri ele alıp, insan faktörünü göz ardı etmektedir (Ahlan ve Lubis, 2011; Chen, Shaw ve Yang, 2006; Kjorvik, 2010; Rezgui ve Marks, 2008). Bunun yanında bilgi güvenliği çözümleri uygulayan kurumlar karakteristik olarak teknik ve prosedürel güvenlik önlemlerine odaklanmaktadır. Ancak, teknik ve prosedürel bakış açısıyla üretilen bilgi güvenliği çözümleri, BİT kullanırken prosedürlere bağlı kalmak istemeyen veya bağlı kalmayan kullanıcılar olduğunda yetersiz kalmaktadır. Kurumsal ve kişisel bilgilerin güvenliğini sadece teknik güvenlik önlemleriyle (güvenlik duvarı, sanal özel ağ, saldırı tespit/önleme sistemi, anti virüs, içerik kontrolü yazılımı, veri şifreleme, kimlik doğrulama, yetkilendirme vb.) sağlamak mümkün değildir (Rezgui ve Marks, 2008). Ayrıca, bunun yanında kurum ve çalışanların güvenlik bilincine sahip olması gerekmektedir.

Bir kurum, maliyetine bakmaksızın paranın satın alabileceği en ileri güvenlik teknolojilerini kullanabilir, sistemler tasarlayabilir ve adeta kendisini bir güvenlik çemberinden geçirebilir. Bu şekilde sadece en son teknolojiyi kullanarak üst seviyede güvenlik önlemleri alabilen bir kurumda bilgi güvenliğinin %100 sağlanmış olduğundan bahsedilemez (Şahinaslan, Kantürk, Şahinaslan ve Borandağ, 2009). Çünkü, kurum çalışanları belirlenen güvenlik önlemlerini takip etmez veya uygulamak istemez ise alınan önlemlerin hiçbir anlamı kalmaz (Chen, Shaw ve Yang, 2006; Kruger ve Kearney, 2006; Puhakainen, 2006).

Zaman içerisinde güvenlik teknolojileri geliştirildikçe, olası teknik açıkları kullanmak/sömürmek zorlaştığı için saldırganlar insan unsurunun zayıflıklarından faydalanmaya başlamışlardır. Bu yüzden kurumlarda güvenliğin en zayıf halkasını insan unsuru oluşturmaktadır (Kritzinger ve Smith, 2008; Mahabi, 2010; Mathisen, 2004; Penmetsa, 2010; Veiga, 2008). Genel bir söylem olarak "bir zincir, en zayıf halkası kadar güçlüdür" sözü bilgi güvenliği için de geçerlidir. Bu kapsamda kurumlarda güvenlik;

a. teknolojiden önce insana yatırım yapılması,

b. kurum çalışanlarının en üsten en alt kademede çalışanına kadar tümünü kapsayan bir bilgi güvenlik farkındalığı oluşturması,
c. kurum çalışanlarının tümünün en üsten en alt kademede çalışanına kadar kendini geliştirmesi,
d. kurum çalışanlarınca bilgi güvenlik faaliyetlerinin benimsenmesi, önemsenmesi ve desteklenmesi

ile anlamlı hale gelebilir (Şahinaslan, Kantürk, Şahinaslan ve Borandağ, 2009).

Son 15-20 yılda bilgi ve iletişim teknolojilerinin yaygınlaşmasıyla günümüzde bilişim sistemleri hemen hemen her iş sürecinin bir parçası olarak yerini almıştır. Bu sebeple bilişim sistemlerinin güvenliği iş süreçlerinin ve faaliyetlerin yürütülebilirliği açısından çok önemlidir. Her hangi bir bilgi sisteminde bilginin sahibi, bilgiyi kullanan ya da bilgi sistemini yönetenlerden biri olmak, kişiyi sorumlu yapmaktadır. Bu sorumluluk Türkiye'de, 5651 sayılı ve "İnternet ortamlarında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi" isimli kanun ile de düzenlenmiştir. Bilgi sistemleri bir zincir olarak düşünüldüğünde, bu zincirin en zayıf halkasının genelde sistemin kullanıcıları olduğu görülmektedir. Bilgi güvenliği seviyesi bu durumda kullanıcılara bağlı olduğundan, kullanıcı farkındalığı bilgi güvenliğinin sağlanmasında son derece kritik bir öneme sahiptir.

Alanyazın incelemesiyle elde edilen sonuçlar bilgi güvenliği farkındalığı açısından yükseköğretim kurumlarının çok iyi durumda olmadığına işaret etmektedir (Cox, Connolly ve Currall, 2001; Rezgui ve Marks, 2008; Vardar, 2009). Bilgi güvenliği uzmanlarıyla gerçekleştirilen bir çalışmada yükseköğretim kurumlarının bilişim sistemleri güvenliği açısından dünyadaki en güvensiz yerlerden biri olduğu ifade edilmektedir (Foster, 2004; Rezgui ve Marks, 2008; Mahabi, 2010). Yapılan testler ve denetimler yükseköğretim kurumları bilgi sistemlerinde birçok açıklıklar ve zayıflıkların bulunduğunu göstermektedir (Mahabi, 2010; Rezgui ve Marks, 2008). Bilgi ve bilişim sistemleri güvenliği eğitimleri diğer kurumlarda olduğu gibi yükseköğretim kurumları için de bir zorunluluktur. ABD'de Winsconsin Üniversitesi tarafından 435 yükseköğretim kurumunda uygulanan ankete katılan enstitülerden sadece üçte birinde öğrenci ve personel için bilgi güvenliği farkındalık eğitimi verildiği tespit edilmiştir (Caruso, 2003). Ülkemizdeki durumun bu ankette çıkan sonuçtan daha iyi olmadığını söylemek mümkündür (Vardar,2009).

Bilginin üretiminden, öğretiminden, sunumundan ve dağıtımından sorumlu temel ve öncü kurumlardan olan üniversiteler ve öğretim elemanları bu görevlerini

yerine getirirken bilgi güvenliği konusunu ön planda tutmak ve kendilerini bu konuda yetiştirmek zorundadırlar. Bu bağlamda, toplumu ve öğrencileri bilinçlendirme görevini üstlenecek olan öğretim elemanlarının bilgi güvenliği farkındalıklarının hangi düzeyde olduğu, bu konuda eksikliklerinin hangi alanlarda yoğunlaştığının belirlenmesi önem arz etmektedir. Bilgi güvenliği farkındalığıyla ilgili yapılan alanyazın taramasında, yurtdışında bilgi güvenliği farkındalığının ölçülmesiyle ilgili Kruger ve Kearney'in (2006) metodolojik bir yaklaşım ortaya koyan ve uluslararası bir maden şirketi için geliştirmiş oldukları "Bilgi güvenliği farkındalığını değerlendirmek için bir prototip" isimli bir çalışmaya ulaşılmıştır. Türkiye'de ise özellikle üniversitelerde görev yapan öğretim elemanlarına yönelik bilgi güvenliği farkındalığıyla ilgili bir çalışmaya ulaşılamamıştır. Dünya'da ve Türkiye'de yapılan çalışmalar daha çok bilgi güvenliği yönetim sistemleri, risk değerlendirmesi, bilgi güvenliği farkındalık eğitimleri ve bilgi güvenliği sorunlarıyla ilgili durum tespiti konu başlıkları altında toplanmaktadır. Yapılan çalışmalar daha çok genel durum tespitine yönelik iken bilgi güvenliğinde en zayıf halka olarak ifade edilen insan unsurunun bilgi güvenliği farkındalık düzeyinin ne olduğunu belirleyecek bir çalışmaya ulaşılamamıştır.

1.2.Amaç

Bu araştırmanın temel amacı; yükseköğretim kurumlarında görev yapan öğretim elemanlarına bilgi güvenliği farkındalığı kazandırmaya yönelik, çoklu ortam materyallerini içeren bir web sitesi geliştirmek ve geliştirilen web sitesinin bilgi güvenliği farkındalığı kazandırmadaki etkisini belirlemektir. Bu temel amaç doğrultusunda araştırmada şu sorulara yanıt aranmıştır:

1. Deney ve kontrol gruplarındaki öğretim elemanlarının öntest bilgi güvenliği farkındalık düzeyi toplam puanları arasında anlamlı bir fark var mıdır?
2. Geliştirilen web sitesini kullanan deney grubu öğretim elemanlarının öntest ve sontest bilgi güvenliği farkındalık ölçeği ve alt faktörleri toplam puanları arasında anlamlı bir fark var mıdır?
3. Geliştirilen web sitesini kullanmayan kontrol grubu öğretim elemanlarının öntest ve sontest bilgi güvenliği farkındalık ölçeği ve alt faktörleri toplam puanları arasında anlamlı bir fark var mıdır?
4. Geliştirilen web sitesini kullanan deney grubu ile siteyi kullanmayan kontrol grubu öğretim elemanlarının bilgi güvenliği farkındalık ölçeği öntest puanları

kontrol edildiğinde, düzeltilmiş sontest puan ortalamaları arasında anlamlı fark var mıdır?

5. Deney ve Kontrol gruplarındaki öğretim elemanlarının sontest bilgi güvenliği farkındalık düzeyi puanları arasında
   a. Deney/Kontrol grubu
   b. Cinsiyet
   c. Unvan
   d. Bilgisayar kullanım süresi

   bağımsız değişkenlerine göre anlamlı bir fark var mıdır?

f. Öğretim elemanlarının geliştirilen web sitesine yönelik görüşleri nelerdir?

1.3.Önem

Bilgi ve iletişim teknolojileri alanında meydana gelen gelişmeler ve değişim hızı ile yaygın olarak kullanılmaya başlayan İnternet üzerinde çalıştırılan çevrimiçi uygulama miktarındaki artış aynı zamanda güvenlik açıklarındaki artışa sebep olmaktadır. Birey ve kurumlar için değerli ve vazgeçilmez bir varlık olan bilginin korunması, bilgi güvenliği konusunu bir zorunluluk haline getirmektedir. Bilginin üretiminden, öğretiminden, sunumundan ve dağıtımından sorumlu temel ve öncü kurumlardan biri olan üniversiteler ve öğretim elemanları bu görevlerini yerine getirirken bilgi güvenliği konusunu ön planda tutmak ve kendilerini bu konuda yetiştirmek zorundadırlar. Bu bağlamda, toplumu ve öğrencileri bilinçlendirme görevi üstlenecek olan öğretim elemanlarının bilgi güvenliği farkındalıklarının hangi düzeyde olduğu, bu konuda eksikliklerinin hangi alanlarda yoğunlaştığının belirlenmesi alanyazında daha önce araştırma konusu yapılmamıştır.

Bu araştırma sonunda yükseköğretim kurumlarında kullanılmak üzere öğretim elemanlarına yönelik bilgi güvenliği farkındalık ölçeği geliştirilmiştir. Alanyazına kazandırılan bu ölçek benzer araştırmalarda veri toplama aracı olarak kullanılabilir. Araştırma bilgi güvenliğinde en zayıf halka olan insan unsurundan kaynaklanan sorunların kaynakları ve çözümlerine ilişkin ipuçları sağlayacak olması nedeniyle güncel ve işlevseldir. Bunlara ek olarak, alanyazında daha önce araştırma konusu yapılmamış olan bilgi güvenliği farkındalık düzeylerinin değerlendirilmesi sebebiyle özgün bir araştırmadır. Geliştirilen çoklu ortam materyalleri ve web sitesiyle, yükseköğretim kurumlarında bilgi güvenliği farkındalığı ile ilgili risklerin etkisinin

azaltılması için öğretim elemanlarına rehberlik edecek, yükseköğretim kurumlarında bilgi güvenliği farkındalığına uygun politika ve stratejilerin geliştirilmesine katkı sağlayacak, eksiklikleri gidermek için düzenlenecek etkinliklere kaynaklık edecektir. Araştırmadan elde edilen bulgular doğrultusunda tasarlanacak çoklu ortam materyalleri ve websitesi ile etkili, verimli ve çekici bilgi güvenliği farkındalık eğitimleri yapılabilecektir. Araştırmadan elde edilen sonuçların araştırmacılara ve uygulayıcılara bundan sonra yapacakları çalışmalarda ışık tutacağı düşünülmektedir.

1.4.Sınırlılıklar

Bu araştırma belirlenen amaç ve alt amaçlar doğrultusunda;

- Problemin ortaya konmasında alanyazın taraması ve uzman görüşmeleriyle,
- Veri toplama araçları olarak anket, görüşme formu, web sitesi değerlendirme formu ve araştırmacı tarafından geliştirilen "Bilgi Güvenliği Farkındalık Ölçeği" ile,
- Bilgi Güvenliği Farkındalık Ölçeği hazırlanmasında Karadeniz Teknik Üniversitesi, Niğde Üniversitesi, Gazi Üniversitesi öğretim elemanları ile elektronik anket uygulaması ile ulaşılan öğretim elemanlarıyla,
- Bilgi güvenliği farkındalığı oluşturmaya yönelik olarak hazırlanan çoklu ortam eğitim materyalleri ve web sitesiyle,
- Öğretim elemanlarının bilgi güvenliği farkındalık düzeylerinin değerlendirilmesi açısından Ankara Üniversitesi'nde görev yapan öğretim elemanlarıyla

sınırlıdır.

1.5.Tanımlar

Araştırmada sıkça kullanılan kavram ve terimlerin kullanılış amacına en uygun düşen tanımları aşağıda verilmiştir:

Bilgi. Verinin belli bir anlam ifade edecek şekilde düzenlenmiş hali ya da işlenmiş veri (Canbek ve Sağıroğlu, 2006, s. 166).

Bilişim. İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik (TDK, 2015).

Bilişim teknolojileri. Bir bilginin toplanmasını, bu bilginin işlenmesini, saklanmasını ve gerektiğinde herhangi bir yere iletilmesi ya da herhangi bir yerden bu bilgiye erişilmesini bugün için elektronik, optik vb. tekniklerle otomatik olarak sağlayan teknolojiler bütünü (Yurdakul ve Çağlayan, 1997).

Bilgi güvenliği. Elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümü ya da bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda istenmeyen kişiler tarafından elde edilmesini önleme (Canbek ve Sağıroğlu, 2006).

Bilgi güvenliği farkındalığı. Bireylerin bilişim teknolojilerini kullanırken kişisel bilgilerinin istenmeyen tehdit ve tehlikelerden korunması amacıyla gerekli güvenlik analizlerinin yapılarak önlemlerin alınarak tehlikelere karşı farkında olma durumu (Vural ve Sağıroğlu, 2008)

Bilgi toplumu. Sosyo-ekonomik faaliyetlerin giderek etkileşimli sayısal iletişim ağlarının katılımıyla veya bu iletişim ağlarının yoğun kullanımıyla gerçekleştirilmesi yanında, bu amaçla kullanılan her türlü teknolojinin ve uygulamanın üretilmesi (TÜBİTAK, 2002).

Güvenlik. Kişi ve kurumların bilişim teknolojilerini kullanırken karşılaşabilecekleri tehdit ve tehlikelerin daha önceden analizlerinin yapılarak gerekli önlemlerin alınmasının sağlanması (Vural ve Sağıroğlu, 2008).

Farkındalık kazandırmak. Hedef kitleyi bir konuda bilinçlendirmek, konuya dikkat çekerek kişilerin üzerine düşünmesini sağlamak

Teknoloji. Kazanılmış yeteneklerin işe koşulmasıyla doğaya egemen olmak için gerekli işlevsel yapılar oluşturma (Alkan, 2005) ya da bireyin uygulamadaki sorunlarını çözmek ve gereksinimlerini karşılamak amacıyla bilimsel ilkeleri, çevrede var olan materyal ve insan gücü kaynaklarını dikkate alarak ve onlardan yararlanarak sorunu çözme etkinliği (Aybar, Göçmenler, Keser, Numanoğlu ve Teker, 2004).

1.6.Kısaltmalar

ABD	Amerika Birleşik Devletleri
AFA	Açımlayıcı Faktör Analizi
BAE	Birleşik Arap Emirlikleri
BGF	Bilgi Güvenliği Farkındalığı
BGFÖ	Bilgi Güvenliği Farkındalık Ölçeği
BGFWSDF	Bilgi Güvenliği Farkındalık Web Sitesi Değerlendirme Formu
BGYS	Bilgi Güvenliği Yönetim Sistemi
BİT	Bilgi ve İletişim Teknolojileri
DFA	Doğrulayıcı Faktör Analizi
FTP	Dosya Transfer Protokolü
GAA	Geniş Alan Ağı
İDÖ	İnternet Destekli Öğretim
İTE	İnternet Temelli Eğitim
KMO	Kaiser-Meyer-Olkin Testi
WTE	Web Temelli Eğitim
YAA	Yerel Alan Ağı

BÖLÜM 2

2.KAVRAMSAL ÇERÇEVE VE İLGİLİ ARAŞTIRMALAR

Bu bölümde, araştırmanın kavramsal çerçevesi ortaya konulmuş, konuyla ilgili kavramsal bilgilere ve ilgili araştırmalara yer verilmiştir.

2.1.Kavramsal Çerçeve

Bu bölümde, araştırmanın kavramsal çerçevesini oluşturan bilgi güvenliği, bilgi güvenliği tehditleri (doğal afetler ve teknik arızalarla ilgili tehditler, prosedürel eksikliklere dayalı tehditler, insan faktöründen kaynaklanan tehditler ve kötücül yazalımlara dayalı tehditler), bilgi güvenliği farkındalığı, bilgi güvenliği farkındalık eğitimi, yaşamboyu öğrenme, yetişkin eğitimi (androgojik modelin varsayımları, androgojik modelin unsurları), uzaktan eğitim (internet temelli eğitim, internet temelli eğtimi gerektiren nedenler) ile ilgili temel kavramlar, ilkeler ve ilgili araştırmalara yer verilmiştir. Kaynak taramasında Ankara Üniversitesi Kütüphane ve Dokümantasyon Daire Başkanlığı web sitesinin sunduğu akademik arama motoru yardımıyla üyesi olunan elektronik kütüphaneler ile Google Akademik kullanılmıştır. Alanyazın incelemesinde, gelişmiş sorgulama ile "bilgi", "güvenlik", "farkındalık", "bilinçlendirme", "bilgi güvenliği", "güvenlik farkındalığı", "bilgi güvenliği farkındalığı", "olgunluk", "ölçme" anahtar kelimeleri ve "information", "security", "awareness", "information security", "security awareness", "information security awareness", "maturity", "measure" anahtar kelimeleri kullanılmıştır. Kaynakların seçiminde tezin kavramsal çerçevesi ve araştırma soruları ile ilişkisi göz önünde bulundurulmuş ve araştırma bulguları sunulmuştur.

2.1.1.Bilgi Güvenliği

Yaşadığımız çağa adını veren bilginin güvenliğinin sağlanmasının günümüze kadar olan değişimi ve gelişimi, bilgi güvenliğinin sağlanmasında izlenilen yöntemlerin anlaşılabilmesi açısından önemlidir. Geçmişten günümüze bilgi güvenliğinin sağlanması için sırasıyla fiziksel güvenlik, haberleşme güvenliği, yayılım güvenliği,

bilgisayar güvenliği ve ağ güvenliği konularında çalışmalar yapılmıştır (Maiwald, 2003).

Bir kurum veya kuruluşun kâr etmek, değer yaratmak, rekabet avantajını ve sürdürülebilir büyümeyi yakalamak için sahip olduğu veya sahip olması gereken, pazar, ürün, teknoloji ve organizasyona ait bilgilerin tamamı bilgi varlıkları olarak tanımlanabilir. Bilgi varlıklarının fiziksel olarak korunması için fiziksel güvenliğin, iletim halindeki bilgilerin güvenliğinin sağlanması için haberleşme güvenliğinin, elektronik sistemlerden istem dışı yayılan sinyallerin kullanılarak önemli bilgilerimize ulaşılmaması için yayılım güvenliğinin, bilgisayarlarımıza erişimin kontrol altına alınması için bilgisayar ve ağ güvenliğinin sağlanması gerekmektedir (Vural, 2007).

Bireyler için en kritik varlık bilgidir. Bilgi, tarih boyunca değişik şekillerde depolanmış ve saklanmıştır. İlk çağlarda, bilgiler; taş, deri, kil tablet, papirüs gibi materyallerin üzerine yazılarak saklanmış ve bugünlere ulaşmıştır. Günümüzde ise bu bilgiler, basılı yayınlar, filmler, delikli kartlar, teyp, disk ve elektronik ortamda bilgiyi kaydeden belge türleri üzerinde depolanarak saklanmaktadır. Bir başka deyişle bilgi, birçok farklı formda bulunabilir, iletilebilir, kâğıda basılabilir, elektronik olarak depolanabilir, posta veya elektronik yolla gönderilebilir, film olarak gösterilebilir ya da sözlü-iletişim yoluyla aktarılabilir. Bu kadar önemli olan bilgi geçmiş zamanlarda fiziksel güvenliği sağlanan ortamlarda saklanmıştır. Fiziksel güvenliğin sağlanabilmesi amacıyla duvarlar örülmüş, kale hendekleri çekilmiş, giriş çıkışları kontrol eden nöbetçiler görev yapmıştır. Bilginin güvenliğini sağlamaya yönelik fiziksel önlemler alınmasına rağmen genellikle bu korumalar yeterli olmamış, bilgilerin çalınması veya istenmeyen kişilerin eline geçmesi engellenememiştir (Maiwald, 2003).

Bilginin güvenliğinin yüksek seviyede sağlanabilmesi için yukarıda açıklanan güvenlik türlerinin tamamının uygulanması gerekmektedir. Bilgi güvenliği, "bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak" tanımlanır (Canbek ve Sağıroğlu, 2006). Bilgiye sürekli olarak erişilebilirliğin sağlandığı bir ortamda, bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi süreci bilgi güvenliği olarak tanımlanabilir. Bilgi güvenliğinin sağlanılmasında uyulması ve uygulanması gereken birçok güvenlik bileşeni vardır. Öncelikle üç ana ilke olan gizlilik, bütünlük ve erişilebilirlik ilkelerine uyulması sonrasında da bu ilkelere ek olarak

değerlendirilebilecek giriş kontrolü, emniyet, inkâr edememe, güvenirlik, kayıt tutma, kimlik tespiti ilkelerine uyulması bilgi güvenliğinin üst düzeyde sağlanabilmesi için gereklidir (Sharp, 2004). Bu unsurlar aşağıda kısaca tanıtılmıştır.

a. Gizlilik: Elektronik ortamlarda taşınan bilginin; yetkisi ve izni olmayan kişiler veya süreçler tarafından elde edilse bile anlamlı olarak ele geçmesinin engellenmesi olarak tanımlanabilir. Gizlilik, statik ortamlar (disk, teyp, cd, dvd, vb.) veya ağ üzerinde bir göndericiden bir alıcıya gönderilen dinamik ortamdaki veriler için sağlanmak zorundadır. Saldırganlar, yetkileri olmayan gizli bilgilere birçok yolla erişebilirler. Burada amaç, saldırganlar tarafından bu bilgiler elde edilse bile anlaşılmasını veya çözülmesini zorlaştıracak yaklaşımlar kullanılarak taşınan bilgiyi çözülemeyecek başka bir formata dönüştürmektir. Gizlilik ilkesinin sağlanmasında şifreleme algoritmaları ve steganografi yöntemleri kullanılmaktadır.
b. Bütünlük**:** Bilginin göndericiden çıktığı haliyle bozulmadan bir bütün olarak alıcısına ulaştırılmasını garanti eden bir güvenlik unsurudur. Bilginin haberleşme sırasında izlediği yollarda değiştirilmemiş, araya yeni veriler eklenmemiş, belli bir kısmı ya da tamamı tekrar edilmemiş ve sırası değiştirilmemiş şekilde alıcısına ulaştırılarak bütünlüğü sağlanır. Bilginin bütünlüğünün sağlanılması için özetleme (hashing) algoritmaları kullanılmaktadır.
c. Erişilebilirlik: Talep edilen bilgiye kullanıcıların yetkisi dâhilinde zamanında erişim yapabilmesi için gerekli olan önlemlerin alınması olarak tanımlanabilir. Erişilebilirlik bilişim sistemlerini kullanan kişiler veya süreçler tarafından büyük bir önem taşımaktadır. Bilişim sistemlerinden kendilerinden beklenen işleri belirlenen bir zaman diliminde yapmaları beklenir. Erişilebilirlik hizmeti, bilişim sistemlerini, kurum içinden ve dışından gelebilecek erişilebilirliği düşürücü tehditlere (Denial of Service Attack-DoS) karşı korumayı hedefler. Bu bileşen sayesinde, kullanıcılar, erişim yetkileri dâhilinde olan bilgilere, güncel, zamanında, hızlı ve güvenli bir şekilde ulaşabilirler. Bilgisayar yazılımlarındaki güvensiz kodlar, sistemin yanlış, bilinçsiz ve eğitimsiz personel tarafından kullanılması veya konfigüre edilmesi, doğal felaketler sistem erişilebilirliğini olumsuz yönde etkileyen önemli faktörlerdir. Bilgi sistemlerine erişilebilirliğin sürekli sağlanması için fiziksel önlemler alınmalı, güvenlik duvarları, casus

savar yazılımlar, atak tespit sistemleri, virüs savar yazılımlar kurulmalı ve güncellenmelidir.

d. Kayıt (Log) tutma: Elektronik ortamda gerçekleşen olayların (bilgisayar ağı üzerinde meydana gelen herhangi bir faaliyetin) daha sonra analiz edilmek üzere kayıt altına alınması olarak tanımlanabilir. Kullanıcının parolasını yazarak sisteme girmesi, web sayfasına bağlanması ve e-posta iletişimi gibi örnekler kayıt altına alınması gereken olaylara örnek olarak verilebilir. Toplanan olay kayıtları üzerinde yapılacak analiz sonucunda, bilinen saldırı türlerinin izlerine rastlanırsa ve saldırı olasılığı yüksek bir aktivite tespit edilirse, atak tespit sistemleri tarafından alarm mesajları üretilerek sistem yöneticileri uyarılır. Kayıt tutma bileşeni saldırıların ve saldırganların belirlenmesi içinde, ayrıca bir önem arz etmektedir. Saldırı olduktan sonra oluşan kayıtlar saldırı tipi ve saldırganın kimliğinin tespit edilmesine yardımcı olur. Kayıt tutulmayan bir sisteminm güvenliğinden bahsedilemeyeceği her zaman hatırda tutulmalıdır.

e. Kimlik tespiti (kanıtlama ve doğrulama): Bilgi sistemlerinden hizmet alan alıcının, iddia ettiği kişi olduğundan emin olunması olarak tanımlanabilir. Örneğin, giriş izni olan herhangi bir elektronik ortama erişildiğinde erişen kişiye sorulan şifreler, bilgisayarını açarken şifre girilmesi kullanıcının kimliğinin tespit edilmesinde kullanılan yöntemlerdir. Günümüzde kimlik tespiti, bilgisayar ağları ve diğer sistemler için de çok önemli bir hizmet haline gelmiştir. Akıllı kartlar, tek kullanımlık parolalar (one time password), jetonlar, elektronik imza kartları, biyometrik teknolojiler kimlik tespitinde kullanılan teknolojilerden bazılarıdır.

f. Güvenirlik: Bilgisayar sistemlerinin beklenen davranışı ile elde edilen sonuçlar arasındaki tutarlılık durumu olarak tanımlanabilir. Diğer bir ifadeyle güvenirlik, herhangi bir bilgi sisteminden ne yapmasını bekliyorsak, sistemin kendisinden beklenileni yaparak her çalıştırıldığında da aynı sonuçları vermesi olarak tanımlanabilir. Örneğin ağ içerisinde yer alan merkezi dağıtıcı anahtarın (switch) 24 saat boyunca kesintisiz çalışması beklenmektedir. Güvenirlik, cihazın çalıştığı zaman dilimi ile çalışması gereken zaman dilimi kıyaslanarak hesaplanmaktadır.

g. İnkâr edememe: Elektronik ortamlarda gönderici ve alıcı arasındaki haberleşmenin inkâr edilmemesi için gerekli olan önlemlerinin alınmasını sağlayan güvenlik unsurudur. Alınan güvenlik önlemleri sayesinde gönderici ile

alıcı arasında ortaya çıkabilecek anlaşmazlıkların, oluşabilecek zararların en aza indirilmesi sağlanır. Bu güvenlik unsuru, özellikle gerçek zamanlı işlem gerektiren bankacılık ve finans bilgi sistemlerinde yoğunlukla kullanılmaktadır. İnkâr edememe unsuru elektronik imza ve açık anahtar altyapısı kullanılarak sağlanmaktadır.

h. Giriş kontrolü (Erişim listeleri): Bilgi sistemlerine erişmek için kimlik tespiti yapılmış olan kullanıcı veya uygulamalara belirlenen yetkilerin atanması, bir kaynağa erişmek için belirli izinlerin verilmesi veya alınması olarak tanımlanabilir.
i. Emniyet: Bilgi sistemlerini tehlikelerden koruyacak olan fiziksel veya teknik çözümlerdir. Bir bilgisayar sisteminin veya yazılımın işlevsel ortamına gömülü olduğunda kendisi veya gömülü olduğu ortam için istenmeyen potansiyel veya bilfiil tehlike oluşturacak etkinlik veya olayları engelleme girişimidir.

2.1.2.Bilgi Güvenliği Tehditleri

Tehdit, bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini olumsuz yönde etkileme olasılığı olan tanımlı risklerdir (Blanding, 2004). Tehditlerin bilgi sistemlerinde etkili olabilmesi için bilgi sistemleri üzerindeki var olan zafiyetleri kullanmaları gereklidir. Tehditlerin bilgi varlıklarına etkisi, tehlikenin oluşma olasılığı, bilgi varlığı üzerindeki açık ve varlığın değeri ile doğru orantılıdır. Tehditler uygun ortam şartlarının oluşmasıyla bilgi sistemlerine zarar verecek kusurları içeren zafiyetlere, zafiyetler saldırganlar tarafından kullanıldığında güvenlik ihlallerine yol açarak bilgi sitemlerine zarar vermektedir.

Tehditler, tehdit kaynağı açısından bakıldığında;

a. Doğal afetler veya teknik arızalarla ilgili tehditler
b. Prosedürel eksiklerle ilgili tehditler
c. İnsan faktöründen kaynaklanan tehditler ve
d. Kötücül yazılımlarla ilgili tehditler,

olarak sıralanabilir.

2.1.2.1. Doğal Afetler ve Teknik Arızalarla İlgili Tehditler

Doğal afetler ve teknik arızalar çoğunlukla önceden tespit edilemedikleri için engellenmeleri çok zordur. Bu tehditlere karşı tüm tedbirler önceden planlanmalı ve uygulanmalıdır. Deprem, yangın, su baskını, sel, ani sıcaklık değişimleri, toprak kayması, kasırgalar, fırtınalar ve çığ düşmesi gibi afetler meydana gelebilecek tehditlere örnek olarak verilebilir. Doğal afet ve teknik arızalarla ilgili tehditlere verilebilecek diğer örnekler aşağıda maddeler halinde verilmiştir. Bunlar;

a. Güç kaynağının arızalanması,
b. Yangın söndürme sistemindeki arızalar,
c. Telefon santral arızası,
d. Aktif cihaz (yönlendirici, anahtar, vb.) arızaları,
e. Sunucu bilgisayarlarda oluşabilecek yazılım veya donanım arızaları,
f. Kripto sistemlerdeki hatalar (algoritma zayıflığı, anahtarların yetersizliği, vb.),
g. Havalandırma sistemi arızaları,
h. Kamera sistemlerinin arızaları,
i. Kapı giriş-çıkışsisteminde meydana gelen arızalar,
j. Terör saldırıları (bombalama, kundaklama, vb.),
k. Ayaklanmalar, gösteriler, eylemler, protestolar ve
l. Veri depolama ağı ve yedekleme sistemlerinde meydana gelen arızalar

olarak sıralanabilir.

Doğal afetler ve teknik arızlarla ilgili tehditlerden herhangibirinin meydana gelmesi genellikle tüm bilgi sistemlerinin zarar görmesine veya çalışmamasına sebebiyet vermektedir. Bu tür tehditleri en az indirmek için kurumsal yapıya uygun felaket senaryoları üretilmeli ve felaketten en kısa zamanda nasıl geriye dönülebileceğiyle ilgili (disaster recovery) iş devamlılığı konusundaki çalışmalar önceden yapılmalıdır.

2.1.2.2. Prosedürel Eksikliklere Dayalı Tehditler

Bu tehdit türü kurumsallaşma süreçlerini tamamlayamayan kurum ve kuruluşlarda görülür. Prosedürel eksiklikler kendi arasında teknik ve idari olmak üzere iki gruba ayrılmaktadır.

İdari Prosedür Eksiklikleri:

a. Personel işe alma ve işe son vermede güvenlik prosedürlerinin olmaması
b. Güvenlikle ilgili görev ve sorumlulukların verilmesinde eksiklikler
c. Çalışanların güvenlik kural ve prosedürlerinden habersiz olması veya bu konuda eksik bilgilerinin olması
d. Görevlerin ayrıştırılması ve görev rotasyonu prosedürlerinin olmaması
e. Acil durumlarda veya felaket anlarında devreye alınacak *Bilgi Süreklilik Planları*nın olmaması
f. Güvenlik Politikası ve prosedürlerinin olmaması
g. Güvenlik bilinçlendirme eğitimlerinin planlanması ve uygulanmasına ait eksiklikler
h. Tüm iş süreçlerinin belgelendirilmesine yönelik eksiklikler.

Teknik Prosedür Eksiklikleri

a. Bilgi yedekleme prosedürlerinin olmaması
b. Yardım masası (bilgisayar, kurulum ve bakım) prosedürleri eksikliği
c. Bilgi envanterinin tutulmaması ve güncelliğini sağlayacak mekanizmanın olmaması
d. Bilgi sistemleri izleme prosedürlerinin olmaması
e. Ağ hizmetleri (e-posta, internet, dosya paylaşımı, vb.) kullanım prosedürlerinin olmaması
f. Etki alanı hizmet (Şifre değiştirme, hesap açma, vb) prosedürlerinin eksikliği
g. Sunucu hizmetleri (dns, dhcp, etki alanı, vb.) planlama ve yönetim prosedür eksikliği
h. İletişim hatlarının (ses, veri, vb.) denetimi ve yönetimine ait prosedür eksikliği.

2.1.2.3. İnsan Faktöründen Kaynaklanan Tehditler

İnsan faktöründen kaynaklanan tehditleri istem dışı veya bilinçli olarak yapılan kullanıcı davranışları olarak iki grupta incelemekte fayda vardır. Herhangi bir sistem üzerinde yetkiye sahip olan bir kullanıcının, bilgi sistemlerini bilinçsiz ve bilgisizce, yeterli eğitime sahip olmadan kullanması sonucu bilginin gizlilik, bütünlük ve erişilebilirlik ilkelerinin birinin veya birkaçının ihlal edilmesine sebep olan bilmeyerek veya ihmalkârlık sonucu yapılan kullanıcı davranışlarını insan faktöründen kaynaklanan istem dışı tehditler olarak tanımlanabilir. Son kullanıcılar, yazılım geliştiriciler, sistem

yöneticileri gibi değişik düzeyde bilgi sahibi olan insanlar tarafından istem dışı veya ihmalkârlık sonucu yapılan davranışlardan kaynaklanan bazı tehditler maddeler halinde aşağıda sıralanmıştır (Canbek ve Sağıroğlu, 2006; Vural, 2007). Bunlar:

a. Güvenlik politikalarına uymama veya ihlal etme
b. Güvenlik önlem ve kontrolleri almadan yazılım geliştirme
c. Temizlik görevlisinin sunucunun fişini çekmesi
d. Eğitilmemiş çalışanın yapılandırma ayarlarını kurcalaması
e. Bilişim sistemlerinin yanlış kullanımı veya yönetimi
f. Eksik veya hatalı yapılandırma
g. Erişim haklarının ayarlanamaması
h. Sistem kayıtlarının (log) analiz edilmeden silinmesi veya hiç tutulmaması
i. Bilgisayar başında olunmayan zamanlarda parola korumalı ekran koruyucuyu devreye almama
j. Hatalı yedekleme veya yedek almama
k. Gereksiz servislerin hizmete açılması
l. Antivirüs programını bilgisayarı yavaşlatıyor gerekçesi ile devre dışı bırakma
m. Tanımadığı kişilerden gelen e-postaların eklerini açma veya e-postalar aracılığıyla istenilen gizli bilgileri verme
n. Şifresini unutan kullanıcıların şifrelerini telefon yoluyla değiştirme
o. Sistemlerin başlangıç (default) ayarlarında bulunması ve
p. Şifrelerin masa üzerinde küçük yazılı kâğıtlarda tutulması

olarak verilebilir.

İnsan faktöründen kaynaklanan ikinci tehdit türü işyerine kızgın veya küskün olan ve hiçbir beklentisi olmayan sorunlu personelin görevini ve yetkisini kötüye kullanarak bilinçli olarak yaptığı kötücül davranışlardır. Bu kişiler günümüzde yerel saldırgan (internal hacker) olarak adlandırılmaktadır. Yerel saldırganların yapmış olduğu saldırılar sonrasında kurumlar yüksek oranda zarara uğramaktadır. Bilinçli olarak yapılan kötücül davranışlardan kaynaklanan bazı tehditler maddeler halinde aşağıda sıralanmıştır.

a. Yetkisi ve görevi dâhilinde olmayan bilgisayar sistemlerine girmek ve içerisindeki gizli bilgilere erişmek
b. Görevi gereği bildiği üst düzey yetkiye sahip şifreleri kurum dışına menfaat sağlama amacıyla sızdırmak
c. Veri tabanındaki bazı kayıtları silmek, değiştirmek veya tamamen yok etmek

d. Güvenlik sunucularını (güvenlik duvarı, saldırı tespit sistemi, antivirüs, vb.) bilerek yanlış yapılandırma veya devre dışı bırakma
e. Yapılan kötücül davranışların iz bırakmaması amacıyla güvenlik kayıtlarından silinmesi
f. Bilinçli olarak kötücül programların bilgisayarlara bulaştırılması

gibi ve benzeri örnekleri daha da çoğaltmak mümkündür.

Bilinçli olarak yapılan birçok davranış suç teşkil etmektedir. Verilen örneklerden anlaşılacağı gibi bilgisizlik, bilinçsizlik, isteksizlik ve ihmalkârlık ve görevini kötüye kullanma gibi insan hatalarından kaynaklanan tehditler bilgi güvenliği tehditleri arasında önemli bir yer tutmaktadır.

2.1.2.4. Kötücül Yazılımlara Dayalı Tehditler

Saldırganların, donanım veya yazılım açıklıklarını kendi çıkarları için kullanarak istedikleri bilgiye erişebilmelerini sağlayan tehditlerdir. Saldırılar çıkar amaçlı olarak yapılabildiği gibi kendi ünlerini duyurmak isteyen bireysel saldırganlar veya önceden planlanmış belirlenen hedefler doğrultusunda organize olmuş çeteler veya çıkar amaçlı örgütler tarafından yapılmaktadır. Günümüzde saldırıların büyük bir çoğunluğu kötücül yazılımlar (Malicious Programs) olarak adlandırılan programlar aracılığıyla yapılmaktadır. Kötücül yazılımlara dayalı olarak yapılan saldırılarda kullanılan yaygın tehditler maddeler halinde aşağıda sıralanmıştır (Canbek, 2005). Bunlar:

a. Bilgisayar virüsleri (virus)
b. Bilgisayar solucanları (worms)
c. Truva atları (trojan horses)
d. Casus yazılımlar (spyware)
e. Arka kapılar (backdoor)
f. Klavye dinleme sistemleri (keyloggers)
g. Tarayıcı soyma (browser hijacking)
h. Telefon çeviriciler (dialers)
i. Kök kullanıcı takımları (rootkit)
j. Korunmasızlık sömürücüleri (exploit)
k. Tavşanlar (wabbit)
l. Diğer kötücül yazılımlar

2.1.3.Bilgi Güvenliği Farkındalığı

Uygulama yazılımları ve internet tarafındaki gelişmelerle bilgilerin işlenmesi bir değere dönüşmesi daha pratik hale gelmiştir. Tüm bu insan hayatını kolaylaştıracak teknolojik gelişmeler diğer yanda uygunsuz kullanım, bireylerdeki risk algısı zafiyeti, bilgi güvenliği tehditlerinden habersizliği karşısında bir takım olumsuzlukları, kötü amaçlı kullanımları ve bir takım telafisi güç bilgi güvenliği risklerini de bünyesinde taşımaktadır. Yapılan bir takım araştırmalar bize bilgi güvenliği risklerini gidermede insan faktörünü göz ardı ederek oluşturulacak sistemsel bir takım güvenlik çemberlerinin çok etkili ve yararlı olmadığını göstermektedir. Bilgi teknolojileri alanında yapılan yatırımlar sonucunda yazılımsal veya donanımsal açıklar üzerinden bilginin sömürülmesi, uygunsuz kullanımı çok zorlaşmıştır. Bu açıklar yerine insan faktörünü kullanarak bilgiler üzerinde bir takım çıkarlar elde etme gayreti yoğunlaşmış durumdadır. Tüm bu riskler göz önünde tutulduğunda riskleri gidermek ya da olası en düşük düzeyde tutmanın yolu bireyler üzerinde bir farkındalık oluşturmadan geçmektedir. Bunun en temel yolu ise bireylere gerek medya kanallarını kullanarak gerekse okullarda seminerler verilerek gereksinimlere göre farklı kategorilerde eğitim programlarının hazırlanması ve bireyler üzerinde bir farkındalık bilincinin oluşturulması gerekmektedir (Vural, 2007).

İnsan hataları ve ihmalleri birçok hırsızlığın, dolandırıcılığın ya da imkânları kötü kullanmanın kaynağıdır. Dikkatli ve iyi eğitimli bireyler olası güvenlik ihlallerini engelleyebilir. Bu nedenle, toplumun bilgi güvenliği konusunda bilinçlendirilmesi, bu hususta farkındalık yaratılması ve eğitimlerin düzenlenmesi gereklidir. Bilgi güvenliğinin sağlanmasında ne kadar önlem alınmış olsa da insan faktörü göz ardı edilirse hiçbir önlem sonuç vermeyecektir. Çünkü bilgi güvenliği bilinci ve farkındalığı olmayan insanlar bu güvenlik sürecini aksatacaktır. Bilginin korunmasına çalışıldığı günden bu yana insanlar, güvenlik sürecinin en zayıf tarafını oluşturmuşlardır. Birçok teknik ve yönetsel güvenlik kontrolleri uygulansa dahi bu kontroller saldırganlar tarafından en zayıf halka olan insan kullanılarak çeşitli yöntemlerle kolaylıkla aşılabilmektedir. "Gücünüz en zayıf halkanız kadardır" ilkesi bilgi güvenliği içinde geçerlidir. Yapılan araştırmalar göstermiştir ki bilgi güvenliği ihlali olayları genellikle bireyler tarafından yapılmıştır. Bunlardan çoğu bilinçsiz davranışların sonucudur. Nadir de olsa kötü niyetli çalışanların bilgiyi dışarıya sızdırması, kötü amaçlı kullanımı veya yok etmesi de söz konusudur. Bilgi güvenliğini sağlamak için en önemli unsur olan

insan faktörünün bilgi güvenliği konusunda eğitimi şarttır. Bu eğitim, bilginin, nasıl korunacağını, neden korunması gerektiğini öğretmelidir. Bireyler hatalı davranışlarının bilgi güvenliği üzerinde yaratabileceği etkiyi anlamalıdır (Vural, 2007).

2.1.4.Bilgi Güvenliği Farkındalık Eğitimi

Kurumlarda bilgi güvenliğinin sağlanması açısından önemli olan bilgi güvenliği eğitimleri ve bilinçlendirme farklı yöntemlerle çalışanlara periyodik olarak verilmelidir. Bu yöntemler bilinçlendirme toplantıları, kurum içi web üzerinden eğitimler, e-posta yoluyla kullanıcılara bildirimler, yazılar ve duyurular, seminerler, kurum içi bültenler ve güvenlik posterleri şeklinde olabilir. İnsana bağlı güvenlik riski hiçbir zaman tamamen yok edilemese de iyi planlanmış bilgi güvenliği eğitimleri riskin kabul edilebilir bir seviyeye indirilmesine yardımcı olacaktır. Çalışma gruplarının bilgiyi ve bilgi kaynaklarını koruma konusunda üzerlerine düşen sorumlulukları anlaması bilgi güvenliğinin sağlanması açısından kritik bir öneme sahiptir.

Bilgi güvenliği eğitimlerinin temel hedefi çalışanları kurumsal bilgilerin ve bilgi kaynaklarının gizlilik, bütünlük ve erişilebilirlik konusundaki yapması gereken görev ve sorumlulukları konusunda eğitmektir. Bilgi güvenliği eğitimleriyle insanlar sadece bilginin korunması konusunda nasıl katkı sağlayabileceklerini değil, aynı zamanda bilginin neden korunması gerektiğini de öğrenmelidir. Çalışanlar hatalı davranışlarının kurum bilgi güvenliği üzerinde yaratabileceği etkiyi eğitimler aracılığıyla açıkça anlamalıdır. Kullanıcı bilinçlendirme çalışmaları, güvenlik ihlallerinin maliyetini azaltmaya ve kontrollerin kurumun tüm bilgi kaynakları üzerinde dengeli uygulanmasına yardımcı olacaktır.

Güvenlik farkındalık eğitimlerinin amacı, güvenlik ve güvenlik kontrollerinin önemi hakkında kurum çalışanlarında kollektif bir bilinç oluşturmasıdır. Bilinçlendirme mesajları basit ve açık olmalı, bilinçlendirme eğitimleri çalışma gruplarının anlayabileceği basit bir formatta verilmelidir.

Çoğu kurumda güvenliğin sağlanması için yapılması gereken kısıtlamaların kullanıcıların alışkanlıklarıyla ters düşmesinden dolayı güvenlikle ilgili yaptırımların uygulanmasında geç kalınmaktadır. Kurumsal güvenlik uygulamaları başından itibaren uygulanmadığından zamanla her kullanıcının, güvenliğe dikkat etmeksizin farklı kullanım alışkanlıkları edindiği görülmüştür. Bu durum bilgi güvenliği bilinçlendirme eğitiminin uygulanmasını zorlaştırarak, kullanıcılarda güvenlik uygulamalarına karşı

direnç oluşmasını sağlamaktadır. Çünkü sadece kullanıcıları eğitmek değil, aynı zamanda eski alışkanlıklarından kurtarmak gerekmektedir. Kullanıcılara göre kurum güvenlik önlemleri olmaksızın bugüne kadar gayet iyi çalışmıştır ve hiçbir sorunla karşılaşmamıştır. Yeni güvenlik önlemleri hayatı zorlaştırıcı gereksiz değişiklikler olarak görülür. Bilinçlendirme eğitimleri güvenlikle ilgili bilgi vermenin yanında kullanıcı alışkanlıklarından nasıl kurtarılacağı göz önüne alınarak hazırlanmalı, akıcı ve eğlenceli bir içerikle kullanıcılara sunulmalıdır.

Vural (2007) tez kapsamında yaptığı araştırmalarda çoğu kurumda güvenlik bilinçlendirme programının olmadığını tespit etmiş, olan kurumlarda ise genellikle kullanıcıları bilgi güvenliğinin neden önemli olduğu konusunda eğitmeyi başaramadığını tespit etmiştir. Eğitimin başarılı olabilmesi için kullanıcıların kafasındaki neden sorusunun cevabı kullanıcıyı ikna edecek şekilde verilmelidir. Örneğin, güçlü şifrelerin kullanılmasını sağlayan kurallara sahip bir şifre politikasını kullanıcılara güçlü şifreler kullanarak bilgi güvenliği ihlallerini önleyebilirsiniz açıklaması yerine, basit şifrelerin nasıl ve ne kadar kısa sürede kırıldığını, saldırganlar tarafından nasıl kötü niyetli kullanılabildiğini, şifrelerin çalınması durumunda meydana gelebilecek güvenlik ihlallerinin sonuçlarını kendilerini nasıl etkileyeceği konusunda örnekler ve yaşanmış gerçek hikâyelerle desteklemesi eğitimin amacına ulaşmasını sağlayacaktır. Başarılı bir eğitim sonrasında kullanıcıların şifreleme politikasına sahip çıkarak yeni politikanın uygulanmasında gayretli olacakları görülecektir.

Etkili bir bilgi güvenliği için uygun eğitim programının geliştirilebilmesinde dikkat edilmesi gereken hususlar aşağıda maddeler halinde verilmiştir (Önel, 2008; Vural, 2007; Wilson and Hash, 2008).

a. Kurumsal bilgi güvenliği politikalarının oluşturulması: İyi yazılmış bilgi güvenliği politikası başarılı bir eğitim ve bilinçlendirme çalışmasının temelini oluşturur. Bilinçlendirme çalışmasına başlamadan önce tüm üst seviye hedeflerin ve güvenlik programının gereklerinin dokümante edilmiş olması kritik önem taşımaktadır. Güvenlik politikaları kurumun bilgi güvenliği konusundaki önceliklerini yansıtmalıdır. Politikalar oluşturulduktan sonra kullanıcılar politikanın varlık ve içeriğinden haberdar olmalıdır. Kullanıcılar aynı zamanda politikaya uymamanın doğuracağı cezai sonuçlar ve yaptırımlar hakkında da bilgi sahibi olmalıdır.
b. Eğitim ihtiyaçlarının tespiti: Başarılı bir bilinçlendirme ve eğitim programının geliştirilmesindeki ikinci adım kurum personelinin bilgi seviyeleri gözetilerek

mevcut eğitim ihtiyaçlarının belirlenmesidir. Yapılan araştırmalarda bu adımın genellikle göz ardı edilmekte veya geçiştirilmekte olduğu görülmüştür. Çoğu kurumda programların içeriği kullanıcıların ihtiyaçlarına göre değil de, varsayımlara dayanılarak geliştirilmektedir. Kullanıcıların güvenlik konusundaki mevcut bilgi düzeyinin ölçülmesi için gerekli görüldüğünde kullanıcılarla kısa sohbetler yapılması eğitim ihtiyaç ve önceliklerinin doğru tespitine yardımcı olacaktır. Kullanıcıların öğrenme becerisi ve tercihleri, özel ilgi alanları, bilinçlendirme programına karşı duyulan direnç ya da sempati, daha önceki başarılı veya başarısız eğitim girişimleri, daha önceden mevcut bulunan eğitim, kaynak ve materyalleri, programın başarısı için destek alınabilecek kişi veya grupların tespitinin yapılması eğitim ihtiyaç ve önceliklerinin doğru tespitine yardımcı olacaktır. Farklı kıdem, unvan ve iş tanımlarına sahip kullanıcılar ile görüşme, genel kullanıcılara temel güvenlik bilgileri hakkında anket veya kısa soru listesi gönderme, kurumda son zamanlarda karşılaşılmış güvenlik problemlerinin tespiti, sızma testlerinden elde edilen sonuçların değerlendirilmesi, yüz yüze toplantılar gerçekleştirilmesi, bina ve kullanım alanlarının ziyaret edilerek fiziksel güvenlik seviyesinin gözlenmesi (kilitlenmemiş ofis odaları, dolaplar ve güvenliği bulunmayan kişisel bilgisayar) eğitim ihtiyaçlarının tespitinde izlenmesi gereken yöntemlerdir.

c. Gerekli desteğin sağlanması: Eğitim ihtiyaçlarının tespitinden sonraki aşama, yönetimin ve kurum genelinde kullanıcıların desteğinin alınması için yapılması gereken çalışmalardır. Bilinçlendirme ve eğitim programı ihtiyacının kurum genelinde kabul ettirilmesi zor bir iştir. Aslında güvenlik bilinci, güvenlik araçlarından daha önemli bir seviyede değerlendirilmesi gereken önemli bir unsurdur. Yönetim desteğinin sağlanmasındaki birinci hedef kaynak teminidir. Kurumun büyüklüğüne göre gerekli bütçe ve istihdam sağlanmalıdır. Bir diğer önemli hedef ise yönetim kademesindeki personelin davranışları ile tüm kurum çalışanlarına örnek olacak şekilde bilinçlendirme programına değer vermeleri ve programa katılmaları, kurum genelinde kullanıcıların desteğinin alınması için çok önemlidir. Yöneticiler, eğitimin önemini ortaya koyup desteklerse eğitime katılma ve yarar sağlama konusundaki kullanıcı istekliliği daha da artacaktır. Yönetim desteğinin sağlanması için yönetim bilinçlendirme çalışması kurumsal bilgi güvenliği açısından hayati önem taşımaktadır.

d. Eğitim gruplarının belirlenmesi: Bir sonraki önemli adım eğitim alacak grupların seviyelerine göre sınıflandırılmasıdır. Kullanıcılar işlerini yaparken aynı derece veya tipte güvenlik bilincine ihtiyaç duymaz. Kullanıcı grupları arasında gerekli ayrımı yapan ve her gruba sadece ilgili bilgiyi sunan bir bilinçlendirme ve eğitim programı en iyi sonucu elde edecektir. Yaşadığımız bilgi çağında neredeyse her gün bilgi bombardımanına maruz kalınmaktadır. Bilgi güvenliği bilinçlendirilmesi amacıyla iletilmek istenen mesajların kulak ardı edilmemesi için sadece gerekli bilgilerin ilgili gruplara iletilmesi gerekmektedir. Tez kapmasında yapılan araştırmalarda genellikle tek tip programların tüm gruplara uygulandığı ve bilinçlendirme programının istenen başarıya ulaşamadığı tespit edilmiştir. Eğitim grupları kurum ihtiyaçlarına göre güvenlik bilinci seviyesi, teknik bilgi seviyesi, ünvan/yetki, iş fonksiyonu, kullanılan teknolojiler gibi yöntemler izlenerek belirlenebilir.
e. İletişim araçlarının belirlenmesi: Bilinçlendirme programındaki bir sonraki adım eğitim için kullanılacak iletişim araçlarının belirlenmesidir. Her kurum kendine özgü farklı iletişim araçlarına sahiptir. Eğitimde kullanılabilecek kaynakların tespiti yapıldıktan sonra, ilgili kaynakların kullanımına yönelik prosedürler oluşturulmalıdır. Eğitimlerde kullanılabilecek kurumsal iletişim araçlarına e-posta, sesli veya görüntülü çoklu ortam dosyaları, genelgeler, intranet, yazılı yayın (posterler, dergiler, kitaplar, broşürler, kurum yayınları), yüz yüze görüşmeler (toplantılar, sunumlar, eğitim ve güvenlik seminerleri) örnek olarak verilebilir. İletişim aracının seçiminde farklı kitlelerin farklı biçimlerde öğrenmeye açık oldukları düşünülmelidir. Eğitimin etkili ve istenilen düzeyde başarılı olması için ihtiyaçlar ölçüsünde farklı iletişim araçları kullanılabilir.
f. Eğitim stratejisinin geliştirilmesi: Başarılı bir bilinçlendirme çalışmasının uygulanabilmesi için gerekli olan, bir diğer adım tutarlı ve etkili bir eğitim stratejisinin geliştirilmesidir. Strateji geliştirilmeden verilen eğitimler kullanıcılar tarafından düzensiz ve geçici bir çalışma olarak algılanacaktır. Eğitim stratejisinin parçası olarak işe alım sırasında yapılacak bilgilendirme, aylık şirket bülteni, şirket eğitimleri, yıllık güvenlik seminerleri, bilgi güvenliği konusundaki başarılar için teşvik ödülleri, oyunlar, yarışmalar düzenli olarak periyodik şekilde yapılmalıdır. Eğitimler, temel son kullanıcı eğitimi, teknik eğitim, gelişmiş bilgi güvenliği eğitimi (bilgi güvenliği uzmanları ve denetçileri), dönemsel eğitim paketi (her dönem farklı bilgi güvenliği konusuna

odaklanılır) içeriğiyle hazırlanmalı ve ilgili çalışma gruplarına periyodik olarak verilmelidir.

g. Ölçme: Eğitim programının son adımıdır. Verilen eğitimler sonrasında çalışma gruplarının eğitimlerden hangi oranda faydalandığının ölçümlenerek değerlendirmelerin yapılması katılımcılardaki ilerleme ve gerilemelerin ölçümlenmesi açısından önemlidir. Verilen eğitimler sonrasında yapılacak olan sızma testleriyle kullanıcıların seviyeleri ölçümlenebilir.

Artan güvenlik ihlallerinin kaynaklarına dikkat edildiğinde kullanıcıların bilinç ve eğitim seviyelerinde yetersizliklerin ön planda olduğu ortaya çıkmaktadır. Pek çok kullanıcı, bilgi ve bilgi kaynaklarının korunmasının önemi konusunda yeterli bilgiye sahip değildir. İyi tasarlanmış ve sonuçlandırılmış bilinçlendirme ve eğitim çalışması güvenlik zincirinin en kırılgan halkası olan insan faktörünün güçlendirilmesine büyük katkı sağlayacaktır.

Bilinçlendirme programlarında son kullanıcıların bilgilendirileceği alanlar ve içerik örneği aşağıda maddeler halinde sunulmuştur (Önel, 2008; Wilson and Hash, 2003).

a. Sosyal Mühendislik: Telefon yoluyla kandırmaca, e-posta aracılığıyla bilgi alma, sohbet, vb.
b. Şifre kullanımı ve yönetimi: Şifrelerin oluşturulması, değiştirme sıklığı, şifrelerin korunması, şifrelerin uzunluğu, tek kullanımlık şifreler, vb.
c. Kötücül yazılımlardan korunma: Tipleri, bulaşma belirtileri, tarama, temizleme, imzaların güncelleştirilmesi, vb.
d. Güvenlik politikaları: Sorumluluklar, cezai yaptırımlar, vb.
e. E-posta kullanımı: Şüpheli e-postaların ve eklerinin silinmesi, sazan e-postaların tespiti, vb.
f. Web kullanımı: Güvensiz ve yasaklı sitelere girilmemesi, güvenli dosya indirme, vb.
g. Yedekleme ve geri alma: Güvenli yedekleme, periyot, yedekten geriye dönme, vb.
h. Güvenlik ihlali: Kime başvurulmalı, ilk ne yapılmalı, vb.
i. Mobil cihazların güvenliği: Hırsızlık önlemleri, şifreleme, vb.
j. Erişim: En az yetki ilkesi.
k. Masaüstü güvenliği: Şifre korumalı ekran koruyucuları, temiz masa temiz ekran, vb.

l. Fiziksel güvenlik: Bariyerler, kilitli dolaplar, kameralar, vb.
m. Lisanslama: Lisanssız programların zararları, hukuki boyutları, vb.

2.1.5. Yaşamboyu Öğrenme

Her an gelişen ve değişen dünyada insanlar hızlı değişime ve yenilenen ortama uyum sağlayabilmek, gelişmelerin dışında kalmamak için devamlı ve sistemli bir eğitim sürecine ihtiyaç duyarlar. Bu süreç yaşamboyu öğrenme olarak tanımlanabilir.

Günümüzde bilgiye ulaşabilen, ulaştığı bilgiyi kendi yapısına uydurabilen, buna yenilerini katabilen ve bilgileri yayan toplum ya da kişiler güçlü olarak kabul edilmektedir. Bu nedenle, günümüz toplumlarının gereksinimi olan insan profili artık değişmiş, farklılaşmıştır (Soran, Akkoyunlu ve Kavak, 2006). Toplumlar bundan böyle, "kendini geliştiren" ve "yaşamboyu öğrenme" becerilerine sahip bireylere gereksinim duymaktadır.

Yaşamboyu öğrenme, nitelikli okul eğitimi ile bunun sonrasında bireylere yetişkin eğitimi olanaklarının sağlanması ile mümkün olur. Lindeman'a (1969) göre yaşam başlı başına bir öğrenme sürecidir. Fakat her insanın, teknik ve toplumsal değişime ayak uydurabilmek, kendi çevresine ilişkin koşullar altında meydana gelen değişiklikler karşısında hazırlıklı olabilmek ve bireysel gelişimi bakımından tüm gizilgücünü harekete geçirebilmek amacıyla sürekli, maksatlı ve ardışık bir öğrenim görmesi için özgül fırsatlara ihtiyacı vardır. İşte bu fırsatların değerlendirilmesiyle ortaya çıkan öğrenme ortamına yetişkin eğitimi denir (Knowles, 1996, s.3).

Yetişkin eğitiminin hedef grubu, herhangi bir eğitim kurumunun tam zamanlı programına devam eden belli yaş grubundaki çocuk ve gençlerin dışında kalan kişilerdir. Yetişkinlerin bireysel özelliklerinin dikkate alındığı, kuralların esnek tutulduğu, programların içeriğini bireyin ihtiyaçlarının belirlediği ve yetişkinlerin öğrenmeye ihtiyaç duyduğu her konuyu kapsayan eğitime yetişkin eğitimi denilebilir (Knowles, 1996).

2.1.5.1. Yetişkin Eğitimi

Toplum, bireylerin yaşamboyu süren öğrenme ihtiyaçlarına örgün ve yetişkin eğitim programlarını da kapsayan yaygın eğitim yoluyla cevap vermeye çalışmaktadır. Bu temelde, örgün eğitim, bilim ve teknolojide son derece hızlı bir biçimde yaşanan

değişim ve dönüşümün ortaya çıkardığı ihtiyaçlara tek başına cevap vermekten uzak kalmaktadır (Kurt, 2000). Önceki dönemlerle kıyaslandığında daha hızlı bir şekilde yaşanan mesleki hareketlilik (Duman, 2007), bu ihtiyaçlara yönelik yaygın eğitim faaliyetlerinin, bu çerçevede de yetişkinlere yönelik eğitim programlarının tasarlanmasını toplumların gündeminde giderek daha üst sıralara taşımaya başlamıştır.

Kurt'a göre (2000) yetişkin eğitimi, en geniş anlamıyla, sürekli eğitimlerinin ilk dönemini tamamlayan bireylerin bilgi, beceri, anlayış ve davranışlarında değişime yol açmak amacıyla, birbirini izleyen örgütlü etkinliklerden oluşmaktadır. Geray (2002) ve Kocaoğlu'na göre (akt:Kurt, 2000), bilinçli ve planlı olarak yürütülen yetişkin/halk eğitimi, okul çağındayken örgün eğitimden yararlanamamış yetişkinlere bu eksikliği gidermek üzere fırsat hazırlamakta; örgün eğitimden geçmiş olsalar bile, yetişkinlerin pratikteki ilerlemelere, sosyal değişimlere uyumunu sağlamakta; ayrıca okul çağındakilere okul haricinde verilen eğitim ile örgün eğitimi bütünleştirmektedir. Duman (2007), yetişkin(ler) eğitimini, zorunlu eğitim almış kimselerin ihtiyaçlarına göre düzenlemekle, bu kişilerin öğrenmelerine olanak sağlayan planlı, programlı ve düzenli eğitim süreçlerinin tümü olarak tanımlamaktadır. Buna göre yetişkin eğitimi, toplumun ihtiyaç duyacağı bilgi, görgü, beceri, ve yeterlilik seviyesine sahip bir yetişkinler toplumu oluşturmayı; yetişkinleri, içinden çıktıkları toplumun gelişmesini engelleyen problemlerin üstesinden gelmeye yönelik bir anlayışla bu problemleri çözmeye hazırlamayı; varlık nedenlerini gerçekleştirebilmeleri için, yetişkinlere kendi bilgi, anlayış, tutum ve özelliklerini geliştirme imkan ve fırsatı sağlamayı hedefler (Yazar, 2012).

Yetişkin eğitiminin önemi, dünya çapında, zaman içinde anlaşılmış olmakla birlikte, yetişkinlere yönelik eğitim programlarının uzunca bir süre çocuklar için kullanılan yöntem ve tekniklerle sürdürülmesine çalışılmıştır (Kurt, 2000; Malkoç, 1989). Bu çerçevede, çocukların öğrenmesine yardım etme bilimi ve sanatı olarak tanımlanabilecek olan pedagojinin yüzyıllardır kullanılmakta olduğu ilke ve teknikler yetişkinlerin eğitilmesi için bir dönem ödünç alınmış; ancak, edinilen tecrübeler sayesinde, yetişkin eğitim programlarının planlanması sürecinde istifade edilmesi gereken ilke ve tekniklerin çocukların eğitiminde kullanılanlardan farklı olması gerektiği anlaşılmıştır. Böylece, yetişkin eğitimi, amatör öğreticilerin gönüllük temelinde yürüttüğü bir etkinlik olmaktan çıkarak (Geray, 2002), önemli bir uzmanlık sahası haline gelmiş (Malkoç, 1989) ve yetişkinlerin öğrenme sürecine yardım etme

bilim ve sanatı olarak adlandırlabilecek (Knowles, Holton ve Swanson, 2005; Güneş, 1996) andragoji ortaya çıkmıştır.

2.1.5.1.1.Androgojik Modelin Varsayımları

Yetişkin eğitiminde çığır açan androgojik model, Knowles'ın çalışmaları çerçevesinde genel olarak şu varsayımlar üzerinde geliştirilmiştir (Knowles, Holton ve Swanson, 2005; Malkoç, 1989; Geray, 2002):

a. Yetişkinler birşeyi öğrenmeye başlamadan önce bunu neden öğrenmeleri gerektiği (need to know) ve bu çerçevede öğrenme sürecinin nasıl yürütüleceğini, ne öğrenileceğini ve bunu öğrenmenin neden önemli olduğunu bilmelidirler. Bu gereklilik, yetişkinlerin eğitim programlarının planlama süreçlerine dahil edilmeleri; bu mümkün olmuyorsa eğitimde kullanıacak yöntemlerin belirlenmesi sürecine katılmalarıyla bir ölçüde karşılanabilecektir.
b. Yetişkinde benlik kavramı bağımlı bir kişilikten, kendi kendini yönetebilen bağımsız bir kişiliğe doğru gelişmiştir ve yetişkinler kendi başlarına öğrenebilirler. Öğrenmede otonomi, öğrencinin bağımlı (öğretmen=otorite), ilgili (öğretmen=motive edici, rehber), katılımcı (öğretmen=kolaylaştırıcı) ve kendi kendine öğrenen (öğretmen=danışman) olarak özetlenebilecek dört farklı seviyeyle ölçülebilir. Yetişkinin bunlardan hangi sınıflandırmaya dahil olduğu, kişilik özellikleri (sabit) kadar, öğrenilecek konuyla (değişken) ilgilidir. Bazı yetişkin eğiticileri, yetişkin eğitiminin esas amacının kişinin öğrenmede otonomi düzeyini yükseltmek olduğunu ileri sürmektedir. Yetişkinin kendi kendine öğrenme yetisi, öğrenmede otonomi beklentilerini karşılamadığı takdirde, öğrenme sürecini olumsuz etkileyebilecek bir faktöre dönüşebilmektedir.
c. Yetişkinin gittikçe artan ve dolayısıyla öğrenme etkinliklerine giderek çoğalan bir kaynak oluşturan tecrübe birikimi vardır. Bu sebeple, grup tartışmaları, simülasyonlar, problem çözme etkinlikleri, örnek olaylar ve laboratuvar yöntemleri, tek taraflı bilgi aktarımına oranla daha fazla kullanılmalı ve bireylerin tecrübesinden daha çok faydalanılmalıdır. Ayrıca, grup içinde öğrencilerin birbiriyle etkileşimlerinden de yararlanılmalıdır. Diğer yandan, yetişkinlerin tecrübelerindeki farklılıkların, daha fazla kişisel farklılıklara sebep olduğu ve ayrıca kişisel yargıların daha koyu bir biçimde yerleşmesine yol açtığı unutulmamalıdır. Kısaca özetlemek gerekirse, yetişkinlerde tecrübe öğrenmeyi

kolaylaştırıcı ve hızlandırı bir işlev görebileceği gibi, bazı şartlarda öğrenmenin önündeki en büyük engellerden birisi de olabilmektedir. Bu nedenle, öğrenme süreçlerinde eski bilgilerin çözülmesini (unfreezing) sağlayacak bir hazırlık oturumu yapılması da gerekebilecektir.

d. Yetişkinlerin kendisini öğrenmeye hazır hissedişi, toplumsal rollerin gerektirdiği bilgi gereksinimleri ile üstlendikleri sorumluluk ve görevleriyle uyum sağlayacak şekilde gelişir. Yetişkinlerin öğrenmeye hazır hissediş seviyeleri konudan konuya değişir. Öğrenmeye hazır olmayan yetişkinlere, kimi durumlarda (bağımlı kişiliğe sahipse ve konu hakkında yeterli bilgiye sahip değişse) "yönlendirme", kimi durumlarda ise (özgüven veya özveri eksikliği söz konusuysa) "destek" vermek gerekebilir.
e. Yetişkinlerin katılmak istediği eğitim programlarının özünü; ileride gerektiği zaman kullanabileceği konu ağırlıklı bilgiler yerine, hemen uygulayabileceği, günlük problemlerine çözüm getirebilece bilgiler oluşturur. Örgün eğitim herkese gelecekte ihtiyaç duyma ihtimali bulunan bilgileri aktarmaya çalışırken, yetişkinler bilgiye gereksinim duydukları anda ulaşmayı tercih ederler. Yetişkinin kaybedecek zamanı olmadığı için katıldığı eğitim programlarının doğrudan mevcut ihtiyaçlarına çözüm getirmesini arzular.
f. Yetişkinler bazı dışsal güdüleyicilere (daha iyi bir iş, kariyer, maaş gibi) açık olmakla birlikte, eğitime ilgileri ve eğitimdeki başarıları için içsel güdüleyiciler (başarı, iş tatmini, öz saygı, yaşam kalitesi, keyif gibi) daha etkilidir. Bu bakımdan bireyin toplumda oynadığı rol, yetişkin eğitimi açısından önem taşımaktadır. Kişi toplumda yeni görevler aldıkça, bunları arzu ettiği gibi yerine getirmeye yönelik bilgilere ihtiyaç duyabilir. Bu da motivasyonun üst düzeye çıkmasını ve öğrenme hızının artmasını sağlamaktadır.

Pedagojik model eğitim sürecindeki bütün sorumluluğu öğretmene yüklemekte ve neyin, nasıl, ne zaman öğrenileceği ile bunun öğrenilip öğrenilmediği konularındaki bütün kararları öğretmene aldırmaktadır. Bu modelde, okulda ya da kurumlarda önceden tasarlanan programlar çerçevesinde tespit edilen bilgi ve beceriler kazandırılmak istenmektedir. Eğitimin amacına uygun olarak, çocuğun ileride karşılabileceği ya da hiç karşılaşmayacağı problemlerin çözümüne ilişkin bir takım bilgiler önceden (Çözüm → Bilgi-beceri → Problem) öğretilmektedir. Öğrenci, öğrenme sürecinde ilerlemek istiyorsa öğretmenin öğrettiklerini öğrenmek durumundadır. Bunların gerçek hayatta nasıl tatbik edileceğini bilmek zorunda değildir ve kendisine bu şekilde bir yönlendirme

de yapılmamaktadır. Öğretmen öğrenciyi kendisine bağımlı bir birey olarak gördüğünden, öğrenen de zamanla bu rolü benimsemektedir. Öğrencinin tecrübesi önemsiz görülmektedir, zira önemli olan öğretenin, ders kitabı yazarının ve diğer eğitim materyallerini hazırlayanların tecrübeleridir. Bilginin aktarılması için kullanılan araçlar son derece önemlidir. Verilen bilginin elde edilmesiyle öğrenme süreci tamamlanmış sayılır. Öğrenenler dış etkenler ile (karne, not, ödül, ceza vb.) öğrenmeye güdülendirilir (Knowles, Holton ve Swanson, 2005; Geray, 2002).

Androgojik modelin uygulandığı bir yetişkin eğitiminde ise müfredat, öğrenenlerin ihtiyaç ve ilgilerine göre, yine öğrenenlerin katılımıyla belirlenmelidir. Sınıfta otorite paylaşılmakta olup, daha demokratik bir düzenden söz edilebilir. Yetişkinler, çocuklar gibi, iyi bir karneyle motive olmazlar. Eğitimin sonuçlarının doğrudan, somut ve pratik olması ile eğitimden hem kısa, hem de uzun vadede yarar sağlamayı beklerler. Yetişkinler, edindiği yeni bilgi ve becerileri, işinde veya sosyal hayatında derhal kullanabilmeli; bunlardan bugün karşı karşıya kaldığı problemlerin çözümünde (Çözüm → Bilgi-beceri → Problem) yararlanabilmelidir. Yeni fikirleri, ihtiyaç duydukları ölçüde ve daha önceki bilgi birikimleri üzerinden teyit edebildikleri takdirde daha iyi öğrenirler. Mevcut bilgileriyle çelişen hususları öğrenmeleri son derece güç olur. Yekişkinleri pasif bir konuma itecek otoriter öğretme yöntemleri, düşündürmeyi amaçlamayan sınavlar ve katı pedagojik formüllerin yetişkin eğitiminde yeri yoktur. Yetişkinlerin dimağları bilgiyle doldurulması gereken boş kaplar olmadığından, eğitimde en değerli kaynak öğrenenin tecrübeleridir. Dewey'in de altını çizdiği üzere, tecrübe eğitimin çıktısı değil, girdisini oluşturmaktadır. Gerçek eğitim yaşantı aracılığıyla meydana gelir ve her yaşantının, hem daha önce geçmiş olanlardan birşeyler alması, hem de daha sonra gelecek olanların niteliğini bir biçimde değiştirmesi (süreklilik) beklenir. Lindeman'ın kavramsallaştırmasıyla yetişkin eğitimini, otorite kavramanın olmadığı resmi olmayan bir öğrenme sürecinde, ana amacı tecrübenin anlamını ortaya çıkarmak olan, işbirliğine dayalı bir girişim; tutum ve davranışlarımızı oluşturan önyargılarımızın kökenlerine kadar inen düşünsel bir arayış; eğitimi hayatla buluşturan ve yaşamı deneye dönüştüren bir öğrenme tekniği olarak tanımlamak mümkün olabilir. Bu süreçte sadece alçakgönüllü öğretmenlerin iyi birer yetişkin eğitimcisi olarak öne çıkabildiği görülür. Çünkü yetişkin eğitimi sınıflarında öğrenenin tecrübesi öğretmenin bilgisi kadar kıymetlidir. İyi bir yetişkin eğitimi sınıfında öğretmenin mi yoksa öğrencinin mi daha fazla öğrendiğini belirleyebilmek güçtür (Knowles, Holton ve Swarson, 2005; O'Connor, Bronner ve Delaney, 2007; Bilir, 2004;

Geray, 2002; Kurt, 2000; Barutçugil, 2002; Usher, Bryant ve Johnston, 2005; Durakoğlu, Biçer ve Zabun, 2013).

Dikkat çekilen bu farklılıklara rağmen, androgoji karşısında pedagojinin kötü bir model olduğu veya bunlardan birinin diğerini bütünüyle dışarıda bırakacak şekilde, kullanılması gerektiği söylenemez. Yetişkinlerin homojen bir bütünü oluşturduklarını ve her birinin androgojik modelin varsayımlarını olumladığını idda etmek de mümkün değildir (Knowles, Holton ve Swanson, 2005). Bu nedenle, herhangi bir eğitimde hangi modelin ne ölçüde kullanılması gerektiği konusunun planlama aşamasında ciddi bir şekilde değerlendirilmesi gerekmektedir. Nitekim öğrenilecek konu ve öğrenenin durumu, eğitimlerde pedagojik mi, androgojik mi yoksa ikisinin bileşimi bir yaklaşım mı izlenmesi gerektiğini ortaya koyacaktır (O'Connor, Bronner ve Delaney, 2007). Ancak yukarıda deninildiği üzere, yetişkinlere yönelik eğitim faaliyetlerinde, pedagojik modelin birçok dezavantajından, androgojik modelin ise birçok avantajından söz etmek mümkündür.

2.1.5.1.2.Androgojik Modelin Unsurları

Knowles, Holton ve Swanson'a (2005) göre, geleneksel (pedagojik) eğitim "içerik" tabanlıyken, androgojik eğitim "süreç" tabanlı bir model olarak ortaya çıkmıştır. İlkinde belirlenen içeriğin aktarılması önemliyken, ikincisinde öğrenenin bilgi ve beceri edinebilmesi için gerekli süreçlerin sağlanmasına çalışılır. İçerik tabanlı geleneksel eğitimde öğretmen, eğitici veya müfredatı oluşturan kurul hangi bilgi ve becerilerin aktarılması gerektiğine karar verir, bunları mantıksal bir örgü içine oturtur, bilgi veya becerinin aktarılmasında en etkin yöntemin hangisi olduğunu belirler ve bu içeriği belirli bir plan dahilinde sıralar. Androgojik modelde ise eğitici, kolaylaştırıcı veya danışman katılımcıyı aşağıdaki unsurları içeren bir sürecin içine dahil edecek usülleri hazırlamakla sorumludur (Knowles, Holton ve Swanson, 2005; Akın, 2014; Geray, 2002; Kurt, 2000):

a. *Öğrenciyi hazırlama:* Öğrenme faaliyeti başlamadan önce, katılımcılar dört-beş kişilik gruplara bölünerek, edilgen ve proaktif öğrenme arasındaki farklar hakkında bilgilendirilmeli, katılımcıya yaralanabileceği kaynaklar tanıtılmalı, katılımcıyla birebir ilişki kurulmalı, katılımcının programla ilgili gerçekçi beklentiler geliştirmesi sağlanmalı ve proaktif öğrenmenin ihtiyaç duyabileceği becerilerin kullanılacağı mini projeler uygulanmalıdır.

b. *Öğrenmeye uygun bir ortam oluşturma:* Fiziki ortam bakımından, katılımcıların temel ihtiyaç ve beklentilerinin karşılanması önemlidir. Öğrenmeye uygun yerleşim planı; bu çerçevede, arka arkaya dizilmiş sıralar ve başta bir öğretmen masası yerine küçük gruplardan oluşmuş çemberler düşünülebilir. Eğitim sürecinde, öğrenenlerden fiziki ortamla ilgili hissettiklerini paylaşmaları istenebilir. Karşılıklı yapılan bu fikir alışverişi hem halhazırdaki eğitim programı için, hem de sonrakiler için önemli detaylar içerebilir. Ortamda eğitim boyunca ihtiyaç duyulabilecek kaynaklara kolay erişim sağlanabilecek bir düzen kurulmalıdır. Fiziki ortamdan daha fazla önem arz eden psikolojik ortam bakımından ise, karşılıklı saygının, rekabet yerine işbirliğinin, öğretmen-öğrenci arasında karşılıklı güvenin, yargılama değil desteğin, karşılıklı açık ve gerçek bir iletişimin, öğrenmenin sonucunda ortaya çıkacak memnuniyetin ve öğrenciye gösterilen değerin yer aldığı bir ortam oluşturulmalıdır. Baskıcı bir öğretmenin yönetiminde oluşan otoriter bir ortamda öğrenci, emirlere duygusuz bir biçimde itaat etmesi nedeniyle son derece bağımlı bir yapıya bürünür ve bu endişe, utangaçlık, uysallık ve dalkavukluk gibi olumsuz kişilik özelliklerine dönüşebilir. Kapalı ortamlarda da yıkıcı eleştiri, alaycılık, cesaret kırma ve başarısızlık vurgusu hakim olduğundan bireyin özgüveni tahrip olabilir. Sadece eğitim boyunca değil, içinde bulunulan örgütteki genel atmosfer üzerinde de durulmalıdır. Bu bağlamda, genel olarak uygun bir öğrenme ortamı oluşturulması öğrenmenin olmazsa olmaz şartıdır.

c. *Birlikte planlama yapılabilecek bir mekanizma kurulması:* Androgojik modelde, pedagojik modelden bütünüyle farklı olarak, planlama aşamasına katılımcılarıda dahil edecek bir mekanizma geliştirilmeli ve katılımcıların planlama kararlarına iştirakleri sağlanmalıdır. Bireyler planlama ve karar mekanizmalarında bulundukları süreçlere daha istekli katılırlar. Katılımcı sayısı birebir görüşmeleri yürütebilecek sayıda ise eğitim sürecine katılacak olan tüm öğrenenlerin fikirlerine başvurulabilir. Sayı birebir görüşmeye imkan tanımayacak kadar fazla ise, öğrenenler arasından küçük grup temsilcileri seçilip görüşülerek, ihtiyaç anketleri hazırlanarak veya birkaç seçenekten uygun olanı öğrenciye seçtirerek bu süreç tamamlanabilir.

d. *Öğrenme ihtiyaçlarının belirlenmesi:* Yetişkin eğitiminde program geliştirirken ilgi ve ihtiyaç merkezli bir yaklaşım benimsenmelidir. Uygulama aşamasına ancak, katılımcıların ihtiyaçları tam olarak tespit edildikten sonra geçilmelidir.

Öğrenme ihtiyaçlarının belirlenmesinde sadece toplumun/kurumun söz sahibi olması uygun olmayacaktır. Bazen toplumun/devletin/kurumun ihtiyaçları ile bireyin ihtiyaçları farklı olabilir. Toplum/kurum, bireyin /çalışanın farklı konularda kendini geliştirmesini isteyebilecekken; birey/çalışan başka bir konu üstünde öğrenme ihtiyacı içinde olduğunu değerlendirebilir. Her iki ihtiyaç karşılanabileceği gibi, gerektiği takdirde ihtiyaçların çeşitli oranlarda bileşiminin karşılanması yönüne de gidilebilir. Bu takdirde, taviz verilmesi beklenen taraflarla görüşülerek, rızalarının alınması doğru olur. Öğrenme ihtiyaçlarının belirlenmesi, sonraki aşamaların da doğru yürütülmesi açısından son derece önemlidir. Bu amaçla, katılımcılarla birebir görüşmeler yapmak; bu mümkün olmuyorsa küçük gruplar halinde fikir alışverişinde bulunmak, öğretilmesi istenen konular hakkında katılımcıların fikrini almak; öğrenim sırasında veya birbirini izleyen eğitimler sonrasında katılımcıların değerlendirmelerinden yararlanmak ve bu alandaki bilimsel araştırmalardan istifade etmek mümkündür.

e. *Öğrenme ihtiyaçlarını karşılayabilecek program hedefleri belirleme:* Öğrenciyle birlikte, belirlenmiş ihtiyaçlar öğrenme hedeflerine nasıl dönüştürülebilir sorusunun cevabı aranır ve bu sayede programın içeriği oluşturulur. Hedeflerin ölçülebilir olması ve öğrenenlerin ihtiyaçlarına yönelik olması lazımdır.

f. *Öğrenme deneyimlerinden oluşan planlar tasarlama:* Androgojinin en önemli özelliklerinden biri de her katılımcıyı farklı bir birey olarak, kendi öğrenme sürecine göre değerlendirmektir. Katılımcılar, bir eğitim programını takip edderken, hazır olma durumlarına göre kendi öğrenme planlarını oluşturabilirler. Bu süreçte öğretmen, katılımcının kişisel özelliklerini de göz önünde bulundurarak öğrenme planına katkı sağlayabilir. Kaynakların tespiti ve bu kaynakları kullanıp hedefe ulaşmada öğrencilerle işbirliği yapabilmek önemlidir. İhtiyaç duyulan hangi konu, ne zaman ve nasıl öğrenilebilir? Hangi teknikleri kullanmak etkili olabilir? Eğitim sürecine katılacak olan kişilerin en iyi öğrendiği yötem ve teknikler nelerdir? Asgari paydalarda buluşmak mümkündür? gibi soruların cevapları öğretmen ve katılımcıların yapacağı işbirliği ile elde edilebilir.

g. *Öğrenme deneyimlerine uygun teknik ve malzemelerle uygulamaya dökme:* Uygulama aşamasında öğrenenlerin tecrübeleri temelinde en uygun yöntem, teknik ve araç-gereçler kullanılarak deneysel bir öğrenme süreci gerçekleştirilir.

Uygulamada eğitimi verenlerin nitelikleri eğitimin başarısı bakımından son derece önemlidir.

h. *Öğrenmenin çıktılarını değerlendirme ve diğer öğrenme ihtiyaçlarını belirleme:* Öğrenciler, değerlendirme sürecinde hem kendilerini, hem diğer öğrencileri, hem programı, hem de öğretmeni değerlendirerek sürece katkı sağlayabilir. Bunun için katılımcıların program hakkındaki görüşlerinin alınması, eğitim öncesi ile sonrası arasındaki bilgi-beceri farkının ölçülmesi, davranış farklarının belirlenmesi, örgütün performansındaki değişikliklerin izlenmesi gibi çalışmalar yapılabilir. Bunlardaki değişimin başka faktörler tarafından tetiklenip tetiklenmediğinin anlaşılması için kontrol gruplarından da yararlanılmalıdır. Program hakkında eğiticinin, amirlerin görüşlerinin alınması da yarar sağlayabilir. Eğitim sonunda karşılanmayan veya ortaya çıkan ihtiyaçlar tespit edilerek, yeni eğitim programları için hazırlık başlatılabilir.

2.1.6.Uzaktan Eğitim

Yaşamboyu öğrenme ve yetişkin eğitiminin önemli araçlarından biri ise uzaktan eğitimdir. Eğitimin bir kurum olarak karşı karşıya bulunduğu performans gösterme, değişime ve yeniliğe açık olma sorunu ile doğrudan ilgilidir. Bu nedenle son yıllarda eğitim sektöründe öğrenme hedeflerini ve eylem düzeylerini etkili biçimde gerçekleştirmek üzere çağdaş eğitim teknolojileri hızlı bir gelişme içindedir (Alkan, 2005). Bunların en sonuncusu uzaktan öğretimin çeşitli biçimleridir.

Alkan (1981, s.59) uzaktan öğretimi şu şekilde tanımlamaktadır: "*Geleneksel öğrenme-öğretme yöntemlerinin sınırlılıkları nedeniyle sınıf içi etkinliklerin, planlayanlar ve uygulayıcılarla öğrenciler arası iletişim ve etkileşimin özel olarak hazırlanmış öğretim üniteleri ve çeşitli ortamlar yoluyla belirli bir merkezden sağlandığı bir öğretim yöntemidir.*"

Öğrenenin ve öğretmenin aynı ortamda bulunmasını gerektirmeyen uzaktan eğitim, kendi kendine çalışma şeklinin sistematik olarak düzenlenmesidir. Farklı mekânlarda bulunan kişilerin birlikte eğitim görebildiği uzaktan eğitimin dünyada gelişimi için her ne kadar kesin bir başlangıç tarihi belirlenemese de uzaktan eğitimin kullanımına 19. yüzyılda rastlanmaktadır (Verduin ; Clark. 1994, s.15, akt. Bulurman, 2002).

İlk uzaktan eğitim uygulamaları posta hizmetleri ile başlamıştır. Ancak bilgi teknolojisindeki hızlı gelişmeler, 1989'da Tim Berners-Lee'nin web'i (World Wide Web) keşfetmesi ile yaşanmaya başlamıştır. İnternetin eğitim sürecinde yapılacak araştırmalara kolaylık sağlaması, bilgiye kısa sürede ve kısıtlamasız ulaşılabilmesi eğitimciler ve öğrenciler için bulunmaz bir fırsat sağladığı için sanal üniversiteler doğmuştur. İlk olarak Oxford Üniversitesi 1999 yılında internette açık üniversite girişimini başlatmıştır. ABD'nin ilk sanal üniversitelerinden biri olan Phoenix Üniversitesinin 1999' da 48 bin öğrencisi olduğu bilinmektedir (Çakmak ve Karataş, 2008).

Günümüzde artık başta üniversiteler olmak üzere birçok kurum ve kuruluş bilgisayara ve internete dayalı uzaktan eğitim yoluyla öğrenci ve personelinin eğitim gereksinimini karşılamaya çalışmakta ve ayrıca sertifika, diploma vb. hizmetlerle eğitim almak isteyen herkese kapılarını açmaktadır. Artık, eğitim teknolojisinin ileri basamağı sayılan bilgisayar ve internetle desteklenen uzaktan eğitimin, yetişkin eğitimi, ana-baba eğitimi, hizmet içi eğitim gibi çok geniş bir uygulama alanına sahip olduğu (Özen ve Karaman, 2001) ve geniş kitlelere hitap ettiği görülmektedir.

2.1.6.1. İnternet Temelli Eğitim

Mektupla eğitimle başlayan ve çok çeşitli aşamalardan geçtikten sonra teknoloji ve bilişim dünyasının gelişimiyle günümüze gelen uzaktan eğitim, İnternetin kullanılmaya başlamasıyla farklı bir şekle girmiştir. Uzaktan eğitimin en gelişmiş haliyle geniş kitlelere ulaşılmasını sağlayan İnternet temelli eğitim yüz yüze eğitime büyük oranda destek olacak ve eğitimin niteliğini artıracak görünmektedir.

İnternet, aynı ya da farklı yerlerdeki birey ve grupların bilgisayarlar yoluyla bağlanarak metin, veri, ses ve grafik gibi öğeleri paylaştıkları elektronik ortamlardır. Günümüzde pek çok kurum ve organizasyon interneti bir eğitim teknolojisi olarak kullanmaya başlamıştır (Akpınar, 2005, s.127).

Uzaktan eğitimin internet ile birlikte anılmasıyla birlikte internet temelli eğitim kavramı yaygın olarak kullanılmaya başlamıştır. Çakmak ve Karataş (2008) İnternet temelli eğitimi tanımlarken, asıl olarak internetin kullanıldığı, ancak gerektiğinde diğer eğitim teknolojileri (CD, DVD, basılı materyaller vb.), yüz yüze etkileşimler gibi ortamlarla desteklenen planlı bir bilginin hazırlandığı, üretildiği, sunulup değerlendirildiği bir uzaktan eğitim sistemi olarak tanımlanabileceğini belirtmektedir.

Bu tanım daha çok İnternet destekli öğretimi anlatır gözükmektedir. Çünkü İnternet temelli eğitimde ihtiyaç duyulan bütün eğitim materyali İnternet üzerinden sunulmalıdır, fakat İnternet destekli öğretimde İnternetin yanısıra diğer öğretim materyalleri de kullanılabilir. Buna benzer kavram kargaşasına birçok kaynakta rastlamak mümkündür.

İnternet temelli eğitim ile eş anlamlı kullanılan birçok kavram vardır: İnternet temelli öğrenme, İnternete dayalı öğrenme, web tabanlı öğrenme, e-öğrenme, sanal öğrenme gibi. Bu terimler arasında ince farklılıklar olmakla birlikte çoğu zaman birbirinin yerine kullanılmaktadır. Bunların arasındaki önemli ortak özellik uzaktan eğitimin farklı sunuluş biçimlerine sahip olmasıdır (Akpınar, 2005, s.128; Çakmak ve Karataş, 2008).

Akpınar da (2005, s.128-129) İnternet tabanlı öğrenme ile İnternet destekli öğrenme kavramlarını birbirinden ayırmıştır: İnternet tabanlı öğrenme; tartışma listeleri, e-posta, forum, çoklu ortam, sanal sınıf, telekonferans ve video konferans, telefon, televizyon, CD, DVD gibi araç ve yöntemleri kullanarak, belirlenen konu alanlarındaki öğrenmenin tamamen teknolojik ortamlar üzerindeki etkinliklerle gerçekleştiği öğrenme durumudur. Geleneksel öğrenme ortamlarına ve iletişimlerine ek olarak internet ve diğer teknolojilerin yardımcı olunması ya da onları desteklemesi şeklinde gerçekleşen öğrenme durumunu da İnternet destekli öğrenme olarak tanımlamaktadır.

Diğer bir kavram olan Web (www) temelli eğitimin, İnternet temelli eğitim kavramının yerine kullanıldığı zamanlar vardır. Oysaki İnternet temelli eğitim genel anlamda uzaktan eğitimi tanımlayan ortak terim olmakla birlikte www tek başına işe yaramaz; diğer iletişim sistemlerinden e-posta ve FTP (dosya transfer protokolü) de bu amaçla kullanılmaktadır. Web temelli eğitimi tanımlarken www (world wide web)'in İnternet olmadığını, İnternetin iletişim sistemlerinden sadece birisi olduğunu belirtmek gerekir. İnternet uygulamalarının en popüler olanı ve çoğunlukla da internet ile eş anlamlı kullanılan web; istemci ve sunucu bilgisayarlar ile izlenmektedir. Bu iki kavramı açmak gerekirse kısaca; web sayfaları, internet bağlantısıyla tüm dünyaya, sunulan hizmetin yoğunluğu ve türüne göre değişen sunucu adı verilen bilgisayarlarla açılmaktadır (Altun, 2005, s.21). İnterneti bir kap, web'i de onun içine konulan bir şey olarak düşünebiliriz (Çakmak ve Karataş, 2008).

Çakmak ve Karataş (2008) web temelli eğitimi şöyle tanımlamaktadır: Gerek internet gerekse içsel veya dışsal ağ üzerinden bir web tarayıcısıyla eğitimsel içeriğin alıcıya sunumudur. En önemli avantajı birbirinden farklı mekânlarda bulunan çok

sayıda insanın aynı ortamı paylaşabilmesidir. Bundan dolayı dünyada coğrafi olarak dağınık ya da dağınık yapıda olmayan çoğu özel şirket ve kamu kuruluşu, personelini yetiştirmek için internet temelli uzaktan eğitim yöntemini seçmektedir.

2.1.6.2. İnternet Temelli Eğitimi Gerektiren Nedenler

İnternet temelli eğitim bireylere evinden, işinden, oturduğu yerden eğitim almasını sağlayarak geniş kitlelere ulaşmaya olanak veren üçüncü aşama bir uzaktan eğitim teknolojisidir. Geniş kitleler içinde, internetin en önemli ve bilinçli kullanıcıları çocuk ve gençlerin aksine çoğunlukla yetişkinlerdir. Yetişkinler için zaman çok önemlidir. Aile, toplum ve kariyer zorunlulukları gibi seçimler yüzünden yetişkin öğrenenler kendilerini bir yükün altında hissetmekte ve zamanlarını en etkili şekilde kullanmak istemektedirler. Tipik uzaktan eğitim öğrencileri çoğul rollere ve çoğul sosyal topluluklara sahiptirler, bir başka deyişle artık yaşları ilerlemiş, mesleki, ailevi ve sosyal sorumluluklarla başa çıkmaya çalışmaktadırlar. Buna rağmen İnterneti bir öğrenme kaynağı olarak görüp bunun için zaman ayırmakta oldukları gözlenmektedir.

Yetişkinlerle yapılan bir araştırma (Dalkılınç, 2011, s.85) kişilerin bilgi düzeyinde anlamlı ve olumlu yönde bir değişimin internet temelli öğrenme yolu ile sağlanabileceğini göstermiştir. Araştırmaya katılanların internet temelli eğitimle aldıkları bilgileri davranış değişikliğine dönüştürüp, günlük hayatlarına yansıttıkları görülmüştür.

Rosen'in (1996) yaptığı bir çalışmaya göre yetişkinler öğrenme gereksinimlerini internet yoluyla karşılamaktadırlar. Mesela; yazma ve okuma becerilerini geliştirmek veya bir kurs almak, ayrıca çok çeşitli bilgiye erişmek, alışveriş; arkadaşlarla, aile üyeleri ile diğer öğrenicilerle veya elektronik mektup arkadaşları ile iletişim kurmak; eğlence; görsel seyahat ve kişinin bir bilgisayar ve interneti kullanırken hissettiği güç ve kontrol duygusu için internete ihtiyaç duymaktadırlar.

Bilindiği gibi birey ve toplum yaşamında bilgisayar kullanımı oldukça geniş boyutlar kazanmıştır (Keser, 2005). İnsanlar bilgisayarı ve interneti kullanmak zorunda oldukları bir ortamda yaşamak durumunda kalmıştır. Günümüzde bireylerin bilgisayarı ve interneti amacına uygun ve beklentilerine cevap verecek biçimde kullanmayı öğrenmeleri kaçınılmaz hale gelmiştir (Keser, Bayır ve Eren, 2009).

Görüldüğü gibi yetişkinlerle yapılan araştırmalar ve alanyazın incelendiğinde, İTE'i gerektiren nedenlerin neler olduğu, yetişkinlerin öğrenme gereksinimlerini karşılamak için interneti tercih etme nedenlerini şu şekilde sınıflandırılabilir:

- Teknolojik nedenler
- Ekonomik nedenler
- Eğitim sistemi ile ilgili nedenler
- Kadınların sorunu ile ilgili nedenler
- Engelliler ile ilgili nedenler
- Yetişkinlerin eğitim ihtiyacı ile ilgili nedenler.

Internet temelli eğitim, teknolojinin avantajlarını kullanarak yapılan çağdaş uzaktan eğitim şeklidir. Günümüzde internet teknolojileri bir ülkenin uzaktan eğitim performansını etkileyen en önemli unsurlardan biri haline gelmiştir. İçinde bulunulan süreçte eğitim talebinin gittikçe artması, eğitimin amaç ve niteliğinin değişmesini de zorunlu kılmaktadır (Erturgut, 2008, s.82).

Bireyselleştirilmiş ve iletişim olanakları artırılmış teknolojik ders tasarımları geliştikçe, yetişkin toplulukları için de eğitim ihtiyaçlarına yönelik önemli sunumlar gerçekleşmeye başlamaktadır. Özellikle bazı yetişkinler için bu metot resmi ya da resmi olmayan eğitime ulaşmak için tek alternatif olabilir. Çünkü yetişkinler özellikleri gereği ana-baba, çalışan, eş gibi çeşitli sosyal zorunluluklara sahiptir.

Yetişkin öğrenenler için zaman çok kıymetlidir. Bunun için de zaman bakımından etkili ve esnek öğrenme tercihlerine ihtiyaç duyarlar. Diğer taraftan genel öğrenme işlemleri ve yaşam kuralları bakımından uzaktan öğrenen yetişkinlerle sınıf içi öğrenen yetişkinler birbirine benzerdir (Burge, 1988). Yetişkinlerin benzer davranışlar göstermesi normaldir. Çünkü yetişkinler, birçok farklı özellikleri yanında, öğrenme özellikleri bakımından da çocuklar ve gençlerden farklılıklar göstermektedirler. Nasıl ki yetişkinlerin fizyolojik, psikolojik ve toplumsal özellikleri farklı ise öğrenmeye ilişkin özellikleri de farklıdır (Miser, 1999, s.24). Yetişkinler ihtiyaç duydukları alanlarda, öz yönelimli, bireysel, deneyimlerini paylaşabileceği bir ortamda ve sorun merkezli öğrenmek isterler.

Genelde yetişkinlerin, özelde ise öğretim elemanlarının bilgi güvenliği farkındalık düzeylerini arttırmak için internet temelli yetişkin eğitimi bir alternatif olarak düşünülebilir. Çünkü internet üzerinden eğitime, ağ erişiminin olduğu her yerden ve her an ulaşılabilir. İstenildiği kadar konu tekrarı yapma şansı vardır. Eğitim almak için

yaşanılan şehri terk etmek ve yolculuk yapmak gerekmez. Teknoloji okur-yazarı olmayı sağlar. Etkileşim özelliği sayesinde derslerde aktif katılımcı olmayı geliştirir. Bu avantajlar yetişkinlere gereksinim duydukları öğrenme konularını internet temelli eğitim yoluyla vermenin önemine işaret eder.

1980'li yıllarda Knowles, "*Bu yüzyılın sonlarında çoğu eğitim hizmetleri, eğitimcilerin kitle iletişim araçlarını yetişkinlerin öğrenme ilkeleriyle hizmetleri, eğitimcilerin kitle iletişim araçlarını yetişkinlerin öğrenme ilkeleriyle uyumlu kullanmayı öğreneceği telekonferans, kablo ve uydu televizyon, bilgisayar ağları ve henüz keşfedilmemiş diğer yollarla elektronik olarak yayınlanıyor olacak*" tahmininde bulunmuştur. Knowles, eğitimin elektronik yayımı konusunu erken algılamıştır, fakat internet temelli eğitimin gelişmesine rağmen eğitimciler, yetişkin öğrenenleri ve yetişkin öğrenme ilkelerini uzaktan eğitimin merkezine henüz daha yeni yerleştirmeye başlamışlardır (DuCharmeHansen ve Dupin-Bryant, 2004,s.11).

2.2.İlgili Araştırmalar

Bilgi toplumunda en önemli görev üstlenen kurumlardan birisi de üniversitelerdir. Çünkü üniversiteler bilginin üretiminden, öğretiminden, sunumundan ve dağıtımından sorumlu temel kurumlardır. Bilgi ve iletişim teknolojileri diğer bütün kurumları olduğu gibi üniversiteleri de etkilemektedir. Kısa bir süre öncesine kadar üniversitelerdeki çoğu öğrenci ve öğretim elemanının yabancısı olduğu internet teknolojisinin günümüz eğitim ve araştırma dünyasındaki yeri ve önemi düşünülecek olursa, BİT'in üniversiteler üzerindeki etkisi daha kolay anlaşılabilir (Tonta, 1999). Bilgi güvenliğinin sağlanabilmesi için bilgi güvenliğinin en zayıf halkası olan insan unsurunun mutlaka dikkate alınması ve üniversitelerin bilgi güvenliği hakkında toplumu bilinçlendirme konusunda öncü kurumlar olması gerekmektedir. Bu bağlamda, toplumu ve öğrencileri bilinçlendirme görevi üstlenecek olan öğretim elemanlarının bilgi güvenliği farkındalıklarının en üst düzeyde olması beklenen bir durumdur. Bu kapsamda yapılan alanyazın incelemesi çerçevesinde, başta Dünya'da ve Türkiye'de giderek yoğun bir biçimde BİT kullanılan eğitim kurumları olmak üzere bilgi güvenliği ve bilgi güvenliği farkındalığı ile ilgili yapılan çalışmalar tarih sırasına göre özetlenmiştir.

ABD'de 1989 yılı baharında EDUCAUSE isimli topluluk tarafından 8 adet üniversite ve fakülte kampüslerinin yerinde ziyaret edilmesiyle gerçekleştirilmiş,

Yükseköğretimde Bilgi Güvenliği (Information Security in Higher Education) isimli bir çalışma bulunmaktadır. Çalışmada, üniversite ve fakültelerde akademik ve idari bilgi işlemden doğrudan sorumlu yöneticiler ile görüşülmüştür. Çalışma ile tespit edilen hususlar sekiz başlık altında özetlenmiştir. Bu başlıklar, bilgi güvenliği farkındalığı, bilgi güvenliği endişeleri, risk değerlendirmesi, bilgi güvenliği politikaları, güvenlik ve kontrol, bilgi güvenliği yönetimi, bilgi güvenliğinde tasarım, gözden geçirme ve test ile 1990'larda bilgi güvenliği sorunlarıdır (Elliott, Young, Collins, Frawley ve Temares, 1991).

Teknolojinizin Korunması: Elektronik Eğitim Bilgi Güvenliği İçin Pratik Rehber (Safeguarding Your Technology, Practical Guideline For Electronic Education Information Security), on bölümden oluşan ve eğitimde kullanılmak üzere ABD'de Eğitim İstatistikleri Ulusal Merkezi tarafından hazırlanmış olan kılavuz nitelikli bir çalışmadır. Kılavuzda; Eğitimde bilgi güvenliğine neden ihtiyaç olduğu, ihtiyaçların değerlendirilmesi, güvenlik politikası geliştirilmesi ve uygulanması, güvenlik yönetimi, sistemlerin korunması ve eğitim başlıklarını içeren bölümler bulunmaktadır (Szuba, 1998).

Cox, Connolly ve Currall (2001) tarafından İngiltere'de gerçekleştirilen Akademik Ortamda Bilgi Güvenliği Farkındalığının Arttırılması (Raising Information Security Awareness In The Academic Setting) isimli çalışmada üniversitelerdeki bilgi güvenliği farkındalığını arttırmaya yönelik üç yaklaşım önerilmiştir. Çalışmada; üniversitelerin tıpkı diğer kurumlar gibi artık yürütülen faaliyetlerde daha fazla çevrimiçi işlem yaptıkları, araştırma veya idari düzenlemeler ile ilgili kişisel ve gizli mesajların e-posta ile gönderildiği, aslında bilgisayar ve ağ üzerinde bulunan her bir dokümanın bakıldığında saatlerce yapılan bir çalışmanın ürünü olduğu ifade edilmektedir. Ayrıca, üniversite bütçelerinin çevrimiçi harcandığı ve tüm bunlardan dolayı kurumların bilgisayarlara olan bu bağımlılığının daha fazla güvenlik ihtiyacı gerektirdiği vurgulanmaktadır. Burada güvenlik ile virüs taraması, yapılan işlerin yedeğinin alınması, şifre seçimi ve değiştirilmesi gibi kişisel olarak alınabilecek tedbirlerden bahsedilmektedir. Bu konuda kullanıcıların üzerlerine düşen güvenlik konularını anlamaları beklenirken, farkındalığı artırmak maksadıyla kullanıcılar cephesinde karşılaşılan güçlükleri aşmak için tartışma oturumu, kontrol listesi ve web tabanlı öğreticiden oluşan üç yaklaşım önerilmektedir.

Siponen (2001) tarafından kaleme alınan Bilgi Güvenliği Farkındalığının Beş Boyutu (Five Dimension of Information Security Awareness) isimli makalede güvenlik

farkındalığının çeşitli boyutlarını ana hatlarıyla ortaya koyulmakta ve bazı anahtar konular çerçevesinde önemli olan hususlar özetlenmektedir. Makalede bahsedilen beş boyut: organizasyonel, genel kamu, sosyopolitik, bilgisayar etiği ve kurumsal eğitim boyutudur.

İngiltere'de Üniversiteler ve Fakülteler Bilgi Sistemleri Derneği (UCISA) tarafından hazırlanan Bilgi Güvenliği Alet Takımı (Information Security Toolkit), İngiliz Standartlar Enstitüsü BS7799 standartlarını esas alan ve şu anda 3. sürümü yayınlanmış bir kılavuzdur. Hazırlanan kılavuzun amacı, üniversite ve fakültelerin karşı karşıya olduğu bilgi güvenliği olaylarına karşı izlemesi gereken resmi politikanın ortaya konmasıdır. Bilgi Güvenliği Alet Takımı, üniversite ve fakültelerin bilgi güvenliği yönetimi ihtiyaçlarını karşılayacak olan kılavuzluk hizmeti ile örnek politikalardan oluşan bir başlangıç noktası sunmak ve her kurumun karşılaştığı sorunlara ilişkin kendi ihtiyacına uygun çözümler üretmesini sağlamak için hazırlanmıştır (UCISA, 2006).

Kruger ve Kearney (2006), Bilgi Güvenliği Farkındalığını Değerlendirmek için Bir Prototip (A prototype for assessing information security awareness) isimli projede, güvenlik farkındalığının nasıl ölçüleceğini geliştirmek için bir prototip ortaya koymaktadırlar. Prototip, dünyada çeşitli bölgelerde faaliyet gösteren uluslararası bir madencilik şirketinde kullanılmak üzere uyarlanabilir ve kolay kullanılabilir şekilde tasarlanmıştır. Bunun için bölgesel ihtiyaçlara göre her bir soruya farklı ağırlık puanları verilerek soruların önemi ağırlıklandırılmaktadır. Makalede bilgi güvenliği farkındalığını ölçmek için üç temel kategori tanımlamaktadır: Bilgi (ne bildiğiniz), tutum (ne düşündüğünüz) ve davranış (ne yaptığınız).

Puhakainen (2006), Bilgi Güvenliği Farkındalığı için Tasarım Kuramı (A design theory for information security awareness) isimli doktora tezinde iki aşamalı bir çalışma gerçekleştirmiştir. Çalışmanın ilk aşamasında, alanyazın kapsamlı bir şekilde incelenmiştir. İkinci aşamada ise, mevcut yöntemlerin etkinliğine yönelik yeterli kanıt bulunamamasından dolayı güvenlik farkındalığının nasıl artırılacağına yönelik üç yeni kuram geliştirilmiştir (Bilgi sistemleri güvenlik farkındalığı öğretimi, Bilgi sistemleri güvenlik farkındalığı kampanyaları, Ceza ve ödül).

Rezgui ve Marks (2008), Yükseköğretimde Bilgi Güvenliği Farkındalığı: Keşif Amaçlı Çalışma (Information security awareness in higher education: An exploratory study) isimli çalışmada gelişmiş ülkeler ile gelişmekte olan ülkeler arasındaki farklara vurgu yapan, modern üniversitelere dönük tehditleri araştırmıştır. Araştırma, Amerika Birleşik Devletleri, Birleşik Arap Emirlikleri ve İngiltere'de bulunan üç farklı

üniversitede gerçekleştirilmiştir. İngiltere ve Birleşik Arap Emirlikleri'ndeki üniversitelerde yapılan çalışma, görüşme, anket, dokümantasyon ve gözlem yoluyla gerçekleştirilir iken, Amerika Birleşik Devletleri'ndeki üniversitede daha önce gerçekleştirilmiş olan araştırma verileri kullanılmıştır. Çalışmada, yükseköğretimde bilgi sistemi karar vericileri dâhil olmak üzere personelin bilgi güvenliği farkındalığını etkileyen faktörler araştırılmıştır. Çalışma sonucunda dürüstlük, kültürel varsayımlar ve inançlar ile toplumsal koşulların üniversite personelinin davranış ve tutumlarını çalışma yönünde genel olarak, bilgi güvenliği farkındalığında ise bilhassa etkilediğini ortaya koymuştur. Araştırma sonunda çalışma ortamında bilgi güvenliği farkındalığı başlatmak ve desteklemek için bir dizi öneri sunulmuştur.

Mahabi (2010), Bilgi Güvenliği Farkındalığı: Florida Eyalet Üniversitesinde Sistem Yöneticileri ve Son Kullanıcı Görüşleri (Information Security Awareness: System Administrators and End-User Perspectives at Florida State University) isimli doktora çalışmasında sistem kullanıcılarından kaynaklanan güvenlik ihlallerinin sayısını azaltmak için kullanılan yaklaşımlar incelenmektedir. Çalışma kapsamında incelenen yaklaşımlar, teknolojik ve teknolojik olmayan olmak üzere ikiye ayrılmakta ve teknolojik olmayan yaklaşımlar araştırmanın temelini teşkil etmekte ve detaylı olarak değerlendirilmektedir. Mahabi (2010), Florida Eyalet Üniversitesi'nde bilgi güvenliği uygulamaları ve kullanıcı farkındalığı konusundaki araştırmasında özellikle sistem yöneticileri ve kullanıcı algılarını değerlendirmektedir. Elde edilen bulgular, kullanıcıların güvenlik saldırılarına karşı kendilerini korumak için kullanıcı farkındalık eğitimlerine ihtiyaçları olduğunu göstermektedir.

Ahlan ve Lubis (2011), Üniversitede Bilgi Güvenliği Farkındalığı: Sorumluluklar Vasıtasıyla Öğrenilebilirliği Devam Ettirebilme, Performans ve Uyumluluk (Information Security Awareness in University: Maintaining Learnability, Performance and Adaptability through Roles of Responsibility) isimli çalışmada yaşanılan yüzyılda teknolojinin sunduğu bilgiye ulaşım ve kullanılabilirliğin yanında bilgi güvenliği adında yeni bir sorunun ortaya çıktığı ifade edilmektedir. Araştırmada, teknolojinin beraberinde yeni riskleri nasıl ürettiğinin analiz edilmesi için teknoloji yaşam döngüsünün incelenmesi gerektiği vurgulanmaktadır. Analiz yapmak için teknoloji yaşam döngüsünün, yeniliğin yayılması olarak düşünülmesi önerilmektedir. Araştırmada, iş süreçlerini desteklemek için teknolojik yenilikler ya da bilgi teknolojileri çözümleri benimsendiğinden beri, bilgi teknolojileri çözümlerinin korunması ihtiyacının ortaya çıktığı vurgulanmaktadır. Buna göre, kurum içerisinde

farkındalığı arttırmak için iki önemli faktör öne çıkmaktadır. Bunlardan ilki kurumun son kullanıcı tutumunu anlamlı bir biçimde nasıl etkilediği, diğeri ise kurumun bilgi sistemleri farkındalık politikası etkinliğini ölçmek için düzenli bir değerlendirmenin nasıl yapıldığıdır.

Vural (2007), Kurumsal Bilgi Güvenliği ve Sızma (penetrasyon) Testleri isimli yüksek lisans çalışmasında, bilgi güvenliği genel olarak incelenmiş, kurumsal bilgi güvenliği ve standartları değerlendirilmiş, bilgi güvenliğini zafiyete düşüren tehditler gözden geçirilmiş ve Türkiye'deki bilişim hukuku konusu ele alınmıştır. Gerçekleştirilen uygulamalar ile web ortamları için büyük tehdit ve risk içeren SQL enjeksiyon ve sızma testleri genel olarak gözden geçirilerek alınması gereken önlemler detaylı olarak sunulmuştur. Bilgi güvenliğinin sağlanmasında önemli olan insan, teknoloji ve eğitim kavramlarının sızma testleri ile ilişkisi gözden geçirilerek etkisi araştırılmış, tespit edilen tehditlerin giderilmesi ile iyileştirmeye yönelik çözüm önerileri ortaya konmuştur. Tez çalışması sonucu tespit edilen önemli bulgulardan ilki bilgi güvenliğinin öneminin kamu ve özel sektör tarafından kavranamadığı veya son kullanıcılarda yüksek seviyede farkındalığın oluşmadığıdır. Tespit edilen bir diğer bulgu, Türkiye'de sosyal mühendislik kavramının tam olarak anlaşılmadığı veya önemsenmediği, kurumların ve kurum çalışanlarının bu konuda yeterli bilgi sahibi olmadıklarıdır. Tespit edilen bir diğer önemli bulgu ise araştırma kapsamında çoğu kurumda güvenlik eğitimleri ve bilinçlendirme programının olmadığı ve var olan kurumların ise genellikle kullanıcıları bilgi güvenliğinin neden önemli olduğu konusunda eğitmeyi ve bilinçlendirmeyi başaramadığıdır.

Özcan (2009), Kurumsal Bilgi Güvenliği ve COBIT isimli yüksek lisans çalışmasında, bilgi güvenliği kavramları genel olarak incelenmiş, bilgi güvenliğini zafiyete uğratan güncel tehditler ele alınmıştır. Kurumsal bilgi güvenliği ve standartları değerlendirilmiş, kurumlarda bilgi güvenliğine yönelik risklerin önlenmesinde bilgi güvenliği farkındalığının önemi ve oluşturma yöntemleri konusunda öneriler sunulmuştur. Bilgi güvenliği yönetim sistemi (BGYS) ve kurulum aşamaları detaylı olarak izah edilmiştir. BGYS için gerekli faaliyetlerin neler olduğu, nasıl uygulandığı, uygulamalar sırasında karşılaşılan sorunlar ve iş sürekliliğinin sağlanmasında izlenmesi gereken yöntemler ele alınmıştır. Üst seviyede kurumsal bir bilgi güvenliği tesis etmek için teknoloji, insan, eğitim ana başlıklarını içine alan bir yaklaşımın dikkate alınması gerektiği vurgulanmaktadır.

Vardal (2009), Yükseköğretimde Bilgi Güvenliği: Bilgi Güvenlik Yönetim Sistemi için Bir Model Önerisi ve Uygulaması isimli doktora çalışmasında, güvenlikle ilgili standartlar ve en iyi kullanım örneklerinin karşılaştırmalı olarak incelendiği ve yükseköğretim kurumları için önerilen bilgi güvenlik yönetim sistemi modeli (ÖBGYS) önerisinde bulunmaktadır. Önerilen modelin amacı, güvenlikte en zayıf halka olan insan faktörünün güçlendirilmesi ve üniversiteler için kullanımı kolay olan talimat ve ipuçlarının verilmesi olarak ifade edilmektedir. Pilot uygulama için anket ve kontrol listesinin geliştirildiği çalışma Gazi Üniversitesi, Ankara Üniversitesi ve TOBB Ekonomi ve Teknoloji Üniversitesi bilgi işlem daire başkanlıklarında uygulanmıştır. Veriler çevrimiçi anket yöntemiyle toplanmış ve analiz edilmek için SPSS programı ile çözümlenmiştir. Araştırma sonucu oluşturulan ÖBGYS modelinin bileşenleri bilgi ve insan, fiziksel ve çevresel ortam ile teknoloji olarak belirlenmiştir. Üniversitelerde bilgi güvenliği için sorumluluklar konusunda ve bilgi güvenliğinin sağlanabilmesi için yapılması gerekenler hakkında yeterli bilgiye sahip olunmadığı, bu eksikliği giderebilmek için üniversitelerde daha fazla çalışma yapılması, eğitim ve farkındalığın pekiştirilmesi gerektiği tespit edilmiştir.

Gülmüş (2010), Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği isimli yüksek lisans çalışmasında, bilgi güvenliği ve unsurları incelenmiş, kurumsal bilgi güvenliği ve standartları değerlendirilmiştir. Bu kapsamda kurumların bilgi güvenliğini zafiyete uğratacak tehditler ile riskler gözden geçirilmiş, Türkiye'deki bilişim hukuku mevzuatı gözden geçirilmiş, riskli görülen uygulamalar incelenmiştir. Kurumların bilgi varlıklarını korunması için alınacak önlemler tespit edilerek sunulmuştur. Kabul edilebilir seviyede bilgi güvenliği için gerekli olan işlem adımları gözden geçirilmiş, kurumsal bilgi güvenliği üzerine etkileri araştırılmış, tespit edilen risklerin giderilmesi ve risk yönetimine dair çözüm önerileri ortaya konmuştur. Çalışması sonucu tespit edilen önemli bulgulardan ilki bilgi güvenliğinin öneminin kamu ve özel sektör tarafından kavranamadığı veya yüksek seviyede farkındalığın oluşmadığıdır. Önemli diğer bir bulgu, güvenliğin bir ürün veya hizmet olmadığı; insan, teknoloji ve eğitim üçgeninde süreklilik arz eden yönetilmesi zorunlu bir süreç olduğu, bu üç unsur arasında tamamlayıcılık olmadığı sürece yüksek seviyede güvenlikten bahsetmenin mümkün olmayacağı tespitidir. Önemli diğer bir bulgu ise çoğu kurumda güvenlik eğitimleri ve bilinçlendirme programının olmadığı; olan kurumların ise genellikle kullanıcılarını bilgi güvenliğinin neden önemli olduğu konusunda eğitmeyi ve bilinçlendirmeyi başaramadığıdır.

Civelek (2011), Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi isimli çalışmasında BİT ve özellikle internetin günlük hayatta artan şekilde kullanılmaya başlamasıyla meydana gelen gelişmeleri ele almaktadır. Bu kapsamda kişisel verilerin elektronik izdüşümlerinden, oluşan verilerin elektronik ortamda çeşitlenmesi ile bu verilerin suiistimali, siber suçlardaki artış ve kişisel veri ticaretine yönelik yeraltı ekonomisinin oluşumundan bahsetmektedir. Bu bağlamda çalışmada, kişisel veriler ve mahremiyet hakkı, kişisel verilerin siber suçlarla ilişkisi, uluslararası alanda ve karşılaştırmalı hukukta kişisel verilerin korunmasına yönelik yasal ve kurumsal yapılar ile Türkiye'de kişisel verilerin korunmasına ilişkin yasal ve kurumsal ihtiyaçlar bütünsel bir bakış açısıyla incelenmiştir.

Bilgi güvenliği konusunda yapılan araştırmalara bakıldığında, yapılan çalışmaların daha çok bilgi güvenliği yönetim sistemleri temelinde ele alındığı görülmüştür. Bu kapsamda bilgi güvenliği yönetim sistemleri içerisinde ele alınan başlıklarından biri olan bilgi güvenliğine yönelik farkındalık çalışmaları konusu genel olarak en zayıf halka olan insan unsurunun farkındalığının artırılması gerektiği şeklinde vurgulanmaktadır. Fakat bu konuda nasıl bir yol izlenmesi gerektiği ve farkındalık düzeyinin nasıl değerlendirileceği konularında belirsizlikler olduğu görülmektedir. Bu bakımdan bu araştırmanın hem konu hem de deneysel desende yer alan değişkenleri ilişkilendirme bakımından alanyazına yeni katkılar sağlaması ümit edilmektedir.

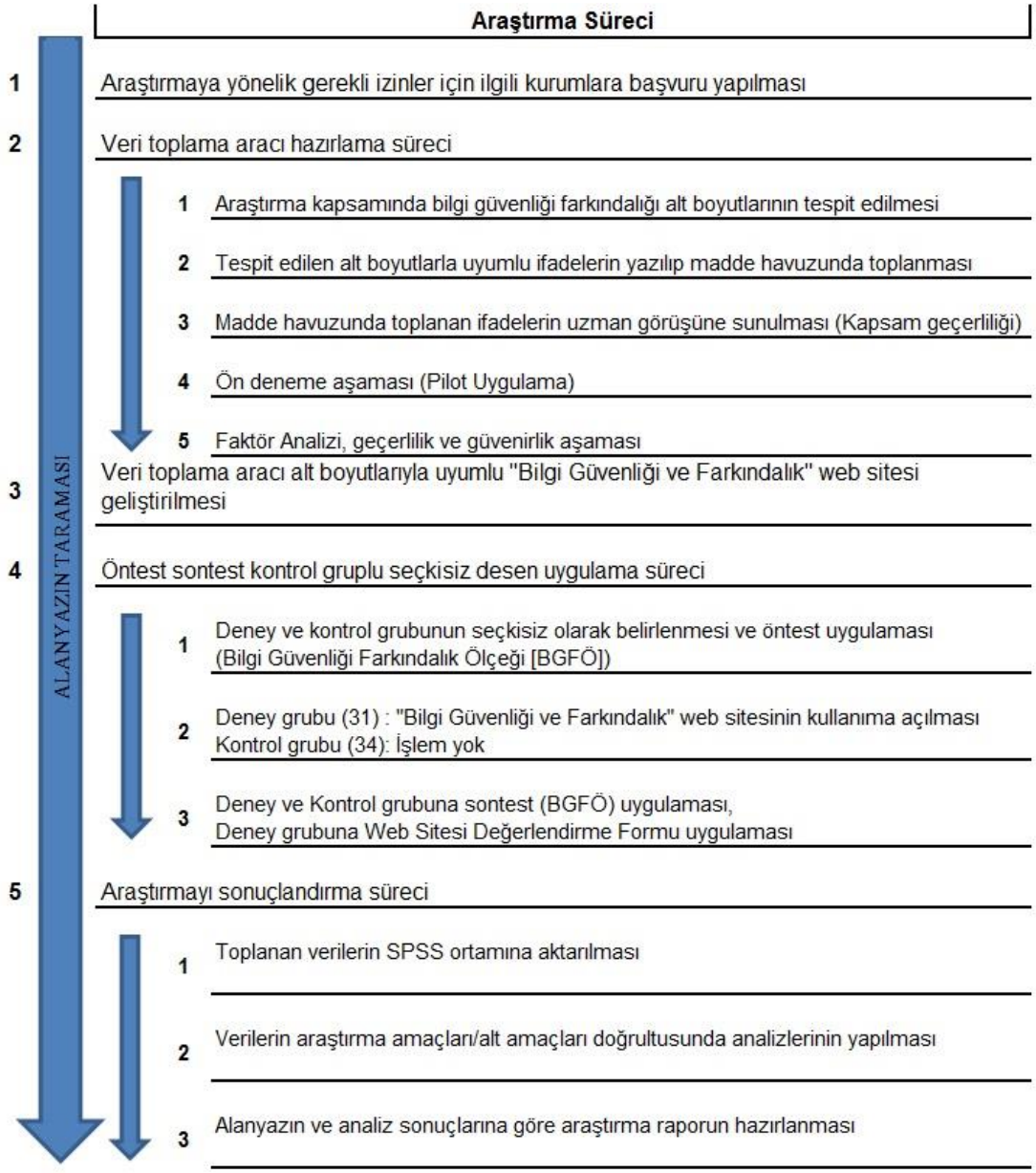
BÖLÜM 3

3.YÖNTEM

Bu bölümde araştırmanın modeli, çalışma grubu, araştırmada kullanılan deneysel desen ve yapılan deneysel işlemler, araştırmanın uygulama basamakları, veri toplama teknik ve araçları, veri toplama teknik ve araçlarının uygulama süreci, araştırmadan elde edilen veriler ve bu verilerin analizinde kullanılan istatistiksel işlemlere yer verilmiştir.

3.1.Araştırma Modeli

Araştırmanın modeli (deseni), araştırma sorularına cevap vermeyi ya da araştırmanın hipotezlerini test etmeyi güvence altına alan, verilerin araştırmanın amacına uygun ve ekonomik olarak toplanmasını ve çözümlenmesini sağlayan koşulların düzenlenmesidir (Balcı, 2009).Bu araştırma iki ayrı bölümden oluşmaktadır. Araştırmanın her bir bölümü için ayrı araştırma modeli söz konusudur. Araştırmanın ilk bölümünde; yükseköğretim kurumlarındaki öğretim elemanları bilgi güvenliği farkındalık ölçeğinin geliştirilmesi ve ön-psikometrik (preliminary) özelliklerinin belirlenmesi amacına yönelik olarak Yurdagül (2005) tarafından tanımlanan kapsam geçerlilik oranı, faktör analizi ve güvenirlik (iç ve test-tekrar test) katsayıları ile madde analizine dayanan kuramsal ölçek geliştirme modeli kullanılmıştır. Araştırmanın ikinci bölümünde ise yükseköğretim kurumlarında görev yapan öğretim elemanlarına bilgi güvenliği farkındalığı kazandırmaya yönelik çoklu ortam materyalleri ve web sitesi geliştirmek ve etkiliğini belirlemek amacına yönelik olarak deneysel desenlerden öntest sontest kontrol gruplu seçkisiz desen tercih edilmiştir. Araştırıma için üzerinde çalışılan konunun etik açıdan uygunluğuna dair Ankara Üniversitesi Etik Kurulu'ndan gerekli izinler alınmıştır. Alınan Etik Kurul Kararı ve ölçek geliştirme izin yazıları EK A.1 ve EK A.2'dedir. Araştırma sürecini açıklamak amacıyla Şekil 1'de görülen sürece ilişkin akış şeması hazırlanmıştır.



Şekil 1. Araştırmanın Gerçekleştirilmesinde İzlenen Süreç

Ölçek geliştirme ilk önce maddelerin hazırlanmasıyla başlayan, daha sonra geçerlik ve güvenirlik çalışması ile devam eden kapsamlı bir çalışmadır. Bir ölçek için pek çok geçerlik ölçütünden söz edilebilirse de Karasar'a (2005, s.151) göre en çok yararlanılanlar: içerik/muhteva/kapsam geçerliği (content validity), uygulama (deneysel) geçerliği (predictive validity) ve yapı geçerliğidir (construct validity). Karasar'a (2005, s.148) göre yapılan bir ölçmede, üç tür güvenirlik ölçütü aranabilir. Bunlar: zamana göre değişmezlik (süreklilik), bağımsız gözlemciler arası uyum ve iç tutarlıktır.

Bu araştırmada ölçek geliştirme bölümünde ilk önce kapsam geçerlik çalışması, daha sonra verilerin faktör analizine uygun olup olmadığı Kaiser-Meyer-Olkin (KMO) Testi ve Barlett Küresellik Testi ile değerlendirilmiştir. Bilgi Güvenliği Farkındalık Ölçeği'nin yapı geçerliğini belirlemek için varimax (maksimum değişkenlik) dik döndürme yöntemi ile faktörleştirme tekniklerinden temel bileşenler analizi kullanılarak Açımlayıcı Faktör Analizi (AFA) yapılmıştır. Ölçeğin alt boyutları ve toplam güvenirlikleri için Cronbach Alfa iç tutarlık katsayısı hesaplanmıştır. Madde geçerliğine kanıt sağlamak amacıyla madde-toplam korelasyonları belirlenmiştir. Ayrıca, AFA ile ortaya koyulan teorik faktör yapısının doğruluğunun test edilebilmesi için Doğrulayıcı Faktör Analizi (DFA) yapılmıştır.

Gerçek deneysel desenler, deneklerin bağımsız değişkenin düzeylerine, gruplara, seçkisiz olarak yerleştirildiği çalışmaları tanımlar (Büyüköztürk ve diğerleri, 2011). Bu araştırmada gerçek deneysel desen türlerinden biri olan öntest sontest kontrol gruplu seçkisiz desen kullanılmıştır. Bu desende ilk olarak daha önce belirlenen denek havuzundan seçkisiz atama ile iki grup oluşturulur. Gruplardan biri deney, diğeri kontrol grubu olarak belirlenir. Daha sonra iki grupta yer alan deneklerin, uygulama öncesinde bağımlı değişkenle ilgili ölçümleri alınır. Uygulama süresince ise etkisi test edilen deneysel işlem deney grubuna verilirken kontrol grubuna verilmez. Son olarak gruplardaki deneklerin bağımlı değişkene ait ölçümleri aynı araç ya da eş formu kullanılarak tekrar elde edilir. Deneysel işlemin etkisini görmek amacıyla deney ve kontrol gruplarının bağımlı değişkene ait ölçüm sonuçları uygun teknikler kullanılarak karşılaştırılır. Desen 2x2'lik karışık desen ya da 2x2'lik split-plot desen olarak da bilinir.

Öntest sontest kontrol gruplu desen, ilişkili bir desendir. Çünkü, aynı kişiler bağımlı değişken üzerinde iki kez ölçülürler. Aynı zamanda ilişkisiz bir desen niteliğine sahiptir. Çünkü farklı deneklerden oluşan deney ve kontrol gruplarının ölçümleri karşılaştırılmaktadır. Bundan dolayı öntest-sontest kontrol gruplu desen bir karışık desendir (Howitt, 1997). Desen, bir denekler havuzunu gerektirir ve denekler yansız atama ile iki gruba ayrılır.

Öntest sontest kontrol gruplu desenin, iki temel avantajı vardır. İlki, aynı denekler üzerinde ölçümler yapıldığından farklı deneysel işlem koşulları altında elde edilen ölçümler pek çok deneyde yüksek düzeyde ilişkili olacaktır. Bu da hata terimini düşürecek ve buna bağlı olarak istatistiksel güç artacaktır. Diğer avantaj ise, daha az denek gerektirmesi ve her bir işlemde aynı denekleri test etmeye bağlı olarak zaman ve

sarf edilen çaba da daha bir ekonomiklik sağlamasıdır. Bu iki avantaja bağlı olarak homojen gruplarda çalışma olanağı, deneysel işlemin gerçek etkisinin belirlenmesine katkı sağlar (Ferguson ve Takane, 1989; Kirk, 1968). Buna karşılık desenin iletme ya da aktarma etkisi olarak isimlendirilen önemli bir dezavantajından söz edilebilir. Bu sorun, önceki işlemler altındaki performansın daha sonraki işlem koşullarındaki performansı etkilemesidir. Bu etki, öğrenilmiş bir davranışa, yorgunluğa ya da can sıkıntısına bağlı olarak ortaya çıkabilir (Ferguson ve Takane, 1989; Wells, 1998). Bu durum, sontest ölçümlerindeki varyansın bir kısmının buna bağlı olarak oluşmasına neden olabilir. Yine bu desende dış geçerlilik, öntestin denekler üzerindeki uyarıcı olan etkisi nedeniyle bir miktar düşer. Sonuçta, sontest puanlarında gözlenen varyansın bir kısmı öntest ile deneysel işlemin etkileşiminden ortaya çıkabilir. Bu da doğal olarak analiz sonuçlarının doğruluk derecesini düşürebilir (Kerling, 1973; Minke, 1997; Robson, 1993).

Büyüköztürk'e (2007) göre deneysel desenlerde temel amaç değişkenler arasında oluşturulan neden sonuç ilişkisini test etmektir. Araştırmacı bu amacını gerçekleştirmek için bağımsız değişkenin düzeyleri olan işlem gruplarına seçkisiz atama yapmak, bağımsız değişkeni manipüle etmek (değişimleme), dışsal değişkenleri kontrol altına almak durumundadır (Borg ve Gall, 1989; Büyüköztürk 2007; Hovardaoğlu, 2000; Kerlinger, 1973). Bu araştırmada yansız atamayı gerçekleştirmek amacıyla Ankara Üniversitesi Eğitim Bilimleri Fakültesinde görev yapmakta olan öğretim elemanlarına, yapılan araştırma ile ilgili açıklama sunularak planlanan çalışmanın aşamaları hakkında bilgilendirme yapılmıştır. Bu kapsamda çalışmaya katılım gönüllülük esasına dayalı ve iki aşamalı olarak ele alınmıştır. Deney ve kontrol grubunu oluşturan öğretim elemanları kendilerini tanımlayan bir kullanıcı kodu oluşturarak öntest ve sontest aşamalarını tamamlamışlardır. Araştırmada kullanılan deneysel desen ve kullanılan simgelerin anlamları Çizelge 1'de sunulmuştur.

Çizelge 1

Araştırmada Kullanılan Deneysel Desen

Grup	Rastgelelik	Ön Test	Deneysel İşlem	Son Test
D_1	R	O_1	X	O_1
K_1	R	O_1		O_1,O_2

D_1 : Deney Grubu

K_1 : Kontrol Grubu

R : Grupların Belirlenmesindeki Rastgelelik

X : Bilgi Güvenliği ve Farkındalık Web Sitesi ile Öğretim

O_1 : Bilgi Güvenliği ve Farkındalık Ölçeği (BGFÖ)

O_2 : Bilgi Güvenliği ve Farkındalık Web Sitesi Değerlendirme Formu (BGFWSDF)

Araştırmanın bağımsız değişkeni web temelli eğitim ortamında kullanılan bilgi güvenliği farkındalık web sitesinde sunulan eğitim, bağımlı değişkeni öğretim elemanlarının bilgi güvenliği farkındalık düzeyleridir. Öntest ve sontest ölçümlerinde "Bilgi Güvenliği Farkındalık Ölçeği" kullanılmıştır. Öntestin iletme etkisi ve uyarıcı etkisini ortadan kaldırmak için deneysel çalışmanın ikinci aşamasına geçmek için üç aylık bir ara verilmişitr. Üç ay sonunda öğretim elemanlarının toplantı, seminer, konferans gibi çalışma programlarındaki iş yoğunluğuna bağlı olarak on dört hafta boyunca devam eden uygulama aşamasına geçilmiştir. On dört haftalık uygulama süreci sonunda deney ve kontrol grubundaki öğretim elemanlarına son test olarak Bilgi Güvenliği Farkındalık Ölçeği uygulanmıştır. Ayrıca deney grubunu oluşturan öğretim elemanlarının, "Bilgi Güvenliği ve Farkındalık Web Sitesi Değerlendirme Formu" ile tasarlanmış olan web sitesi ve çoklu ortam materyallerini değerlendirmesi istenmiştir.

3.2.Çalışma Grubu

Alanyazında, ulaşılması gereken örneklem büyüklüğü konusunda farklı ölçütler ve görüşler bulunmaktadır. Örneklem büyüklüğü, madde ya da faktör sayısı gibi bağıl ölçütlere dayalı olarak tahmin edilmektedir. Genel olarak örneklem büyüklüğünün

ölçekteki madde sayısının 5-10 katı kadar olması istenmektedir (Kass ve Tinsley, 1979; Kline, 1994; Tavşancıl, 2005). Kline (1994) mutlak ölçüt olarak 200 kişilik örneklemin yeterli olacağını, ancak büyük örneklemlerle çalışmanın daha uygun olacağını vurgulamaktadır. Çokluk, Şekercioğlu ve Büyüköztürk (2010), faktör analizinde en az 300 örneklem sayısının uygun olduğu genel kuralını ortaya koymaktadır.

Araştırmanın ölçme aracı geliştirilmesi kısmının çalışma grubunu gönüllülük esasına dayalı olarak başta Karadeniz Teknik Üniversitesi, Niğde Üniversitesi ve Gazi Üniversitesi'nde görevli öğretim elemanları ile elektronik anket uygulamasıyla Eylül 2013 – Nisan 2014 tarihleri arasında kendilerine ulaşılan ve ülkedeki muhtelif üniversitelerde görev yapan toplam 363 öğretim elemanı oluşturmaktadır. Çalışmada yukarıda ifade edilen ölçütler göz ününde bulundurularak 363 kişi üzerinde Faktör Analizi yapılmıştır. Çalışmaya katılan öğretim elemanalarının cinsiyet ve unvanlara göre dağılımı Çizelge 2'de sunulmuştur.

Çizelge 2

Ölçek Geliştirme Çalışmasına Katılan Öğretim Elemanlarının Cinsiyet ve Unvanlara Göre Dağılımı

Unvan	**Katılan Sayı**	**Yüzde (%)**
Öğretim Üyesi	148	40.77
Yardımcı Öğretim Elemanı	215	59.23
Cinsiyet	**Katılan Sayı**	**Yüzde (%)**
Kadın	188	51.79
Erkek	175	48.21
Toplam	**363**	**100.00**

Çizelge 2 incelendiğinde, araştırmaya katılan öğretim elemanlarının %48,20'si (175) erkek ve %51,80'si (188) kadındır. Araştırmaya katılan öğretim elemanlarının %40.77'si (148) öğretim üyesi, %59.23'ü (215) ise yardımcı öğretim elemanıdır.

Araştırmanın ikinci aşaması için Ankara Üniversitesi'nin tamamı dtasarlanmasına karşın, tez danışmanı ve araştırmacı tarafından yetkili makamlarla yapılan görüşmeler neticesinde deneysel kısım Ankara Üniversitesi Eğitim Bilimleri fakültesi ile sınırlı kalmıştır. Bu bağlamda araştırmanın deneysel ikinci aşamasının çalışma grubunu, Ankara Üniversitesi Eğitim Fakültesinde görev yapmakta olan ve Haziran 2014 – Ocak 2015 tarihleri arasında gönüllülük esasına göre çalışmaya katılmayı kabul eden öğretim elemanları oluşturmaktadır. Ankara Üniversitesi Eğitim

Bilimleri Fakültesi'nde görev yapmakta olan 221 öğretim elemanından uygulamalara katılan 136'sı araştırmanın ikinci aşamasında yer alan deneysel çalışma grubunu oluşturmaktadır. Araştırma süreci esnasında 105 öğretim elemanı çalışmanın ikinci aşamasına katılacağını beyan etmiştir. Fakat öğretim elemanlarının ders yükü, toplantı, seminer, konferans gibi çalışma programlarındaki iş yoğunluğu gibi çeşitli sebeplerle çalışmaya iştirak edememesinden dolayı deney grubunda 31 ve kontrol grubunda 34 olmak üzere toplamda 65 öğretim elemanı araştırma sürecini bitirebilmiş ve bu sayılarla araştırmanın istatistiksel analizleri yapılmıştır. Çalışmaya katılan öğretim elemanalarının cinsiyet ve unvanlara göre dağılımı Çizelge 3'te sunulmuştur.

Çizelge 3

Deneysel Çalışmaya Katılan Öğretim Elemanlarının Cinsiyet ve Unvanlara Göre Dağılımı

Unvan	**Katılan Sayı**	**Yüzde (%)**
Öğretim Üyesi	24	36.92
Yardımcı Öğretim Elemanı	41	63.08
Cinsiyet	**Katılan Sayı**	**Yüzde (%)**
Kadın	39	60.00
Erkek	26	40.00
Toplam	**65**	**100.00**

Çizelge 3 incelendiğinde, araştırmaya katılan öğretim elemanlarının %40,00'ı (26) erkek ve %60,00'ı (39) kadındır. Araştırmaya katılan öğretim elemanlarının %36.92'si (24) öğretim üyesi, %63.08'i (41) ise 3 yardımcı öğretim elemanıdır.

Araştırma kapsamında yer alan deneklerin belirlenmesinde ve çalışma gruplarının eşleştirilmesinde bilgi güvenliği farkındalık düzeyleri dikkate alınmıştır. Öğretim elemanlarının bilgi güvenliği farkındalık düzeylerinin belirlenmesinde araştırmacı tarafından geliştirilen "Bilgi Güvenliği Farkındalık Ölçeği" kullanılmıştır.

3.3.Verilerin Toplanması

Bu bölümde, geliştirilen öğrenme ortamları, materyalleri, veri toplamada kullanılan veri toplama araçları, araştırmanın uygulama süreci, verilerin toplanması ve veri analizi ile ilgili bilgilere yer verilmiştir.

3.3.1.Veri Toplama Araçları

Bu araştırmanın verileri; bilgi güvenliği farkındalık düzeylerini tespit etmek amacıyla araştırmacı tarafından geliştirilen EK F'deki "Bilgi Güvenliği Farkındalık Ölçeği" ve "Bilgi Güvenliği ve Farkındalık" isimli web sitesine yönelik öğretim elemanlarının görüşlerini belirlemek için geliştirilen EK B'teki "Bilgi Güvenliği ve Farkındalık Web Sitesi Değerlendirme Formu'ndan" elde edilmiştir. Aşağıda araştırmada veri toplama aracı olarak kullanılan ölçeğin geliştirilmesinde izlenen aşamalar sıralanmıştır.

3.3.1.1.Ölçek Geliştirme Çalışmaları

Ölçek geliştirme çalışmaları, genellikle deneysel süreç ya da kuramsal süreçler ile gerçekleştirilir (Yurdagül, 2005). Deneysel süreçte alanyazın ya da uzman görüşü yaklaşımları sayesinde aday ölçek formu elde edilir ve hedef kitle ile benzer özellikler taşıyan bir örneklem grubuna deneme uygulaması yapılarak ölçek maddelerine ilişkin psikometrik özellikler belirlenerek ideal maddelerden nihai form elde edilir. Bu sürecin karekteristik özellikleri ise; nicel bir çalışma özelliği taşıması, genellikle faktör analizlerinin kullanılması ve büyük örneklem gerektirmesidir. Bu sürece ilişkin genel yaklaşım ve bilgiler Tezbaşaran (2008) tarafından ayrıntılı olarak açıklanmıştır.
Ölçme aracının geliştirilmesinde Karasar (2004) ve Balcı (2009) tarafından önerilen; madde havuzu aşaması, uzman görüşü aşaması, ön deneme aşaması, faktör analizi aşaması ve güvenirlik hesaplama aşaması adımlarından oluşan bir yol izlenmiştir.

3.3.1.1.1.Ölçeği oluşturan madde havuzu aşaması.

Bu aşamada alanyazın incelenerek bilgi güvenliği farkındalığı kavramına ilişkin göstergelerin neler olabileceği araştırılmıştır. Çalışmada tespit edilmiş kategoriler, göstergeler dikkate alınmış ve bu göstergeler çerçevesinde maddeler yazılmıştır. Bilgi güvenliği farkındalığına ilişkin kategoriler, göstergeler ve madde sayıları Çizelge 4'de sunulmuştur. Bilgi güvenliği farkındalığına ilişkin her bir gösterge göz önünde bulundurularak toplamda 90 maddelik bir havuz oluşturulmuştur.

Çizelge 4

Bilgi Güvenliği Farkındalığına İlişkin Kategori, Gösterge ve Madde Sayıları

Kategoriler	**Göstergeler**	**Madde Sayısı**
Genel Güvenlik	Bilgi güvenliği, Bilgi güvenliği sorumluğu, Anti-virüs yazılımları, Güvenlik duvarı, Şifre seçimi ve korunması, Virüs ve casus yazılımlar, Bazı yaygın söylenceler, İyi güvenlik alışkanlıkları, Çocukların güvenli şekilde çevrimiçi tutulması, Verilerin güvence altına alınması	34
Saldırı ve Tehditler	Çevrimiçi ticaret tuzakları, Sosyal mühendislik ve sazan avlama / yemleme saldırıları, Siber zorbalık, Aldatmacalar ve şehir efsaneleri, Kimlik hırsızlığı, Casus yazılımlar, Virüsler, solucanlar ve truva atları, Hizmet aksattırma saldırıları, Bozuk yazılım dosyaları, Kök kullanıcı takımı (rootkit) ve botnet'ler, Sahte anti-virüs yazılımları	21
E-posta ve İletişim	Anlık mesajlaşma ve sohbet odaları, Ücretsiz e-posta servislerinin faydaları ve riskleri, Mesaj sağanağı, Sosyal ağ siteleri, Dijital imza, E-posta istemcileri, E-posta ekleri	8
Mobil Cihazlar	Elektronik cihazlar için siber güvenlik, Cep telefonları ve kişisel dijital yardımcılar, Şahsi internet-etkin cihazlar ile seyahat, Taşınabilir cihazlarda veri güvenliği ve fiziksel güvenlik, Kablosuz ağ güvenliği, USB sürücüleri	8
Mahremiyet	Dosyaların etkili bir şekilde silinmesi, Mahremiyetin korunması, Şifrelerin ilave önlemler ile desteklenmesi, Şifrelemenin anlaşılması	8
Güvenli Gezinme	Telif hakkı ihlalleri, Web sitesi sertifikaları, Web tarayıcıları, Aktif içerik ve çerezler, Web tarayıcılara ait güvenlik ayarları, Çevrimiçi güvenli alışveriş, Bluetooth teknolojisi, Uluslararası etki alan adları	6
Yazılım ve Uygulamalar	Son kullanıcı lisans sözleşmeleri, Dosya paylaşım teknolojileri ve riskler, Yazılım yamaları, Internet protokolü ses teknolojisi, İşletim sistemleri	5
Toplam		**90**

3.3.1.1.2.Geçerlik analizleri aşaması.

Bir ölçme aracının bireylerin davranışlarını tahmin etmedeki başarısı büyük ölçüde ölçme aracının geçerli ve güvenilir olmasına bağlıdır (Büyüköztürk, 2004). Bir maddenin ölçmek, bir başka ifade ile tanımlamak istediği özelliği ne derece doğru ölçtüğü ölçeğin geçerliği ile ilgilidir (Balcı, 2009; Karasar, 2004). Geçerlik, bir ölçme aracının ölçmeyi amaçladığı özelliği, başka herhangi bir özellikle karıştırmadan, tam ve aynı zamanda doğru olarak ölçmesidir. Geçerlik, bir ölçme aracının ölçmek üzere hazırlandığı amacı ölçme derecesidir. Bir ölçeğe ilişkin geçerlik kanıtlarının elde

edilmesinin birçok yolu söz konusudur (Özgüven, 1999; Tezbaşaran, 2008). Bu kapsamda öncelikle uzman görüşüne başvurularak hazırlanan ölçme aracının kapsam geçerliliğine sahip olması sağlanmıştır.

3.3.1.1.3.Kapsam geçerlik çalışmaları.

Bilindiği gibi ölçülmek istenilen özellik ile ölçek maddeleri arasındaki bağıntı, ölçme aracının geçerliğine ilişkindir. Ölçek maddesinin ölçülmesi amaçlanan özelliği kapsama (kapsam geçerliği) ya da maddenin ilgili yapıyı yorma (yapı geçerliği) gücünü belirlemek amacıyla önsel çalışmalara ihtiyaç vardır (McGartland vd., 2003). Yine ölçme aracının geçerliğini etkileyen diğer faktörler de ölçek geçerliği için göz önüne alınması gereken noktalardır; ölçek maddesinin anlaşılabilir olması, hedef-kitleye uygunluğu vb. Önsel çalışmalarda elde edilen uzman görüşleri arasındaki uyum/uyumsuzluk aynı zamanda kapsam ya da yapı geçerliği için birer kestirim niteliğinde kullanılmaktadır.

Kapsam geçerliği çalışmalarında, Lawshe (1975) kapsam geçerliği tekniğinden yararlanılmıştır. Lawshe tekniği olarak bilinen yaklaşım 6 aşamadan oluşmaktadır:

- Alan uzmanları grubunun oluşturulması
- Aday ölçek formlarının hazırlanması
- Uzman görüşlerinin elde edilmesi
- Maddelere ilişkin kapsam geçerlilik oranlarının elde edilmesi
- Ölçeğe ilişkin kapsam geçerlilik indekslerinin elde edilmesi
- Kapsam geçerlilik oranları/indeksi ölçülerine göre nihai formun oluşturulması.

Lawshe tekniğinde, en az 5 ve en fazla ise 40 uzman görüşüne ihtiyaç vardır. Her bir maddeye yönelik uzman görüşleri, "gereksiz", "gerekli, ancak düzeltilmeli" ve "gerekli" şeklinde üçlü derecelendirilmektedir. Kapsam geçerliğinin yanı sıra benzer şekilde maddenin anlaşılabilirliği, hedef kitleye uygunluğu vb. amacıyla da uzman görüşleri derecelendirilebilir.

Buna göre, uzmanların herhangi bir maddeye ilişkin görüşleri toplanarak kapsam geçerlilik oranları (KGO) elde edilir. KGO, herhangi bir maddeye ilişkin "Gerekli" görüşünü belirten uzman sayısının, maddeye ilişkin görüş belirten toplam uzman sayısının yarısına oranının 1 eksiği ile elde edilir.

$$KGO = \frac{Ng}{N/2} - 1$$

Burada; Ng, maddeye "gerekli" diyen uzmanların sayısını ve N ise maddeye ilişkin görüş belirten toplam uzman sayısını göstermektedir. Yukarıdaki eşitliğe göre; uzmanların yarısı maddeye ilişkin "gerekli" şeklinde görüş bildirdiklerinde KGO=0, yarısından fazlası "gerekli" şeklinde görüş bildirmiş ise KGO>0 ve uzmanların yarısından azı "gerekli" şeklinde görüş bildirmiş ise KGO<0 olacaktır.

KGO değerleri negatif ya da 0 (sıfır) değer içeriyorsa böyle maddeler ilk etapta elenen maddelerdir. KGO değerleri pozitif olan maddeler için istatistiksel ölçütler ile anlamlılıkları test edilirler. Elde edilen KGO'larının istatistiksel olarak anlamlılığını test etmek için kapsam geçerlilik ölçütleri için ilgili alanyazında önceleri birikimli normal dağılımdan yaralanılmakta iken, hesaplama kolaylığı açısından α=0,05 anlamlılık düzeyinde KGO'larının minimum değerleri Veneziano ve Hooper (1997) tarafından tabloya dönüştürülmüştür. Tabloya dönüştürülen değerler Çizelge 5'te sunulmuştur. Buna göre, uzman sayısına ilişkin minimum değerler aynı zamanda maddenin istatistiksel anlamlılığını vermektedir.

Çizelge 5

α=0,05 Anlamlılık Düzeyinde KGO'ları için Minimum Değerler

Uzman Sayısı	**Minimum Değer**	**Uzman Sayısı**	**Minimum Değer**
5	0,99	13	0,54
6	0,99	14	0,51
7	0,99	15	0,49
8	0,78	20	0,42
9	0,75	25	0,37
10	0,62	30	0,33
11	0,59	35	0,31
12	0,56	40+	0,29

Kaynak. Veneziano ve Hooper, 1997, 67-70.

Çalışmanın bu aşamasında madde havuzunun oluşturulmasının ardından oluşturulan 90 maddelik deneme formu, uzman görüşleri alınmak üzere bilgi güvenliği alanında bilgi sahibi olan ve çalışma konusu hakkında bilgilendirilen Bilgisayar ve Öğretim Teknolojileri Eğitimi alanından 13 uzman, Bilgisayar Mühendisliği alanından 4 uzman, Bilgisayar Enformatik/Bilgi Teknolojileri alanından 4 uzman, Elektronik Mühendisliği alanından 1 uzman ve Bilişim Hukuku alanından 1 uzman olmak üzere toplam 23 uzman tarafından değerlendirilmiştir. Hazırlanan uzman değerlendirme

formundaki her bir madde, bilgi güvenliği farkındalığını ölçebilme, ilgili alt boyutla ilişkili olma, ifadenin anlaşılırlığı başlıkları altında değerlendirilmiştir. Daha sonra, bu oranların istatistiksel olarak anlamlılığı α=0,05 anlamlılık düzeyinde Veneziano ve Hooper (1997) tarafından tabloya dönüştürülmüş olan kapsam geçerlik ölçütüyle (KGO20 = 0.42) karşılaştırılarak bu değerin altında olan maddeler çalışma kapsamından çıkarılmıştır. Elde edilen kapsam geçerlik oranları doğrultusunda ölçekten 23 madde çıkarılmış, bazı maddeler üzerinde ise düzeltmeler yapılmıştır. Son durumda 67 maddelik bir form oluşturulmuştur. Bilgi Güvenliği Farkındalık Ölçeği' nin kapsam geçerliği için uzman görüşüne dayalı istatistiksel işlemlerden elde edilen verilerin bulguları Çizelge 6'da sunulmuştur.

Çizelge 6

BGFÖ Alt Boyutları ve Kapsam Geçerlik Oranları

Alt Boyut	**Bşl.Madde Sayısı**	**Bşl.KGO**	**Madde Sayısı**	**KGO**
01. Genel Güvenlik	34	0.49	18	0.87
02. Saldırı ve Tehditler	21	0.80	18	0.93
03. E-posta ve İletişim	8	0.77	7	0.88
04. Mobil Cihazlar	8	0.86	7	0.94
05. Mahremiyet	8	0.88	7	0.96
06. Güvenli Gezinme	6	0.70	5	0.83
07.Yazılım ve Uygulamalar	5	0.81	5	0.84
Toplam	**90**	**0.76**	**67**	

Uzman Sayısı	**23**
Kapsam Geçerlik Ölçütü	**0.39**
Kapsam Geçerlik İndeksi	**0.89**

Toplam 23 alan uzmanın ölçek alt boyutları ve maddelerine ilişkin belirtmiş oldukları görüşler üzerinden, yöntem bölümünde açıklanan Lawsh tekniği formülü yardımıyla kapsam geçerlik oranları hesap edilmiştir. Çizelge 5'te görüldüğü üzere 23 uzman için kapsam geçerlik ölçütü 0,39'dur. 0,39 kapsam geçerlik ölçütünün altında kalan yedi alt boyuttaki toplam 23 madde elenmiş ve ölçek formu 67 madde olarak belirlenmiştir. Faktör Analiz yapılmak üzere 67 maddeden oluşan formun kapsam geçerlik indeksi 0,89 olarak hesaplanmıştır. Lawsh tekniğine göre kapsam geçerliği ile ilgili yapılan hesaplamaları içeren detaylı çizelgeler EK D'de sunulmuştur.

Bireylerin, ölçekteki maddelere katılma düzeylerini belirlemek üzere “hiç katılmıyorum (1)”, “katılmıyorum (2)”, “kararsızım (3)”, “katılıyorum (4)” ve “kesinlikle katılıyorum (5)” şeklinde Likert tipi beşli derecelendirme ölçeği kullanılmıştır. Geliştirilen ve ön deneme aşamasında kullanılan 67 maddelik ölçek formu “Bilgi Güvenliği Farkındalık Ölçeği” olarak adlandırılmış ve “BGFÖ” olarak kısaltılmıştır.

3.3.1.1.4.Ön deneme aşaması.

Oluşturulan ölçeğin elektronik formu, çalışma hakkında bilgi içeren açıklayıcı bir e-posta ve bağlantı adresi ile Karadeniz Teknik Üniversitesi ve Niğde Üniversitesi’nde görev yapan tüm öğretim elemanlarına (N=2870) dekanlıklar aracılığıyla gönderilmiştir. Çalışmaya gönüllü olarak katılan öğretim elemanları, bu bağlantı aracılığıyla ölçeği çevrimiçi ortamda doldurmuşlardır. Veri toplama sürecinin ikinci ayında çevrimiçi ortamda katılım 34 kişi ile sınırlı kalmıştır. Çalışma grubuna ait katılım miktarını artırmak için elektronik formla beraber Karadeniz Teknik Üniversitesi ve Niğde Üniversitesi’ne dekanlıklar aracılığıyla basılı anket uygulaması gerçekleştirilmiştir. Basılı anket uygulamasıyla toplamda katılım miktarı çalışma grubu için 134 kişi ile sınırlı kalmıştır. Katılım miktarını artırmak maksadıyla Gazi Üniversitesi’ne dekanlık aracılığıyla basılı anket uygulaması gerçekleştirilmiştir. Ayrıca, eş zamanlı olarak çevrimiçi ortamda hazırlanan ikinci bir bağlantı ülke genelinde yükseköğretim kurumlarında görev yapan diğer öğretim elemanlarına çalışma hakkında bilgi içeren açıklayıcı bir e-posta ve bağlantı adresi ile birlikte gönderilmiştir. Toplamda beş ay süren veri toplama süreci sonunda 407 öğretim elemanı, oluşturulan formun elektronik veya basılı halini doldurmuştur [Adnan Menderes Üniversitesi (11), Bahçeşehir Üniversitesi (18), Başkent Üniversitesi (9), Dokuz Eylül Üniversitesi (10), Gazi Üniversitesi (77), GaziOsmanPaşa Üniversitesi (6), Gülhane Askeri Tıp Akademisi (22), Hacettepe Üniversitesi (4), Hitit Üniversitesi (3), İstanbul Üniversitesi (5), Kara Harp Okulu (4), Karadeniz Teknik Üniversitesi (51), Kocaeli Üniversitesi (3), Muğla Sıtkı Koçman Üniversitesi (4), Niğde Üniversitesi (77), Pamukkale Üniversitesi (8), Şifa Üniversitesi (4), Üsküdar Üniversitesi (10)].

Veri analizine başlamadan önce hatalı veriler ve kayıp değerler incelenmiş ve düzeltilmiştir. Yapılan inceleme sonucunda öğretim elemanlarının doldurduğu 407 formdan 363’nün istatistiksel analize uygun olduğu tespit edilmiş, bu doğrultuda

ölçeğin geçerlik ve güvenirlik çalışması yapılmıştır. Ölçek geliştirme sürecine katılan öğretim elemanlarının unvanlara göre dağılımı Çizelge 7'deki gibidir

Çizelge 7

Çalışmaya Katılan Öğretim Elemanlarının Unvanlara Göre Dağılımı

Unvan	**Katılan Sayı**	**Yüzde (%)**
Prof. Dr.	20	5.51
Doç. Dr.	40	11.02
Yrd. Doç. Dr.	88	24.24
Öğr. Grv. Dr.	16	4.41
Öğr. Grv.	63	17.36
Arş. Grv. Dr.	9	2.48
Arş. Grv.	99	27.27
Okutman Dr.	1	0.28
Okutman	5	1.38
Uzm. Dr.	2	0.55
Uzm.	10	2.75
Unvan Belirtmeyen	10	2.75
Toplam	**363**	**100.00**

Araştırmaya katılan öğretim elemanlarının %48,20'si (175) erkek ve %51,80'si (188) kadındır. Araştırmaya katılan öğretim elemanlarının yaş aralığı 23 ile 65 arasında değişmekte olup yaş ortalaması ise 35,47'dir.

3.3.1.2.Faktör analizi aşaması.

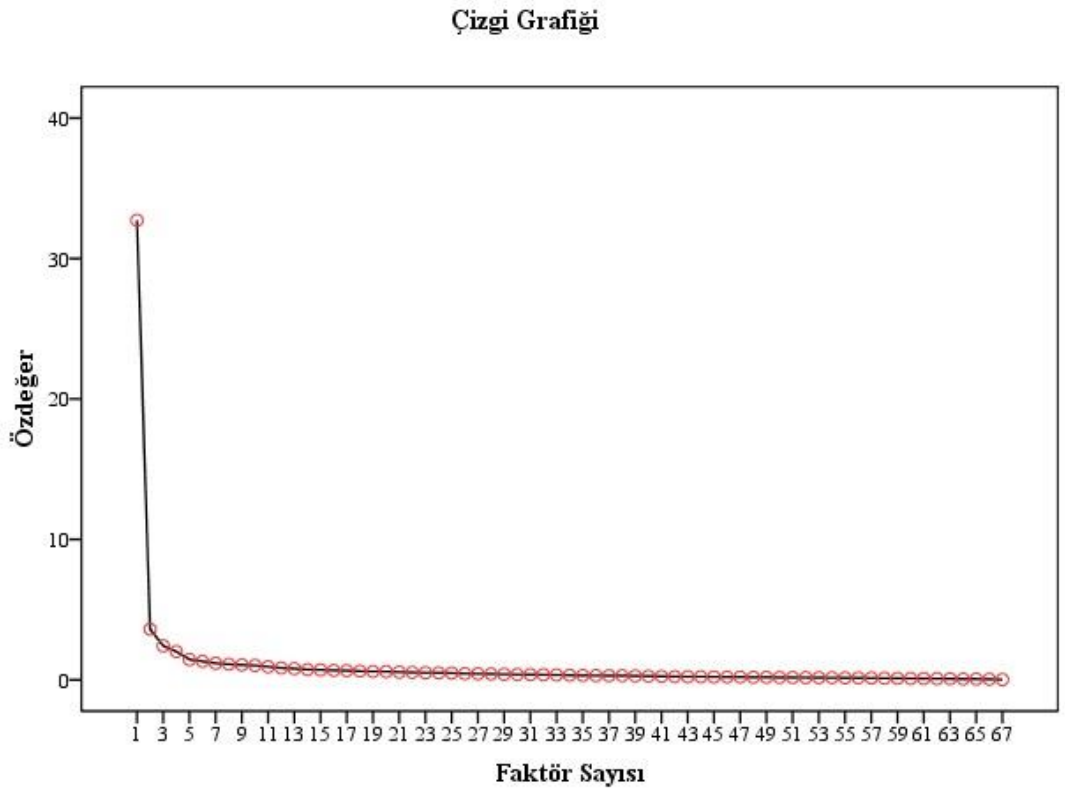
Çakmak ve diğerleri (2014), ölçek geliştirme çalışmalarında ideal olan durumun, Açımlayıcı Faktör Analizi (AFA) ve Doğrulayıcı Faktör Analizlerinin (DFA) farklı örneklem gruplarından elde edilen veriler üzerinde yapılması gerektiğini ifade etmektedir. Ancak, alanyazındaki ölçek geliştirme çalışmalarını incelediklerinde aynı örneklem grubunun rasgele olarak alt gruplara bölünerek elde edilen veriler üzerinde de AFA ve DFA çalışmaları yapılabildiğini vurgulamaktadırlar.

Alanyazında, ulaşılması gereken örneklem büyüklüğü konusunda farklı ölçütler ve görüşler bulunmaktadır. Örneklem büyüklüğü, madde ya da faktör sayısı gibi bağıl ölçütlere dayalı olarak tahmin edilmektedir. Genel olarak örneklem büyüklüğünün ölçekteki madde sayısının 5-10 katı kadar olması istenmektedir (Kass ve Tinsley, 1979; Kline, 1994; Tavşancıl, 2005). Kline (1994) mutlak ölçüt olarak 200 kişilik örneklemin yeterli olacağını, ancak büyük örneklemlerle çalışmanın daha uygun olacağını

vurgulamaktadır. Çokluk, Şekercioğlu ve Büyüköztürk (2010), faktör analizinde en az 300 örneklem sayısının uygun olduğu genel kuralını ortaya koymaktadır. Bu çalışmada gerek zaman gerekse de maddi olanaklar göz önünde bulundurularak, araştırmaya katılan grup rasgele olarak iki alt gruba bölünmüştür (n1=363; n2=200). İlk grup üzerinde AFA, diğer grup üzerinde ise DFA yapılmıştır.

Faktör yapısını ortaya koymak için öncelikle döndürülmemiş temel bileşenler analizi gerçekleştirilmiştir. Faktör sayısının belirlenmesinde Kaiser-Guttman ilkesi uyarınca özdeğerleri 1'den büyük faktörlerin incelenmesi yoluna gidilmiş; faktör özdeğerlerine ilişkin çizgi grafiği ve açıkladıkları varyans oranları incelenmiştir (Zwick ve Velicer, 1986). Çünkü Faktör analizinde, sadece öz değerleri 1 ve 1'in üzerinde olan faktörler kararlı olarak kabul edilir (Büyüköztürk, 2002; Çokluk ve ark., 2010). Ölçek, özdeğerleri 1'den büyük 10 faktör yapısına sahiptir. Bu faktörlerin sırasıyla özdeğeri ve açıklanan toplam varyansa katkı düzeyleri: 1.faktör:32,73; %48,85, 2.faktör: 3,61; %5,38, 3.faktör: 2,42; %3,62, 4.faktör: 2,02; %3,01, 5.faktör: 1,45; %2,17, 6.faktör: 1,32; %1,97, 7 faktör: 1,18; %1,77, 8.faktör: 1,11; %1,66, 9.faktör: 1,07; %1,60 ve 10.faktör: 1,03; %1,54 şeklindedir. AFA başlangıç özdeğerleri 1'den büyük faktör yapısını gösteren detaylı çizelge EK E'de sunulmuştur. Bu değerler tek başlarına ele alındığında ölçeğin on faktörlü bir yapı gösterebileceği düşünülmektedir. Ancak, alanyazın incelendiğinde bu değerlerin tek başına incelenmesinin gerçekte var olandan fazla sayıda faktör üretilmesine yol açabileceği; faktör yapılarına karar verebilmek için bunların yanında dikkate alınması gereken temel bir ölçütün ortaya konulan çözümün kuramsal olarak temellenebilmesi olduğu görülmektedir (Zwick ve Velicer, 1986). Tek faktörlü desenlerde açıklanan varyansın %30 ve daha fazla olması yeterli görülebilir. Çok faktörlü desenlerde ise açıklanan varyansın daha yüksek olması beklenir. Açıklanan varyansı arttırmak için iki tür yol izlenir. Bunlardan ilki, önemli faktör sayısını arttırmak, ikincisi ise açıklanan madde seçiminde daha yüksek faktör yük değerini aramaktır (Büyüköztürk, 2002).

Buradan yola çıkarak, daha sağlıklı karar verebilmek açısından temel bileşenler analizi uygulanmasına ve ortaya çıkan yapıların kuramsal olarak değerlendirilmesine karar verilmiştir. Bu bilgiler ışığında, AFA analizine başlarken öz değer 2 ve faktör yük değeri 0.55 olarak kabul edilmiştir. Şekil 2'de faktör özdeğerlerine ilişkin çizgi grafiği sunulmaktadır.



Şekil 2. Faktör Özdeğerlerine İlişkin Çizgi Grafiği.

AFA sonucunda ölçeğin öz değerinin 2'den büyük 4 faktör altında toplandığı görülmüştür. Bu 4 faktörün ölçeğe ilişkin açıkladığı varyans ise %60,86'dır. AFA sonucu oluşan maddeler binişiklik ve faktör yük değerlerinin kabul düzeyini karşılayıp karşılamaması açısından değerlendirilmiştir. Çok faktörlü desenlerde, binişik ve yük değeri düşük olan maddeler bir arada olabilir. Kesin bir kural olmamakla birlikte, madde çıkarma işlemine binişik maddelerden başlanması tercih edilebilir (Çokluk ve ark., 2010). Binişik ve yük değeri düşük olan maddeler ölçekten çıkartılarak AFA 34 kez tekrarlanmıştır. Nihai AFA sonucu oluşan, maddelere ilişkin faktör yükleri ve ortak faktör varyansı Çizelge 8'de sunulmuştur.

Çizelge 8

Faktör Yük Değerleri ve Ortak Faktör Varyansı

Alt Boyut	Madde	F1	Ortak Faktör Varyansı	Alt Boyut	Madde	F2	Ortak Faktör Varyansı
Saldırı ve Tehditler	S33	0.88	0.81	Kişisel Verilerin Korunması	S41	0.74	0.57
	S32	0.87	0.79		S44	0.74	0.62
	S30	0.84	0.76		S46	0.72	0.64
	S31	0.81	0.76		S45	0.72	0.61
	S36	0.79	0.73		S61	0.70	0.65
	S22	0.79	0.67		S42	0.68	0.58
	S35	0.78	0.73		S43	0.68	0.64
	S34	0.78	0.70		S39	0.67	0.47
	S28	0.76	0.73		S38	0.67	0.52
	S26	0.75	0.71		S8	0.66	0.53
	S20	0.72	0.66		S9	0.63	0.47
	S29	0.71	0.66		S6	0.61	0.47
	S25	0.71	0.68		S51	0.60	0.46
	S21	0.67	0.69		S1	0.59	0.40
	S27	0.65	0.64		S10	0.59	0.40
	S23	0.62	0.57		S40	0.58	0.46
					S2	0.58	0.43
					S62	0.58	0.43
Özdeğer:			**17.74**	**Özdeğer:**			**2.85**
Açıklanan Varyans:			**31.97**	**Açıklanan Varyans:**			**28.59**
Açıklanan Toplam Varyans:							**60.57**

İki faktörlü yapının açıklayabildiği toplam varyans %60,57 düzeyindedir. Alanyazında çok faktörlü ölçek yapılarında, sosyal bilimlerde açıklanan varyansın %40 ile %60 arasında olması yeterli olarak kabul edilir (Tavşancıl, 2005). Bu ölçüte dayanarak elde edilen iki faktörlü ölçek yapısı öğretim elemanlarına yönelik bilgi güvenliği farkındalığını ölçmek için yeterli bulunmuştur. Ölçekte yer alan otuz dört maddenin tamamı için faktör yük değerleri .58'in üzerinde kalmıştır. Alanyazında .45 ve üzerinde faktör yük değeri gösteren maddeler ölçekte kesinlikle tutulması gereken maddeler olarak nitelenmektedir (Büyüköztürk, 2011: 124; Kline, 2000: 167-168). Bu ölçüte dayanarak ölçeğin iki faktör altında 34 maddenin tamamını içermesine karar verilmiştir. Geliştirilen ölçek EK F'de sunulmaktadır.

3.3.1.3.Madde analizleri (ayırt edici geçerlik).

Ölçekte yer alan her bir maddenin, ölçmek istediği özelliği ölçüp ölçmediği ve ölçtükleri özellik açısından kişileri ayırt etmede ne kadar yeterli olduklarının belirlenmesi amacıyla ilk olarak madde-toplam korelasyonları hesaplanmıştır. İkinci olarak ise toplam puana göre üst %27 ve alt %27'lik grupların madde puanları arasındaki farkın anlamlılığı için t-testi kullanılmıştır. Ayrıca, ölçeğin güvenirliğini belirlemek için Cronbach Alfa iç tutarlılık katsayısına bakılmıştır. Ölçekte yer alan her bir madde için madde-toplam korelasyonları ve toplam puana göre belirlenen üst ve alt %27'lik grupların madde puanları arasındaki farkın anlamlılığını irdeleyen bağımsız t-testi sonuçları Çizelge 8'de sunulmaktadır.

Çizelge 9'da da görüldüğü gibi Faktör analizi ile belirlenen ve iki boyuttan oluşan 34 maddenin madde analizleri yapılmıştır. Buna göre; saldırı ve tehditler faktöründe madde-toplam test korelasyonları incelendiğinde değerler r=.72 ile r=.85 arasında değişmektedir. Kişisel verilerin korunması faktöründe madde-toplam test korelasyonları incelendiğinde değerler r=.59 ile r=.77 arasında değişim göstermektedir. Madde- toplam korelasyonlarının .30 ve daha yüksek olması ölçek maddelerinin geçerliğine bir kanıt olarak kullanılmaktadır (Nunnally ve Bernstein, 1994). Madde-toplam test korelasyonları incelendiğinde, her bir madde için (r=.30)'un üzerindedir. Bu durum, ölçek maddelerinin ölçülmek istenen özelliği ölçme amacına hizmet ettiğine işaret etmektedir. Ayrıca, ölçeğin t-testi sonuçlarına göre %27 alt ve üst gruplarının madde puanları arasındaki farklara ilişkin t-testi değerlerinin 9.18-23.04 arasında değiştiği ve hepsinin de anlamlı olduğu ($p < .001$) görülmektedir. Üst %27'lik grubun tüm maddelere ilişkin madde puan ortalamaları alt %27'lik grubun madde puan ortalamalarından anlamlı biçimde yüksektir. Buna göre ölçekte yer alan maddeler aynı davranışı; bir başka deyişle öğretim elemanlarına yönelik bilgi güvenliği farkındalığını ölçmekte ve farklı farkındalık seviyelerindeki katılımcıları anlamlı biçimde ayırt edebilmektedir. Hem madde-toplam korelâsyonları hem de üst ve alt %27'lik grupların madde ortalama puanlarına ilişkin t-testi sonuçları ayırt ediciliği en yüksek olarak 33. ve en düşük olarak 62. maddeyi göstermektedir.

Çizelge 9

Üst ve Alt %27'lik Grup Madde Puanları Farkı Anlamlılığı Bağımsız T-Testi

F1	Madde	Düzeltilmiş Madde-Toplam Korelasyonu	Üst-Alt %27 Farkın Anlamlılık Testi	F2	Madde	Düzeltilmiş Madde-Toplam Korelasyonu	Üst-Alt %27 Farkın Anlamlılık Testi
Saldırı ve Tehditler	S20	0.79	21.75*	Kişisel Verilerin Korunması	S01	0.59	10.04*
	S21	0.80	22.40*		S02	0.62	11.32*
	S22	0.79	16.64*		S06	0.64	12.56*
	S23	0.72	16.92*		S08	0.69	12.30*
	S25	0.80	22.26*		S09	0.65	11.79*
	S26	0.83	23.04*		S10	0.58	10.12*
	S27	0.76	17.92*		S38	0.68	12.33*
	S28	0.83	21.05*		S39	0.61	9.18*
	S29	0.78	20.57*		S40	0.63	13.02*
	S30	0.83	18.43*		S41	0.68	11.34*
	S31	0.85	20.52*		S42	0.72	15.88*
	S32	0.84	17.39*		S43	0.76	17.15*
	S33	0.84	16.57*		S44	0.75	13.04*
	S34	0.81	20.00*		S45	0.74	14.28*
	S35	0.82	20.48*		S46	0.77	16.57*
	S36	0.83	19.97*		S51	0.63	10.18*
					S61	0.77	16.17*
					S62	0.61	12.61*

3.3.1.4.Güvenirlik analizleri.

Güvenirlik bir test veya ölçme aracının ölçtüğü şeyi ne derece doğru ölçtüğü ile ilgilidir. Likert tipi ölçeklerin güvenirliğini ölçmek için Cronbach Alpha kat sayısı kullanılmıştır ki bu değer uyarlanan ölçek ve ölçeğin alt ölçekleri için iç tutarlılığı/homojenliği hakkında bilgi verir (Tezbaşaran, 2008). Ayrıca, ölçeğin güvenirliği için yarılama (split half) yöntemi kullanılmıştır. Split-half (iki eşit parçaya bölme) tekniği, bir ölçme aracının güvenirliğini belirlemede kullanılan yöntemlerden biridir. Bu kapsamda Guttman ve Spearman değerleri hesaplanmıştır.

BGFÖ maddelerinin ve alt boyutlarının Cronbach Alpha iç tutarlık değeri belirlenmiş ve ölçek formunun güvenilir olduğu tespit edilmiştir.

Ölçeğin güvenirliğini ortaya koymak amacıyla Cronbach Alfa iç tutarlılık katsayısı hesaplanmıştır. Genel olarak, güvenilirlik katsayılarının .70 veya daha yüksek olması, yeterli olarak değerlendirilmektedir (Nunnally, 1978). Ölçeğin tümüne ait Cronbach Alfa iç tutarlılık katsayısı .97, birinci alt faktöre ilişkin Cronbach Alfa iç tutarlılık katsayısı .97, ikinci alt faktöre ilişkin Cronbach Alfa iç tutarlılık katsayısı .94 olarak hesaplanmıştır. Bunun yanında yarılama (split-half) yöntemi ile yapılan güvenirlik analizleri sonucunda ölçeğin birinci yarısı için Alpha katsayısı α1=.95 olarak, ikinci yarısı için Alpha katsayısı α1=.95 olarak, Spearman Brown katsayısı SB=.93 olarak, Guttman yarılama katsayısı G=.93 olarak hesaplanmıştır. Tüm bu bulgular ölçeğin tatmin edici düzeyde güvenirliğe sahip olduğunu göstermektedir. Bunun yanında madde-toplam korelasyonlarının yüksekliği de ölçeğin iç tutarlılığının gücüne işaret etmektedir.

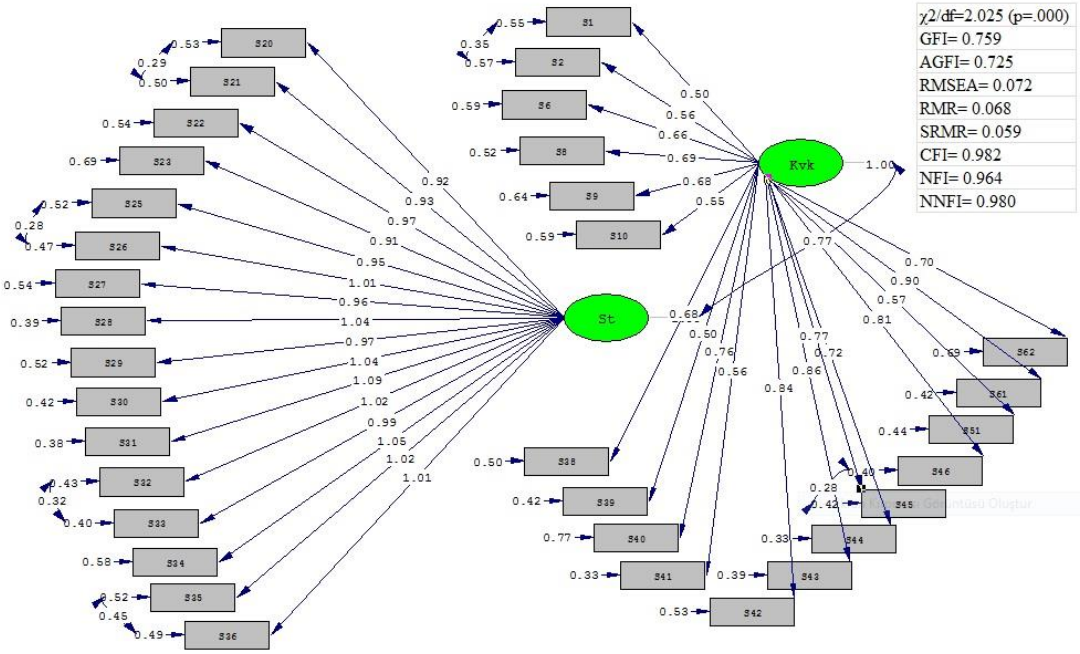
3.3.1.5.Doğrulayıcı Faktör Analizi

AFA sonrasında ortaya çıkan modelin, yapı geçerliğini değerlendirmek için DFA yapılmıştır (Kline, 2005). Bu çalışmada model uyum indeksleri olarak Ki-Kare ($\chi 2$) İyilik Uyumu, İyilik uyum İndeksi (GFI), Düzenlenmiş İyilik Uyum İndeksi (AGFI), Yaklaşık Hataların Ortalama Karekökü (RMSEA), Artık Ortalamaların Karekökü (RMR), Standardize Edilmiş Artık Ortalamaların Karekökü (SRMR), Karşılaştırmalı Uyum İndeksi (CFI), Normlaştırılmış Uyum İndeksi (NFI) ve Normlaştırılmamış Uyum İndeksi (NNFI) göz önünde bulundurulmuştur.

İki faktörden oluşan yapıya ilişkin olarak gerçekleştirilen doğrulayıcı faktör analizlerinde model üzerinde hiçbir sınama yapılmadan ve önerilen modifikasyonlar gerçekleştirilmeden önce ulaşılan uyum iyiliği indeksleri şöyledir: [$\chi 2$/df=3.587 (p=.000); GFI= 0.630; AGFI= 0.581; RMSEA= 0.114; RMR= 0.077; SRMR= 0.066; CFI= 0.953; NFI= 0.936; NNFI= 0.950]. Analizler sonucunda ortaya çıkan modifikasyon önerileri incelendiğinde; S36 ve S35; S33 ve S32; S46 ve S45; S2 ve S1; S21 ve S20; S26 ve S25 maddeleri arasında altı modifikasyon önerisinin ortaya çıktığı görülmüştür.

Kuramsal olarak incelendiğinde; bu maddelerin benzer durumları ölçtükleri, dolayısıyla iki madde arasında gizil bir ilişkinin kabul edilebilir olacağı görülmüş ve modifikasyon önerisi dikkate alınmıştır.

Modifikasyonun ardından modele ilişkin uyum iyiliği indeksleri şu şekilde oluşmuştur: [χ2/df=2.025 (p=.000); GFI= 0.759; AGFI= 0.725; RMSEA= 0.072; RMR= 0.068; SRMR= 0.059; CFI= 0.982; NFI= 0.964; NNFI= 0.980]. Şekil 3'te iki faktörlü yapıya ilişkin yapısal eşitlik modeli ve Çizelge 10'da ölçek maddelerine ilişkin t ve R2 (çoklu korelasyon katsayısı) değerleri sunulmaktadır.



Şekil 3. İki Faktörlü Yapıya İlişkin Yapısal Eşitlik Modeli.

Tablo halinde sunulan yapısal eşitlik modelinde uyum indeksleri kriterleri ve kabulü için kesme noktaları göz önüne alınarak modelin uyum iyiliği indeksleri incelendiğinde Ki-Kare/serbestlik derecesi iyilik uyumu değerinin 2.025 olduğu görülmektedir [küçük örneklemler için 2.5'in altındaki modellerde mükemmel uyum], (Çokluk ve arkadaşları, 2010; Kline, 2005). Hesaplanan RMSEA değerinin .07 olduğu görülmektedir [iyi uyum] (Brown, 2006; Jöreskog ve Sörbom, 1993). Modelin GFI değeri .76 ve AGFI değeri .73 için zayıf uyuma sahip olduğu söylenebilir [GFI, AGFI > .90 mükemmel uyum; GFI> .85 ve AGFI>.80 kabul edilebilir uyum] (Jöreskog ve Sörbom, 1993). Alanyazın irdelendiğinde bu indekslerin aldıkları değerlerin örneklem büyüklüğünden etkilenebildikleri görülmektedir (Şimşek, 2007: 48). Örneklem büyüklüğü etkilerinden arındırılmış uyum iyiliği indekslerinden olan CF, NFI ve NNFI üzerinde durulmuştur. CFI, NFI ve NNFI değerlerinin .95'den büyük olduğu

görülmektedir [CFI, NFI, NNFI > .95 mükemmel uyum] (Sümer, 2000; Thompson, 2004). RMR ve SRMR değerinin .08'den küçük olması iyi uyuma sahip olduğunu göstermektedir (Brown, 2006; Byrne, 1994). Modele ilişkin t değerleri incelendiğinde tüm gözlenen değişkenlerin gizil değişken tarafından .01'lik anlamlılık düzeyinde yordanabildiği görülmektedir.

Çizelge 10

Maddelere İlişkin t ve R^2 Değerleri.

F1	Madde	t	R2	F2	Madde	t	R2
Saldırı ve Tehditler	S31	15.50	0.76	Kişisel Verilerin Korunması	S27	13.46	0.63
	S28	15.15	0.74		S46	13.23	0.62
	S30	14.91	0.72		S20	13.16	0.61
	S33	14.74	0.71		S44	13.07	0.61
	S32	14.72	0.71		S45	12.63	0.58
	S26	14.31	0.68		S42	12.49	0.57
	S36	14.12	0.67		S23	12.15	0.55
	S35	14.08	0.67		S41	11.09	0.48
	S61	13.86	0.66		S08	11.05	0.48
	S34	13.85	0.66		S38	11.04	0.48
	S43	13.73	0.65		S40	10.29	0.43
	S29	13.70	0.65		S51	10.21	0.43
	S02	9.10	0.65		S06	10.18	0.42
	S22	13.60	0.64		S09	10.10	0.42
	S25	13.52	0.64		S62	10.06	0.42
	S21	13.51	0.63		S39	9.43	0.38
					S10	8.90	0.34
					S01	8.46	0.31

Önemli bir ölçüt de her bir gözlenen değişken için açıklanan varyansı ifade ederek, gözlenen değişkenin gizil değişkendeki değişimin ne kadarını açıklayabildiğini ortaya koyan R2 değeridir (Şimşek, 2007: 86). Sunulan modele ilişkin λx, t ve R2 değerleri incelendiğinde bilgi güvenliği farkındalığının ölçümüne en yüksek katkıyı sırasıyla 31, 28, 30, 33 ve 32. maddelerin, en düşük katkıyı ise sırasıyla 1, 10, 39, 62, 9. maddelerin sağladığı görülmektedir. Bu bulgu, açımlayıcı faktör analizinde elde edilen bulguları doğrulamaktadır.

3.3.1.5. BGFÖ Alt Faktörleri *ile Farkındalık Düzeyi Puanları*

Ölçeğin alt faktörleri (saldırı ve tehditler, kişisel verilerin korunması), faktörlere dahil olan sorular, ölçekten alınan en düşük ve en yüksek puanlara ilişkin puanlar ile farkındalık düzeyleri Çizelge 11'da sunulmuştur.

Çizelge 11

Ölçek Alt Faktörleri, Faktörlere Dahil Olan Sorular ile En Düşük ve En Yüksek Farkındalık Düzeyi Puanları.

Faktör/Alt FaktörAdı	**Faktöre Dâhil Olan Sorular**	**En Düşük Puan**	**En Yüksek Puan**	**Farkındalık Düzeyi**		
				Düşük	**Orta**	**Yüksek**
Bilgi Güvenliği ve Farkındalık Ölçeği	1-34	34	170	34-102	103-136	137-170
Saldırı ve Tehditler	1-6 23-34	18	90	18-54	55-72	73-90
Kişisel Verilerin Korunması	7-22	16	80	16-48	49-64	65-80

Çizelge 11'da da görüldüğü gibi kullanıcıların bilgi güvenliği farkındalık ölçeği ve faktörlerine ilişkin verebilecekleri en düşük ve en yüksek puan göz önünde bulundurularak; bilgi güvenliği farkındalık düzeyi toplam puanı 34-102 arası "Düşük", 103-136 arası "Orta", 137-170 arası ise "Yüksek"; saldırı ve tehditler faktörü toplam puanı 18-54 arası "Düşük", 55-72 arası "Orta", 73-90 arası "Yüksek"; kişisel verilerin korunması toplam puanı 16-48 arası "Düşük", 49-64 arası "Orta", 65-80 arası "Yüksek" olarak belirlenmiştir.

3.3.1.6. Bilgi Güvenliği ve Farkındalık Web Sitesi Değerlendirme Formu

Araştırmanın sekizinci alt amacında belirtildiği üzere, öğretim elemanlarının geliştirilen web sitesine yönelik görüşlerini belirlemek için araştırmacı tarafından öğretim elemanlarının görüşlerini belirlemeye yönelik bir form geliştirilmiştir. Geliştirilen bu öğretim elemanları görüşlerini belirleme formuyla bilgi güvenliği

farkındalığına yönelik geliştirilen web sitesiyle ilgili öğretim elemanlarının görüşleri alınmıştır.

Araştırmacı tarafından geliştirilen öğretim elemanları görüşlerini belirleme formu kapsam geçerliliği açısından uzmanlara inceletilerek üzerinde gerekli düzenlemelerin yapılması sağlanmış ve araca son şekli verilmiştir. Araştırmanın deney grubundaki öğretim elemanları için 6 sorudan oluşan "Bilgi Güvenliği ve Farkındalık Web Sitesi Değerlendirme Formu" Ek B'de sunulmuştur.

Oluşturulan öğretim elemanlarının görüşlerini belirleme formu uygulama sonrasında son test ile beraber deney grubundaki öğretim elemanlarına elektronik olarak uygulanmıştır. Öğretim elemanlarının "Bilgi Güvenliği ve Farkındalık" web sitesi öğrenme ortamına ilişkin görüşleri öğretim elemanları görüşlerini belirleme formuna verilen yanıtlara dayalı olarak tespit edilmiştir.

3.3.2. Bilgi Güvenliği ve Farkındalık Web Sitesi

Araştırma kapsamında çalışma grubunca kullanılan öğrenme ortamları yetişkin eğitimi kuramının bileşenleri göz önünde bulundurularak tasarlanmıştır. Yetişkinlerin öğrenme ilkeleri göz önüne alınarak internet temelli bir uzaktan eğitim programında nasıl ve hangi düzeyde yer alması gerektiği konusunda Ankara Üniversitesi'nde görev yapan ve alan uzmanı beş öğretim elemanı ile görüşmeler yapılmış, bu ilkelere ilişkin öğretim elemanı beklentileri ortaya konulmuştur. Öğretim elemanlarının öğrenmeye ilişkin durumları ve öğrenme ortamından beklentileri göz önüne alınarak, eğitim teknolojisi alan uzmanlarının da değerlendirmeleri sonucunda öğrenenlerin yapısına uygun bir düzeyde öğrenen özerkliğinin sağlandığı öğrenme ortamı tasarımına gidilmiştir.

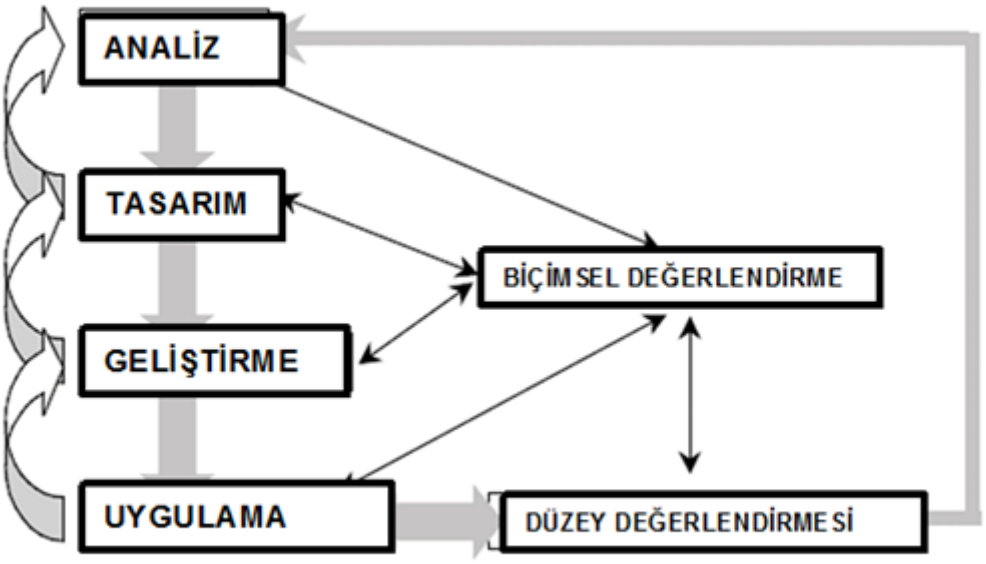
Öğretim tasarımı, öğrenme ve öğretim ilkelerinin; öğretim materyal, etkinlik, bilgi kaynakları ve değerlendirme için kullanılacak tasarımlara dönüştürülmesini sağlayan sistematik ve yansıtıcı süreçtir (Smith and Ragan,1999). Sistematik öğretim tasarımı için önerilen pek çok farklı model bulunmaktadır. Birçok öğretim ortamı tasarlama modeli olmasına rağmen genel olarak tüm öğretim ortamları tasarımı 5 aşamadan oluşmaktadır. Bunlar analiz, tasarım, geliştirme, uygulama ve değerlendirme aşamalarıdır. En çok kullanılan model ADDIE modeli olarak da bilinir. Diğer öğretim ortamı tasarlama modelleri ADDIE modeli temelinde geliştirilmiştir (Cowell, Hopkins,

Mcwhorter ve Jorden, 2006). Sıralı bir şekilde her basamağın çıktısı bir sonraki basamağın girdisi olarak kullanılmaktadır.

3.3.2.1. ADDIE Modeli Bileşenleri.

ADDIE modeli bileşenleri analiz, tasarım, geliştirme, uygulama ve değerlendirmedir. Modele ait bileşenler aşağıda kısaca açıklanmakta ve model Şekil 4'te sunulmaktadır.

Analiz (**A**nalyze): Analiz aşaması modeldeki diğer aşamaların temelini oluşturur. Analiz aşamasında tasarımcı öğrenme problemini, amaç ve hedefleri, hedef kitlenin ihtiyaçlarını, mevcut bilgileri ve diğer ilgili özellikleri belirler. Analiz aşamasında ayrıca öğrenme ortamı, sınırlılıklar ve süre gibi unsurlar belirlenir. Bu aşamada özel analizler yapılır. İhtiyaç analizi, öğrenen analizi, görev analizi bu aşamada yapılması gereken temel analizlerdir. Bu aşamada hazırlanacak olan öğretim materyalinin amaçları elde edilir. Bu aşamada elde edilen veriler tasarım aşamasında ön bilgi olarak kullanılır.



Şekil 4. ADDIE Modelinin Bileşenleri

Tasarım (**D**esign): Tasarım aşaması analiz kısmında elde edilen bilgiler kullanılarak öğretim materyalinin geliştirilmesi için strateji belirlenmesini ve bir plan

oluşturulmasını temel alır. Bu aşamada analiz sürecinde belirlenen öğretimin amaçlarına nasıl ulaşılacağının taslağı oluşturulur. Bu aşamada elde edilen taslaklar ve planlar geliştirme sürecinin temelini oluşturulur ve bu plan ve taslaklara göre öğretim materyali geliştirilir. Öğrenme hedeflerinin belirlenmesi için sistematik bir süreçtir. Genellikle detaylı prototipler, tasarım, kullanıcı arayüzü gibi unsurlar belirlenir. Analiz aşamasında belirlenen problemin çözümüne yönelik çalışma yapılır. Gerekli kaynaklar belirlenir.

Geliştirme (**D**evelopment): Tasarım aşamasında belirlenen içerik ve diğer materyaller hazırlanır. Bu aşama içerisinde hem analiz hem de tasarım aşamalarını içerir. Bu aşamanın amacı öğrenme materyalini geliştirmektir. Bu aşamada materyalin içerisinde yer alacak tüm öğeler (içerik, animasyon, gezinim, ses, oyun v.b.) birleştirilerek materyal geliştirilir.

Uygulama (**I**mplementation): Uygulama aşamasında geliştirilen materyal son kullanıcı tarafından kullanılır. Bu aşamanın amacı materyalin etkili bir şekilde sunumunu sağlamaktır. Yapılacak uygulamalar ve bu uygulamaların sonuçlarına göre materyalin eksiklikleri ile iyi yönleri belirtilir. Belirlenen eksikler giderilerek hatasız ve son kullanıcının isteklerine uygun bir materyal üretilir.

Değerlendirme (**E**valuation): Sürece veya ürüne yönelik bir değerlendirme yapılır. Sürece yönelik değerlendirme süreklilik arz eder, analiz aşamasında başlar ve modelin diğer aşamalarında devam eder. Ürüne yönelik değerlendirme ise, önceden belirlenmiş olan değerlendirme kriterlerine göre değerlendirmeyi ve kullanıcı geri bildirimlerini içerir. Uygulamadan edinilen geri bildirimlere göre gerekli iyileştirmeler yapılır. Bu aşamada materyalin etkinliği ve etkileri ölçülür. Değerlendirme tüm tasarım boyunca yapılır. Bu tür bir değerlendirme tasarım sürecinin genel olarak değerlendirilmesini sağlar. Değerlendirme, Biçimlendirici ve Düzey Belirleyici değerlendirmeler şeklinde yapılır.

- *Biçimlendirici Değerlendirme*: Aşamalar arasında yapılan değerlendirmelerdir. Bu değerlendirmenin amacı ürünün son halini elde edilinceye kadar materyalin geliştirilmesidir.
- *Düzey Belirleyici Değerlendirme*: Materyalin son hali oluşturulduktan sonra yapılan değerlendirmedir. Bu değerlendirme genel olarak materyalin kalitesini ve etkililiğini belirler. Düzey belirleyici değerlendirme genel olarak materyal hakkında bir karar vermek ve kullanılabileceği şartları belirlemek için yapılır.

3.3.2.2. Öğretim Materyallerinin ADDIE Modeline Göre Tasarımı.

Hazırlanan web tabanlı öğretim materyali mevcut problemlere cevap verebilmek, öğretim elemanlarının bilgi güvenliği farkındalık düzeylerini arttırmaya yönelik ihtiyacını karşılayabilmek amacıyla öğretim tasarım modellerinden ADDIE modeli kullanılmıştır. Bu maksatla Ankara Üniversitesi Eğitim Bilimleri Fakültesi öğretim elemanlarına ön-test olarak uygulanan Bilgi Güvenliği Farkındalık Ölçeği sonuçlarından yararlanılmıştır. BGFÖ sonuçlarından hareketle öğretim elemanlarının bilgi güvenliği farkındalığı konusundaki ihtiyaç analizi gerçekleştirilmiştir. Bu aşamada elde edilen veriler tasarım aşamasında ön-bilgi olarak kullanılmıştır. Ayrıca benzer siteler, incelenmiştir (Bilgimi Koruyorum, MEB web sitesi vb). Tasarım aşamasında, analiz sürecinde belirlenen öğretimin amaçlarına nasıl ulaşılacağının taslakları oluşturulmuştur. Bu aşamada elde edilen taslaklar ve planlar geliştirme sürecinin temelini oluşturmuş, bu plan ve taslaklara göre öğretim materyali geliştirilmiştir. Geliştirme sürecinde kullanılan ADDIE modelinin önemli bir parçası olan biçimlendirici değerlendirme çerçevesinde web tabanlı öğretim materyallerinde her bir öğe alan uzmanı olan öğretim elemanlarının fikir ve değerlendirmeleri ile geliştirilmiştir. Alan uzmanlarının geribildirim ve önerileri dikkate alınarak araştırmacı gerekli görülen düzeltmeleri yapmıştır. Hazırlanan web tabanlı öğretim materyalleri araştırmacı tarafından geliştirilmiştir. Bu durum ortamın bir bütünlük içinde hazırlanmasını kolaylaştırmıştır.

3.3.2.3. Öğretim Materyali ve Materyalin Bileşenleri.

Web tabanlı öğretim materyali ADDIE modelindeki her aşama dikkate alınarak tasarlanmıştır. Motivasyonu ve kullanılabilirliği sağlayacak tasarım ilkelerinden yararlanılmıştır.

Hazırlanan web tabanlı öğretim materyali öğrenen merkezli olarak tasarlanmıştır. Öğretim elemanları ortama girdiği zaman ana ekran üzerinde kısa yoluna ulaşabilecekleri, Bilgi Güvenliği ve Farkındalık Web Sitesini tanıtan ve site içeriğinde sunulan her bir bölümün nasıl kullanılacağı hakkında kısa açıklamaları anlatan ve Şekil 5'te ekran görüntüsü görülen bir kullanım kılavuzu bulunmaktadır. Bilgi Güvenliği ve Farkındalık Web Sitesi kullanım kılavuzu EK C'de sunulmaktadır.

Şekil 5. Bilgi Güvenliği ve Farkındalık Web Sitesi Giriş Sayfası

Öğretim elemanlarının bilgi güvenliği farkındalık düzeyini arttırmak maksadıyla hazırlanmış olan web sitesinde sunulan içeriğe ulaşmak için sitenin alt orta bölümünde bulunan "BGF Eğitimi için lütfen tıklayınız." metni tıklandığında Şekil 6'da görülen web sayfası açılmaktadır.

Şekil 6. Bilgi Güvenliği ve Farkındalık Eğitimi Ana Sayfası

Tasarlanan web tabanlı öğretim materyali 4 temel başlık üzerinde oluşturulmuştur. Bunlar;

- Güvenlik Eğitimi Bölümleri
- Uygulamalar
- Sunular
- Yardımcı Kaynaklar

Araştırma kapsamında bilgi güvenliği farkındalığı konularıyla ilgili flash animasyonla desteklenmiş video şeklinde öğrenme materyalleri hazırlanıp öğretim elemanlarının erişimine açılmıştır. Hazırlanan bilgi güvenliği farkındalığı konu içeriklerine karar verilirken "Bilgi Güvenliği Farkındalık Ölçeği" geliştirirken kullanılan kategori, gösterge ve maddeleri ile yapılan alanyazın incelemeleri doğrultusunda bir taslak eğitim içeriği oluşturulmuştur. Hazırlanan bu taslakla ilgili uzman görüşleri alınmış ve uzman görüşleri doğrultusunda eğitim içeriğine son şekli verilmiştir. Son şekli verilen eğitim içeriğiyle ilgili; bilgi güvenliğine giriş, korsanlık, korsanlık türleri (telefon çeviricileri, klavye dinleme sistemleri, casus yazılımlar, Truva atları, virüsler, solucanlar), bilgi güvenliği tehdit ve riskleri (dijital saldırı, saldırı nasıl gerçekleşir, saldırı olası değerler, insan ilişkileri, çöp karıştırmak, kimlik avı, virüs ve zararlı kodlar, casus yazılım), önlemler (otomatik güncelleştirme, kişisel bilgisayar kullanımı, işletim sistemi lisansı, işletim sistemi otomatik güncelleme, antivirüs programı, güvenlik duvarı, casussavar yazılım/reklamsavar yazılım, lisanslı yazılım kullanımı, e-posta, mesaj sağanağı, internet bağlantısı, kablosuz ağ cihazı –modem-, çevirmeli bağlantı, solocan ve zararlı yazılımlar, internet bankacılığı, şifre güvenliği, güvenli gezinme, otrum güvenliği, kişisel bilgilerin korunumu, aile bireyleri, e-posta güvenliğ, sohbet programları, kablosuz bağlantı güvenliği, paylaştırılmış dosya/klasör güvenliği) konularını kapsayan 87 ayrı bölüm ve toplam 50 dakikalık güvenlik eğitimi videolarından oluşan öğrenme içerikleri hazırlanmıştır. Konuları pekiştirmek için bilgi güvenliği ne demektir, Bilgi güvenliği neden bu kadar önemli, Bilgi güvenliğinde yanlış bilinenler, Bilgi güvenliği ve kullanıcı sorumluluğu, Kötü niyetli yazılım ne demektir, konu başlıklarında Articulate Persenter 13 ile sunu şeklinde öğrenme içerikleri hazırlanmıştır. Ayrıca Bilgi güvenliği ne demektir, Bilgi güvenliği neden bu kadar önemli, Bilgi güvenliğinde yanlış bilinenler, Bilgi güvenliği ve kullanıcı sorumluluğu, Kötü niyetli yazılım ne demektir, Diğer kötü niyetli yazılımlar, Bilgisayara giriş güvenliği, Casus yazılım:bulgu ve önlemler, Çocuklar için güvenli internet ve Sosyal

mühendislik saldırıları konu başlıklarıyla ilgili alanyazından derlenen bilgiler öğretim elemanlarına ders notu şeklinde hazırlanmıştır. Ayrıca, bu konularda daha detaylı bilgilerin sunulduğu diğer web sitelerinin bağlantı adresleri ders notlarının sonunda paylaşılmıştır.

3.3.2.4. Kullanılan Teknolojiler.

Öğrenme ortamları, çoklu ortam öğrenme materyalleri, anket ve web sitesi değerlendirme uygulaması geliştirilirken veri tabanının oluşturulması ile verilerin kaydedilmesi amacıyla MySQL veri tabanı, PHP programlama dili, elektronik anket uygulaması için LimeSurvey 2.05+, öğrenme ortamlarının oluşturulmasında Adobe Dreamweaver Sürüm.13, Articulate Presenter 13, Adobe Flash Professional CC, Microsoft Office Professional Plus 2010 ve web sitesinden verilerin alınmasında Dat.Net dilinden ve MS Excel uygulamasından faydalanılmıştır.

3.4.Bilgi Güvenliği Farkındalık Eğitimi Uygulama Aşaması

Araştırmanın ikinci aşaması için ADDIE öğretim tasarım modeli esaslarınca yetişkinlerin öğrenme ilkeleri gözetilerek tasarlanan Bilgi Güvenliği ve Farkındalık Web Sitesi ile ilgili alan uzmanlarının görüşleri alınarak web sitesi ve çoklu ortam materyallerine son şekli verilmiştir. Ön-test ile son-test arasında oluşabilecek iletme ya da aktarma etkisini ortadan kaldırmak için uygulamaya geçmeden önce üç aylık bir ara verilmiştir. Daha sonra Bilgi Güvenliği ve Farkındalık isimli web sitesi gönüllülük esasına göre belirlenmiş olan deney grubunun kullanımına açılmıştır. Deney grubunda bulunan öğretim elemanlarının akademik takvimlerinde planlı olan toplantı, seminer, idari görevler, akademik çalışmalardan kaynaklı zaman problemlerinden dolayı web sitesinin kullanıma açık kalma süresi 12 hafta boyunca devam etmiştir. Deney grubunda bulunan öğretim elemanlarına ihtiyaç durumunda araştırmacı tarafından web sitesi kullanımı hakkında bire bir eğitim verilmiş ve tasarlanan web sitesinden en üst seviyede yararlanmaları sağlanmıştır. Planlanan bu süre sonunda deney ve kontrol grubuna öntest olarak sunulan Bilgi Güvenliği Farkındalık Ölçeği sontest olarak tekrar uygulanmıştır. Ayrıca, deney grubunda bulunan öğretim elemanlarına Bilgi Güvenliği ve Farkındalık Web Sitesini değerlendirmeleri maksadıyla Bilgi Güvenliği ve Farkındalık Web Sitesi Değerlendirme Formu uygulanmıştır.

3.4.Verilerin Çözümlenmesi ve Yorumlanması

Elde edilen veriler, tanımlayıcı, karşılaştırmalı ve açıklayıcı istatistiksel yöntemler kullanılarak analiz edilmiş ve ilgili alanyazın çerçevesinde tartışılmıştır. Araştırmada, öğretim elemanlarına uygulanan veri toplama aracından elde edilen verilerin analizinde SPSS 17 (The Statistical Package for The Social Sciences) istatistik programı, LISREL 8.71 istatistik paket programı kullanılmıştır.

Araştırmanın ilk bölümünde, Bilgi Güvenliği Farkındalık Ölçeğini (BGFÖ) geliştirmek, elde edilen verileri çözümlemek için aşağıdaki istatistiksel çalışmalar gerçekleştirilmiştir. İlk aşamada alanyazın taraması ile 90 maddelik havuz oluşturulmuştur. Kapsam geçerliği için 23 uzmanın görüşüne sunulmuştur. Böylece ölçekten 23 madde elenmiş ve kapsam geçerliği sağlanmıştır. 67 maddeden oluşan ölçek öğretim elemanlarına uygulanmıştır. Ölçeğin geçerliğini belirlemek amacıyla faktör analizi yapılmıştır. Bu amaçla çalışma grubu büyüklüğünü ve elde edilen verilerin seçilen analiz için uygun ve yeterli olup olmadığını belirlemek için KMO testi, verilerin çok değişkenli normal dağılımdan gelip gelmediklerini belirlemek için Barlett küresellik testi yapılmıştır. Faktörlerin açıkladığı varyans değerine bakılmıştır. Varimax dik döndürme tekniği kullanılarak maddelerin faktörlere dağılımına bakılmıştır. Birden fazla faktörden yük alan maddelerin yer aldıkları faktörlerdeki yük farkları % 10'dan daha düşük olduğunda madde elemesine gidilmiştir. Faktörler ve içerdikleri maddeler tablolaştırılmıştır. Madde ayırt edicilik analizleri yapılarak çalışma grubunun alt ve üst %27'lik grupların aritmetik ortalamalarının anlamlılığı t-testi ile sınanmıştır. Daha sonra faktörler ve toplam puan için ayırt edicilik analizleri yapılarak alt ve üst % 27'lik grupların aritmetik ortalamalarının anlamlılığı t-testi ile sınanmıştır. Geçerlikle ilgili bu analizlerden sonra ölçek madelerinin (iç tutarlık) değerini belirlemek amacıyla (Cronbach Alpha) Güvenirlik Analizi yapılmıştır. Öte yandan, yarılamam (split half) yöntemi ile yapılan güvenirlik analizleri sonucu ölçeğin birinci yarısı ve ikinci yarısı için alpha katsayısı belirlenmiştir. Ölçeğin ayrıca yüksek bir güvenirliğe sahip olup olmadığına bakmak için Spearman Brown değeri ve Gutmann değeri hesaplanmıştır.

Araştırmanın ikinci bölümünde, deneysel desen ile elde edilen verilere ait tanımlayıcı bulgulara ilişkin istatistikler, aritmetik ortalama ($\overline{X}$), standart sapma (SS), frekans (f) ve yüzde (%) şeklinde gösterilmiştir. "Gruplardaki denek sayısı arttıkça kullanılan testin gücü ve güvenirliği artar. Gruplardaki denek sayısı fazla ise verilerin normal dağılıma uyma olasılığı artar, dolayısı ile parametrik test kullanma şansı artmış

olur. Gruplardaki denek sayısı az olduğunda ise (30'un altında) parametrik olmayan testler tercih edilmek zorunda kalınır. Veri dağılımının normal, varyansların eşit, birbirinden bağımsız ve rastgele seçilmiş olan deneklerin sayılarının 30'dan fazla olduğu durumlarda parametrik testler uygulanır" (Yılmaz, 2015; Öztuna ve Elhan, 2015). Bu varsayımdan dolayı, araştırmada parametrik istatistikler kullanılmıştır.

Demografik bilgiler ile bilgi güvenliği farkındalık düzeyi arasındaki ilişkinin belirlenmesi amacıyla bağımsız gruplar için t-testi (cinsiyet, unvan, mesleki kıdem, bilgisayar kullanım süresi, internet kullanım süresi) ve bağımsız gruplar için tek faktörlü varyans analizi – ANOVA testi- (cinsiyet, unvan, mesleki kıdem, bilgisayar kullanım süresi, internet kullanım süresi) yapılmıştır. Gerçekleştirilen deneysel işlemler sonunda deneysel işlemlerin gruplar üzerindeki etkisini belirlemek amacıyla ön test bilgi güvenliği farkındalık düzeyi puanları kontrol edilerek son test bilgi güvenliği farkındalık düzeyi puanları karşılaştırmıştır. Bu karşılaştırma işlemi için kovaryans analizi (ANCOVA) yapılmıştır. Veri analizinde anlamlılık düzeyi .05 olarak esas alınmış; .01 ve .001 düzeyinde anlamlı olanlar ayrıca belirtilmiştir.

İlişkisiz örneklemler t-testi, ilişkili örneklemler t-testi ve tek faktörlü varyans analizinin uygulanabilmesi için öncelikli olarak bu testin varsayımlarının karşılanıp karşılanmadığı kontrol edilmiştir. Bu analizin yapılabilmesi için bağımlı değişkene ait ölçüm değerlerinin en az aralık ölçeğinde olmasının yanı sıra bağımlı değişkene ilişkin ölçümlerin dağılımının her iki grupta da normal dağılım göstermesi şartı aranmaktadır. Normal dağılım özelliğinin incelenmesinde kullanılan yöntemlerden biri olarak kabul edilen çarpıklık ve basıklık katsayılarının sıfır (0) olması ölçümlerin aritmetik ortalama değerine göre tam simetrik dağılımını göstermektedir. Ancak, bu değerlerin ±1 değerleri arasında kalması da ölçümlerin normal dağılımdan önemli bir sapma göstermediği şeklinde yorumlanabilir (Büyüköztürk, 2011).

Ölçekteki sorulara verilen yanıtlar; kesinlikle katılıyorum: 5, katılıyorum: 4, kararsızım: 3, katılmıyorum: 2 ve hiç katılmıyorum: 1 şeklinde kodlanmıştır. Bilgi güvenliği farkındalık düzeyini belirlemek amacıyla yanıtlardaki toplam puanlar hesaplanmıştır. Yüksek puanlar, daha çok bilgi güvenliği farkındalığına sahip olunduğu; düşük puanlar daha az bilgi güvenliği farkındalığına sahip olduğu anlamına gelmektedir.

Öğretim elemanlarının açık uçlu sorulardan oluşan bilgi güvenliği ve farkındalık web sitesi değerlendirme formuna verdikleri yanıtlar içerik analizi ile çözümlenmiştir. Analiz sürecinde değerlendirme sorularını kapsayacak biçimde temalar

oluşturulmuştur. Temaların oluşturulması sürecinde, araştırmacı ve bir alan uzmanı, birbirlerinden bağımsız olarak değerlendirme metinlerinden temalar çıkartmışlar, daha sonra bir araya gelerek aralarında fikir birliğine varmış ve değerlendirme temalarına son şeklini vermişlerdir.

BÖLÜM 4

4.BULGULAR VE YORUM

Bu bölümde, araştırmanın alt problemlerinin çözümü için toplanan verilerin çeşitli istatistiksel analizler kullanılarak çözümlenmesi ile elde edilmiş olan bulgulara ve bu bulguların yorumlarına yer verilmiştir.

4.1.Araştırmanın II. Aşamasına Katılan Öğretim Elemanlarının Demografik Özelliklerine İlişkin Bulgu ve Yorumlar

Araştırmanın ikinci aşamasına katılan deney ve kontrol grupları öğretim elemanlarının demografik özellikleri; cinsiyet, unvan, mesleki kıdem, bilgisayar kullanım süresi, internet kullanım süresi, bilgisayar kullanım eğitim alma durumu, eğitim içerisinde bilgi güvenliği konu başlıklarının bulunma durumu, eğitimde sunulan bilgi güvenliği konu başlıklarının yeterliği değişkenleri açısından incelenmiş, elde edilen bulgular yorumlanarak aşağıda verilmiştir.

Araştırmaya katılan deney ve kontrol gruplarındaki öğretim elemanlarının cinsiyetlerine göre dağılımı Çizelge 12'de sunulmaktadır.

Çizelge 12

Deney ve Kontrol Grubu Öğretim Elemanlarının Cinsiyetlere Göre Dağılımı.

Cinsiyet	**Deney Grubu**		**Kontrol Grubu**		**Genel Toplam**	
	f	**%**	**f**	**%**	**f**	**%**
Erkek	18	58.06	21	61.76	39	60.00
Kadın	13	41.94	13	38.24	26	40.00
Genel Toplam	**31**	**100.00**	**34**	**100.00**	**65**	**100.00**

Çizelge 12'de de görüldüğü gibi araştırmadaki deney ve kontrol grubunu oluşturan öğretim elemanlarının (65 öğretim elemanı) cinsiyetlerine göre dağılımı incelendiğinde; çoğunun kadın öğretim elemanlarından ($f_{(Kadın)}$=39) oluştuğu söylenebilir. Diğer bir bulgu araştırmaya katılan öğretim elemanlarının cinsiyete göre deney ve kontrol gruplarına dağılımında oransal olarak tam anlamıyla olmasa da bir eşitliğin söz konusu olduğudur. Deney ve kontrol gruplarındaki kadın ve erkek öğretim

elemanları arasındaki oransal farklılığın nedeni deneysel çalışmanın yapıldığı Ankara Üniversitesi Eğitim Bilimleri Fakültesinde görev yapan öğretim elemanlarının daha çok kadın öğretim elemanından oluşuyor olmasındadır ($f_{(Kadın)}$=143, $f_{(Erkek)}$=78). Araştırmaya katılan öğretim elemanlarının deney ve kontrol gruplarına dağılımında cinsiyete göre bir eşitliğin olması ise yansızlık kuralına göre öğretim elemanlarının gruplara dağılımındaki tesadüfi bir sonuçtur.

Araştırmaya katılan deney ve kontrol gruplarındaki öğretim elemanlarının unvanlara göre dağılımı Çizelge 13'te sunulmaktadır.

Çizelge 13

Deney ve Kontrol Grubu Öğretim Elemanlarının Unvanlara Göre Dağılımı.

Unvan	**Deney Grubu**		**Kontrol Grubu**		**Genel Toplam**	
	f	**%**	**f**	**%**	**f**	**%**
Prof. Dr.	7	22.58	5	14.71	12	18.46
Doç. Dr.	3	9.68	2	5.88	5	7.69
Yrd. Doç. Dr.	1	3.23	6	17.65	7	10.77
Öğr. Grv.	2	6.45	3	8.82	5	7.69
Arş. Grv.	14	45.16	17	50.00	31	47.69
Diğer	4	12.90	1	2.94	5	7.69
Genel Toplam	**31**	**100.00.**	**34**	**100.00**	**65**	**100.00**

Çizelge 13'te de görüldüğü gibi araştırmadaki deney ve kontrol grubunu oluşturan öğretim elemanlarının (65 öğretim elemanı) unvanlarına göre dağılımı incelendiğinde; çoğunun yardımcı öğretim elemanından ($f_{(Yrd.Öğr.Elm.)}$=41) oluştuğu söylenebilir. Diğer bir bulgu da araştırmaya katılan öğretim elemanlarının unvanlarına göre deney ve kontrol gruplarına dağılımında oransal olarak tam anlamıyla olmasa da bir eşitliğin söz konusu olduğudur. Deney ve kontrol gruplarındaki öğretim üyesi ve yardımcı öğretim elemanları arasındaki oransal farklılığın nedeni deneysel çalışmanın yapıldığı Ankara Üniversitesi Eğitim Bilimleri Fakültesinde görev yapan öğretim elemanlarının daha fazla yardımcı öğretim elemanından oluşuyor olmasındadır ($f_{(Yrd.Öğr.Elm.)}$=132, $f_{(Öğr.Üyesi)}$=89). Araştırmaya katılan öğretim elemanlarının deney ve kontrol gruplarına dağılımında unvana göre bir eşitliğin olması ise yansızlık kuralına göre öğretim elemanlarının gruplara dağılımındaki tesadüfi bir sonuçtur.

Araştırmaya katılan deney ve kontrol gruplarındaki öğretim elemanlarının mesleki kıdemlerine göre dağılımı Çizelge 14'te sunulmaktadır.

Çizelge 14

Deney ve Kontrol Grubu Öğretim Elemanlarının Mesleki Kıdemlerine Göre Dağılımı.

Mesleki Kıdem	**Deney Grubu**		**Kontrol Grubu**		**Genel Toplam**	
	f	**%**	**f**	**%**	**f**	**%**
1-10 Yıl	13	41.94	20	58.82	33	50.77
11-20 Yıl	6	19.35	6	17.65	12	18.46
21-30 Yıl	8	25.81	6	17.65	14	21.54
31-40 Yıl	4	12.90	2	5.88	6	9.23
Genel Toplam	**31**	**100.00**	**34**	**100.00**	**65**	**100.00**

Çizelge 14'te de görüldüğü gibi araştırmadaki deney ve kontrol grubunu oluşturan öğretim elemanlarının (65 öğretim elemanı) mesleki kıdemlerine göre dağılımı incelendiğinde; yarıdan biraz fazlasının (%50,77) 1-10 yıllık mesleki kıdeme sahip öğretim elemanından ($f_{(1\text{-}10\ Yıllık.Öğr.Elm.)}$=33) oluştuğu, bunu %21,54 ile 21-30 yıllık mesleki kıdemli öğretim elemanlarının ($f_{(21\text{-}30\ Yıllık.Öğr.Elm.)}$=14) takip ettiği, bunu %18,46 ile 11-20 yıllık mesleki kıdemli öğretim elemanlarının ($f_{(11\text{-}20\ Yıllık.Öğr.Elm.)}$=12) takip ettiği, en düşük oranın %9,23 ile 31-40 yıllık meskeli kıdemli öğretim elemanlarından ($f_{(31\text{-}40\ Yıllık.Öğr.Elm.)}$=6) oluştuğu görülmektedir. Deney ve kontrol gruplarındaki öğretim elemanlarının mesleki kıdemleri arasındaki oransal farklılığın nedeni deneysel çalışmanın yapıldığı Ankara Üniversitesi Eğitim Bilimleri Fakültesinde görev yapan öğretim elemanlarının daha çok yardımcı öğretim elemanlarından oluşuyor olmasındadır ($f_{(Yrd.Öğr.Elm.)}$=132, $f_{(Öğr.Üyesi)}$=89). Araştırmaya katılan öğretim elemanlarının deney ve kontrol gruplarına dağılımında mesleki kıdeme göre bir eşitliğin olması ise yansızlık kuralına göre öğretim elemanlarının gruplara dağılımındaki tesadüfi bir sonuçtur.

Araştırmaya katılan deney ve kontrol gruplarındaki öğretim elemanlarının bilgisayar kullanım sürelerine göre dağılımı Çizelge 15'te sunulmaktadır.

Çizelge 15

Deney ve Kontrol Grubu Öğretim Elemanlarının Bilgisayar Kullanım Sürelerine Göre Dağılımı.

Bilgisayar Kullanımı	**Deney Grubu**		**Kontrol Grubu**		**Genel Toplam**	
	f	**%**	**f**	**%**	**f**	**%**
1-10 Yıl	2	6.45	6	17.65	8	12.31
11-20 Yıl	15	48.39	22	64.71	37	56.92
21-30 Yıl	14	45.16	6	17.65	20	30.77
Genel Toplam	**31**	**100.00**	**34**	**100.00**	**65**	**100.00**

Çizelge 15'te de görüldüğü gibi araştırmadaki deney ve kontrol grubunu oluşturan öğretim elemanlarının (65 öğretim elemanı) bilgisayar kullanım sürelerine göre dağılımı incelendiğinde; öğretim elemanlarının %57'sinin 11-20 yıl arası bilgisayar kullanan öğretim elemanından ($f_{(11\text{-}20\ Yıl.Öğr.Elm.)}$=37) oluştuğu, bunu %31 ile 21-30 yıl arası bilgisayar kullanan öğretim elemanlarının ($f_{(21\text{-}30\ Yıl.Öğr.Elm.)}$=20) takip ettiği, en düşük oranın %12,31 ile 1-10 yıl arası bilgisayar kullanan öğretim elemanlardan ($f_{(1\text{-}10Yıl.Öğr.Elm.)}$=8) oluştuğu görülmektedir. Öğretim elemanlarının mesleki kıdemleri göz önünde bulundurulduğunda, öğretim elemanlarının bilgisayar kullanım yaşının ilkokul dönemlerinde başladığı söylenebilir. Bunun sebebi olarak kişisel bilgisayarların son 30 yıl içerisinde insan hayatında daha fazla yer işgal ediyor olması gösterilebilir.

Araştırmaya katılan deney ve kontrol gruplarındaki öğretim elemanlarının internet kullanım sürelerine göre dağılımı Çizelge 16'da sunulmaktadır.

Çizelge 16

Deney ve Kontrol Grubu Öğretim Elemanlarının İnternet Kullanım Sürelerine Göre Dağılımı.

İnternet Kullanımı	**Deney Grubu**		**Kontrol Grubu**		**Genel Toplam**	
	f	**%**	**f**	**%**	**f**	**%**
1-10 Yıl	6	19.35	11	32.35	17	26.15
11-20 Yıl	23	74.19	21	61.76	44	67.69
21-30 Yıl	2	6.45	2	5.88	4	6.15
Genel Toplam	**31**	**100.00**	**34**	**100.00**	**65**	**100.00**

Çizelge 16'da da görüldüğü gibi araştırmadaki deney ve kontrol grubunu oluşturan öğretim elemanlarının (65 öğretim elemanı) internet kullanım sürelerine göre dağılımı incelendiğinde; araştırmaya katılan çalışma grubu öğretim elemanlarının %67,69'nun 11-20 yıl arası internet kullanan öğretim elemanından ($f_{(11\text{-}20\ Yıl.Öğr.Elm.)}$=44) oluştuğu, bunu %26,15 ile 1-10 yıl arası internet kullanan öğretim elemanlarının ($f_{(1\text{-}10\ Yıl.Öğr.Elm.)}$=17) takip ettiği, en düşük oranın %6,15 ile 21-30 yıl arası internet kullanan öğretim elemanlardan ($f_{(1\text{-}10Yıl.Öğr.Elm.)}$=8) oluştuğu görülmektedir. Öğretim elemanlarının mesleki kıdemleri göz önünde bulundurulduğunda, öğretim elemanlarının internet kullanım yaşının ilkokul dönemlerinde başladığı söylenebilir. Bunun sebebi gelişen

teknolojinin günlük hayatta internet kullanımını kolaylaştırması ve son yıllarda insan hayatında daha fazla yer işgal etmesi olarak ifade edilebilir.

Araştırmaya katılan deney ve kontrol gruplarındaki öğretim elemanlarının bilgisayar kullanımı eğitimi almalarına göre dağılımı Çizelge 17'de sunulmaktadır.

Çizelge 17

Deney ve Kontrol Grubu Öğretim Elemanlarının Bilgisayar Kullanımı Eğitimi Almalarına Göre Dağılımı.

Bilgisayar Eğitimi	**Deney Grubu**		**Kontrol Grubu**		**Genel Toplam**	
	f	**%**	**f**	**%**	**f**	**%**
Evet	19	63.33	23	65.71	42	64.62
Hayır	11	36.67	12	34.29	23	35.38
Genel Toplam	**30**	**100.00**	**35**	**100.00**	**65**	**100.00**

Çizelge 17'de de görüldüğü gibi araştırmadaki deney ve kontrol grubunu oluşturan öğretim elemanlarının (65 öğretim elemanı) bilgisayar kullanım eğitimi almalarına göre dağılımı incelendiğinde; araştırmaya katılan çalışma grubu öğretim elemanlarının 2/3'nin bilgisayar kullanım eğitimi alan öğretim elemanından ($f_{(Evet.Öğr.Elm.)}$=42), geriye kalan 1/3'lik kesimin ise bilgisayar kullanım eğitimi almayan öğretim elemanından ($f_{(Hayır.Öğr.Elm.)}$=23) oluştuğu görülmektedir.

Araştırmadaki deney ve kontrol grubunu oluşturan öğretim elemanlarının cinsiyet, unvan, mesleki kıdem, bilgisayar ve internet kullanım süresi ve bilgisayar eğitimi alma değişkenlerine göre incelenmesi sonucu iki grubunda birbirine benzer özellikler taşıdığı, gruplar arasındaki küçük farklılıkların yansız atamadan kaynaklandığı şeklinde yorumlanabilir.

4.2.Deney ve Kontrol Grubundaki Öğretim Elemanlarının Öntest Bilgi Güvenliği Farkındalık Düzeyi Puanlarına İlişkin Bulgu ve Yorumlar

Araştırmanın ikinci alt amacında, deney grubu ile kontrol grubundaki öğretim elemanlarının öntest bilgi güvenliği farkındalık düzeyi puanları arasında anlamlı bir fark olup olmadığı sorusuna yanıt aranmıştır. İlişkisiz örneklemler için t-testi, iki ilişkisiz örneklem ortalamaları arasındaki farkın manidar olup olmadığını test etmek için kullanılır.

Çalışma grubunda yer alan öğretim elemanlarının öntest toplam ölçüm değerlerine ilişkin aritmetik ortalama değerlerinde gözlenen değişimin istatistiksel olarak anlamlılığını test etmek amacıyla öncelikli olarak bağımlı değişkene ilişkin ölçüm değerleri arasındaki farkların normal dağılım gösterip göstermediği kontrol edilmiştir. Çizelge 18'de öntest ölçüm değerlerine ait betimsel istatistikler sunulmaktadır. Deney grubuna ait öntest ölçüm değerlerine ilişkin elde edilen çarpıklık (-0,481) ve basıklık (-0,995) katsayıları ile kontrol grubuna ait öntest ölçüm değerlerine ilişkin elde edilen çarpıklık (0.096) ve basıklık (-0,898) katsayıları incelendiğinde bu değerlerinin normal dağılım gösterdiğini söylemek mümkündür. Bu nedenle ortalama değerlerinin karşılaştırılmasında ilişkisiz örneklemler t-testi kullanılmıştır.

Çizelge 18

Deney ve Kontrol Grubu Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Ölçeği Öntest Ölçüm Değerlerine ait Betimleyici İstatistikler.

Betimleyici İstatistikler	**Deney Grubu**	**Kontrol Grubu**
N	31	34
Aritmetik Ortalama	121.97	108.53
Standart Sapma	33.40	21.54
Ortanca	123.06	108.59
Mod	129.00	104.00
En Düşük Toplam Ölçüm	53	67.00
En Yüksek Toplam Ölçüm	167	149.00
Dizi Genişliği (Ranj)	114	82.00
Çarpıklık	-0.481	0.096
Basıklık	-0.995	-0.898

Deney ve kontrol grubundaki öğretim elemanlarının öntest bilgi güvenliği farkındalık düzeyi puanlarına ait ilişkisiz örneklemler t-testi analizi sonuçları Çizelge 19'da sunulmaktadır.

Çizelge 19

Deney ve Kontrol Grubu Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Ölçeği Öntest Toplam Puanlarına ait İlişkisiz Örneklemeler T-Testi Analizi Sonuçları.

Gruplar	**N**	**$\bar{X}$**	**SS**	**Sd**	**t**	**p***
Deney Grubu	31	121.97	33,40	63	1.945	0.056
Kontrol Grubu	34	108.53	21,54			

p* ≤ .05 düzeyinde anlamlıdır.

Çizelge 19 incelendiğinde deney grubu öğretim elemanları bilgi güvenliği farkındalık ölçeği öntest toplam puanları ortalamasının $\overline{X}$=121.97, kontrol grubu öğretim elemanları bilgi güvenliği farkındalık ölçeği öntest toplam puanları ortalamasının ise $\overline{X}$=108.53 olduğu görülmektedir. Araştırmanın deneysel bölümüne katılan öğretim elemanlarının bilgi güvenliği farkındalık ölçeği öntest toplam puanları incelendiğinde de görüldüğü gibi, araştırma grupları arasında anlamlı bir farklılık bulunmamıştır [$t_{(63)}$=1.945, p<.05]. Başka bir anlatımla, öğretim elemanlarının deneysel işlem öncesi bilgi güvenliği farkındalık düzeyleri arasında anlamlı bir farklılık bulunmamıştır. Bu bulgu deney ve kontrol grubunu oluşturan öğretim elemanlarının birbirine denk olduğu şeklinde yorumlanabilir.

4.3. Deney Grubundaki Öğretim Elemanlarının Öntest Sontest Bilgi Güvenliği Farkındalık Düzeyi Puanlarına İlişkin Bulgu ve Yorumlar

Araştırmanın üçüncü alt amacında, geliştirilen web sitesini kullanan deney grubu öğretim elemanlarının öntest ve sontest bilgi güvenliği farkındalık ölçeği ile alt faktörleri toplam puanları arasında anlamlı bir fark olup olmadığı sorusuna yanıt aranmıştır.

Deney grubunda yer alan öğretim elemanlarının öntest sontest toplam ölçüm değerlerine ilişkin aritmetik ortalama değerlerinde gözlenen değişimin istatistiksel olarak anlamlılığını test etmek amacıyla öncelikli olarak bağımlı değişkene ilişkin ölçüm değerleri arasındaki farkların normal dağılım gösterip göstermediği kontrol edilmiştir. Çizelge 20'de öntest sontest ölçüm değerlerine ait betimsel istatistikler sunulmaktadır. Deney grubuna ait öntest ölçüm değerlerine ilişkin elde edilen çarpıklık (-0,481) ve basıklık (-0,995) katsayıları ile sontest ölçüm değerlerine ilişkin elde edilen çarpıklık (-0.952) ve basıklık (0.174) katsayıları incelendiğinde bu değerlerinin normal dağılım gösterdiğini söylemek mümkündür. Bu nedenle ortalama değerlerinin karşılaştırılmasında ilişkili örneklemler t-testi kullanılmıştır.

Çizelge 20

Deney Grubu Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Ölçeği Öntest Sontest Ölçüm Değerlerine ait Betimleyici İstatistikler.

Betimleyici İstatistikler	**Öntest**	**Sontest**
N	31	31
Aritmetik Ortalama	121.97	142.84
Standart Sapma	33.40	22.81
Ortanca	123.06	148.00
Mod	129.00	144.56
En Düşük Toplam Ölçüm	53	97
En Yüksek Toplam Ölçüm	167	170
Dizi Genişliği (Ranj)	114	73
Çarpıklık	-0.481	-0.952
Basıklık	-0.995	0.174

Geliştirilen web sitesini kullanan deney grubundaki öğretim elemanlarının öntest ve sontest bilgi güvenliği farkındalık düzeyi puanlarına ait ilişkili örneklemler t-testi analizi sonuçları Çizelge 21'de sunulmaktadır.

Çizelge 21

Deney Grubu Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Ölçeği Öntest ve Sontest Toplam Puanlarına ait İlişkili Örneklemeler T-Testi Analizi Sonuçları.

Ölçüm (BGFÖ)	**N**	$\bar{X}$	**SS**	**Sd**	**t**	**p***
Öntest	31	121.97	33.40	30	4.73	0.000
Sontest	31	142.84	22.81			

Çizelge 21'de de görüldüğü gibi geliştirilen web sitesini kullanan deney grubundaki öğretim elemanlarının öntest sontest bilgi güvenliği farkındalık düzeyi toplam puanlarında anlamlı bir artış olduğu bulunmuştur [$t_{(30)} = 4.73$, $p < .05$]. Deney grubundaki öğretim elemanlarının öntest bilgi güvenliği farkındalık düzeyi toplam puanları ortalaması uygulama öncesinde $\bar{X}$=121.97 iken, "Bilgi Güvenliği ve Farkındalık" web sitesiyle çalışma sonrası sontest bilgi güvenliği farkındalık düzeyi toplam puanları ortalaması $\bar{X}$=142.84'e çıkmıştır. Bu bulgu geliştirilen web sitesiyle çalışmanın bilgi güvenliği farkındalık düzeyini arttırmada önemli bir etkiye sahip olduğu şeklinde yorumlanabilir.

Geliştirilen web sitesini kullanan deney grubundaki öğretim elemanlarının "Saldırı ve Tehditler" alt faktörü öntest ve sontest toplam puanlarına ait ilişkili örneklemler t-testi analizi sonuçları Çizelge 22'de sunulmaktadır.

Çizelge 22

Deney Grubu Öğretim Elemanlarının "Saldırı ve Tehditler"Alt Faktörü Öntest ve Sontest Toplam Puanlarına ait İlişkili Örneklemeler T-Testi Analizi Sonuçları.

Ölçüm (Saldırı ve Tehditler)	**N**	$\overline{X}$	**SS**	**Sd**	**t**	**p***
Öntest	31	50.65	18.92	30	5.10	0.000
Sontest	31	63.00	15.25			

Çizelge 22'de de görüldüğü gibi geliştirilen web sitesini kullanan deney grubundaki öğretim elemanlarının saldırı ve tehditler alt faktörü öntest sontest farkındalık düzeyi toplam puanlarında anlamlı bir artış olduğu bulunmuştur [$t_{(30)} = 5.10$, $p < .05$]. Deney grubundaki öğretim elemanlarının saldırı ve tehditler alt faktörü öntest sontest farkındalık düzeyi toplam puanları ortalaması uygulama öncesinde $\overline{X}=50.65$ iken, "Bilgi Güvenliği ve Farkındalık" web sitesiyle çalışma sonrası sontest bilgi güvenliği farkındalık düzeyi toplam puanları ortalaması $\overline{X}=63.00$'e çıkmıştır. Bu bulgu geliştirilen web sitesiyle çalışmanın saldırı ve tehditler alt faktörü farkındalık düzeyi toplam puanlarını arttırmada önemli bir etkiye sahip olduğu şeklinde yorumlanabilir.

Geliştirilen web sitesini kullanan deney grubundaki öğretim elemanlarının "Kişisel Verilerin Korunması" alt faktörü öntest ve sontest toplam puanlarına ait ilişkili örneklemler t-testi analizi sonuçları Çizelge 23'te sunulmaktadır.

Çizelge 23

Deney Grubu Öğretim Elemanlarının "Kişisel Verilerin Korunması" Alt Faktörü Öntest ve Sontest Toplam Puanlarına ait İlişkili Örneklemeler T-Testi Analizi Sonuçları.

Ölçüm (Kişisel Verilerin Korunması)	**N**	$\overline{X}$	**SS**	**Sd**	**t**	**p***
Öntest	31	71.32	15.77	30	3.88	0.001
Sontest	31	79.84	8.37			

Çizelge 23'te de görüldüğü gibi geliştirilen web sitesini kullanan deney grubundaki öğretim elemanlarının kişisel verilerin korunması alt faktörü öntest sontest farkındalık düzeyi toplam puanlarında anlamlı bir artış olduğu bulunmuştur [$t_{(30)} = 3.88$, $p < .05$]. Deney grubundaki öğretim elemanlarının kişisel verilerin korunması alt faktörü öntest farkındalık düzeyi toplam puanları ortalaması uygulama öncesinde $\overline{X}=71.32$ iken, "Bilgi Güvenliği ve Farkındalık" web sitesiyle çalışma sonrası sontest farkındalık düzeyi toplam puanları ortalaması $\overline{X}=79.84$'e çıkmıştır. Bu bulgu geliştirilen web sitesiyle çalışmanın kişisel verilerin korunması alt faktörü farkındalık düzeyi toplam puanlarını arttırmada önemli bir etkiye sahip olduğu şeklinde yorumlanabilir.

4.4. Kontrol Grubundaki Öğretim Elemanlarının Öntest Sontest Bilgi Güvenliği Farkındalık Düzeyi Puanlarına İlişkin Bulgu ve Yorumlar

Araştırmanın dördüncü alt amacında, geliştirilen web sitesini kullanmayan kontrol grubu öğretim elemanlarının öntest ve sontest bilgi güvenliği farkındalık ölçeği ile alt faktörleri toplam puanları arasında anlamlı bir fark olup olmadığı sorusuna yanıt aranmıştır.

Kontrol grubunda yer alan öğretim elemanlarının öntest sontest toplam ölçüm değerlerine ilişkin aritmetik ortalama değerlerinde gözlenen değişimin istatistiksel olarak anlamlılığını test etmek amacıyla öncelikli olarak bağımlı değişkene ilişkin ölçüm değerleri arasındaki farkların normal dağılım gösterip göstermediği kontrol edilmiştir. Çizelge 24'te öntest sontest ölçüm değerlerine ait betimsel istatistikler sunulmaktadır. Kontrol grubuna ait öntest ölçüm değerlerine ilişkin elde edilen çarpıklık (0.096) ve basıklık (-0,898) katsayıları ile sontest ölçüm değerlerine ilişkin elde edilen çarpıklık (0.118) ve basıklık (-0.860) katsayıları incelendiğinde bu değerlerinin normal dağılım gösterdiğini söylemek mümkündür. Bu nedenle ortalama değerlerinin karşılaştırılmasında ilişkili örneklemler t-testi kullanılmıştır.

Çizelge 24

Kontrol Grubu Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Ölçeği Öntest Sontest Ölçüm Değerlerine ait Betimleyici İstatistikler.

Betimleyici İstatistikler	**Öntest**	**Sontest**
N	34	34
Aritmetik Ortalama	108.53	108.44
Standart Sapma	21.54	21.39
Ortanca	108.59	104.00
Mod	104.00	108.50
En Düşük Toplam Ölçüm	67.00	68.00
En Yüksek Toplam Ölçüm	149.00	149.00
Dizi Genişliği (Ranj)	82.00	81.00
Çarpıklık	0.096	0.118
Basıklık	-0.898	-0.860

Geliştirilen web sitesini kullanmayan kontrol grubundaki öğretim elemanlarının öntest ve sontest bilgi güvenliği farkındalık düzeyi puanlarına ait ilişkili örneklemler t-testi analizi sonuçları Çizelge 25'de sunulmaktadır

Çizelge 25

Kontrol Grubu Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Ölçeği Öntest ve Sontest Toplam Puanlarına ait İlişkili Örneklemeler T-Testi Analizi Sonuçları.

Ölçüm (BGFÖ)	**N**	$\overline{X}$	**SS**	**Sd**	**t**	**p***
Öntest	34	108.53	21.54	33	0.42	0.675
Sontest	34	108.44	21.39			

Çizelge 25'de de görüldüğü gibi geliştirilen web sitesini kullanmayan kontrol grubundaki öğretim elemanlarının öntest sontest bilgi güvenliği farkındalık düzeyi toplam puanlarında anlamlı bir artış olmadığı bulunmuştur [t(33) = 0.42, p> .05]. Kontrol grubundaki öğretim elemanlarının bilgi güvenliği farkındalık düzeyi toplam puanları ortalaması öntest uygulamasında $\overline{X}$=108.53 iken, sontest uygulaması sonrası $\overline{X}$=108.44 olduğu görülmektedir. Bu bulgu geliştirilen web sitesiyle çalışmayan kontrol grubunun bilgi güvenliği farkındalık düzeyinde bir değişiklik olmadığı şeklinde yorumlanabilir.

Geliştirilen web sitesini kullanmayan kontrol grubundaki öğretim elemanlarının "Saldırı ve Tehditler" alt faktörü öntest ve sontest toplam puanlarına ait ilişkili örneklemler t-testi analizi sonuçları Çizelge 26'da sunulmaktadır.

Çizelge 26

Kontrol Grubu Öğretim Elemanlarının "Saldırı ve Tehditler" Alt Faktörü Öntest ve Sontest Toplam Puanlarına ait İlişkili Örneklemeler T-Testi Analizi Sonuçları.

Ölçüm (Saldırı ve Tehditler)	**N**	$\overline{X}$	**SS**	**Sd**	**t**	**p***
Öntest	34	41.24	12.15	33	0.15	0.881
Sontest	34	41.21	12.10			

Çizelge 26'da da görüldüğü gibi geliştirilen web sitesini kullanmayan kontrol grubundaki öğretim elemanlarının saldırı ve tehditler alt faktörü öntest sontest farkındalık düzeyi toplam puanlarında anlamlı bir artış olmadığı bulunmuştur [t(33) = 0.15, p> .05]. Kontrol grubundaki öğretim elemanlarının saldırı ve tehditler alt faktörü farkındalık düzeyi toplam puanları ortalamasının öntest uygulaması öncesinde $\overline{X}$=41.24 iken, sontest uygulaması sonrası farkındalık düzeyi toplam puanları ortalamasının $\overline{X}$=41.21 olduğu görülmektedir. Bu bulgu geliştirilen web sitesiyle çalışmayan kontrol grubunun saldırı ve tehditler alt faktörü farkındalık düzeyinde bir değişiklik olmadığı şeklinde yorumlanabilir.

Geliştirilen web sitesini kullanan kontrol grubundaki öğretim elemanlarının "Kişisel Verilerin Korunması" alt faktörü öntest ve sontest toplam puanlarına ait ilişkili örneklemler t-testi analizi sonuçları Çizelge 27'de sunulmaktadır.

Çizelge 27

Kontrol Grubu Öğretim Elemanlarının "Kişisel Verilerin Korunması" Alt Faktörü Öntest ve Sontest Toplam Puanlarına ait İlişkili Örneklemeler T-Testi Analizi Sonuçları.

Ölçüm (Kişisel Verilerin Korunması)	**N**	$\overline{X}$	**SS**	**Sd**	**t**	**p***
Öntest	34	67.29	10.13	33	0.36	0.721
Sontest	34	67.24	9.97			

Çizelge 27'de de görüldüğü gibi geliştirilen web sitesini kullanmayan kontrol grubundaki öğretim elemanlarının kişisel verilerin korunması alt faktörü öntest sontest farkındalık düzeyi toplam puanlarında anlamlı bir artış olmadığı bulunmuştur [t(33) = 0.36, p> .05]. Kontrol grubundaki öğretim elemanlarının kişisel verilerin korunması alt faktörü farkındalık düzeyi toplam puanları ortalamasının öntest uygulaması öncesinde $\overline{X}$=67.29 iken, sontest uygulaması sonrası farkındalık düzeyi toplam puanları

ortalamasının $\overline{X}$=67.24 olduğu görülmektedir. Bu bulgu geliştirilen web sitesiyle çalışmayan kontrol grubunun saldırı ve tehditler alt faktörü farkındalık düzeyinde bir değişiklik olmadığı şeklinde yorumlanabilir.

4.5.Deney ve Kontrol Grubu Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Ölçeği Öntest Puanları Kontrol Edildiğinde Sontest Bilgi Güvenliği Farkındalık Düzeyi Puanlarına İlişkin Bulgu ve Yorumlar

Araştırmanın beşinci alt amacında, geliştirilen web sitesini kullanan deney grubu öğretim elemanları ile siteyi kullanmayan kontrol grubu öğretim elemanlarının bilgi güvenliği farkındalık ölçeği öntest puanları kontrol edildiğinde, düzeltilmiş sontest puan ortalamaları arasında anlamlı fark bir fark olup olmadığı sorusuna yanıt aranmıştır.

Geliştirilen web sitesini kullanan deney grubu öğretim elemanları ile siteyi kullanmayan kontrol grubu öğretim elemanlarının bilgi güvenliği farkındalık ölçeği ve alt faktörleri öntest puanları kontrol edildiğinde, düzeltilmiş sontest puan ortalamaları ait kovaryans analizi kullanılarak test edilmiştir. Grupların son test başarı puanlarına ilişkin aritmetik ortalama ($\overline{X}$), standart sapma değerleri (SS) ile kovaryans analizi sonucunda hesaplanan ve çoklu karşılaştırma testinde temel alınan son test düzeltilmiş ortalama puanları ($\overline{X}$), Çizelge 28'de sunulmaktadır.

Çizelge 28

Deney ve Kontrol Grubu Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Ölçeği Öntest Toplam Puanları Kontrol Altına Alındığında Sontest Toplam Puanlarına ait Aritmetik Ortalama, Standart Sapma Değerleri ile Son Test Düzeltilmiş Ortalamaları.

Ölçüm (BGFÖ)	**N**	**Son Test BGFÖ Puanı**		**Düzeltilmiş Son Test BGFÖ Puanı**	
		$\overline{X}$	**SS**	**$\overline{X}$**	**SH**
Deney Grubu	31	142.84	22.81	139.57	2.17
Kontrol Grubu	34	108.85	21.39	114.79	2.11

Çizelge 28'de de görüldüğü gibi deney grubunda bulunan öğretim elemanlarının bilgi güvenliği farkındalık ölçeği ön test bilgi güvenliği farkındalık düzeyi toplam puanları kontrol altına alındığında, son test bilgi güvenliği farkındalık düzeyi toplam puanlarının aritmetik ortalaması $\overline{X}$=142.84, düzeltilmiş ortalaması ise $\overline{X}$=139.57'dir.

Kontrol grubunda bulunan öğretim elemanlarının bilgi güvenliği farkındalık ölçeği ön test bilgi güvenliği farkındalık düzeyi toplam puanları kontrol altına alındığında, son test bilgi güvenliği farkındalık düzeyi toplam puanlarının aritmetik ortalaması $\overline{X}$=108.85, düzeltilmiş ortalaması ise $\overline{X}$=114.79'dur. Grupların son test bilgi güvenliği farkındalık düzeyi toplam puanları arasında görülen bu farkın anlamlı olup olmadığını test etmek için kovaryans analizi yapılmış ve elde edilen sonuçlar Çizelge 29'da sunulmaktadır.

Çizelge 29

Deney ve Kontrol Grubu Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Ölçeği Öntest Toplam Puanları Kontrol Altına Alındığında Sontest Toplam Puanlarına ait Kovaryans Analizi Sonuçları.

Varyansın Kaynağı	**Kareler Toplamı**	**Serbestlik Derecesi (sd)**	**Kareler Ortalaması**	**F**	**Anlamlılık Düzeyi (p)**
Kovaryans Değişimi (Öntest)	5736.572	1	5736.572	41.24	.000
Gruplama Ana etkisi	2934.336	1	2934.336	21.10	.000
Hata	8484.376	61	139.088		
Toplam	49886.462	64			

Öntest bilgi güvenliği farkındalık düzeyi ortalama puanları kontrol altına alınıp, grupların düzeltilmiş sontest bilgi güvenliği farkındalık düzeyi ortalama puanları açısından gruplama ana etkisinin anlamlı olup olmadığını belirlemek amacıyla Çizelge 29'daki p değerine bakıldığında bu değerin .05'ten küçük olduğu görülmektedir. Buna bağlı olarak çalışma gruplarının ön test puanları kontrol altına alındığında, grupların son test düzeltilmiş ortalama puanları açısından gruplama ana etkisinin anlamlı olduğu görülmektedir [F(1,61): 21.10; p= .000 < .05]. Bir başka deyişle, "Bilgi Güvenliği ve Farkındalık" isimli web sitesini kullanan deney grubundaki öğretim elemanlarının ($\overline{X}$=139.57), tasarlanan web sitesini kullanmayan kontrol grubu öğretim elemanlarının ($\overline{X}$=114.79) düzeltilmiş sontest bilgi güvenliği farkındalık düzeyi ortalama puanlarına göre daha yüksek olduğu anlaşılmaktadır.

4.6.Deney ve Kontrol Grubundaki Öğretim Elemanlarının Sontest Bilgi Güvenliği Farkındalık Düzeyi Puanlarının Çeşitli Değişkenlere Göre Farklılaşma Durumuna İlişkin Bulgu ve Yorumlar

Araştırmanın altıncı alt amacında, deney ve kontrol gruplarındaki öğretim elemanlarının sontest bilgi güvenliği farkındalık düzeyi puanları arasında

- Çalışma Grubu (Deney, Kontrol grubu)
- Cinsiyet (Kadın, Erkek)
- Unvan (Öğretim Üyesi, Yardımcı Öğretim Elemanı)
- Bilgisayar kullanım süresi (1-10 Yıl, 11-20 Yıl, 21-30 Yıl)

bağımsız değişkenlerine göre anlamlı bir fark olup olmadığı sorusuna yanıt aranmıştır.

Çalışma grubunda yer alan öğretim elemanlarının sontest toplam ölçüm değerlerine ilişkin aritmetik ortalama değerlerinde gözlenen değişimin istatistiksel olarak anlamlılığını test etmek amacıyla öncelikli olarak bağımlı değişkene ilişkin ölçüm değerleri arasındaki farkların normal dağılım gösterip göstermediği kontrol edilmiştir. Çizelge 30'da sontest ölçüm değerlerine ait betimsel istatistikler sunulmaktadır. Deney grubuna ait sontest ölçüm değerlerine ilişkin elde edilen çarpıklık (-0,952) ve basıklık (0.174) katsayıları ile kontrol grubuna ait sontest ölçüm değerlerine ilişkin elde edilen çarpıklık (0.118) ve basıklık (-0,860) katsayıları incelendiğinde bu değerlerinin normal dağılım gösterdiğini söylemek mümkündür. Bu nedenle ortalama değerlerinin karşılaştırılmasında ilişkisiz örneklemler t-testi ve ilişkisiz örneklemler için tek faktörlü varyans analizi (ANOVA) kullanılmıştır.

Çizelge 30

Deney ve Kontrol Grubu Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Ölçeği Sontest Ölçüm Değerlerine ait Betimleyici İstatistikler.

Betimleyici İstatistikler	Deney Grubu	Kontrol Grubu
N	31	34
Aritmetik Ortalama	142.84	108.44
Standart Sapma	22.81	21.39
Ortanca	148.00	104.00
Mod	144.56	108.50
En Düşük Toplam Ölçüm	97	68.00
En Yüksek Toplam Ölçüm	170	149.00
Dizi Genişliği (Ranj)	73	81.00
Çarpıklık	-0.952	0.118
Basıklık	0.174	-0.860

4.6.1. Çalışma Grubu (Deney, Kontrol grubu)

Araştırmanın altıncı alt amacında, deney grubu ile kontrol grubundaki öğretim elemanlarının sontest bilgi güvenliği farkındalık düzeyi puanları arasında çalışma grubuna (Deney ve Kontrol Grubu) göre anlamlı bir fark olup olmadığı sorusuna yanıt aranmıştır.

Deney ve kontrol grubundaki öğretim elemanlarının sontest bilgi güvenliği farkındalık düzeyi puanlarına ait ilişkisiz örneklemler t-testi analizi sonuçları Çizelge 31'de sunulmaktadır.

Çizelge 31

Deney ve Kontrol Grubu Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Ölçeği Sontest Toplam Puanlarına ait İlişkisiz Örneklemeler T-Testi Analizi Sonuçları.

Gruplar	**N**	**$\overline{X}$**	**SS**	**Sd**	**t**	**p***
Deney Grubu	31	142.84	22.81	63	6.28	0.000
Kontrol Grubu	34	108.44	21.39			

Çizelge 31 incelendiğinde deney grubu öğretim elemanları bilgi güvenliği farkındalık ölçeği sontest toplam puanları ortalamasının $\overline{X}$=142.84, kontrol grubu öğretim elemanları bilgi güvenliği farkındalık ölçeği sontest toplam puanları ortalaması ise $\overline{X}$=108.44 olduğu görülmektedir. Araştırmaya katılan öğretim elemanlarının bilgi güvenliği farkındalık ölçeği sontest toplam puanları incelendiğinde araştırma grupları arasında deney grubu lehinde anlamlı bir farklılık olduğu görülmektedir [$t_{(63)}$=6.28, p<.01]. Bu bulgu, bilgi güvenliği farkındalık düzeyi ile tasarlanan web sitesini kullanan deney grubu arasında anlamlı bir ilişkinin olduğu şeklinde de yorumlanabilir. Hesaplanan eta-kare korelasyon katsayısı değeri 0,39'dur. Buna göre bilgi güvenliği farkındalık düzeyi puanlarında gözlenen varyansın yaklaşık %39'unun gruba bağlı olduğu şeklinde ifade edilebilir. Etki büyüklüğü olarak da isimlendirilen eta-kare korelasyon katsayısı, bağımsız değişkenin ya da faktörün bağımlı değişkendeki toplam varyansın ne kadarını açıkladığını gösterir ve 0 ile 1 arasında değişir. 0,01 "küçük", 0,06 "orta" ve 0,14 "geniş" etki büyüklüğü olarak yorumlanır. Cohen standardize edilmiş etki büyüklüğü indeksi olan d değeri karşılaştırılan ortalamaların birbirinden kaç standart sapma uzaklaştığını yorumlama imkânı verir. Cohen d değeri -∞ ile +∞

arasında değer alabilir. Buna göre hesaplanan Cohen d değeri 1,56'dır. Bu sonuçta deney ve kontrol grubu öğretim elemanlarının bilgi güvenliği farkındalık ölçeği sontest toplam puanları arasındaki farkın 1,56 standart sapma kadar olduğunu gösterir.

4.6.2. Cinsiyet (Kadın, Erkek)

Araştırmanın altıncı alt amacında, deney grubu ile kontrol grubundaki öğretim elemanlarının sontest bilgi güvenliği farkındalık düzeyi puanları arasında cinsiyete (Kadın ve Erkek) göre anlamlı bir fark olup olmadığı sorusuna yanıt aranmıştır.

Deney ve kontrol grubundaki öğretim elemanlarının cinsiyete göre sontest bilgi güvenliği farkındalık düzeyi puanlarına ait ilişkisiz örneklemler t-testi analizi sonuçları Çizelge 32'de sunulmaktadır.

Çizelge 32

Deney ve Kontrol Grubu Öğretim Elemanlarının Cinsiyete Göre Bilgi Güvenliği Farkındalık Ölçeği Sontest Toplam Puanlarına ait İlişkisiz Örneklemeler T-Testi Analizi Sonuçları.

Gruplar	**N**	**$\overline{X}$**	**SS**	**Sd**	**t**	**p***
Erkek	26	131.00	28.23	63	1.46	0.148
Kadın	39	120.74	27.30			

Çizelge 32 incelendiğinde erkek öğretim elemanları bilgi güvenliği farkındalık ölçeği sontest toplam puanları ortalamasının $\overline{X}$=131.00, kadın öğretim elemanları bilgi güvenliği farkındalık ölçeği sontest toplam puanları ortalamasının ise $\overline{X}$==120.74 olduğu görülmektedir. Araştırmaya katılan öğretim elemanlarının bilgi güvenliği farkındalık ölçeği sontest toplam puanları incelendiğinde cinsiyete göre anlamlı bir farklılık bulunmadığı görülmektedir [$t_{(63)}$=1.44, p>.05].

4.6.3. Unvan (Öğretim Üyesi, Yardımcı Öğretim Elemanı)

Araştırmanın altıncı alt amacında, deney grubu ile kontrol grubundaki öğretim elemanlarının sontest bilgi güvenliği farkındalık düzeyi puanları arasında unvana (Öğretim üyesi ve Yardımcı Öğretim Elemanı) göre anlamlı bir fark olup olmadığı sorusuna yanıt aranmıştır.

Deney ve kontrol grubundaki öğretim elemanlarının unvana sontest bilgi güvenliği farkındalık düzeyi puanlarına ait ilişkisiz örneklemler t-testi analizi sonuçları Çizelge 33'te sunulmaktadır.

Çizelge 33

Deney ve Kontrol Grubu Öğretim Elemanlarının Unvanlara Göre Bilgi Güvenliği Farkındalık Ölçeği Sontest Toplam Puanlarına ait İlişkisiz Örneklemeler T-Testi Analizi Sonuçları.

Gruplar	**N**	**$\overline{X}$**	**SS**	**Sd**	**t**	**p***
Öğretim Üyesi	24	118,38	26,44	63	1.44	0.154
Yardımcı Öğretim Elemanı	41	128,63	28,38			

Çizelge 33'te de görüldüğü gibi öğretim üyesi unvanlı öğretim elemanları bilgi güvenliği farkındalık ölçeği sontest toplam puanları ortalamasının $\overline{X}$=118.38, yardımcı öğretim elemanı unvanlı öğretim elemanları bilgi güvenliği farkındalık ölçeği sontest toplam puanları ortalamasının ise $\overline{X}$=128.63 olduğu görülmektedir. Araştırmaya katılan öğretim elemanlarının bilgi güvenliği farkındalık ölçeği sontest toplam puanları incelendiğinde unvanlara göre anlamlı bir farklılık bulunmadığı görülmektedir [$t_{(63)}$=1.44, p>.05].

4.6.4. Bilgisayar kullanım süresi (1-10 Yıl, 11-20 Yıl, 21-30 Yıl)

Araştırmanın altıncı alt amacında, deney grubu ile kontrol grubundaki öğretim elemanlarının sontest bilgi güvenliği farkındalık düzeyi puanları arasında bilgisayar kullanım süresi (1-10 Yıl, 11-20 Yıl ve 21-30 Yıl) göre anlamlı bir fark olup olmadığı sorusuna yanıt aranmıştır.

Deney ve kontrol grubundaki öğretim elemanlarının bilgisayar kullanım süresine göre sontest bilgi güvenliği farkındalık düzeyi puanlarına ait betimsel istatistikler Çizelge 34'de, ilişkisiz örneklemler için tek faktörlü varyans analizi sonuçları Çizelge 35'de sunulmaktadır.

Çizelge 34

Deney ve Kontrol Grubu Öğretim Elemanlarının Bilgisayar Kullanım Süresine Göre Bilgi Güvenliği Farkındalık Ölçeği Sontest Toplam Puanlarına ait Betimsel İstatistik Sonuçları.

Bilgisayar Kullanım Süresi	**N**	**$\bar{X}$**	**SS**
1-10 Yıl	8	114,25	31,68
11-20 Yıl	38	123,00	26,38
21-30 Yıl	19	133,00	28,70

Çizelge 35

Deney ve Kontrol Grubu Öğretim Elemanlarının Bilgisayar Kullanım Süresine Göre Bilgi Güvenliği Farkındalık Ölçeği Sontest Toplam Puanlarına ait İlişkisiz Örneklemeler İçin Tek Faktörlü Varyans Analizi Sonuçları.

Varyansın Kaynağı	**Kareler Toplamı**	**Serbestlik Derecesi (sd)**	**Kareler Ortalaması**	**F**	**Anlamlılık Düzeyi (p)**
Gruplararası	2290.962	2	1145.481	1.492	0.223
Gruplariçi	47595.500	62	767.669		
Toplam	49886.462	64			

Çizelge 34 ve Çizelge 35 incelendiğinde öğretim elemanlarının bilgi güvenliği farkındalık düzeyleri arasında bilgisayar kullanım süresine göre anlamlı bir fark olmadığı görülmektedir [$F(2,62)=1.49$, $p>.05$] Başka bir ifadeyle, deney ve kontrol grubu öğretim elemanlarının bilgi güvenliği farkındalık ölçeği sontest puanları bilgisayar kullanım süresine göre değişmemektedir. Her ne kadar bilgisayar kullanım süresi artıkça farkındalık düzeyinin artması gerektiği düşünülse de, bilgisayar kullanım süresi açısından bir farklılık bulunmamıştır. 1990 yılı başından itibaren fakültedeki akademik personele masa üstü bilgisayar verilmiştir. Daha sonra 2000 yılların başında laptop ve 2010 yılından itibaren tablet verilmiştir. Ayrıca akademik personel, donanım açısından desteklenmiş ve bilgisayar okur-yazarlığı ve günlük kullanım sürelerindeki artış, yıllara bağlı bir farklılık oluşturmamış ve elde edilen bulgular bu beklentiyi doğrulamamıştır.

4.7.Deney Grubundaki Öğretim Elemanlarının Geliştirilen Web Sitesine Yönelik Görüşlerine İlişkin Bulgu ve Yorumlar

Araştırmanın yedinci alt amacında, deney grubundaki öğretim elemanlarının geliştirilen web sitesine yönelik görüşlerinin ne olduğu sorusuna yanıt aranmıştır. Deney grubundaki öğretim elemanların "Bilgi Güvenliği ve Farkındalık" web sitesine ilişkin görüşleri elektronik ortamda açık uçlu görüş formu kullanılarak toplanmıştır. Görüş formu kullanılarak elde edilen veriler içerik analizi yöntemiyle incelenmiştir. İçerik analizi sonucunda elde edilen görüşlerin dağılımı frekans (f) şeklinde ifade edilerek, öğretim elemanlarının görüşlerinden örnekler verilmiştir.

4.7.1. "Bilgi Güvenliği ve Farkındalık" Web Sitesinin Faydalı Olduğu ve Katkı Sağladığına İlişkin Bulgu ve Yorumlar

Deney grubu öğretim elemanlarının bilgi güvenliği farkındalığı ile ilgili tasarlanmış olan çoklu ortam materyalleri ile web sitesinin kullanımına yönelik belirtmiş oldukları görüşlere ilişkin içerik analizi yapılmıştır. İçerik analizi sonucu ortaya çıkan alt temalar Çizelge 36'da sunulmaktadır.

Çizelge 36

Deney Grubunda Yer Alan Öğretim Elemanlarının Tasarlanmış Olan Çoklu Ortam Materyalleri ile Web Sitesine İlişkin Görüşleri.

Alt Temalar	**f**
Evet	15
Diğer	6
Oldukça/Çok/Kesinlikle	4
Kısmen	2

Çizelge 36'da da görüldüğü gibi deney grubundaki öğretim elemanlarının tasarlanmış olan çoklu ortam materyalleri ile web sitesinin kullanımını faydalı bulduğu ve katkı sağladığı sorusuna en çok "Evet" (f=15) şeklinde olumlu görüş belirtirken bunu sırasıyla, "Oldukça/Çok/Kesinlikle" (f=4) ve "Kısmen" (f=2) olumlu alt teması takip etmektedir. Deney grubundaki öğretim elemanlarının bu konuya ilişkin görüş ve değerlendirmelerinden bazıları şu şekildedir:

"Evet.. İçerikleri oldukça güzel ve faydalı. Daha önce Bilgi güvenliği ile bir materyali inceleme fırsatım olmamıştı. Oldukça yararlı bulduğumu söylemek isterim."

"Evet detaylı kesinlikle detaylı olarak bilgi edinmemi sağladı."

"evet.. videolar gayet etkili ve önemli noktalara değinerek hazırlanmış."

"Evet. Tüm boyutlar farklı seviyelerdeki bilgi sahiplerine yönelik bulunabiliyor. Uygulamaya yönelik içerik olması faydalı."

"iyi tasarım"

"Genel bilgilendirme açısından faydalı buluyorum"

"Alanım gereği, daha önceden bildiğim bilgiler vardı. Bir iki noktada bilmediğim konular vardı, öğrenmiş oldum. Bu site halka açılırsa (tez çalışması bittiğinde) öğrencilerime de kaynak olarak göstermek isterim."

"Çok yararlı bir sayfa. Tavşan kavramını ilk kez duydum. Bilgisayarımızda neler yapılabileceğini öğrendim."

"Bilgi güvenliği farkındalığı ile ilgili tasarlanmış olan çoklu ortam materyalleri ile web sitesinin titizlikle hazırlandığını düşünmekle ve bu siteyi çok beğenmekle birlikte, bazı hususların bana çok teknik geldiğini belirtmeliyim. Belki de siteyi incelemek için daha fazla zaman harcamak ve anlamadığım konularda bir uzmana danışmak benim açımdan sitenin anlaşılabilirliğini artıracaktır. Hazırlayanları kutluyorum."

"Oldukça faydalı buldum. Bilgi güvenliği ne yazık ki yakından takip etmediğimiz bir konu. Buna bahane oluşturabilecek çok sayıda gerekçeyi ortaya sürmek için ayırdığımız zamanı bilgi güvenliği konusunda önlem almak için ayırmıyoruz ne yazık ki."

Genel olarak değerlendirildiğinde ise "Bilgi Güvenliği ve Farkındalık" web sitesinin kullanımının faydalı olduğu ve katkı sağladığı, ayrıca genel bilgilendirme ve farkındalık yarattığı sonucuna varılmaktadır.

4.7.2. "Bilgi Güvenliği ve Farkındalık" Web Sitesinin Kullanımında Yaşanan Zorluklara İlişkin Bulgu ve Yorumlar

Deney grubu öğretim elemanlarının bilgi güvenliği farkındalığı ile ilgili tasarlanmış olan çoklu ortam materyalleri ile web sitesinin kullanımında ne tür zorluklar yaşadıklarına yönelik belirtmiş oldukları görüşlere ilişkin içerik analizi yapılmıştır. İçerik analizi sonucu ortaya çıkan alt temalar Çizelge 37'de sunulmaktadır.

Çizelge 37

Deney Grubunda Yer Alan Öğretim Elemanlarının Tasarlanmış Olan Çoklu ortam Materyalleri ile Web Sitesi Kullanımına İlişkin Görüşleri.

Alt Temalar	**f**
Herhangi bir zorluk/sıkıntı/sorun yaşamadım/karşılaşmadım	18
Diğer	4
Genel tasarım	3
Video tasarım	2

Çizelge 37 incelendiğinde deney grubundaki öğretim elemanlarının tasarlanmış olan çoklu ortam materyalleri ile web sitesinin kullanımına ilişkin ne tür zorluklar yaşandı sorusuna en çok "Herhangi bir zorluk/sıkıntı/sorun yaşamadım/karşılaşmadım" (f=18) şeklinde olumlu görüş belirtirken bunu sırasıyla, "Genel tasarım" (f=3) ve "Video tasarım" (f=2) konusunda tavsiyeleri içeren temalar takip etmektedir. Deney grubundaki öğretim elemanlarının bu konuya ilişkin görüş ve değerlendirmelerinden bazıları şu şekildedir:

"kullanımı kolay"

"Herhangi bir zorlukla karşılaşmadım"

"Bilgi güvenliği kaynak bankası gibi aslında. Birden fazla amaç için kullanılabilirim. Kullanımı kolay."

"Açıkçası tıklayabileceğim bir yer aradım öncelikle. sonrasında kullanım bilgilerini gördüm."

"Herhangi bir zorluk yaşamadım. Her şey çok ince düşünülmüş."

"Herhangi bir zorluk yaşamadım. Sadece ilk defa giriş yaptığımda henüz kılavuzu okumadığım için siteye nasıl ulaşacağımı bulamamıştım."

"Herhangi bir zorluk yaşamadım. site gayet sade bir dille hazırlanmış ve gereksiz dikkat dağıtıcı materyallerden kaçınılmış."

"Her hangi bir sıkıntı yaşamadım. Gayet kullanışlı ve açık."

"Web sitesinin kullanımında herhangi bir zorlukla karşılaşmadım."

"Yönlendirmelerde hiç bir eksik ya da anlaşılmayan bölüm göremedim o nedenle bariz bir zorluk yaşamadım."

Geliştirilen çoklu ortam materyalleri ve web sitesinin tasarımında konu başlıklarının detaylı olması ve videoların bu bakış açısıyla tasarlanması, süre olarak videoların 50 dakika uzunluğunda olması bazı kullanıcılar tarafında eleştiri konusu olarak ifade edilmiştir. Deney grubundaki öğretim elemanlarının değerlendirmelerinden bazıları şu şekildedir:

"Zaman alıcı"

"İşlemlerin karmaşıklığı beni çoğu zaman yoruyor"

"Tek tek dosyaları açmak biraz zordu. Bütünlüklü tek bir sunum ve film yapılabilir."

Genel olarak değerlendirildiğinde ise "Bilgi Güvenliği ve Farkındalık" web sitesinin kullanımında herhangi bir zorluk yaşanmadığı sonucuna varılmaktadır. Genel tasarım ve video tasarımı konularındaki eleştiri konuları web sitesinin iyileştirilmesinde öneri olarak değerlendirilecektir.

4.7.3. "Bilgi Güvenliği ve Farkındalık" Web Sitesinin Desteklenmesi Gereken Alt Konulara İlişkin Bulgu ve Yorumlar

Deney grubu öğretim elemanlarının bilgi güvenliği farkındalığı ile ilgili tasarlanmış olan çoklu ortam materyalleri ile web sitesi hangi tür alt konularla desteklenmelidir sorusuna yönelik belirtmiş oldukları görüşlere ilişkin içerik analizi yapılmıştır. İçerik analizi sonucu ortaya çıkan alt temalar Çizelge 38'de sunulmaktadır.

Çizelge 38

Deney Grubunda Yer Alan Öğretim Elemanlarının Tasarlanmış Olan Çoklu Ortam Materyalleri ile Web Sitesi Hangi Tür Alt Konularla Desteklenmesine İlişkin Görüşleri.

Alt Temalar	**f**
İçerik Yeterli/İhtiyaç Yok	9
Diğer	6
Fikrim Yok	4
Konular sunu/seslendirme/video/yaşanmış örnekler ile desteklenmeli	4
Mobil Cihazlar/Siber Saldırı Türleri/Güvenli Alış-Veriş	3
Bilgisayar ve İletişim Teknolojileri Kullanımında Etik	1

Çizelge 38 incelendiğinde deney grubundaki öğretim elemanlarının tasarlanmış olan çoklu ortam materyalleri ile web sitesinin hangi tür alt konularla desteklenmeli sorusuna en çok "İçerik Yeterli/İhtiyaç Yok" (f=9) şeklinde olumlu görüş belirtirken bunu sırasıyla, "Diğer" (f=6), "Konular sunu/seslendirme/video/yaşanmış örneklerle desteklenmeli" (f=4), "Fikrim Yok" (f=4), "Mobil Cihazlar/Siber Saldırı Türleri/Güvenli Alışveriş" (f=3) ve "Bilgisayar ve İletişim Teknolojileri Kullanımında Etik" (f=1) konusunda teklifleri içeren temalar takip etmektedir. Deney grubundaki öğretim elemanlarının bu konuya ilişkin görüş ve değerlendirmelerinden bazıları şu şekildedir:

"Farkındalık oluşturma açısından yeterli görüyorum"

"Bilgi güvenliği konusunda oldukça kapsamlı. Bunun ötesi eğitimcilerin ve kullanıcıların ilgi ve çalışma alanının ötesine geçer ve Bilgisayar sistemleri uzmanlığına girer diye düşünüyorum."

"Bence farkındalık yaratmak amacıyla gayet yeterli..."

"Ben herhangi bir eksik görmedim. Her konuyla ilgili çoklu sunular ve ek kaynaklar verilmiş."

"konu başlıkları sunularla desteklenmeli"

"Bilgilendirme ağırlıklı olmalıdır."

"Seslendirme olabilir. Özellikle uzun metinler içeren paketlerde ekrandan yazı okumak bir hayli yorucu olabiliyor."

"soruyu anladığımdan emin değilim. Tasarlanmış olan çoklu ortam materyalleri' bu öbeğin anlamını bildiğimden dahi emin değilim"

"Uygulamalar geliştirilebilir"

"Belki "Bilgisayar ve İletişim Teknolojileri Kullanımında Etik" alt konusu (eğer böyle bir konu varsa) konulabilir."

"Genel bilgilendirme için yeterlidir ancak özellikle bayanların ilgisini çekebileceğini düşündüğüm güvenli alışveriş ile ilgili konulara yer verilebilir."

"Siber saldırı (tehdit) türleri arttırılabilir, bununla birlikte siber saldırı araç ve silahları, savunma, güvenlik standartları ve güvenlik için kritik kontroller vb"

"bence konuların anlatımı yanı sıra anlatılan konular ile alakalı kullanıcıların daha önce karşılaştıkları deneyimlerde örnek olarak verilebilir. böylece eğitimi alan hedef kitledeki bireyler bilgileri daha da somutlaştırarak anlamaları kolaylaşabilir. "

"Mobil cihazlarla ilgili konularda daha detaya inilmelidir."

"Bilgi güvenliğini sağlamamız için yapılması gerekenler, tek bir başlık altında sıralanabilir, hızlandırılmış bir özet kısmına yer verilebilirdi."

"Web sitesinde yer alan sekmeler tıklandığında ayrıntılı bilgiler yazılı metinler halinde sunulmakta. Aynı metinlerin videoları yer alabilir. İlerde yazılı metni görsel metne dönüştürmek ve bu biçimde açıklamalara da yer vermek etkili olur ve daha geniş bir kullanıcı kitlesi oluşmasına katkı sağlar."

Genel olarak değerlendirildiğinde ise “Bilgi Güvenliği ve Farkındalık” web sitesinde sunulan içeriğin bilgi güvenliği farkındalığı için yeterli olduğu sonucuna varılmaktadır. Kullanıcılar tarafından içeriğin zenginleştirilmesi için sunulan Mobil cihazlar, siber saldırı türleri, güvenli alış-veriş, bilgisayar ve iletişim teknolojileri kullanımında etik konu başlıkları, web sitesinin iyileştirilmesinde öneri olarak değerlendirilecektir.

4.7.4. "Bilgi Güvenliği ve Farkındalık" Web Sitesinin Kullanılabilirliğinin Değerlendirilmesine İlişkin Bulgu ve Yorumlar

Deney grubu öğretim elemanlarının bilgi güvenliği farkındalığı ile ilgili tasarlanmış olan çoklu ortam materyalleri ile web sitesinin kullanılabilirliğini 100 puan üzerinden değerlendirecek olsanız kaç puan verirdiniz sorusuna yönelik belirtmiş oldukları görüşlere ilişkin içerik analizi yapılmıştır. İçerik analizi sonucu ortaya çıkan alt temalar Çizelge 39'da sunulmaktadır.

Çizelge 39
Deney Grubunda Yer Alan Öğretim Elemanlarının Tasarlanmış Olan Çoklu Ortam Materyalleri ile Web Sitesinin Kullanılabilirliğinin 100 Puan Üzerinden Değerlendirilmesine İlişkin Görüşleri.

Alt Temalar	**f**
90	7
95	6
99-100	5
70-79	4
80-85	3
65	1
Not vermeyen	1

Çizelge 39 incelendiğinde deney grubundaki öğretim elemanlarının tasarlanmış olan çoklu ortam materyalleri ile web sitesinin kullanılabilirliğini 100 puan üzerinden değerlendirmeleri sorusuna en çok "90" (f=7) şeklinde olumlu görüş belirtirken bunu sırasıyla, "95" (f=6), "99-100" (f=5), "70-79" (f=4), "80-85" (f=3) ve "65" (f=1) puanı içeren temalar takip etmektedir. Deney grubundaki öğretim elemanlarının bu konuya ilişkin görüş ve değerlendirmelerinden bazıları şu şekildedir:

" 90. Bu puanı vermemin asıl amacı videoların sayfa içinde açılması ve eğitimlerin aynı sayfa içinde verilmesi."

" 90. tek eksik bana göre yukarıda belirttiğim gibi örneklendirme."

" 90 puan veririm. Kullanımı basit, kolay erişilebilir ve anlaşılabilir bir arayüzü var. İnternet ve bilgisayarla yeni tanışanlar açısından yeterli bilgi mevcut."

" 90. Çünkü web sitesindeki başlıklar ve başlık içerikleri bilgi güvenliği konusunda karşılaşılabilecek en temel zorlukları ve sorunları gözler önüne seriyor.

" 95. Hem kişisel öğrenme hem de bir ders içerisinde kullanılabilecek birçok bölüm var."

" 95 Tekrarlar var gibi geldi. Bu nedenle not kırdım. Çok yararlı olduğunu düşünüyorum."

" 99. Oldukça güzel ve kullanışlı hazırlanmış. Emekleriniz için teşekkür ederiz."

" 100 ihtiyaçlarıma üst düzeyde yanıt verdi"

" 100 puan verirdim; çünkü her bir ayrıntı, düşünülmüş ve çok anlaşılır biçimde hazırlanmış."

"Yeterince kapsamlı görünüyor, iyi tasarlanmış ama zaman alıcı. 95 puan veriyorum."

" 100. Kullanımı gayet kolay, sade ve anlaşılabilir. Tasarlanmış materyaller için 90, web sitesinin kullanabilirliği için 95 puan. Materyallerdeki içerik orta düzey kullanıcı için yararlı fakat değişen tehdit yöntem ve saldırı araçları karşısında güvenlik için bu içerik yeterli mi? Ya da biz 3. parti kullanıcılar sadece materyallerle tasarlanan içeriği ne kadar uyguluyoruz? Amaç farkındalık sağlamak ise yeterli. Web sitesinin kullanabilirliğine gelince, konu başlıkları, süresi ve konudan konuya geçişler ve site içinde gezinme oldukça sade, bu da okuyucunun takibini ve sitedeki materyalin kullanımına yönelik tasarlanmış. Yardımcı kaynaklar da sayfalar ekran ekran verilse daha iyi olurdu. Konu bağlamına göre kimi başlıklarda sayfalar çok uzamış. Yardımcı kaynaklar kör sayfalarda verilmiş. Başa dönmek veya gezinmeye olanak tanımıyor. Gömülen PowerPoint ve animasyon sayfalarında ki gibi olsaydı daha güzel olurdu."

" 80 puan verirdim. Çünkü bilgi güvenliğini içeren sunumların yanında değerlendirme soruları gibi eğitici ögelerin web sayfasına eklenmesini beklerdim. Ayrıca flash animasyonlar bölümünde durdur ve büyük ekran butonunun konulması takip açısından daha yararlı olabilirdi."

Genel olarak değerlendirildiğinde ise "Bilgi Güvenliği ve Farkındalık" web sitesinin kullanılabilirliği 100 üzerinden 88 olarak değerlendirilmiştir. Kullanıcılar tarafından içeriğin zenginleştirilmesi için sunulan konu başlıkları, web sitesinin iyileştirilmesinde öneri olarak değerlendirilecektir.

4.7.5. "Bilgi Güvenliği ve Farkındalık" Web Sitesinin Kullanım Memnuniyetine İlişkin Bulgu ve Yorumlar

Deney grubu öğretim elemanlarının bilgi güvenliği farkındalığı ile ilgili tasarlanmış olan çoklu ortam materyalleri ile web sitesini kullanmaktan memnun musunuz sorusuna yönelik belirtmiş oldukları görüşlere ilişkin içerik analizi yapılmıştır. İçerik analizi sonucu ortaya çıkan alt temalar Çizelge 40'ta sunulmaktadır.

Çizelge 40
Deney Grubunda Yer Alan Öğretim Elemanlarının Tasarlanmış Olan Çoklu Ortam Materyalleri ile Web Sitesinin Kullanım Memnuniyetine İlişkin Görüşleri.

Alt Temalar	**f**
Evet/Memnunum/Memnun Kaldım	17
Kısmen	5
Fikrim Yok	5

Çizelge 40 incelendiğinde deney grubundaki öğretim elemanlarının tasarlanmış olan çoklu ortam materyalleri ile web sitesinin kullanılabilirliğini 100 puan üzerinden değerlendirmeleri sorusuna en çok "Evet/Memnunum/Memnun Kaldım" (f=17) şeklinde olumlu görüş belirtirken bunu sırasıyla, "Kısmen" (f=5) ve "Fikrim Yok" (f=5) puanı içeren temalar takip etmektedir. Deney grubundaki öğretim elemanlarının bu konuya ilişkin görüş ve değerlendirmelerinden bazıları şu şekildedir:

"evet, çünkü bilmediğim konularda farkındalığımı arttırdı"

"Evet. Bilgilerimi güncelledi yanlış bildiklerimin farkına varmamı sağladı."

"Evet, özellikle öğrencilerim için güzel bir kaynak olurdu (tez bittikten sonra halka açılırsa)."

"Memnunum. Yanıt verirken doğru kaynaklara ulaştığımı varsayıyorum."

"Yararlı buldum ama sanki biraz daha kısa olsaydı daha mı iyi olurdu acaba."

"Evet. Her şey çok anlaşılır ve pratik. Bilmediğim ama bizim için çok önemli konular hakkında çok kısa sürede bilgi alabiliyoruz."

"WEB sitesi bilgi güvenliği konusunda şifre dışında bilmediğim birçok şey olduğunu görmeme neden oldu."

"Evet memnunuz Çünkü yüzeysel bilgiye sahip olduğum bir konuda biraz daha derinlemesine bilgi sahibi olmuş oldum. Kendimi korumak için neler yapabilirim öncekinden daha fazla bilgiye sahibim. Bu konuda tanıdıklarıma nasıl yardımcı olabilirim onu öğrendim."

"Evet. Bilgi güvenliği için gerekli bilgiler herkes için gayet kolay anlaşılabilir seviyede."

"Memnunum. Temel başvuru kaynağı olarak kullanılabilir. Site yayında olduğu sürece öğrencilerimin de yararlanmasını, kullanmasını istiyorum. BÖTE bölümü son sınıfa kadar gelmiş öğrencilerin arasında hala bazı konularda bilgi açığı olanlar var. Bu açığı kapatması açısından tamamlayıcı bir rol de üstlenebilir."

"evet memnunum. aslında bir çok kavramı eğitim alanımdan dolayı biliyorum fakat elimizin altında böyle bir kaynağın olması unuttuğumuz noktalarda veya hiç karşılaşmadığımız durumlarda bize rehber olabilecek nitelikte."

"Web sitesini kullanmaktan memnun kaldım. Daha önce böyle bir materyali inceleme fırsatım olmadığı için her açıdan yararlı buldum. Parça parça videolu anlatım sayfa tasarımını çok beğendim."

"Web sitesini kullanmaktan memnunum. Arayüz basit ve anlaşılır bir biçimde iyi tasarlanmış, bilgilendirmeler anlaşılır durumdadır."

"Memnunum. Hem içerik hem de çoklu ortam materyallerinin zenginliği açısından kullanışlı bir site olmuş. "

"Memnunum. Daha önce de belirttiğim gibi en temel problemlere değiniliyor ve en sık karşılaştığımız sorunlar açıklamaları ve çözümleriyle birlikte ele alınıyor. İşe vuruk bir süreç yaşamanızı ve sistemden verim almanızı sağlıyor."

"Genel bir farkındalık oluşturması açısından memnun oldum. Daha detaylı teknik bilgi de almak isterdim."

"kısmen. Sade olmasını daha çok tercih ederim."

Genel olarak değerlendirildiğinde ise öğretim elemanlarının "Bilgi Güvenliği ve Farkındalık" web sitesini kullanmaktan memnun olduğu sonucuna varılmaktadır.

4.7.6. "Bilgi Güvenliği ve Farkındalık" Web Sitesinde Eksik Olan Özelliklere İlişkin Bulgu ve Yorumlar

Deney grubu öğretim elemanlarının bilgi güvenliği farkındalığı ile ilgili tasarlanmış olan çoklu ortam materyalleri ile web sitesinde eksik olan özellikler sorusuna yönelik belirtmiş oldukları görüşlere ilişkin içerik analizi yapılmıştır. İçerik analizi sonucu ortaya çıkan alt temalar Çizelge 41'de sunulmaktadır.

Çizelge 41
Deney Grubunda Yer Alan Öğretim Elemanlarının Tasarlanmış Olan Çoklu Ortam Materyalleri ile Web Sitesinde Eksik Olan Özellikler Sorusuna İlişkin Görüşleri.

Alt Temalar	**f**
Yeterli	12
Çeşitli Konular	5
Video/Görsel Destekli/Etkileşimli İçerik	2
Fikrim Yok	2
Değerlendirme Aracı	1
Antivirüs Programı Kurulumu/Güncellenmesi	1
Çevrimiçi Destek Hattı	1

Çizelge 41 incelendiğinde deney grubundaki öğretim elemanlarının tasarlanmış olan çoklu ortam materyalleri ile web sitesinde eksik olan özellikler sorusuna en çok

“Yeterli” (f=12) şeklinde olumlu görüş belirtirken bunu sırasıyla, “Çeşitli Konular” (f=5), “Video/Görsel Destekli/Etkileşimli İçerik” (f=2), “Fikrim Yok” (f=2), “Değerlendirme Aracı” (f=1), “Antivirüs Programı Kurulumu/Güncellemesi” (f=1) ve “Çevrimiçi Destek Hattı” (f=1) konu başlıklarını içeren temalar takip etmektedir. Deney grubundaki öğretim elemanlarının bu konuya ilişkin görüş ve değerlendirmelerinden bazıları şu şekildedir:

"çoklu ortam materyali çeşitlendirilebilir, etkileşimli içerik sunulabilir"

"Kullanım kılavuzunda hareketli gösterimler kullanılsa daha iyi olur. Sadece oklarla göstermek yerine animasyon gibi bir şeyler kullanılabilirdi."

"Video ve görsel destekli açıklamalar. Görsel okuyarak öğrenen çok sayıda insana rastlıyoruz. Metin okumak kimi zaman rağbet görmüyor."

"Çoğu zaman eksik kalan senaryo ve gerçek hayat durumlarıyla ilişkilendirme video ve durum örnekleriyle sağlanmış. Eğitimcilere ek kaynak olacak farklı seviyedeki öğrencilere yönelik değerlendirme aracı destek olabilir."

"Antivirüs programının kurulması, güncellenmesi bu tür bilgiler de olsa daha iyi olurdu."

"belli zaman aralıkları ile çevrimiçi hizmet verilebilir bence. kullanıcılardan daha özellikli sorunların çözülmesine imkan tanımak için."

Genel olarak değerlendirildiğinde ise “Bilgi Güvenliği ve Farkındalık” web sitesinde sunulan içeriğin bilgi güvenliği farkındalığı için yeterli olduğu sonucuna varılmaktadır. Kullanıcılar tarafından içeriğin zenginleştirilmesi için sunulan etkileşimli içerik, çevrimiçi yardım desteği, kişisel tecrübelerin paylaşımı ve metinlere sesli okuma yeteneği konu başlıkları, web sitesinin iyileştirilmesinde öneri olarak değerlendirilecektir.

4.8. Araştırmacının Uygulama Esnasında Elde Ettiği Bulgular

Bu araştırma kapsamında, gerek ölçek geliştirme aşamasında gerekse deneysel çalışma aşamasında karşılaşılan en büyük sorun, öğretim elemanlarının araştırmaya katılımı seviyesinin beklenen düzeyin altında ve az olmasıdır.

Yapılan çalışma ile ilgili Etik Kurulu kararı alınmış, çalışma grubu içinde yer alan üniversitelere resmi yazı ile başvuru yapılmıştır. Ölçek geliştirme safhasında, araştırmacı tarafından ilgili üniversiteler ve öğretim üyeleri yerinde ziyaret edilerek basılı anket dağıtılmış, ayrıca elektronik anket uygulaması geliştirilmiştir. Görüşülen tüm öğretim elemanları konunun güncel ve önemli olduğunu ifade etmişlerdir. Ölçek geliştirme aşaması, Eylül 2013- Nisan 2014 tarihleri arasında toplamda ulaşılabilen öğretim elemanı sayısı 363 ile sınırlı kalmıştır.

Deneysel çalışma, Haziran 2014-Ocak 2015 tarihleri arasında gerçekleştirilmiştir. Deneysel çalışma öncesinde, "Bilgi Güvenliği ve Farkındalık" web sitesi ve planlanan çalışma, Ankara Üniversitesi Eğitim Bilimleri Fakültesi Kurulu'nda duyurulmuştur. Fakülte Kurulu üyeleri (Anabilim Dalı, Bölüm Başkanları dâhil) bu tür bir eğitime ihtiyaç olduğunu belirtmişler ve verilecek eğitime katılmakta yarar gördüklerini vurgulamışlardır. Planlanan ikinci safha ile ilgili açıklama içerikli e-posta Ankara Üniversitesi Eğitim Bilimleri Fakültesi öğretim elemanlarına iki kez farklı zamanlarda duyurulmuştur. Toplam 221 öğretim elemanından 136 tanesi öntest uygulamasına katılmıştır. Öntest uygulamasına katılan öğretim elemanlarının %5'i (6) elektronik form, %95'i (129) ise basılı anket uygulaması doldurmayı tercih etmişlerdir. Öntest bilgi güvenliği farkındalık ölçeğini dolduran ve araştırmanın ikinci aşamasına gönüllü katılmayı kabul eden 106 öğretim elemanı ile sürece devam edilmesi kararı alınmıştır. Öntest sonrası üç aylık süre ile iletme/aktarma etkisini ortadan kaldırmak için çalışmaya ara verilmiştir. Üç aylık aranın ardından öğretim elemanları e-posta ile tekrar konu hakkında bilgilendirilmiştir. "Bilgi Güvenliği ve Farkındalık" Web Sitesi'nin öğretim elemanlarının hizmetine sunulması 12 hafta boyunca devam etmiştir. Planlanan süre sonunda öğretim elemanlarının sontest uygulamasına katılımı 65 katılımcı ile tamamlanabilmiştir. Sontest uygulamasına katılan öğretim elemanlarının sadece 31 tanesi deney grubunda yer almıştır.

Deneysel aşamaya katılımın az olması, öğretim elemanlarının bu tür eğitimleri elektronik olarak almaya yatkın olmadıkları şeklinde yorumlanabilir. Hedef kitle olarak öğretim elemanları ile planlanan benzer araştırma çalışmalarında, bu husus göz önünde

bulundurulmalıdır. Araştırmaya katılan grup, “araştırmacı”, “danışman”, “koordinatör” görevlerini üstlenen ve araştırmada veri toplamanın, deneysel işleme katılımcıları dâhil etmenin birebir güçlüğünü yaşayan bilim insanları olmalarına karşın “iş yoğunluğu”, “toplantı”, “konferans”, “bilimsel etkinlikler” vb. nedenleri göstererek beklenen desteği sağlamamıştır. Bunların yanı sıra araştırmanın deneysel deseni, “tek grup öntest sontest desen” olarak da desenlenebilir olmasına rağmen sağlık bilimlerinde sıklıkla kullanılan bir desen olan ve alan uzmanlarının görüşü alınarak “öntest sontest kontrol gruplu desen” ile modellenmiştir. Araştırmada başlangıç öngörüsü olarak tasarlanan desenin yaşanan süreç içerisinde “tek grup öntest sontest desen” olarak değiştirilmesi düşünülse de, alanyazında benzer desen ile gerçekleştirilen araştırmaların olması ve Ankara Üniversitesi Eğitim Bilimleri Fakültesi Ölçme Değerlendirme Anabilim Dalı öğretim üyeleri ile yapılan görüşmeler neticesinde kalması gerektiği görüşü belirtilmiştir. Bu gerekçelerden dolayı, araştırma deseninde değişiklik yoluna gidilmemiştir.

BÖLÜM 5

5.SONUÇ VE ÖNERİLER

Bu araştırmada yükseköğretim kurumlarındaki öğretim elemanlarına yönelik bilgi güvenliği farkındalık düzeylerinin değerlendirilmesi çalışması, iki aşamalı olarak gerçekleştirilmiştir. Araştırmanın sınırlılıkları çerçevesinde; alanyazın taraması sonucu elde edilen veriler ışığında birinci aşamada ölçek geliştirme çalışması, ikinci aşama ise öğretim elemanlarının bilgi güvenliği farkındalık düzeylerini arttırmaya yönelik geliştirilen "Bilgi Güvenliği ve Farkındalık" web sitesinin, öğretim elemanlarının bilgi güvenliği farkındalık düzeylerini artırmaya etkisinin belirlenmesi çalışması gerçekleştirilmiştir.

Bu bölümde, çalışmalar sonucu elde edilen araştırma bulgularına dayalı olarak, varılan sonuçlar 5.1 başlığında ve geliştirilen öneriler 5.2 başlığı altında sunulmuştur.

5.1.Sonuçlar

Bu araştırmanın amacı; yükseköğretim kurumlarında görev yapan öğretim elemanlarına bilgi güvenliği farkındalığı kazandırmaya yönelik, çoklu ortam materyallerini içeren bir web sitesi geliştirmek ve geliştirilen web sitesinin bilgi güvenliği farkındalığı kazandırmadaki etkisini belirlemektir.

Araştırma kapsamında, öğretim elemanlarının bilgi güvenliği farkındalık düzeyini belirlemek amacıyla "Bilgi Güvenliği Farkındalık Ölçeği" geliştirilmiştir. Yapılan analizler sonucunda geçerliliği ve güvenirliği kanıtlanan ölçek, kişisel bilgiler ve bilgi güvenliği farkındalık ölçeği olmak üzere iki ana bölümden oluşmaktadır. Ölçekte, "saldırı ve tehditler" ve "kişisel verilerin korunması" olmak üzere iki alt boyut ve 34 maddeden oluşmaktadır. Geliştirlen ölçek kullanılarak çalışma grubunda yer alan öğretim elemanlarının bilgi güvenliği farkındalık düzeylerini belirlemek için kullanılabilecek geçerli ve güvenilir bir ölçek elde edilmiştir.

Araştırmanın ikinci aşamasında alanyazın taraması ve uzman görüşüne göre uygun olduğu sonucuna varılan çoklu ortam materyalleri ve web sitesi geliştirilmiştir.

Araştırma kapsamında geliştirilen ve çoklu ortam materyalerini içeren “Bilgi Güvenliği ve Farkındalık” web sitesinin etkiliğini değerlendirmek amacıyla öğretim elemanlarından 65 katılımcı (31 deney grubu, 34 kontrol grubu) ile 12 hafta boyunca bilgi güvenliği farkındalık eğitimi uygulaması yapılmıştır. Eğitim uygulamasının öğretim elemanlarının bilgi güvenliği farkındalık düzeylerinde yaptığı değişimi ölçmek amacıyla araştırma kapsamında geliştirilen ölçek eğitim öncesinde öntest, sonrasında sontest olarak uygulanmıştır. Öntest sontest ölçümlerinin karşılaştırmasına ve öğretim elemanlarının görüşlerine bağlı olarak; geliştirilen çoklu ortam materyalerini içeren web sitesi ile verilen eğitimin öğretim elemanlarına bilgi güvenliği farkındalığı kazandırmada etkili olduğu sonucuna ulaşılmıştır. Öğretim elemanlarının uygulama öncesinde ölçeğin alt boyutlarındaki bilgi farkındalık düzeyi düşük iken; uygulama sonrasında bilgi güvenliği farkındalık düzeylerinde artış meydana gelmiştir. Her bir alt boyuta ilişkin elde edilen bulgular; verilen eğitimin öğretim elemanlarının alt boyutlardaki bilgi güvenliği farkındalık düzeyini geliştirmede önemli bir etkiye sahip olduğunu ortaya koymaktadır.

Deneysel aşamaya katılan öğretim elemanları tarafından geliştirilen çoklu ortam materyalleri ve web sitesi kullanımının faydalı olduğu ve katkı sağladığı, web sitesinin kullanılabilirliğini iyi düzeyde (88/100 puan) değerlendirdikleri ve uygulama öncesine kıyasla bilgi güvenliği farkındalığı konusunda bilinçlendikleri sonucuna ulaşılmıştır. Öğretim elemanlarının bilgi güvenliği farkındalık eğitimi ve uygulamaya ilişkin görüşleri ise çoklu ortam materyalleri ile sunulan eğitim süresinin daha kısa olması ve öğrencilerin yanı sıra idari personelinde bu tür bir eğitime ihtiyaç duyduklarına işaret etmektedir.

5.2.Öneriler

Bu bölümde, çalışmalar sonucu elde edilen araştırma bulgularına dayalı olarak, uygulamaya ve ileride yapılacak araştırmalara yönelik geliştirilen önerilere yer verilmiştir.

Uygulamaya Yönelik Öneriler

Araştırma kapsamında geliştirilen çoklu ortam materyalleri ve web sitesi, öğretim elemanları hedef alınarak alanyazın taraması ve uzman görüşü ile elde edilen

verilere göre tasarlanmıştır. Sitenin geliştirilmesine yönelik hedef kitle beklentileri ile ilgili görüş açık uçlu sorularla alınmıştır. Bu bağlamda web site uyarlanabilirlik açısından portal yapısına dönüştürülebilir. Geliştirilen sitedeki mevcut çoklu ortam materyallerine ilave, sitenin geliştirilip güncellenmesine yönelik öğretim elemanlarının önerileri arasında aşağıdaki başlıklar yer almaktadır:

- Hazırlanan bilgi notları seslendirme yapılarak kullanıcıya alternatif öğrenme fırsatı sunulabilir.
- Örnek olarak hazırlanan "şifre güç ölçer uygulaması" benzeri uygulamalar ile bilgi güvenliği farkındalık konuları çeşitlendirilebilir.
- Bilgi güvenliği farkındalığı ile ilgili konular, "örnek senaryolar" ile videoya çekilerek konu zenginliği kazandırılabilir.
- Bilgi güvenliği farkındalığı konularıyla ilgili kullanıcıların yaşadıkları tecrübeleri paylaşabileceği bir "blog" web sitesine eklenebilir.
- Bilgi güvenliği farkındalığı konu başlıkları arttırılabilir (Siber saldırı türleri, siber saldırı araç ve silahları, siber savunma, güvenlik standartları vb).
- Çoklu ortam materyalleri, etkileşimli içerik ile sunulabilir.
- Geliştirilen web sitesi "yönetim içerik sistemi" kullanılarak çevrimiçi destek hizmeti sunacak bir yapı ile desteklenebilir.

Prototip şeklinde hazırlanan web sitesinde sunulan konu başlıkları farkındalık yaratmak için yeterlidir. Kullanıcıları farkındalık yaratmadan bir ileri aşamaya taşıyacak daha detaylı sunularla desteklenmesi, bilgi güvenliği alandaki önemli bir eksikliği giderecektir. Bu nedenle, bireylerin kendilerini sürekli yenileyebilmelerini desteklemek amacıyla bilgi güvenliği farkındalık web sitesi ve çoklu ortam materyallerinin güncellenmesi ve çeşitlendirilmesi büyük önem taşımaktadır.

İleride Yapılabilecek Araştırmalara Yönelik Öneriler

- Benzer araştırmalarda "iş yoğunluğu", "toplantı", "konferans", "bilimsel etkinlikler" vb. nedenlerden dolayı veri toplama sürecinde beklenen katılımın sağlanamama riski yüksektir.
- Araştırmaya katılımı artırmak için elektronik anket, basılı materyal ve birebir görüşme ile anket katılım oranı arttırılabilir.

- Farklı hedef kitlelere (öğretmenler, öğrenciler, diğer kurumlarda çalışanlar vb.) yönelik benzer araştırmalar yapılabilir.
- Bilgi güvenliği şemsiyesi altında bir alt başlık olan "farkındalık" konusunun kurumların uygulamış olduğu "Bilgi Güvenliği Yönetim Sistemleri" içerisindeki yeri, önemi ve kurumların bu konuya harcamış olduğu kaynakların incelenmesi bir araştırma konusu olarak ele alınabilir.
- Bilgi güvenliği farkındalığı yanında etik internet kullanımı konusunun birlikte incelenmesi yapılacak çalışmalara farklı bir boyut katacaktır.
- Yükseköğretim kurumlarında yönetimin bilgi güvenliği farkındalığı konusunu nasıl algıladıkları ve bu farkındalığı arttırmaya yönelik ne tür çalışmalar yaptığı/yapması gerektiği konusu araştırılabilir.
- Yükseköğretim kurumlarında "bilgi güvenliği kültürü" geliştirmek için neler yapılması gerektiği araştırılabilir.
- Araştırma kapsamında geliştirilen ölçek, çoklu ortam materyalleri ile web sitesi Türkiye'deki tüm Üniversite öğretim elemanlarına uygulanabilir. Böylelikle Türkiye genelinde bilgi güvenliği farkındalık düzeyi değerlendirmesi araştırılabilir.

KAYNAKLAR

Acılar, A. (2009). İşletmelerde bilgi güvenliği ve örgüt kültürü. *Organizasyon ve Yönetim Bilimleri Dergisi*, I(1), 25-33.

Ahlan, A. R., and Lubis, M. (2011). Information security awareness in university: maintaining learnability, performance and adaptability through roles of responsibility. *2011 7th International Conference on Information Assurance and Security (IAS)* (s. 246-250). Malacca, Malaysia: MIR Labs Ltd.

Akın, G. (2014). Andragoji kavramı ve anfragoji ile pedagoji arasındaki fark. *Ankara Üniversitesi Eğitim Bilimleri Fakültesi Dergisi*, 47(1), 279-300.

Akpınar, Y. (2005). *Bilgisayar destekli eğitimde uygulamalar (2.b.)*. Ankara: Anı Yayıncılık.

AlAboodi, S. S. (2006). A *new approach for assessing the maturity of ınformation security*. Retrieved from ISACA: http://www.isaca.org

Alkan, C. (1981). *Açık Üniversite*. Ankara: Ankara Yayınları.

Alkan, C. (1988). *Modüler programlama ve Türkiye'de uygulaması*. http://dergiler.ankara.edu.tr /dergiler/40/511/6269.pdf adresinden ulaşılmıştır.

Alkan, C., Deryakulu, D. ve Şimşek, N. (1995). *Eğitim teknolojisine giriş*. Ankara: Önder Matbaacılık Ltd. Şti.

Alkan, C. (2005). *Eğitim teknolojisi.* (5.b.). Ankara: Anı Yayıncılık.

Aslan, Ö. (2007). *Bilgi toplumunda teknolojinin ve teknoloji politikalarının yeri* (Yayımlanmamış Doktora Tezi). İstanbul Üniversitesi, İstanbul.

Altun, A. (2005). *Eğitimde İnternet uygulamaları*. Ankara: Anı Yayıncılık.

Aybar, K., Göçmenler, G., Keser, H., Numanoğlu, M. ve Teker, N. (2004). *Eğitim teknolojileri terimleri sözlüğü*. Ankara: Yaygın Eğitim Enstitüsü Matbaası.

Balcı, A. (2009). *Sosyal bilimlerde araştırma yöntem, teknik ve ilkeler.* (7.b.). Ankara: Pegem Akademi.

Bulurman, B. (2002). On-line eğitim. *Endüstri İlişkileri ve İnsan Kaynakları Dergisi*, 4(2), 3-56.

Barutçugil, İ. (2002). *Eğiticinin eğitimi*. İstanbul: Kariyer.

Bilir, M. (2004).Çağdaş yetişkin eğitimi liderlerinden Eduard Christian Lindeman (1885-1953) yaşamı, eğitim görüşü ve hizmetleri. *Ankara Üniversitesi Eğitim Bilimleri Fakültesi Dergisi*, 37(2), 15-25.

Berberoğlu, B. (2010). Bilgi toplumu ve bilgi ekonomisi oluşturma yolunda Türkiye ve Avrupa Birliği. *Marmara Üniversitesi İ.İ.B.F. Dergisi*, XXIX(II), 111-131.

Blanding, F. S. (2004), *An introduction to LAN/WAN security, information security management handbook (fifth edition)*. New York : Auerbach Publications.

Burge, L. (1988). Beyond andragogy: some explorations for distance learning design. *Journal of Distance Education*, 3(1), 5-23.

Büyüköztürk, Ş. (2011). *Sosyal bilimler için veri analizi el kitabı* (13. b.). Ankara: Pegem Akademi.

Büyüköztürk, Ş., Çakmak, E. K., Akgün, Ö. E., Karadeniz, Ş. ve Demirel, F. (2011). *Bilimsel araştırma yöntemleri* (8. b.). Ankara: Pegem Akademi.

Büyüköztürk, Ş., Çokluk, Ö. ve Köklü, N. (2010). *Sosyal bilimler için istatistik* (6. b.). Ankara: Pegem Akademi.

Canbek, G. (2005). *Klavye dinleme ve önleme sistemleri analiz, tasarım ve geliştirme* (Yayımlanmamış Yüksek Lisans Tezi). Gazi Üniversitesi, Ankara.

Canbek, G. ve Sağıroğlu, S., (2006), *Bilgi ve bilgisayar güvenliği: casus yazılımlar ve korunma yöntemleri*. Ankara:Grafiker Yayıncılık.

Canbek, G. ve Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Politeknik Dergisi*, 9(3), 165-174.

Caruso, J. B. (2003). *Information technology security: governance, strategy, and practice in higher education*. Wisconsin, Madison: EDUCAUSE Center For Applied Research ECAR.

Chen, C. C., Shaw, R., & Yang, S. C. (2006). Mitigating ınformation security risks by ıncreasing user security awareness: a case study of an ınformation security awareness system. ınformation technology. *Learning and Performance Journal*, 24(1), 1-14.

Civelek, D. Y. (2011). *Kişisel verilerin korunması ve bir kurumsal yapılanma önerisi* (Uzmanlık Tezi). T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı, Ankara.

Cowell, C., Hopkins, P.C., McWhorter, R. ve Jorden, D.L. (2006). Alternative training models. *Advances in Developing Human Resources*, Vol.8, No.4, USA.

Cox, A., Connolly, S., & Currall, J. (2001). Raising information security awareness in the academic setting. Glasgow, United Kingdom.

Çakmak, E. K., ve Karataş, S. (2008). Temel kavramlar ve kuramsal temeller. H. İ. Yalın (Ed.). *İnternet temelli eğitim*. Ankara: Nobel Yayın.

Çirasun, E. (2011). *Enformasyon toplumu ve bilgi çağında Türkiye'nin gelişim süreci* (Yayımlanmamış Yüksek Lisans Tezi). Marmara Üniversitesi, İstanbul.

Çokluk, Ö., Şekercioğlu, G. ve Büyüköztürk, Ş. (2010). *Sosyal bilimler için çok değişkenli istatistik spss ve lısrel uygulamaları*. Ankara: Pegem Akademi.

Dalkılınç, M. (2011). *Ofis çalışanlarında e-öğrenme ve interaktif yöntemlerle sunulan ergonomi eğitiminin, kas iskelet sistemi yaralanmaları ile ilişkili risk faktörleri üzerine etkisi* (Yayınlanmamış Doktora Tezi). Hacettepe Üniversitesi, Ankara.

Ducharme-Hansen, B. A. and Dupin-Byrant, P. A. (2004).*Web based distance education for adults*. Malabar, Florida: Krieger Publishing Company.

Duman, A. (2007). *Yetişkinler eğitimi.* Ankara: Ütopya.

Durakoğlu, A., Biçer, B. Ve Zabun, B. (2013).Paulo Freire's alternative education model. *Antropologist*, 16(3), 523-530.

Elliott, R., Young, M. O., Collins, V. D., Frawley, D. And Temares, M. L. (1991). *Information security in higher education.* Retrieved from CAUSE: https://net.educause.edu/ir/library/pdf/PUB3005.pdf

Erturgut, R. (2008). İnternet temelli uzaktan eğitimin örgütsel, sosyal, pedagojik ve teknolojik bileşenleri. *Bilişim Teknolojileri Dergisi*, 1(2), 79-85.

Friedman, T. L. (2007). T*he world is flat*. New York: Picador Reading Group.

Foster, A. L. (2004). Insecure and Unaware. *Chronicle of Higher Education*, 50(35), 33-35.

Gemci, C. ve Bay, Ö. F. (2011). *Yapay zeka temelli bilgi güvenliği yönetim sistemi yaklaşımı*. TMMOB(Elektrik): www.emo.org.tr/ekler/4847ee98ac2a5d6_ek.pdf adresinden ulaşılmıştır.

Geray, C. (2002). *Halk eğitimi.* Ankara: İmaj.

Güneş, F. (1996). *Yetişkin eğitimi (halk eğitimi).* Ankara: Ocak Yayınları.

Gülmüş, M. (2010). *Kurumsal bilgi güvenliği yönetim sistemleri ve güvenliği* (Yayımlanmamış Yüksek Lisans Tezi). Yıldız Teknik Üniversitesi, İstanbul.

Karasar, N. (2005). *Bilimsel araştırma yöntemi kavramlar ilkeler teknikler*. Ankara: Nobel Yayınları.

Keser, H (2005) *İnsan-bilgisayar etkileşimi ve sağlığa etkisi*. Ankara: Nobel Yayıncılık.

Keser, H., Bayır, Ş. ve Eren, N. Z. (2009). *Görme engellilere yönelik bilişim teknolojileri sunduğu olanaklar ve yararlanma koşulları*. 3. Uluslararası Bilgisayar ve Öğretim Teknolojileri Eğitimi Sempozyumu içinde (891-897), Trabzon.

Kjorvik, H. (2010). *İmplementing and improving awareness in information security*. (Master's thesis). University of Agder, Grimstad.

Knowles, Malcolm (1996) (S. Ayhan, Çev.). *Yetişkin öğrenenler*. Ankara: Ankara Üniversitesi Basımevi

Knowles, M., Holton, E.F. ve Swanson, R.A. (2005). *The adult learner: the definitive classic in adult education and human resorce development (6th Ed.).* San Diego: Elsevier.

Kritzinger, E., & Smith, E. (2008). Information security management:An information security retrieval and awareness model for industry. *Computer and Security*, 27, 224-231.

Kruger, H., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computer and Security*, 25, 289-296.

Kurt, İ. (2000). *Yetişkin eğitimi.* Ankara: Nobel Yayın Dağıtım.

Lindeman, E. C.(1969) (C. Şentürk, Çev.). Yetişkin eğitiminin anlamı. Ankara: MEB Basımevi.

Mahabi, V. (2010). *Information security awareness: system administrators and end-user perspectives at Florida State University* (Doctorate of Philosophy). The Florida State University, Florida.

Maiwald, E.,(2003). Network Security: A Beginner's Guide Summary. *McGraw-Hill Osborne Media,* California,USA.11(5), 4-11.

Malkoç, G. (1989). Yetişkin eğitiminin gerekliliği. *Marmara Üniversitesi Atatürk Eğitim Bilimleri Dergisi,* 1, 88-95.

Mathisen, J. (2004). *Measuring information security awareness - a survey showing the Norwegian way to do it* (Master's thesis). Gjovik University, Hogskolen.

Miser, R. (1999). *Halk eğitimi ve toplum kalkınması*. Ankara: Milli Eğitim Bakanlığı Yayınları.

O'Connor, N.O., Bronner, M. ve Delaney, C. (2007). *Learning at work: how to support individual and organizational learning.* Amherst, Massachusetts: HRD Press.
Usher, R., , Bryant, L. ve Johnston, R. (2005). *Adult education and the postmodern challange.* New York: Routledge.

Penmetsa, M. K. (2010).A*a methodology for measuring information security maturity in Norwegian and Indian msme's with special focus on people factor*. (Master's thesis). Gjovik University, Hogskolen.

Puhakainen, P. (2006). A *design theory for ınformation security awareness* (Master's thesis). Acta University of Oulu Faculty of Science Department of Information Processing Science, Oulu.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. Computer & Security, 27, 241-253.

Önel, D. (2008). *Bilgi güvenliği bilinçlendirme süreci oluşturma kılavuzu.* Kocaeli: UEKAE.

Özcan, B. (2009). *Kurumsal bilgi güvenliği ve COBIT* (Yayımlanmamış Yüksek Lisans Tezi). Haliç Üniversitesi, İstanbul.

Özen, Ü. Ve Karaman, S. (2001). Web tabanlı uzaktan eğitimde sistem tasarımı. *Akdeniz İktisadi ve İdari Bilimler Fakültesi Dergisi,* 2, 81-102.

Öztuna, D. ve Elhan, A.H. (2015). *Gruplar arası ve grup içi karşılaştırma yöntemleri*. http://file.toraks.org.tr/TORAKSFD23NJKL4NJ4H3BG3JH/mse-ppt-pdf/D_OZTUNA_H_ELHAN.pdf adresinden ulaşılmıştır.

Rosen, D.J. (1996). *How adult literacy practitioners are using the İnternet*. Retrieved from http://www.alri.org/pubs/teacherfocusgroups.html

Sharp, E. D. (2004. *Information security in the Enterprise, Information Security Management Handbook* (Fifth Edition). New York :Auerbach Publications.

Siponen, M. T. (2001). Five dimensions of ınformation security awareness. *Computer and Society*, 7, 24-29.

Smith P. L. ve Ragan, T. J. (1999). *Instructional design* (2nd ed). New York: Wiley and Sons, Inc.

Soran, H., Akkoyunlu, B. ve Kavak, Y. (2006). Yaşam boyu öğrenme becerileri ve eğiticilerin eğitimi programı: Hacettepe Üniversitesi örneği. *Hacettepe Üniversitesi Eğitim Fakültesi Dergisi* , 30, 201-210.

Szuba, T. (1998). *Safeguarding your technology, practical guidelines for electronic education information security*. Retrieved from NCES:http://nces.ed.gov/pubs98/98297.pdf

Şahinaslan, E., Kandemir, R. ve Şahinaslan, Ö. (2009). Bilgi güvenliği farkındalık eğitimi örneği. *Akademik Bilişim '09 - XI.Akademik Bilişim Konferansı Bildirileri* içinde (s. 189-194). Urfa.

Şahinaslan, E., Kantürk, A., Şahinaslan, Ö. ve Borandağ, E. (2009). Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri. *Akademik Bilişim '09 - XI.Akademik Bilişim Konferansı Bildirileri* içinde (s. 597-602). Şanlıurfa.

Tandoğan, M., Özer, B., Akkoyunlu, B., Kaya, Z., Odabaşı, F., Deryakulu, D. ve İmer, G. (1998). Ç*ağdaş eğitimde yeni teknolojiler*. Eskişehir: T.C.Anadolu Üniversitesi Açıköğretim Fakültesi Yayınları.

Tezbaşaran, A. A., (2008). *Likert tipi ölçek geliştirme kılavuzu*. Ankara:TPD.

Tonta, Y. (1999). Bilgi toplumu ve bilgi teknolojisi. *Türk Kütüphaneciliği Dergisi, 13(4), 363-375.*

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). *İnvestigating information security awareness: research and practice gaps*. Information Security Journal: A Global Perspective, 207-227.

TÜBİTAK. (2002). *Bilgi toplumu politikaları üzerine bir değerlendirme*. TÜBİTAK: http://turkoloji.cu.edu.tr/GENEL/bilgi_toplumu.pdf adresinden ulaşılmıştır.

UCISA (2006). *Information security toolkit*. Retrieved from UCISA: http://www.ucisa.ac.uk/istoolkit.

Vardal, N. (2009). *Yükseköğretimde bilgi güvenliği: bilgi güvenlik yönetim sistemi için bir model önerisi ve uygulaması* (Yayımlanmamış Doktora Tezi). Gazi Üniversitesi, Ankara.

Veiga, A. D. (2008). *Cultivating and assessing information security culture* (Doctorate of Philosophy). University of Pretoria, Pretoria.

Veneziano L. ve Hooper J. (1997). A method for quantifying content validity of health-related questionnaires. *American Journal of Health Behavior*, 21(1), 67-70.

Vural, Y. (2007). *Kurumsal bilgi güvenliği ve sızma (penetrasyon) testleri* (Yayımlanmamış yüksek lisans tezi). Gazi Üniversitesi, Ankara.

Vural, Y. ve Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 23(2), 507-522.

Vural, Y. ve Sağıroğlu, Ş. (2011). Kurumsal bilgi güvenliğinde güvenlik testleri ve öneriler. *Gazi Üniversitesi Mimarlık Mühendislik Fakültesi Dergisi*. 26(1), 89-103.

Wilson, M. And Hash, J., (2003). *Building an information technology security awareness and traing program.* Washington:U.S. Goverment Printing Office.

Yazar, T. (2012). Yetişkin eğitiminde hedef kitle. *Dicle Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 4(7), 21-30.

Yılmaz, H. (2015). *Örneklem büyüklüğünün saptanması ve istatistiksel testler*. http://www.tavsiyeediyorum.com/makale_298.htm adresinden ulaşılmıştır.

Yurdakul, C., Çağlayan, M.U. (1997). B*ilgi teknolojileri Türkiye için nasıl bir gelecek hazırlamakta.* Ankara:Türkiye İş Bankası Kültür Yayınları, Ankara.

Yurdagül, H. (2005). Ölçek geliştirme çalışmalarında kapsam geçerliği için kapsam geçerlik indekslerinin kullanılması. *XVI. Ulusal Eğitim Bilimleri Kongresi* içerisinde (s.1-6). Pamukkale Üniversitesi Eğitim Fakültesi. Denizli.

EKLER

EK A.1 Ankara Üniversitesi Etik Kurul Kararı

T.C.
ANKARA ÜNİVERSİTESİ REKTÖRLÜĞÜ
Genel Sekreterlik

Sayı : 85434274-50.04.04- 69318
Konu :

Ankara

13 Aralık 2013

EĞİTİM BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

İlgi : 20/09/2013 tarihli ve 98761816-100/40124 sayılı yazınız.

Enstitünüz doktora öğrencilerinden Can Güldüren'in "Yükseköğretim Kurumlarındaki Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Düzeylerinin Değerlendirilmesi" başlıklı tezi ile ilgili olarak Ankara Üniversitesi Etik Kurulunun 05/12/2013 tarihli toplantısında alınan 158/887 sayılı kararının bir örneği ilişikte gönderilmektedir.

Bilgilerinizi saygılarımla rica ederim.

Prof.Dr.Erkan İBİŞ
Rektör

EKLER :
1- Karar Örneği (1 sayfa)

Adres: Ankara Üniversitesi Rektörlüğü 06100 - Tandoğan / ANKARA Tel: 0 (312) 212 60 40-50 Faks: 0 (312) 212 60 49

ANKARA ÜNİVERSİTESİ
ETİK KURULU
KARAR ÖRNEĞİ

Karar Tarihi : **05/12/2013**

Toplantı Sayısı : **158**

Karar Sayısı : **887**

887-Üniversitemiz Eğitim Bilimleri Enstitüsü doktora öğrencilerinden **Can Güldüren**'in "Yükseköğretim Kurumlarındaki Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Düzeylerinin Değerlendirilmesi" başlıklı tezine ilişkin 06/09/2013 tarihli "İnsan Üzerinde Yapılan Klinik Dışı Araştırmalar Başvuru Formu" Etik Kurulumuzca incelenmiştir.

Yapılan görüşmeler ve incelemeler sonucunda, **Can Güldüren**'in "Yükseköğretim Kurumlarındaki Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Düzeylerinin Değerlendirilmesi" başlıklı tezinin, araştırma protokolüne uyulmak koşuluyla, uygulanmasının etik açıdan uygun olduğuna oybirliği ile karar verildi.

ASLININ AYNIDIR
05/12/2013
Aynur AKAY
Genel Sekreterlik Şube Müdürü

EK A.2 Uygulama İzin Yazıları

T.C.
ANKARA ÜNİVERSİTESİ REKTÖRLÜĞÜ
Öğrenci İşleri Daire Başkanlığı

Sayı : 14267719-302.99/67374 07.12.2013
Konu : Can GÜLDÜREN'in uygulama izin yazısı hk.

EĞİTİM BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

İlgi : 28.10.2013 tarih ve 98761816-302.99/40788 sayılı yazınız.

Enstitünüz Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı/Eğitim Teknolojisi Doktora Programı öğrencisi Can GÜLDÜREN'in, Prof. Dr. Hafize KESER danışmanlığında yürüttüğü "Yükseköğretim Kurumlarındaki Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Düzeylerinin Değerlendirilmesi " konulu tez çalışması kapsamında Karadeniz Teknik Üniversitesi ve Niğde Üniversitesinde görevli öğretim elemanlarına Bilgi Güvenliği Farkındalık Düzeyi Belirleme Ölçeği uygulama isteği hakkında ilgili Üniversite Rektörlüklerinden alınan yazı örnekleri ilişikte sunulmuştur.

Bilgilerinizi ve gereğini saygı ile rica ederim.

Prof.Dr.Sibel Ayşıl ÖZKAN
Rektör a.
Rektör Yardımcısı

Ekler :
1 - Yazı örneği (1 sayfa)
2 - Yazı örneği (1 sayfa)

Not: 5070 sayılı Elektronik İmza Kanununu gereği bu belge elektronik imza ile imzalanmıştır.

Tandoğan Yerleşkesi Dögol Caddesi 06100 Tandoğan/Ankara /ANKARA
Telefon No: 0312 215 90 01 Belge Geçer No: 0312 223 43 67
e-posta: auogrisl@ankara.edu.tr internet adresi: -

Ayrıntılı bilgi için:
S.ARSLAN
MEMUR

KARGC

T.C.
NİĞDE ÜNİVERSİTESİ REKTÖRLÜĞÜ
Öğrenci İşleri Daire Başkanlığı

Sayı: 69972237/399/1773 26/11/2013
Konu: Can GÜLDÜREN' in uygulama izin yazısı

ANKARA ÜNİVERSİTESİ REKTÖRLÜĞÜNE
(Öğrenci İşleri Daire Başkanlığı)

İlgi: Ankara Üniversitesi Rektörlüğü Öğrenci İşleri Daire Başkanlığının 08/11/2013 tarih ve 14267719-302.99/58645 sayılı yazısı.

Üniversiteniz Eğitim Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı/Eğitim Teknolojisi Doktora Programı öğrencisi Can GÜLDÜREN' in Prof. Dr. Hafize KESER danışmanlığında yürüttüğü **"Yükseköğretim Kurumlarındaki Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Düzeylerinin Değerlendirilmesi"** konulu tez çalışması kapsamında Üniversitemizde görevli öğretim elemanlarına Bilgi Güvenliği Farkındalık Düzeyi Belirleme Ölçeğini uygulama isteği, Üniversitemiz Fen-Edebiyat Fakültesi Dekanlığınca ve Niğde Zübeyde Hanım Sağlık Hizmetleri Meslek Yüksekokulu Müdürlüğünce uygun görülmemiş olup diğer birimler tarafından uygun görülmüştür.

Bilgilerinize arz ederim.

Prof. Dr. Murat ALP
Rektör a.
Rektör Yardımcısı

Bu belge 5070 sayili Kanun'a uygun olarak E-imza ile imzalanmistir.
Evrakin E-imzali aslina http://eimza.nigde.edu.tr/eimza/default.aspx linkinden (x2m6bVt4) koduyla erisebilirsiniz

Niğde Üniversitesi Öğrenci İşleri Daire Başkanlığı Merkez Yerleşke Bor Yolu Üzeri 51240 - Niğde
Tel: 0388 225 27 00 Belgeç: 0388 225 27 01 e-posta: ogrenci@nigde.edu.tr

T.C. KARADENİZ
TEKNİK ÜNİVERSİTESİ
Rektörlük

KARADENIZ
TECHNICAL UNIVERSITY
Rector's Office

GENEL SEKRETERLİK
Öğrenci İşleri Daire Başkanlığı

Sayı/Ref : 76127911/ 595/2336
Konu/Subj. : Tez Çalışması

22/11/2013

T.C.
ANKARA ÜNİVERSİTESİ REKTÖRLÜĞÜ
(Öğrenci İşleri Daire Başkanlığı)

İLGİ: 08.11.2013 gün ve 14267719-302.99/58645 sayılı yazınız;

Üniversiteniz Eğitim Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Anabilim Dalı Eğitim Teknolojisi Doktora Programı öğrencilerinden Can GÜLDÜREN' in; **"Yükseköğretim Kurumlarındaki Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Düzeylerinin Değerlendirilmesi"** konulu tez çalışması kapsamında hazırlamış olduğu **"Bilgi Güvenliği Farkındalık Düzeyi Belirleme"** ölçeğini Üniversitemiz Eğitim Bilimleri Enstitüsünde görev yapan öğretim elemanlarına uygulama isteği uygun görülmüştür.

Bilgilerinizi rica ederim.

Prof.Dr.Hikmet ÖKSÜZ
Rektör a.
Rektör Yardımcısı

61080 - Trabzon / TÜRKİYE
TEL.:+90 (462) 377 30 00 FAX: +90 (462) 325 79 73 E-mail:head@jbsd.ktu.edu.tr Web: www.ktu.edu.tr

Evrak Tarih ve Sayısı: 07/02/2014-11542

T.C.
GAZİ ÜNİVERSİTESİ
Personel Daire Başkanlığı

Sayı : 51894716-903.07.01-
Konu : Can GÜLDÜREN

SAĞLIK BİLİMLERİ FAKÜLTESİ DEKANLIĞINA

İlgi : 31.01.2014 tarih ve 9464 sayılı yazımız.

Ankara Üniversitesi Eğitim Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Anabilim Dalı Eğitim Teknolojisi Doktora Programında "Yükseköğretim Kurumlarındaki Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Düzeylerinin Değerlendirilmesi" isimli tez çalışmasını yürüten Can GÜLDÜREN'in konuya ait anket çalışmasını Fakültenizde görevli Öğretim Elemanlarına uygulamak istemesi Rektörlüğümüzce uygun görülmüştür.

Bilgilerinizi ve gereğini rica ederim.

Prof.Dr. Süleyman BÜYÜKBERBER
Rektör

Gazi Üniversitesi Rektörlüğü Personel Daire Başkanlığı 06500 Teknikokullar / Ankara
Tel:0 (312) 202 24 00 Faks:0 (312) 215 20 34
E-Posta :personel@gazi.edu.tr Web Adresi :http://personel.gazi.edu.tr/

EK B. Bilgi Güvenliği ve Farkındalık Web Sitesi Değerlendirme Formu

1. Bilgi güvenliği farkındalığı ile ilgili tasarlanmış olan çoklu ortam materyalleri ile web sitesinin kullanımının size faydalı olduğunu ve katkı sağladığını düşünüyor musunuz?

2. Bilgi güvenliği farkındalığı ile ilgili tasarlanmış olan çoklu ortam materyalleri ile web sitesinin kullanımında ne tür zorluklar yaşadınız?

3. Tasarlanmış olan çoklu ortam materyalleri ile web sitesi sizce hangi tür alt konularla desteklenmelidir?

4. Tasarlanmış olan çoklu ortam materyalleri ile web sitesinin kullanılabilirliğini 100 puan üzerinden değerlendirecek olsanız kaç puan verirsiniz? Neden bu puanı verdiğinizi kısaca açıklayınız.

5. Tasarlanmış olan çoklu ortam materyalleri ile web sitesini kullanmaktan memnun musunuz? Nedenleri ile birlikte açıklayınız.

6. Size göre tasarlanmış olan çoklu ortam materyalleri ile web sitesinde eksik olan özellikler nelerdir? varsa bu konuyla ilgili önerilerinizi yazınız.

EK C. Bilgi Güvenliği ve Farkındalık Web Sitesi Kullanım Kılavuzu

Günümüzde kurumlar ve bireylerin sahip olduğu en değerli varlıkları olan bilginin; "gizlilik", "bütünlük" ve "erişilebilirlik" nitelikleri bakımından sürekli korunması gerekmektedir.

Korunma bir takım fiziksel ve sistemsel önlemlerin yanında bireylerin bilgi güvenliğine ilişkin tehdit ve risklerden, kurum bilgi güvenlik politika ya da kurallarından haberdar olması, bu tehditlere nasıl karşı koyabileceği, olası riskleri mümkün olabilecek en düşük risk düzeyinde nasıl tutabileceği konusunda bilgilenmesiyle mümkün olabilir.

Güvenliğin en zayıf halkası olarak da kabul edilen insan faktörü üzerinde çeşitli farkındalık programları uygulanması gerekmektedir. Bu programların en başında ise bilgi güvenliği farkındalık eğitimi yer alır.

Bu web sitesi; bilgi güvenliği temel farkındalık eğitimi içinde yer alması gereken ana konuları (Genel Güvenlik, Saldırı ve Tehditler, E-posta ve İletişim, Mobil Cihazlar, Mahremiyet, Güvenli Gezinme, Yazılım ve Uygulamalar) içeren temel bir bilgi güvenliği farkındalık eğitim örneği sunmayı amaçlamaktadır. "Bilgi Güvenliği ve Farkındalık" Web Sitesi Ana Sayfası ekran görüntüsü Şekil EK C.1'de sunulmaktadır.

Şekil EK C.1. "Bilgi Güvenliği ve Farkındalık" Web Sitesi Ana Sayfası

Bilgi güvenliği farkındalık düzeyini artırmak maksadıyla hazırlanmış olan web sitesinde sunulan içeriğe ulaşmak için sitenin alt orta bölümünde bulunan "BGF Eğitimi için lütfen tıklayınız." metnini tıklayınız. Bu işlem sonucunda tarayıcınızın ekranında yeni bir sekme olarak çeşitli çoklu ortam materyallerinin kısa yollarını gösteren, "**BGF Eğitimi ve Yardımcı Kaynaklar**" başlığına sahip web sayfası açılacaktır. Açılacak olan sayfanın ekran görüntüsü Şekil EK C.2'de sunulmaktadır.

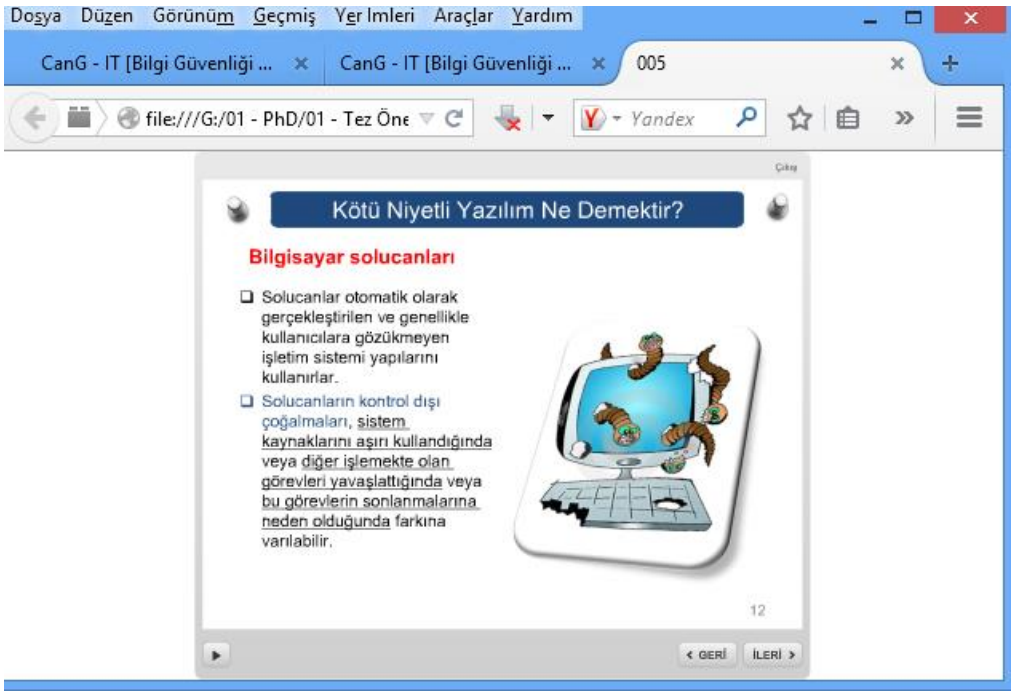
Şekil EK C.2. "BGF Eğitimi ve Yardımcı Kaynaklar" Ana Sayfası

Bu bölümde bilgi güvenliği ile ilgili hazırlanmış olan sunular, çeşitli konularda derlenmiş olan bilgi notları, flash animasyonla hazırlanmış olan 87 ayrı bölümden oluşan ve yaklaşık 50 dakikalık "**Güvenlik Eğitimi Videoları**" modülü ile "**Şifre Güç Ölçer**" uygulaması ile şifre seçiminde dikkat edilmesi gereken minimum gereksinimler uygulamalı olarak kullanıcıya anlık dönütler ile sunulmaktadır.

BGF Eğitimi ve Yardımcı Kaynaklar bölümünde; bilgi güvenliğinin temel tanıtımı, bilgi güvenliğini gelişim süreci, bilgi güvenliği süreçleri, bilgi güvenliğinin neden bu kadar önemli olduğu, bilgi güvenliği hakkında yanlış bilinenler, bilgi güvenliğinde kullanıcı olarak sorumluluklar, bilgi ve bilgi güvenliğinde insan unsurunun önemi, Bilgi ve iletişim (BiT) teknolojilerinde yaşanan hızlı gelişime bağlı olarak bilişim korsanlığının kısa tarihçesi, BiT gelişmeyle beraber hayatımıza giren kötü niyetli yazılımlar, kötü niyetli yazılımların tespit ve önleme yöntemleri, casus yazılımlar ve kullanılan teknikler, son kullanıcı lisans sözleşmeleri, en zayıf halka olarak insan unsuru kullanılarak gerçekleştirilen sosyal mühendislik saldırıları, kişisel veri kavramı ve tarihsel gelişimi, bilgisayara giriş güvenliği, çocuklar için güvenli internet vb. konu başlıklarında hazırlanmış olan sunu bilgi notlarına ilgili konu başlığını tıklayarak ulaşabilirsiniz.

Hazırlanan sunu ve yardımcı kaynaklardan "Kötü Niyetli Yazılım (Malware) Ne Demektir" bağlantısına tıklandığında Şekil EK C.3'tekine benzer bir sekme tarayıcınızın sekmesinde açılacaktır. Açılan ekran üzerinde Powerpoint ile hazırlanmış olan içerik sunulmaktadır. Ekranın sol alt kösesinde bulunan "**durdur/oynat**" tuşu sayfaları incelemek ve okuma süresini uzatmak için tasarlanmıştır. Ekranın sağ alt

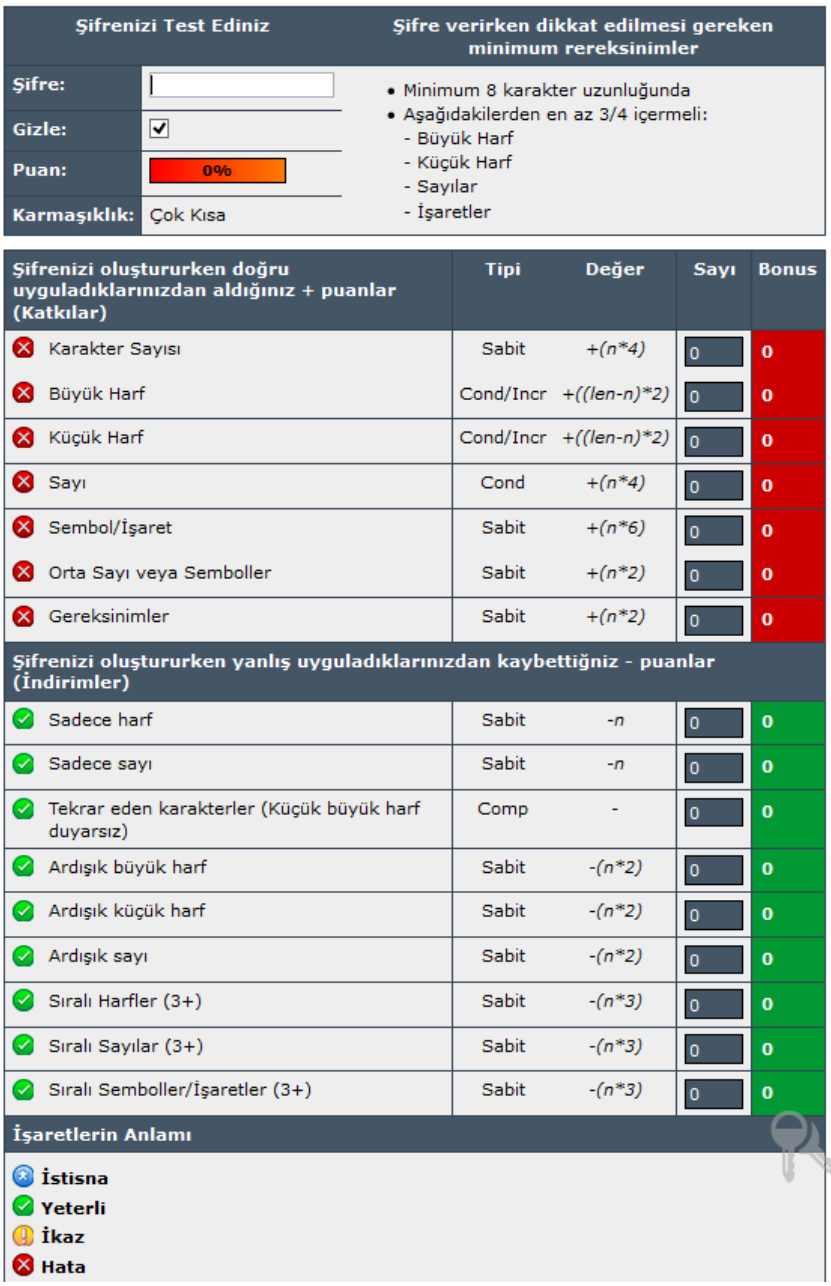
köşesinde bulunan "**geri/ileri**" tuşu sayfalar arasında gezinmek için tasarlanmıştır. İncelenen içerikle ilgili çalışmanız tamamlandığında sağ üst köşede bulunan "**çıkış**" tuşu açık olan tarayıcı sekmesinin kapatılması için tasarlanmıştır.



Şekil EK C 3. "Kötü Niyetli Yazılım (Malware) Ne Demektir" Sunusu

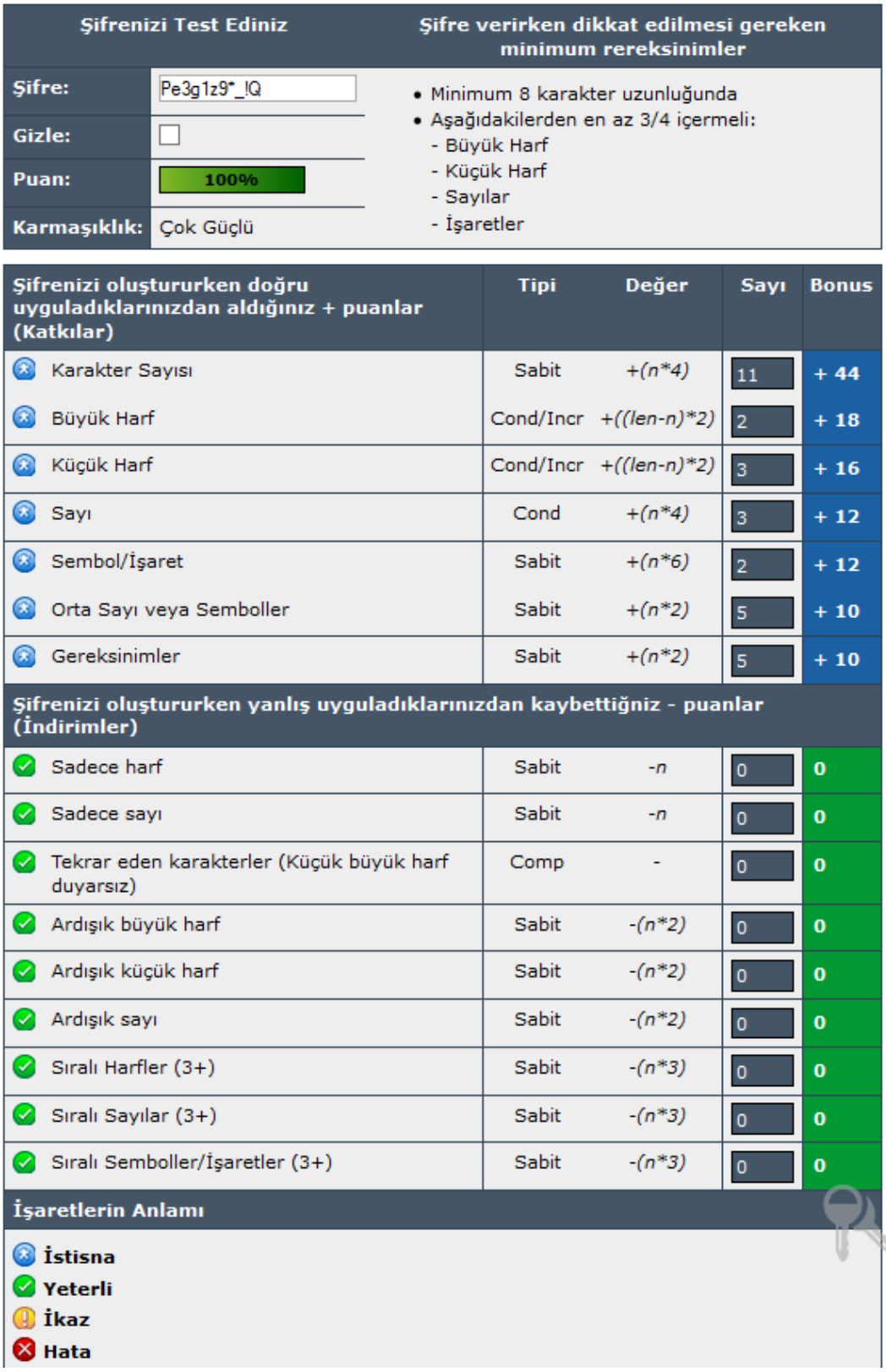
Sunu ve yardımcı kaynaklar bölümünde bulunan "**Şifre Güç Ölçer ile şifrelerinizi test edin**" bağlantısına tıklandığında Şekil EK C.4'te ekran görüntüsü sunulan içeriğin olduğu bir sekme tarayıcınızın sekmesinde açılacaktır.

Uygulama ile şifre oluştururken dikkat edilmesi gereken minimum gereksinimler ile büyük harf, küçük harf, sayı ve işaretler ile oluşturulan şifrelerde dikkat edilmesi gereken hususlar kontrol edilmektedir. Oluşturduğunuz şifrenin daha güçlü olması gereken için "**dikkat edilmesi gereken hususlar** " uygulama tarafından size anında dönüt olarak verilmektedir. Ayrıca oluşturduğunuz şifrenizin "**karmaşıklığı**" ile size önerilen kurallara uymaktan dolayı aldığınız "**puan**" uygulama tarafından hesaplanarak anında size gösterilmektedir.



Şekil EK C 4. "Şifre Güç Ölçer" Uygulaması Ekran Görüntüsü

Uygulama üzerinde bulunan "**Gizle**" tiki kullanılarak oluşturulan şifre üzerinde inceleme yapmak ve dikkat edilmesi gereken kuralları pekiştirmek için kullanılan alfa nümerik karakterleri görmek mümkün olmaktadır. Uygulama'nın açıldığı sekmede şifre seçiminde yapılan hatalar, güçlü şifre ne demektir, nasıl oluşturulur, hatırlanması kolay ve güçlü şifre önerileri, şifrelerin korunması başlıklarında kısa kısa bilgiler sunulmaktadır. Şekil EK C.5'te bütün kuralların uygulandığı güçlü bir şifre örneği sunulmaktadır.



Şifrenizi Test Ediniz		Şifre verirken dikkat edilmesi gereken minimum rereksinimler
Şifre:	Pe3g1z9*_!Q	• Minimum 8 karakter uzunluğunda • Aşağıdakilerden en az 3/4 içermeli: - Büyük Harf - Küçük Harf - Sayılar - İşaretler
Gizle:	☐	
Puan:	100%	
Karmaşıklık:	Çok Güçlü	

Şifrenizi oluştururken doğru uyguladıklarınızdan aldığınız + puanlar (Katkılar)	Tipi	Değer	Sayı	Bonus
Karakter Sayısı	Sabit	+(n*4)	11	+ 44
Büyük Harf	Cond/Incr	+((len-n)*2)	2	+ 18
Küçük Harf	Cond/Incr	+((len-n)*2)	3	+ 16
Sayı	Cond	+(n*4)	3	+ 12
Sembol/İşaret	Sabit	+(n*6)	2	+ 12
Orta Sayı veya Semboller	Sabit	+(n*2)	5	+ 10
Gereksinimler	Sabit	+(n*2)	5	+ 10
Şifrenizi oluştururken yanlış uyguladıklarınızdan kaybettiğiniz - puanlar (İndirimler)				
Sadece harf	Sabit	-n	0	0
Sadece sayı	Sabit	-n	0	0
Tekrar eden karakterler (Küçük büyük harf duyarsız)	Comp	-	0	0
Ardışık büyük harf	Sabit	-(n*2)	0	0
Ardışık küçük harf	Sabit	-(n*2)	0	0
Ardışık sayı	Sabit	-(n*2)	0	0
Sıralı Harfler (3+)	Sabit	-(n*3)	0	0
Sıralı Sayılar (3+)	Sabit	-(n*3)	0	0
Sıralı Semboller/İşaretler (3+)	Sabit	-(n*3)	0	0

İşaretlerin Anlamı

İstisna
Yeterli
İkaz
Hata

Şekil EK C 5. Bütün Kuralların Uygulandığı Güçlü Bir Şifre Örneği Ekran Görüntüsü

Sunu ve yardımcı kaynaklar bölümünde bulunan "**Güvenlik Eğitimi Bölümleri**" altındaki bağlantılara tıklandığında Şekil EK C.6'da örnek ekran görüntüsü gösterilene benzer içeriğin olduğu bir sekme tarayıcınızın sekmesinde açılacaktır.

Şekil EK C 6. "Güvenlik Eğitim Videoları" Ekran Görüntüsü

Açılan sekme üzerinde toplamda 12-15 arasında değişen bölümden oluşan flash animasyonla hazırlanmış güvenlik eğitimi seti konu bütünlüğü içerisinde ve bir akış sırası ile sunulmaktadır. Her bir flash animasyonu aktif hale getirmek için "**konu başlığı**" farenin sol tuşu ile tıklamak yeterlidir. Seçilen video ekranın ortasında oynatılacaktır. Bir sonraki konuya geçmek içim sonraki konu başlığı tıklanacaktır. Açık olan sekmedeki konular tamamlandığında "**Sonraki Sayfa**" tuşuna tıklanarak seyredilmek istenen ilgili bölüm ile devam edilebilecektir. Sayfalar arasında gezinti ve sayfa içerisindeki rastgele yöntem ile de gezilebilir. "Güvenlik Eğitim Videoları" yaklaşık 50 dakikalık bir süreyi kapsamaktadır. Şekil EK C.7'de örnek ekran görüntüsü sunulmaktadır.

Şekil EK C 7. "Önlemler-II" Konu Başlığına Tıklandığında Açılan Örnek Ekran Görüntüsü

Teşekkürler

EK D. Bilgi Güvenliği Farkındalık Ölçeği ve Alt Boyutları Kapsam Geçerliği Analiz Çalışmaları

Çizelge EK.D.1'de kapsam geçerlik oranlarının elde edilmesine ilişkin kullanılan bilgi güvenliği farkındalığı alt boyutları ve madde sayısı ile kapsam geçerlik indeksi ve alan uzman sayısı verilmiştir.

Çizelge EK D.1

BGFÖ Alt Boyutları ve Madde Sayıları.

Alt Boyut	Madde Sayısı
01. Genel Güvenlik	34
02. Saldırı ve Tehditler	21
03. E-posta ve İletişim	8
04. Mobil Cihazlar	8
05. Mahremiyet	8
06. Güvenli Gezinme	6
07. Yazılım ve Uygulamalar	5
	90

Uzman Sayısı	**23**
Kapsam Geçerlik Ölçütü	**0.39**

Toplam 23 alan uzmanın maddelere ilişkin belirtmiş oldukları görüşler üzerinden, yöntem bölümünde izah edilen Lawsh tekniğiformülü yardımı ile kapsam geçerlik oranları elde edilmiştir. Daha sonra, bu oranların istatistiksel olarak anlamlılığı Veneziano ve Hooper (1997) tarafından hazırlanan α=0,05 anlamlılık düzeyinde Kapsam Geçerlik Oranları (KGO) için minimum değerler ile (KGO23=0,39) karşılaştırılarak belirlenmiştir. Ölçeğin bütününe ilişkin kapsam geçerlik indeksi de yine aynı değerler ile karşılaştırılmıştır.

Kapsam geçerlik indeksi (KGO), α =0,05 düzeyinde anlamlı olan ve nihai forma alınacak maddelerin toplam KGO ortalamaları üzerinden elde edilir. Eğer ölçülmek istenilen özellik birden fazla boyutta toplanmış ise her bir boyut için KGO elde edilmelidir. Çizelge EK D 1'de 7 boyut söz konusu olduğu varsayımı ile KGO>0,39 olduğundan ölçek istatistiksel olarak anlamlı olduğu söylenebilir. KGO değerleri her bir alt boyut için geçerli olup, her bir alt boyut için, alt boyutta yer alan maddeler dikkate alınarak elde edilmektedir. Yapılan işlemler ve kapsam geçerlilik indekslerine ait hesaplanan değerler Çizelge EK D.2 ile Çizelge EK D.9 arasında özetlenmiştir.

Çizelge EK D.2
BGFÖ Genel Güvenlik Alt Boyutu ve Madde KGO'ları.

Genel Güvenlik Madde Nu.	Gereksiz	Gerekli	Gerekli ancak düzeltilmeli	Kapsam Geçerlik Oranları	Genel Güvenlik Madde Nu.	Gereksiz	Gerekli	Gerekli ancak düzeltilmeli	Kapsam Geçerlik Oranları
1	2	17	4	0.48	1	2	21		0.83
2	2	15	6	0.30	4	0	23		1
3	3	16	4	0.39	6	1	22		0.91
4	0	21	2	0.83	12	1	22		0.91
5	4	16	3	0.39	13	1	22		0.91
6	1	21	1	0.83	16	0	23		1
7	3	17	3	0.48	17	2	21		0.83
8	2	18	3	0.57	18	1	22		0.91
9	3	19	1	0.65	20	1	22		0.91
10	3	19	1	0.65	21	2	21		0.83
11	6	11	6	-0.04	22	1	22		0.91
12	1	18	4	0.57	24	4	19		0.65
13	1	18	4	0.57	26	0	23		1
14	3	17	3	0.48	27	3	20		0.74
15	2	19	2	0.65	28	3	20		0.74
16	0	19	4	0.65	29	1	22		0.91
17	2	12	9	0.04	33	1	22		0.91
18	1	21	1	0.83	34	2	21		0.83
19	3	19	1	0.65	**Uzman Sayısı**				**23**
20	1	21	1	0.83	**Kapsam Geçerlik Ölçütü**				**0.39**
21	2	16	5	0.39	**Kapsam Geçerlik İndeksi**				**0.87**
22	1	14	8	0.22					
23	6	14	3	0.22					
24	4	16	3	0.39					
25	6	14	3	0.22					
26	0	16	7	0.39					
27	3	19	1	0.65					
28	3	18	2	0.57					
29	1	20	2	0.74					
30	2	17	4	0.48					
31	0	4	0	-0.65					
32	5	18	0	0.57					
33	1	21	1	0.83					
34	2	20	1	0.74					
Uzman Sayısı				**23**					
Kapsam Geçerlik Ölçütü				**0.39**					
Kapsam Geçerlik İndeksi				**0.49**					

Çizelge EK D.3

BGFÖ Saldırı ve Tehditler Alt Boyutu ve Madde KGO'ları.

Saldırı ve Tehditler Madde Nu.	**Gereksiz**	**Gerekli**	**Gerekli ancak düzeltilmeli**	**Kapsam Geçerlik Oranları**	**Saldırı ve Tehditler Madde Nu.**	**Gereksiz**	**Gerekli**	**Gerekli ancak düzeltilmeli**	**Kapsam Geçerlik Oranları**
1	1	21	1	0.83	1	1	22		0.91
2	1	19	3	0.65	2	1	22		0.91
3	0	22	1	0.91	3	0	23		1
4	0	22	1	0.91	4	0	23		1
5	1	20	2	0.74	5	1	22		0.91
6	0	23	0	1	6	0	23		1
7	2	20	1	0.74	7	2	21		0.83
8	1	21	1	0.83	8	1	22		0.91
9	0	23	0	1	9	0	23		1
10	0	23	0	1	10	0	23		1
11	1	21	1	0.83	11	1	22		0.91
12	3	20	0	0.74	13	2	21		0.83
13	2	18	3	0.57	14	0	23		1
14	0	22	1	0.91	15	1	22		0.91
15	1	21	1	0.83	16	1	22		0.91
16	1	19	3	0.65	18	1	22		0.91
17	4	18	1	0.57	19	2	21		0.83
18	1	22	0	0.91	Uzman Sayısı				**23**
19	2	19	2	0.65	Kapsam Geçerlik Ölçütü				**0.39**
20	2	21	0	0.83	Kapsam Geçerlik İndeksi				**0.93**
21	3	20	0	0.74					
Uzman Sayısı				**23**					
Kapsam Geçerlik Ölçütü				**0.39**					
Kapsam Geçerlik İndeksi				**0.80**					

Çizelge EK D.4

BGFÖ E-posta ve İletişim Alt Boyutu ve Madde KGO'ları.

E-posta ve İletişim Madde Nu.	Gereksiz	Gerekli	Gerekli ancak düzeltilmeli	Kapsam Geçerlik Oranları	E-posta ve İletişim Madde Nu.	Gereksiz	Gerekli	Gerekli ancak düzeltilmeli	Kapsam Geçerlik Oranları
1	1	20	2	0.74	1	1	22		0.91
2	1	22	0	0.91	2	1	22		0.91
3	1	21	1	0.83	3	1	22		0.91
4	3	20	0	0.74	4	3	20		0.74
5	5	18	0	0.57	6	1	22		0.91
6	1	22	0	0.91	7	2	21		0.83
7	2	21	0	0.83	8	1	22		0.91
8	1	19	3	0.65	**Uzman Sayısı**				**23**
Uzman Sayısı				**23**	**Kapsam Geçerlik Ölçütü**				**0.39**
Kapsam Geçerlik Ölçütü				**0.39**	**Kapsam Geçerlik İndeksi**				**0.88**
Kapsam Geçerlik İndeksi				**0.77**					

Çizelge EK D.5

BGFÖ Mobil Cihazlar Alt Boyutu ve Madde KGO'ları.

Mobil Cihazlar Madde Nu.	Gereksiz	Gerekli	Gerekli ancak düzeltilmeli	Kapsam Geçerlik Oranları	Mobil Cihazlar Madde Nu.	Gereksiz	Gerekli	Gerekli ancak düzeltilmeli	Kapsam Geçerlik Oranları
1	0	22	1	0.91	1	0	23		1
2	1	22	0	0.91	2	1	22		0.91
3	1	22	0	0.91	3	1	22		0.91
4	3	18	2	0.57	5	1	22		0.91
5	1	21	1	0.83	6	1	22		0.91
6	1	22	0	0.91	7	0	23		1
7	0	23	0	1	8	1	22		0.91
8	1	21	1	0.83	**Uzman Sayısı**				**23**
Uzman Sayısı				**23**	**Kapsam Geçerlik Ölçütü**				**0.39**
Kapsam Geçerlik Ölçütü				**0.39**	**Kapsam Geçerlik İndeksi**				**0.94**
Kapsam Geçerlik İndeksi				**0.86**					

Çizelge EK D.6

BGFÖ Mahremiyet Alt Boyutu ve Madde KGO'ları.

Mahremiyet Madde Nu.	**Gereksiz**	**Gerekli**	**Gerekli ancak düzeltilmeli**	**Kapsam Geçerlik Oranları**	**Mahremiyet Madde Nu.**	**Gereksiz**	**Gerekli**	**Gerekli ancak düzeltilmeli**	**Kapsam Geçerlik Oranları**
1	1	22	0	0.91	1	1	22		0.91
2	0	23	0	1	2	0	23		1
3	0	23	0	1	3	0	23		1
4	1	22	0	0.91	4	1	22		0.91
5	0	22	1	0.91	5	0	23		1
6	0	23	0	1	6	0	23		1
7	5	18	0	0.57	8	1	22		0.91
8	1	20	2	0.74	**Uzman Sayısı**				**23**
Uzman Sayısı				**23**	**Kapsam Geçerlik Ölçütü**				**0.39**
Kapsam Geçerlik Ölçütü				**0.39**	**Kapsam Geçerlik İndeksi**				**0.96**
Kapsam Geçerlik İndeksi				**0.88**					

Çizelge EK D.7

BGFÖ Güvenli Gezinme Alt Boyutu ve Madde KGO'ları.

Güvenli Gezinme Madde Nu.	**Gereksiz**	**Gerekli**	**Gerekli ancak düzeltilmeli**	**Kapsam Geçerlik Oranları**	**Güvenli Gezinme Madde Nu.**	**Gereksiz**	**Gerekli**	**Gerekli ancak düzeltilmeli**	**Kapsam Geçerlik Oranları**
1	3	19	1	0,65	1	3	20		0,74
2	2	21	0	0,83	2	2	21		0,83
3	0	22	1	0,91	3	0	23		1
4	3	18	2	0,57	5	0	23		1
5	0	21	2	0,83	6	5	18		0,57
6	5	16	2	0,39	**Uzman Sayısı**				**23**
Uzman Sayısı				**23**	**Kapsam Geçerlik Ölçütü**				**0,39**
Kapsam Geçerlik Ölçütü				**0,39**	**Kapsam Geçerlik İndeksi**				**0,83**
Kapsam Geçerlik İndeksi				**0,7**					

Çizelge EK D.8

BGFÖ Yazılım ve Uygulamalar Alt Boyutu ve Madde KGO'ları.

Yazılım ve Uygulamalar					Yazılım ve Uygulamalar				
Madde Nu.	**Gereksiz**	**Gerekli**	**Gerekli ancak düzeltilmeli**	**Kapsam Geçerlik Oranları**	**Madde Nu.**	**Gereksiz**	**Gerekli**	**Gerekli ancak düzeltilmeli**	**Kapsam Geçerlik Oranları**
1	1	22	0	0.91	1	1	22		0.91
2	3	18	2	0.57	2	3	20		0.74
3	2	21	0	0.83	3	2	21		0.83
4	2	21	0	0.83	4	2	21		0.83
5	1	22	0	0.91	5	1	22		0.91
Uzman Sayısı				**23**	**Uzman Sayısı**				**23**
Kapsam Geçerlik Ölçütü				**0.39**	**Kapsam Geçerlik Ölçütü**				**0.39**
Kapsam Geçerlik İndeksi				**0.81**	**Kapsam Geçerlik İndeksi**				**0.84**

Çizelge EK D.9

BGFÖ ve Alt Boyutları KGO'ları.

Alt Boyut	**Madde Sayısı**	**Kapsam Geçerlik Oranları**
01. Genel Güvenlik	18	0.87
02. Saldırı ve Tehditler	18	0.93
03. E-posta ve İletişim	7	0.88
04. Mobil Cihazlar	7	0.94
05. Mahremiyet	7	0.96
06. Güvenli Gezinme	5	0.83
07. Yazılım ve Uygulamalar	5	0.84
	67	
Uzman Sayısı		**23**
Kapsam Geçerlik Ölçütü		**0.39**
Kapsam Geçerlik İndeksi		**0.89**

EK E. Açımlayıcı Faktör Analizi Başlangıç Özdeğerleri

Çizelge EK E.1

Açımlayıcı Faktör Analizi Başlangıç Özdeğerleri.

	Başlangıç Özdeğerleri			**Toplam Faktör Yükleri**			**Faktör Yüklerinin Döndürülmüş Toplamları**		
Madde	**Toplam**	**Varyans %**	**Yığılmalı %**	**Toplam**	**Varyans %**	**Yığılmalı %**	**Toplam**	**Varyans %**	**Yığılmalı %**
1	32.73	48.85	48.85	32.73	48.85	48.85	13.01	19.42	19.42
2	3.61	5.38	54.23	3.61	5.38	54.23	12.06	18.00	37.42
3	2.42	3.62	57.85	2.42	3.62	57.85	5.00	7.47	44.89
4	2.02	3.01	60.86	2.02	3.01	60.86	3.89	5.80	50.69
5	1.45	2.17	63.03	1.45	2.17	63.03	3.48	5.19	55.88
6	1.32	1.97	65.00	1.32	1.97	65.00	3.11	4.64	60.52
7	1.18	1.77	66.77	1.18	1.77	66.77	2.42	3.61	64.13
8	1.11	1.66	68.42	1.11	1.66	68.42	2.03	3.03	67.16
9	1.07	1.60	70.02	1.07	1.60	70.02	1.71	2.56	69.71
10	1.03	1.54	71.56	1.03	1.54	71.56	1.24	1.85	71.56
11	0.94	1.40	72.96						
12	0.84	1.26	74.22						
13	0.80	1.19	75.41						
14	0.74	1.10	76.51						
15	0.72	1.07	77.58						
16	0.67	1.01	78.59						
17	0.66	0.98	79.57						
18	0.62	0.93	80.50						
19	0.60	0.90	81.40						
20	0.59	0.88	82.28						
21	0.56	0.83	83.11						
22	0.53	0.80	83.90						
23	0.51	0.76	84.66						
24	0.50	0.75	85.41						
25	0.49	0.73	86.14						
26	0.45	0.67	86.82						
27	0.43	0.65	87.46						
28	0.42	0.63	88.09						
29	0.40	0.60	88.69						
30	0.38	0.57	89.27						
31	0.37	0.56	89.82						
33	0.35	0.52	90.90						
34	0.34	0.50	91.40						
35	0.32	0.48	91.88						
32	0.37	0.55	90.38						

(devam ediyor)

Çizelge EK E.1 (devam)

Açımlayıcı Faktör Analizi Başlangıç Özdeğerleri.

	Başlangıç Özdeğerleri			Toplam Faktör Yükleri			Faktör Yüklerinin Döndürülmüş Toplamları		
Madde	**Toplam**	**Varyans %**	**Yığılmalı %**	**Toplam**	**Varyans %**	**Yığılmalı %**	**Toplam**	**Varyans %**	**Yığılmalı %**
36	0.31	0.46	92.34						
37	0.30	0.45	92.79						
38	0.30	0.45	93.23						
39	0.28	0.43	93.66						
40	0.27	0.40	94.06						
41	0.26	0.38	94.44						
42	0.24	0.36	94.80						
43	0.23	0.34	95.14						
44	0.23	0.34	95.48						
45	0.21	0.32	95.80						
46	0.20	0.31	96.11						
47	0.20	0.30	96.41						
48	0.19	0.28	96.69						
49	0.18	0.28	96.97						
50	0.17	0.26	97.23						
51	0.17	0.25	97.48						
52	0.16	0.25	97.73						
53	0.16	0.24	97.97						
54	0.15	0.23	98.19						
55	0.14	0.21	98.41						
56	0.14	0.21	98.62						
57	0.13	0.20	98.82						
58	0.12	0.18	99.00						
59	0.11	0.16	99.16						
60	0.11	0.16	99.32						
61	0.10	0.14	99.46						
62	0.09	0.13	99.59						
63	0.08	0.12	99.71						
64	0.06	0.10	99.81						
65	0.06	0.09	99.89						
66	0.05	0.07	99.96						
67	0.03	0.04	100.00						

EK F. Veri Toplama Aracı

I.BÖLÜM
(KİŞİSEL BİLGİLER)

1. Cinsiyetiniz?
( ) Erkek ( ) Kadın

2. Unvanınız?
( ) Prof. Dr. ( ) Öğr. Grv. Dr. ( ) Arş. Grv. ( ) Uzm. Dr. ( ) Diğer
( ) Doç. Dr. ( ) Öğr. Grv. ( ) Okutman Dr. ( ) Uzm.
( ) Yrd. Doç. Dr. ( ) Arş. Grv. Dr. ( ) Okutman ( ) Öğr. Pl.

3. Mesleki kıdeminiz?
( ) 1-5 Yıl ( ) 11-15 Yıl ( ) 21-25 Yıl ( ) 31-35 Yıl ( ) 41 ve üzeri
( ) 6-10 Yıl ( ) 16-20 Yıl ( ) 26-30 Yıl ( ) 36-40 Yıl

4. Fakülte-Bölüm / Enstitü / Meslek Yüksekokulu?
Yazıyla belirtiniz: …….

5. Kaç yıldır bilgisayar kullanıyorsunuz?
( ) 1-5 Yıl ( ) 11-15 Yıl ( ) 21-25 Yıl ( ) 31-35 Yıl ( ) 41 ve üzeri
( ) 6-10 Yıl ( ) 16-20 Yıl ( ) 26-30 Yıl ( ) 36-40 Yıl

6. Kaç yıldır internet kullanıyorsunuz?
( ) 1-5 Yıl ( ) 11-15 Yıl ( ) 21-25 Yıl ( ) 31-35 Yıl ( ) 41 ve üzeri
( ) 6-10 Yıl ( ) 16-20 Yıl ( ) 26-30 Yıl ( ) 36-40 Yıl

7. Bilgisayar kullanımıyla ilgili eğitim aldınız mı? ( ) Evet ( ) Hayır

8. Bir önceki soruya cevabınız “Evet” ise, bu eğitimi nerede aldınız?
( ) Lisansüstü eğitim ( ) Hizmet içi eğitim ( ) Diğer (Belirtiniz: .....)
( ) Lisans eğitimi ( ) Özel kurs

9. Bu eğitim içerisinde bilgi güvenliği ile ilgili konular yer alıyor muydu?
( ) Evet ( ) Hayır

10. Aldığınız eğitim içerisinde sunulan bilgi güvenliği ile ilgili konuları yeterli buluyor musunuz?
( ) Evet ( ) Hayır

II. BÖLÜM

(BİLGİ GÜVENLİĞİ FARKINDALIK DÜZEYİ BELİRLEME ÖLÇEĞİ)

Aşağıda bilgi güvenliği farkındalığına yönelik görüşlerinizi tanımlayan 34 madde bulunmaktadır. Aşağıdaki ifadelere ne derece katılıp-katılmadığınızı seçeneğin yanındaki kutuya (X) işareti koyarak belirtiniz. Lütfen her soruyu dikkatli okuyunuz ve boş madde bırakmayınız.

S.Nu.	Maddeler	Hiç Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Tamamen Katılıyorum
1	Bilgi güvenliğinin ne anlama geldiğini biliyorum.					
2	Bilgi güvenliği ile ilgili sorumluluklarımın ne olduğunu biliyorum.					
3	Kullandığım bilgi sistemlerinde tanımlanmış olan kuralları nasıl uygulayacağımı biliyorum.					
4	Bilgi sistemlerinde kullanılan virüs koruma yazılımını nasıl kullanacağımı biliyorum.					
5	Bilgisayarımdaki virüs koruma yazılımının gerçek zamanlı koruma (realtime protection) özelliğini kullanmaktayım.					
6	Bilgisayarımdaki virüs koruma yazılımının otomatik güncelleştirme yapmasını sağlayabilirim.					
7	Bilgisayarıma kötü niyetli kod (malicious code) bulaşıp bulaşmadığını anlayabilirim.					
8	Kötü niyetli yazılımlara (malware) karşı alınması gereken güvenlik tedbirlerini biliyorum.					
9	Aldatmaca (hoax) nedir biliyorum.					
10	Zincir e-postalara (chain e-mail) karşı nasıl hareket etmem gerektiğini biliyorum.					

S.Nu.	Maddeler	Hiç Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Tamamen Katılıyorum
11	Bilgisayarımda casus yazılım (spyware) olup olmadığını anlayabilirim.					
13	Bilgisayarıma casus yazılım yüklenmesini engelleme yöntemlerini biliyorum.					
13	Kimlik hırsızlığı (identity theft) nedir biliyorum.					
14	Kimlik hırsızlığına karşı alınması gereken güvenlik tedbirlerini biliyorum.					
15	Sahte virüs koruma yazılımının ne olduğunu biliyorum.					
16	Hizmet aksatma (Denial of Service - DoS) saldırısı nedir biliyorum.					
17	Kimlik avı (phishing) saldırısı nedir biliyorum.					
18	Sosyal mühendislik (social engineering) saldırısı nedir biliyorum.					
19	Sosyal mühendislik saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum.					
20	Siber zorbalık (cyberbullying) nedir biliyorum.					
21	Siber zorbalığa karşı kendimi nasıl koruyacağımı biliyorum.					
22	Siber zorbalığa karşı çocukları nasıl koruyacağımı biliyorum.					
23	Dijital imza (digital signature) nedir biliyorum.					

S.Nu.	Maddeler	Hiç Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Tamamen Katılıyorum
24	Şüpheli veya bilinmeyen kaynaklardan gelen özellikle eklentisi olan e-postaları açmanın taşıdığı riski biliyorum.					
25	E-posta gönderirken "Gizli" (BCC) alanının sağladığı avantajları biliyorum.					
26	İstenmeyen elektronik posta (spam) nedir biliyorum.					
27	İstenmeyen elektronik posta miktarını azaltmak için gerekli bilgiye sahibim.					
28	Sosyal ağ sitelerini (social networking sites) güvenli olarak nasıl kullanacağımı biliyorum.					
29	USB sürücülerini (USB drives) kullanırken dikkat edilmesi gereken hususları biliyorum.					
30	Taşınabilir cihazlara (portable devices) yönelik fiziksel güvenliği sağlamak ile ilgili dikkat edilmesi gereken konuları biliyorum.					
31	Taşınabilir cihazlara yönelik veri güvenliği ile ilgili dikkat edilmesi gereken konuları biliyorum.					
32	Kişisel mahremiyet nedir biliyorum.					
33	Çevrimiçi güvenli alışveriş yapmak için gerekli olan güvenlik tedbirlerini biliyorum.					
34	Mavidiş (Bluetooth) teknolojisi ile veri aktarımı konusunda bilgi sahibiyim.					

ÖZGEÇMİŞ

Ası ve Soyadı : Can GÜLDÜREN

Doğum Tarihi : 07 Aralık 1969

İletişim Bilgileri : Kazım Özalp Mah. Küçüksu Sok. Çakar Apt. No:13/6 Çankaya/ANKARA

E-Posta Adresi : cangulduren@yahoo.com

Öğrenim Durumu :

Derece	**Bölüm/Program**	**Üniversite**	**Yıl**
Y.Lisans	İşletme/Yönetim Organizasyon	Selçuk Üniversitesi	2005
Y.Lisans	BÖTE/Eğitim Teknolojisi	Ankara Üniversitesi	2004
Sertifika Programı	Bilgisayar Mühendisliği	Orta Doğu Teknik Üniversitesi	1998
Lisans	İşletme	K.H.O.	1991

İş Deneyimi :

Unvan	**Görev Yeri**	**Yıl**
Alb.	K.K.Loj.K.lığı Bilgi Sistemleri Yöneticiliği	2013- Devam Ediyor
Yb.-Alb.	TSK Sağ.K.lığı ASOS Proje Yöneticiliği	2009-2013
Ütğm.-Yb.	K.K..Per.Bşk.lığı YBS Proje Yöneticiliği	1998-2009
Tğm./Ütğm.	TSK'da Bl./Bt.larda Tk.K.lığı/Bt.Sb.lığı	1991-1997