

Bilgi Teknolojileri Kullanım Kùltürü ve Farkındalık Yöntemlerinin Geliştirilmesi

Bu tez Bilgi Güvenliđi Mühendisliđi'nde Tezli Yüksek Lisans Programının bir koşulu olarak

Faruk YAKARYILMAZ
tarafından

Fen Bilimleri Enstitüsü'ne
sunulmuştur.



Bu tezi okuduk, kapsam ve nitelik açısından Bilgi Güvenliđi Mühendisliđi alanında Yüksek Lisans derecesi için tümüyle uygun olduđu görüşüne vardık.

ONAYLAYANLAR:

Prof. Dr. Ensar Gül
(Tez Danışmanı)

.....
Ensar Gül

Dr. Oktay Adaher
(Tez Eş-danışmanı)

.....
Oktay Adaher

Prof. Dr. Selim Zaim

.....
Selim Zaim

Dr. Öğr. Üyesi Hüseyin Yüce

.....
Hüseyin Yüce

Bu tez İstanbul Şehir Üniversitesi, Fen Bilimleri Enstitüsü tarafından belirlenen tüm koşullara uygundur.

ONAY TARİHİ:

16 Kasım 2018

MÜHÜR/İMZA:



Yazarlık Beyanı

Ben, Faruk YAKARYILMAZ, başlığı, 'Usage Culture of Information Technologies and Development of Awareness Methods' olan tezin ve içinde sunulan bilgilerin şahsıma ait olduğunu beyan ederim. Ayrıca:

- Bu çalışmanın bütünü veya esası bu üniversitede Yüksek Lisans derecesi elde etmek üzere çalıştığım süre içinde gerçekleştirilmiştir.
- Daha önce bu tezin herhangi bir kısmı başka bir derece veya yeterlik almak üzere bu üniversiteye veya başka bir kuruma sunulduysa bu açık biçimde ifade edilmiştir.
- Başkalarının yayımlanmış çalışmalarına başvurduğum durumlarda bu çalışmalara açık biçimde atıfta bulundum.
- Başkalarının çalışmalarından alıntıladığımda kaynağı her zaman belirttim. Tezin bu alıntılar dışında kalan kısmı tümüyle benim kendi çalışmamdır.
- Esaslı yardım aldığım bütün kaynaklara teşekkür ettim.
- Tezde başkalarıyla birlikte gerçekleştirilen çalışmalar varsa onların katkısını ve kendi yaptıklarımı tam olarak açıkladım.

İmza:

Tarih:

16 Kasım 2018

Usage Culture of Information Technologies and Development of Awareness Methods

Faruk YAKARYILMAZ

Abstract

In recent years, due to technological developments, technology usage and information security in all segments of the society have manifested itself in various areas. Families who are the core of the society are not used in a technology culture and the awareness of information security is not fully provided brings many risks. For this reason, many studies have been carried out in the world and in Turkey. In this thesis, in order to develop a technology usage culture and information security awareness method in families, awareness trainings were conducted to parents on the subject in 120 schools in Üsküdar and a questionnaire survey was conducted on 2118 parents during the trainings. Survey results were analyzed by frequency and chi-square methods. According to the findings; 43% of the parents of social media users did not determine the age of social media use for their children. It was revealed that 66% of the parents who shared information publicly on social media did not have secure social media usage knowledge. According to the findings and literature survey, it has been shown that awareness methods can be developed for families in various ways. In Turkey, relevant institutions, civil society organizations and private sector are working hand to hand on this issue. The role of human in information security should not be forgotten, along with the technical solutions such as hardware and software.

Keywords: Information Security, Awareness, Technology Usage Culture, Parent, Child

Bilgi Teknolojileri Kullanım Kùltürü ve Farkındalık Yöntemlerinin Geliştirilmesi

Faruk YAKARYILMAZ

ÖZ

Son yıllarda teknolojik gelişmelere baęlı olarak toplumun tüm kesimlerinde teknoloji kullanımı ve bilgi güvenlięi çeşitli alanlarda kendini göstermektedir. Toplumun çekirdeęi olan ailelerde teknoloji bir kùltür dahilinde kullanılmaması ve bilgi güvenlięi farkındalıęının tam olarak saęlanmaması birçok riski beraberinde getirmektedir. Bu sebeple, dünyada ve ÷lkemizde birçok çalıřma yapılmaktadır. Bu tezde, ailelerde teknoloji kullanım kùltürü ve bilgi güvenlięi farkındalık yöntemi geliřtirmek için mevcut durum arařtırmasına ek olarak Üsküdar'daki 120 okulda konuyla ilgili olarak ebeveynlere yönelik farkındalık eęitimleri gerçekleştirilmiř, eęitim sırasında 2118 ebeveyn üzerinde anket arařtırması yapılmıřtır. Anket sonuçları frekans ve ki-kare yöntemleri ile analiz edilmiřtir. Bulgulara göre; sosyal medya kullanıcısı olan ebeveynlerin %43'ü çocuęuna sosyal medya kullanım yařı belirlemedi. Sosyal medyada herkese açık paylařım yapan ebeveynlerin %66'sı güvenli sosyal medya kullanım bilgisine sahip olmadığı ortaya çıkmıřtır. Bulgular ve literatür arařtırmalarına göre ailelerde çeşitli şekillerde farkındalık yöntemlerinin geliřtirilebileceęi açıklanmıřtır. Ülkemizdeki ilgili kurum, sivil toplum kuruluşları ve özel sektörün el birlięiyle bu konuda çalıřma yapması büyük önem arz etmektedir. Donanım ve yazılım gibi teknik çözümlerle beraber insanın bilgi güvenlięindeki rolü unutulmamalıdır.

Anahtar Sözcükler: Bilgi Güvenlięi, Farkındalık, Teknoloji Kullanım Kùltürü, Ebeveyn, Çocuk

Teşekkür

Çalışmalarım süresince bilgi ve desteğini esirgemeyen, tecrübelerini motive ederek aktaran hocalarım Prof. Dr. Ensar GÜL'e ve Dr. Oktay ADALIER'e, bütün sorularıma cevap verdiği ve zaman ayırdığı için Prof. Dr. Selim ZAIM'e şükran ve teşekkürlerimi sunarım.

Ders ve tez sürecinde sabrımı eksik etmeyen eşim Mürşide YAKARYILMAZ'a ve çocuklarıma şükranlarımı ve teşekkürlerimi sunarım.



İçindekiler

Yazarlık Beyanı	ii
Abstract	iii
Öz	iv
Teşekkür	v
Şekil Listesi	viii
Tablo Listesi	ix
1 Giriş	1
1.1 Amaç ve Kapsam	3
1.2 Tezin Sağladığı Faydalar ve Özgün Değer	4
2 Literatür Araştırması	5
3 Uygulama	14
3.1 Mevcut Durum Araştırması	15
3.1.1 Geçmiş Yaşam Analizi	15
3.1.2 Kuşaklar	16
3.1.2.1 X Kuşağı	17
3.1.2.2 Y Kuşağı	18
3.1.2.3 Z Kuşağı	20
3.1.3 Yeni Dünya ve Dijital Yaşam	20
3.1.4 Gerçekleşmiş Olaylar ve Örnekler	21
3.1.4.1 Bilgi Güvenliğine İlişkin Örnekler	21
3.1.4.2 BT Kullanım Kültürüne İlişkin Örnekler	25
3.1.4.3 Teknoloji Bağımlılığına ve Siber Zorbalığa İlişkin Örnekler	28
3.2 Hipotezlerin Belirlenmesi	29
3.3 Ana Kütle ve Örneklem Seçimi	29
3.4 Anket Sorularının Hazırlanması	30
3.5 Nicel Verilerin Toplanması	30
3.6 Anket Sonuçlarının Analizi	30
3.6.1 Çocuğun yaşı ile çocuğun evde internete girdiği ortamlar arasındaki ilişki (Hipotez 1)	35

3.6.2	Çocuğun cinsiyeti ile çocuğun internette geçirdiği süre arasındaki ilişki (Hipotez 2)	36
3.6.3	Çocuğun internette geçirdiği süre ile ebeveynin çocuğuna sosyal medya kullanım yaşı belirleyip belirlememesi arasındaki ilişki (Hipotez 3)	37
3.6.4	Ebeveynin güvenli sosyal medya kullanım bilgisi olup olmaması ile sosyal medyada yapılan paylaşımların gizliliği arasındaki ilişki (Hipotez 4)	38
3.6.5	Ebeveynin güvenli sosyal medya kullanım bilgisi olup olmaması ile ebeveynin daha önceden farkındalık eğitimi alması arasındaki ilişki (Hipotez 5)	39
3.6.6	Ebeveynin sosyal medyada yaptığı paylaşımların gizliliği ile ebeveynin çocuğuna sosyal medya kullanım kuralı belirleyip belirlememesi arasındaki ilişki (Hipotez 6)	40
3.6.7	Ebeveynin çocuğuna sosyal medya kullanım kuralı belirleyip belirlememesi ile ebeveynin çocuğuna sosyal medyada tanımadığını insanlarla iletişim kurmaması konusunda uyarıp uyarmaması arasındaki ilişki (Hipotez 7)	40
3.7	Bulguların Yorumlanması: Bilgi Teknolojileri Kullanım Kültürü ve Farkındalık Yöntemlerinin Geliştirilmesi	41
3.7.1	Çocuklarda BT Kullanım Kültürü ve Farkındalık Yöntemlerinin Geliştirilmesi	42
3.7.1.1	BT ve sosyal medya kullanım kültürü	42
	Siber zorbalık	42
	Sosyal medya üzerinden yanlış yönlendirme	45
	Teknoloji bağımlılığı	46
3.7.1.2	Bilgi güvenliği farkındalığı	49
3.7.2	Ebeveynlerde BT Kullanım Kültürü ve Farkındalık Yöntemlerinin Geliştirilmesi	50
3.7.2.1	BT ve sosyal medya kullanım kültürü	50
	İnternet yalanları	51
	Çocukların erken yaşta yanlış kullanım ile teknolojiye teslim edilmesi	53
	Bireyselleşen internet kuşağını bekleyen teknolojik tehditler	55
	Aile mahremiyeti	56
	Duygusal karışıklık ve umursamazlık	57
3.7.2.2	Bilgi güvenliği farkındalığı	58
	Sosyal mühendislik	58
	Siber saldırılar	59
	Kişisel verilerin korunması	60
4	Tartışma ve Sonuç	61
A	Anket	64
B	Hipotezler	66
	Kaynaklar	67

Şekil Listesi

3.1	Çalışmanın adımları.	14
3.2	Yüksek tutarlı fatura ile ortalama e-postası.	22
3.3	Sahte banka web sitesi ile ortalama örneği.	23
3.4	Kargo firmasından adres değişikliği formu ile adres bilgilerine erişim ortalaması.	23
3.5	Başlıklı kısa mesaj ile banka bilgileri ortalaması.	24
3.6	Kamu kuruluşlarının kişisel bilgileri açık etmesi örneği.	24
3.7	Kamu kuruluşundan açık edilen kişisel bilgiler.	24
3.8	Sosyal medyada kişisel bilgilerin açık edilmesi örneği.	25
3.9	Sosyal medyada dini değerler üzerinden yanlış yönlendirme örneği.	25
3.10	Sosyal medyada milli değerler üzerinden yanlış yönlendirme örneği.	26
3.11	Sosyal medyada kuruluşları hedef alan yanlış yönlendirme örneği.	27
3.12	İki kurumu hedef alan sahte belge ile yanlış yönlendirme örneği.	27
3.13	Fotoğrafta montaj ile devlet televizyonuna iftira ve algı oluşturma örneği.	28

Tablo Listesi

2.1	Çocukların evde internete girdiği ortamlar [1].	10
2.2	İnternet kullanım amacı [2].	11
2.3	Kamu çalışanlarının 8 odak alanındaki farkındalık seviyeleri [3].	11
2.4	Çocukların evde internete girdiği ortamlar [4]	12
3.1	Çalışmanın Hipotezleri	29
3.2	Frekans analizi sonuçları.	31
3.3	Frekans analizi sonuçları (devam).	32
3.4	Frekans analizi sonuçları (devam).	33
3.5	Çocuğun yaşı ile çocuğun evde internete girdiği oda arasındaki ilişki. . . .	35
3.6	Çocuğun cinsiyeti ile çocuğun internette geçirdiği süre arasındaki ilişki. . .	36
3.7	Çocuğun internette geçirdiği süre ile ebeveynin çocuğuna sosyal medya kullanım yaşı belirlemesi arasındaki ilişki.	37
3.8	Ebeveynin güvenli sosyal medya kullanım bilgisi olup olmaması ile sosyal medyada yapılan paylaşımların gizliliği arasındaki ilişki.	38
3.9	Ebeveynin güvenli sosyal medya kullanım bilgisi olup olmaması ile ebeveynin daha önceden farkındalık eğitimi alması arasındaki ilişki.	39
3.10	Ebeveynin sosyal medyada yaptığı paylaşımların gizliliği ile ebeveynin çocuğuna sosyal medya kullanım kuralı belirleyip belirlememesi arasındaki ilişki.	40
3.11	Ebeveynin çocuğuna sosyal medya kullanım kuralı belirleyip belirlememesi ile ebeveynin çocuğuna sosyal medyada tanımadığı insanlarla iletişim kurmaması konusunda uyarıp uyarmaması arasındaki ilişki.	41
A.1	Ebeveynlerde Teknoloji Kullanım Kültürü ve Bilgi Güvenliği Farkındalık Anketi.	64
A.2	Ebeveynlerde teknoloji kullanım kültürü ve bilgi güvenliği farkındalık anketi (devam).	65
B.1	Çalışmanın Hipotezleri	66

Bölüm 1

Giriş

Bilgi, bugüne kadar yapılmış bütün tanımların dışında; insanların nesnelere ve olaylar arasındaki birbirlerini etkileyen ve tetikleyen ilişkilerini anlamalarına hizmet eden, insanlığın nesnelere ve olaylar üzerindeki baskı ve gücünü artıran bir unsurdur.

İnsanoğlu var olduğu ilk zamandan bu yana sürekli bir değişim ve gelişim içerisinde. İnsanlığın gelişimi ise biriktirdiği, koruduğu bilgilerle devam etmiştir. Bu bilgilerin gizliliği, bütünlüğü ve erişilebilirliği her zaman önemli olmuştur.

İnternetin gelişimi ve yaygınlaşması ile artık hemen hemen her insanın dijital dünyada bir karşılığı oluşmuştur. Bu karşılık bazen bir vatandaşlık numarası bazen de bir metinsel ifade olarak karşımıza çıkmaktadır. Günümüz insanının bankacılıktan sosyal medyaya, resmi belgelere erişimden sinema bileti almaya kadar birçok ihtiyacını karşılayan teknolojilerin arkasında tümüyle mahrem veri ve bilgiler bulunmaktadır. Bu veri ve bilgiler; resmi düzenlemelerle, bilgiyi saklayan kuruluşların bilgi güvenliği politikalarıyla veya yüksek maliyetli teknolojik yatırımlarla korunmaya çalışılmaktadır. Çok yüksek maliyetli donanım ve yazılımlarla korunmaya çalışılan veri ve bilgiler insan faktörünün zayıflığı ile teknik bilgi ve uğraş gerektirmeden çalınabilmekte ve kişi/kurumlar aleyhine sonuçlara kadar kullanılabilir. Bu korunan bilgilere kötü niyetli taraflarca her zaman farklı yöntemlerle erişilmeye çalışılacaktır. Bu bilgileri korumada çalışan donanım ve yazılımları yöneten insan faktörünün en az kullanılan donanım ve yazılımlar kadar mükemmel olması gerekmektedir. Bu açıdan en büyük ve kıymetli mahrem bilgilerin sahiplerinden olan kamu kurumlarındaki çalışanların bilgi güvenliği farkındalığının yüksek olması ülkemiz ve toplumumuz açısından çok değerlidir.

Mahrem bilgilerin sadece şirket veya kuruluşlar tarafından değil, bilginin asıl sahibi olan kişilerce de korunması gerekmektedir. Bu yüzden toplumu oluşturan ailelerde bilgi güvenliği farkındalığının anne ve baba rolü üzerinden öğrenilmesi ve diri tutulması gerekmektedir. Anne babalarda bilgi güvenliği farkındalığı ne kadar ileri seviyede bir kültür olarak oluşursa gelecek nesillerimiz olan çocuklara aktarılması o kadar kolay ve faydalı olacaktır.

Farkındalık, herhangi bir konuda duyarlı, bilinçli olmak şeklinde ifade edilebilir. Bilgi güvenliği farkındalığı da sadece eğitimlerle sağlanabilecek bir olgu değildir. Topluma bu duyarlılığın kazandırılması için eğitimler ile beraber bu farkındalığı sürdürülebilir hale getirecek çeşitli yöntem ve materyallerin kullanılması gerekmektedir. Bu yüzden dünyada farkındalık eğitimleri yerine farkındalık programları düzenlenerek bilgi güvenliği alanında toplumun duyarlı hale getirilmesi için çalışmaların yapıldığı gözlenmektedir. Bu konuda özellikle üniversite ve standart belirleyen organizasyonlar tarafından rapor ve yönerge mahiyetinde yayınlar bulunmaktadır [5, 6].

Dünyada ve ülkemizde toplumun bilgi güvenliğini sağlamak üzere birçok kurum ve kuruluş yasal düzenlemelerin oluşturulması üzerine çalışmaktadır. Toplumun korumayı amaçlayan bu düzenlemelerin toplum tarafından öğrenilmesi ve bunlara karşı duyarlı davranması, yasaların uygulanışını toplumla bütünleştirecektir. Bu bütünleşme için en doğru yöntemlerden biri olarak, topluma bilgi güvenliği farkındalığının kazandırılması gerekli olduğu kanısına varılmıştır.

Ülkemiz toplumunun genelinde teknolojiye ve teknolojinin içinde dolaşan bilgileri korumaya yönelik doğru bir kültür bulunmamaktadır. Bilgi güvenliği kültürünün, toplumun farklı kesimlerine kazandırılması gerekmektedir. Teknoloji kullanımına ve tüketimine kolayca alışan toplumumuzda, doğru bilgi güvenliği kültürünün kazandırılması için birçok yöntem bulunmaktadır. Bu yöntemlerin toplumun farklı kesimlerinde yaş grupları, ihtiyaçlar ve tehditler bağlamında tartışılması, değerlendirilmesi ve sonuçlarının ölçülmesi günümüzde oldukça önemlidir.

Bilgi güvenliği kültürünün olmamasına ek olarak toplumumuzda teknoloji kullanım kültürünün yanlış şekillenmesinden dolayı teknoloji bağımlılığı, siber zorbalık ve sosyal medyanın zararlı tarafları, aile yapısının ve beraberinde toplumsal bozulmanın etkisini artıracak tahmin edilmektedir. Bu yüzden bilgi güvenliği farkındalık programlarına sosyal medyanın bilgi güvenliğini tehdit eden taraflarının eklenmesi gerekmektedir. Bu sayede olası siber zorbalık gibi olaylar engellenerek gençlerin daha huzurlu bir ortamda yetişmesi sağlanabilecektir. Ayrıca insanlar, yeterli farkındalık düzeyine sahip olmadığı için sosyal medya platformlarında paylaşılan yalan ve yanlış haberleri teyit etmeden birçok olumsuz duruma sebep olmaktadır. Günümüzde internet ortamları kolay ve uzaktan erişilebilen ortamlar olduğu için kolaylıkla yanlış bilgilerin söylendiği ve yayıldığı ortamlardır. İnsanlar bu ortamda kendilerini oldukları gibi değil, olmak istedikleri ya

da görünmek istedikleri gibi gösterebilmektedir. Gerçek ve sanal kişilikler arasında çok büyük farklar bulunmaktadır. Bu ortamda farklı amaçlarla birçok yalan içerik kolayca yayılabilmekte ve hatta toplumlar bu şekilde galeyana getirilebilmektedir. Bu tür içerikler, özellikle sosyal medya platformlarında farklı zamanlarda toplumsal ve manevi değerleri hedef alarak yayılmaktadır. Bilişim çağında yaşamamız bizlere birçok imkan sunmaktadır. Artık cebimizdeki bir telefon veya evimizdeki bir bilgisayar aracılığıyla tüm dünya ile hızlı bir şekilde iletişim kurabiliyoruz. Maalesef bilgi teknolojilerin bizlere sağladığı faydalar aynı zamanda bazı riskler taşımaktadır. Bu riskleri aşağıda kısaca sıralanmıştır.

- Teknolojiyi kullanan bir çocuk, dışarıdaki her türlü insanla ve grupla iletişime açıktır.
- Çocuklar, kötü niyetli sanal saldırılara hedef olduğunun farkında olamayabilir.
- Evlerdeki bilgisayarlar, tabletler ve telefonlar insanları dünyayı açtığı gibi, aileyi de dünyaya açık bir hedef haline getirebilir.
- Sanal dünyada mahremiyet sağlamak ve korumak, gerçek hayattaki kadar kolay değildir.
- Sanal ortamda çok kolay yalan yanlış bilgi oluşturulabilmekte ve bu da çok basit yöntemlerle yayılabilmektedir.
- Tüm dünyada aileleri etkileyen siber zorbalık adı altında yeni bir tehdit çıkmıştır.
- Teknoloji bağımlılığı, çocuğun çalışma motivasyonunu azaltma noktasında görülen en büyük problemler arasındadır.

Toplumumuzun bilgi güvenliği farkındalığına ve doğru teknoloji kullanım kültürüne sahip olması konusunda ulusal bir strateji geliştirilmemektedir. Milli bir bakış açısı ile bu durum değerlendirilmemektedir.

Bilgi kayıpları, teknoloji bağımlılığı, siber zorbalık ve sosyal medya zararlarının aile ve gençlik kesimlerinde doğru bir kültürün ve buna bağlı farkındalığın kazandırılması toplumumuz ve geleceğimiz açısından oldukça önemlidir. Bu çalışma kapsamında bahsi geçen konularda farkındalık yöntemlerinin geliştirilmesi, uygulanması, bu süreçte yaşanan güçlükler, anket sonuçları, değerlendirme ve sonuçlara yer verilmiştir.

1.1 Amaç ve Kapsam

Tez çalışması, Üsküdar'daki çocuk ve ebeveynlerde teknoloji kullanım kültürü ve bilgi güvenliği farkındalığındaki durumunu tespit etmeyi, farkındalık oluşturma yöntemi geliştirmeyi amaçlamaktadır. Farkındalık durumunun tespiti için yapılan eğitimler sırasında

ebeveynlere anket uygulanmış ve mevcut durum ortaya konmuştur. Ayrıca bu durumu etkileyen sebepler değerlendirilerek farkındalık oluşturma yöntemlerinin belirlenmesinde kullanılmıştır. Farkındalık oluşturmada kullanılacak yöntemlerin geliştirilmesi için Üsküdar ölçeğindeki mevcut durum ve eğitimlerle sağlanan ilerlemenin sonuçları kullanılmıştır. Bu bulgular, ulusal ölçekteki karşılığı ve ülkemizin her yerinde uygulanabilirliği göz önünde bulundurularak hedef kitlelerin farkındalığını geliştirmede kullanılmıştır.

Tez kapsamında, teknoloji kullanım kültürü ve bilgi güvenliği farkındalığındaki mevcut durumun sebep ve sonuçlarının tespitinde ailedeki kuşaklar arası ihtiyaçların analizi ve yorumlanması yapılmıştır. Farkındalık oluşturma yöntemlerinde kullanılacak faaliyetlerin kapsamı ve niteliği belirlenerek, ulusal çaptaki benzer çalışmalara öncülük edilmesi amaçlanmaktadır.

Bu çalışma, özellikle son yıllarda akıllı telefon tablet ve bilgisayarların daha erişilebilir olması, evlerde ve akıllı cihazlarda internet erişiminin her an mümkün olması nedeniyle ailelerin çokça zararını gördüğü, olumsuz olarak etkilendiği teknoloji bağımlılığı, özellikle çocukların maruz kaldığı siber zorbalık konularının yanı sıra bilgi güvenliği, sosyal mühendislik konularında da farkındalık oluşturmak ve bu tehditlere karşı alınabilecek genel tedbirler ile ilgili gerçekleştirilebilecek bilgilendirme çalışmalarını ve ilgili yöntemleri kapsamaktadır.

1.2 Tezin Sağladığı Faydalar ve Özgün Değer

Tez, ailelerde bilgi güvenliği farkındalığının artmasını ve teknoloji kullanım kültürünün doğru oluşturulmasını amaçlamaktadır. Bu durum ışığında, tezin sağladığı faydalar aşağıda açıklanmıştır.

- Toplumsal fayda olarak, belirli bir ilçede devlet okullarında çocukları olan tüm ebeveynleri kapsamı bakımından oldukça önemli ve değerlidir. Hedef kitle olarak eski ve köklü bir yerleşim yeri olan Üsküdar'da yaklaşık olarak 90.000 tekel ebeveyn (anne veya baba) bulunmaktadır.
- Toplumumuzun teknolojiye yanlış adapte olmasından kaynaklanan bilgi güvenliği sorunlarının, özellikle genç nesilde karşılaşılan teknoloji bağımlılığı ve siber zorbalık gibi örneklerinin çoğalması, farkındalık faaliyetlerini ve buna ilişkin geliştirilecek içeriği, yapılacak çalışmaları daha da değerli kılmaktadır.
- Farkındalık faaliyetleri kapsamında ölçülecek çeşitli durum tespiti ve değerler ile sonraki benzer çalışmalara altlık oluşturulacaktır.

Bölüm 2

Literatür Araştırması

Bu tez kapsamında; çocuk ve ebeveynlerin teknoloji kullanım kültürü ve bilgi güvenliği farkındalık yöntemlerinin geliştirilmesi üzerine bir araştırma yapılmıştır. Bu doğrultuda; ebeveynler, çocuk ve gençlerde güvenli internet ve sosyal medya kullanımı, bilgi güvenliği farkındalığı ile teknoloji kullanım kültürü konularında yapılmış bilimsel yayınlar incelenmiştir.

[7], 0-8 yaş aralığındaki çocukların ve ebeveynlerin internet ve mobil cihaz kullanımları, potansiyel ve maruz kaldıkları riskler üzerine bir çalışma yapmıştır. Bu çalışma kapsamında, kullandıkları teknolojiler vasıtasıyla maruz kaldıkları ve potansiyel riskler ile ebeveynlerin farkındalıkları ve başa çıkma stratejilerinin belirlenmesi araştırılmıştır. Erzurum'da yaşayan 0-8 yaş grubundaki 41 çocuk ve ebeveynleri ile görüşme ile elde edilen bulgulara göre; çocukların büyük bölümünün mobil cihazları ilk kez ebeveynlerinden gördükleri ve cihazlarda daha çok oyun oynama ve video izleme faaliyetlerinde buldukları tespit edilmiştir. Ebeveynlerin de mobil cihazları daha çok eğlence aracı olarak kullandıkları tespit edilmiştir. Araştırma sonucuna göre; ebeveynler, mobil cihazların çocuklar için birçok riski barındırdığının farkında olup bunlara karşı alınabilecek önlemler konusunda yetersiz kaldıkları ortaya çıkmıştır.

[8], ebeveynlerin bilgi güvenliği farkındalık durumlarına yönelik görüşlerinin belirlenmesi üzerine bir çalışma yapmıştır. Beşinci ve altıncı sınıf öğrencilerinin ebeveyni olan 91 ebeveyn üzerinde yapılan anket araştırması sonucunda elde edilen bulgulara göre; ebeveynlerin, çocuklarına bilgi güvenliğini sağlamak üzerine uyarılarda bulunduğu fakat somut olarak çocuklarına bilgi veremedikleri görülmüştür. Ayrıca, ebeveynlerin sosyal ağlardaki kişisel paylaşımlarda riskli davranışlarda buldukları da tespit edilmiştir. Çözüm önerisi olarak ebeveynlerin bu konularda hazırlanmış eğitimlerle bilinçlendirilebileceği ve çocuklarını yönlendirebileceği vurgulanarak, en önemli nokta olarak ebeveynlere

güvenli bilgi ve iletişim teknolojilerinde kullanma davranışlarının kazandırılması gerektiği ifade edilmiştir.

[9], İstanbul'daki 5 ortaokulda bulunan 497 kız, 307 erkek öğrenci üzerinde yaptığı çalışma ile siber zorbalık ile saldırganlık ilişkisini araştırmıştır. Araştırma sonucunda, siber zorbalık ile saldırganlık düzeyi arasında anlamlı ilişki olduğu saptanmıştır. Erkeklerin kız öğrencilere oranla daha fazla siber zorbalık ve saldırganlık düzeyine sahip olduğu, daha fazla siber mağduriyete uğradığı görülmüştür. Sınıf düzeyi arttıkça öğrencilerin siber zorbalık ve siber mağduriyet düzeyleri, saldırganlık düzeyleri ve saldırganlık alt boyutlarından sözel, fiziksel, dolaylı saldırganlık, öfke ve düşmanlık düzeyleri arttığı görülmüştür. Öğrencilerin akademik başarıları arttıkça siber zorbalık, siber mağduriyet ve saldırganlık düzeylerinin azaldığı görülmüştür. Ailesinin sosyoekonomik düzeyi düşük olan öğrencilerin siber mağduriyet düzeyinin ailesinin sosyoekonomik düzeyi yüksek olan öğrencilerin siber mağduriyet düzeyinden yüksek olduğu saptanmıştır. Ailesi düşük gelirli öğrencilerin saldırganlık düzeyi fazla olduğu belirlenmiştir. Baba eğitim düzeyi arttıkça siber zorbalık düzeyinin azaldığı saptanmıştır. Baba eğitim düzeyi arttıkça sözel saldırganlık ve öfkede saldırganlık düzeyi düşmektedir.

[10], Sivas il merkezinde bulunan 6 ortaokuldaki 779 öğrenci üzerinde yürüttüğü internet bağımlılığı ve siber zorbalık davranışları ile ilişkili değişkenleri incelediği çalışmada internet bağımlılığı davranışı ile cinsiyet ve internet kullanım yeri arasında bir ilişki olduğunu tespit etmiştir. İnternet bağımlılığı davranışının erkek öğrencilerde kız öğrencilere göre daha fazla olduğu görülmüştür. Evde ve internet kafede internet kullanan öğrencilerin okulda internet kullanan öğrencilere göre daha fazla internet bağımlılığı davranışı gösterdiği saptanmıştır. Siber zorbalık ile sınıf düzeyi, cinsiyet, evde bilgisayar varlığı ve internet kullanım yeri arasında bir ilişki olduğu saptanmıştır. 8. sınıf öğrencilerinin 7. sınıf öğrencilerine göre daha fazla siber zorbalık davranışı gösterdiği saptanmıştır. Erkek öğrencilerin kız öğrencilere göre daha fazla siber zorbalık davranışı gösterdiği saptanmıştır. İnternet kafede internet kullanan öğrencilerin evde ve okulda internet kullanan öğrencilere göre daha çok siber zorbalık davranışı gösterdikleri belirlenmiştir. Son olarak ortaokul öğrencilerinin siber zorbalık ile internet bağımlılığı davranışları arasında orta düzeyde pozitif ilişki olduğu saptanmıştır.

[11], İstanbul'daki 476 üniversite öğrencisi üzerinde yürüttüğü üniversite öğrencilerinin siber zorbalık ve siber mağduriyet düzeylerinin sosyal uyum ve bazı kişisel değişkenlere göre incelendiği çalışmada, sosyal uyum düzeyi ile siber zorbalık ve siber mağduriyet arasında anlamlı bir ilişki olduğunu ortaya koymuştur. Sosyal uyumu düşük düzeyde olan öğrencilerin siber zorbalık ve siber mağduriyet sıra ortalaması, sosyal uyumu orta ve yüksek olan öğrencilerin siber zorbalık ve siber mağduriyet sıra ortalamasından yüksek çıkmıştır. Sosyal uyumu orta düzeyde olan öğrencilerin siber zorbalık ve siber mağduriyet

sıra ortalaması, sosyal uyumu yüksek olan öğrencilerin siber zorbalık ve siber mağduriyet sıra ortalamasından yüksek çıkmıştır. Ayrıca erkek öğrencilerin siber zorbalık ve siber mağduriyet sıra ortalaması, kız öğrencilerin siber zorbalık ve siber mağduriyet sıra ortalamasından yüksek çıkmıştır. Anne-baba tutumuna göre öğrencilerin siber zorbalık puanlarının anlamlı olarak farklılık gösterdiği ortaya konmuştur. Ebeveyn tutumu otoriter baskıcı olanların siber zorbalık düzeyleri, tutarsız-dengesiz, demokratik-hoşgörülü, aşırı koruyucu ve son olarak ilgisiz olanların siber zorbalık düzeylerinden yüksek çıkmıştır. Araştırmaya göre ekonomik düzeyin siber zorbalık ve siber mağduriyet arasında anlamlı bir ilişki olmadığı tespit edilmiştir. Son olarak online ortamda kimliğini gizleyen öğrencilerin siber zorbalık ve siber mağduriyet düzeyleri, online ortamda kimliğini gizlemeyen öğrencilerin siber zorbalık ve siber mağduriyet düzeylerinden yüksek çıkmıştır.

[12], İstanbul ilinin Bağcılar ilçesindeki 5 resmi ortaokulun 6.,7.,8. sınıflarında eğitim gören 191'i kız, 118'i erkek olmak üzere 309 öğrenci üzerinde gerçekleştirdiği ortaokul öğrencilerinin siber zorbalık, siber mağduriyet ve insani değerleri arasındaki ilişkiyi incelediği çalışmada çeşitli bulgulara ulaşılmıştır. Erkek öğrencilerin kızlara göre daha fazla siber zorbalık yaptığı tespit edilmiştir. 8. sınıf öğrencilerinin, 6. sınıf öğrencilerine göre daha fazla siber zorbalık yaptığı tespit edilmiştir. İnterneti sosyal ağlar ve eğlence amaçlı kullanan öğrenciler ile interneti ders çalışmak için kullanan öğrenciler arasında anlamlı bir fark tespit edilerek, eğlence amaçlı kullananların siber zorbalık yaptığı bulgusuna ulaşılmıştır. Siber zorbalık durumları ile günlük internet kullanım süresi arasında anlamlı, pozitif yönde ve orta düzeyde bir ilişki olduğu bulunmuştur. Erkek öğrencilerin daha fazla siber mağdur oldukları tespit edilmiştir. 8. sınıf öğrencilerinin 6. sınıf öğrencilerine göre daha fazla siber mağduriyet yaşadıkları tespit edilmiştir. İnterneti sosyal ağlar ve eğlence amaçlı kullanan öğrenciler ile interneti ders çalışmak için kullanan öğrenciler arasında anlamlı bir fark tespit edilerek, eğlence amaçlı kullananların daha fazla siber mağduriyet yaşadığı bulgusuna ulaşılmıştır. Öğrencilerin siber zorbalık durumları ile siber mağdur olmaları arasında anlamlı, pozitif ve orta düzeyde bir ilişki olduğu tespit edilmiştir. Siber zorbalık durumu ile insani değer durumları incelenmiştir. Siber zorbalık durumu ile barışçı olma, saygı ve dürüstlük faktörleri ile dostluk/arkadaşlık ve hoşgörü faktörleri arasında anlamlı ve negatif yönde ilişkinin olduğu tespit edilmiştir.

[13], araştırma evrenini İstanbul ilinin Çekmeköy ilçesinde faaliyet gösteren 10 özel ve resmi okulda yer alan 779 öğrencinin (% 56,7'si kız, % 43,3'ü erkek) oluşturduğu ortaöğretim (lise) öğrencilerinin siber zorbalık ve internet saldırganlık düzeyleri ile sosyal medyaya ilişkin tutumlarını incelediği çalışmada çeşitli bulgulara ulaşılmıştır. Bu çalışmada erkek öğrencilerin kız öğrencilere göre siber zorbalık davranışları göstermeye daha yatkın olduğu tespit edilmiştir. Siber mağdur olma ile cinsiyet farklılığı arasında anlamlı bir farklılık bulunamamıştır. Araştırma evreninde bulunan öğrencilerin yaşları 14 ile 17'den büyük olarak açıklanmıştır. Öğrenci yaşları ile siber zorba olma ve siber mağdur olma

arasında anlamlı bir farklılık bulunmamaktadır. Araştırma evreninde bulunan öğrencilerin % 90,9'unun anne-babası birlikte, % 9,1'inin ise ayrı yaşamaktadır. Çalışmada, anne-babası ayrı yaşayan öğrencilerin siber zorba ve siber mağdur olma olasılıkları daha yüksek olduğu ifade edilmiştir. Öğrencilerin annelerinin eğitim seviyesinin siber zorba ve siber mağdur olma durumlarında belirleyici rol oynadığı ifade edilmiştir. Annesi ilkokul, ortaokul ve lise mezunu olan öğrencilerin siber mağdur olma durumunun daha yüksek olduğu ifade edilmiştir. Annelerde olduğu gibi babaların eğitimi durumu da öğrencilerin siber zorba ve siber mağdur olma durumu ile yakından alakalı olduğu tespit edilmiştir. Öğrencilerin babalarının eğitim durumları yükseldikçe siber zorba ve siber mağdur olma durumu azalmaktadır. Öğrencilerin % 88,4'ü bir sosyal medya platformuna üye iken % 11,6'sı herhangi bir sosyal medya üye değildir. Araştırma sonucunda sosyal medya üyeliği bulunan öğrencilerin siber mağdur olma düzeyleri daha yüksek olduğu tespit edilmiştir. Sosyal medya kullanım sıklığı ile öğrencilerin siber zorba ve siber mağdur olma durumları arasında yakın ilişki olduğu ifade edilmiştir. Sosyal medya kullanım sıklığı arttıkça siber zorba ve siber mağdur olma olasılığının arttığı ifade edilmiştir.

[14], araştırma evreni Afyonkarahisar ilinin Şuhut ilçesinde öğrenim gören 669 lise öğrencisinden oluşmaktadır. Ailedeki stres yaşantıları az olan öğrencilerin daha az siber zorbalık davranışı sergilediğini tespit etmiştir. Ailedeki koruyucu etkenleri yüksek düzeyde algılayan öğrenciler, siber zorbaca davranışlara daha az maruz kalmaktadır. Anne-baba tutumu demokratik olan öğrencilerin diğer öğrencilere göre daha az siber zorbalık davranışı sergilediği ve daha az siber mağduriyet yaşadığı tespit edilmiştir. Odasında internete bağlı bilgisayar olan öğrencilerin, odasında internete bağlı bilgisayar olmayan öğrencilere göre daha fazla siber zorbalık yaptığı ve daha fazla siber mağduriyet yaşadığı tespit edilmiştir. İnternet kullanımları ebeveynleri tarafından kontrol edilmeyen öğrencilerin, kontrol edilen öğrencilere göre daha fazla siber zorbalık yaptığı ve daha fazla siber mağduriyet yaşadığı tespit edilmiştir.

[15], Cumhuriyet Üniversitesi Eğitim Fakültesinde öğrenim gören farklı bölümlerdeki 487 öğrenciden oluşan araştırma evreninde yaşam boyu öğrenme argümanı olarak teknoloji bağımlılığı ve yaşama yansımaları araştırdığı çalışmada teknoloji bağımlılığına ait alt boyutlardan olan kontrol güclüğü ile cinsiyet arasındaki bir ilişki olduğunu tespit etmiştir. Buna göre, kız öğrencilerin erkek öğrencilere göre daha yüksek düzeyde kontrol güclüğü yaşadığı ortaya çıkmıştır. Okul öncesi öğretmenliği öğrencilerinin teknoloji bağımlılık seviyeleri, sınıf öğretmenliği öğrencilerine göre anlamlı derecede yüksek olduğu tespit edilmiştir. Ek olarak fen bilgisi öğretmenliği bölümü öğrencilerinin teknoloji bağımlılık seviyelerinin sınıf öğretmenliği öğrencilerine göre anlamlı derecede yüksek olduğu tespit edilmiştir.

[16] yaptığı çalışmada Avrupa Çevrimiçi Çocuklar (EU Kids Online) projesine dahil olan 23 ülke ve Türkiye'nin bulguları incelenerek, çocukların ve ebeveynlerinin internet kullanımları, çocukların internetteki faaliyetleri, karşılaştıkları riskler ve ebeveynlerin çocuklarının internet yaşantıları ile ilgili farkındalıkları araştırmıştır. Türkiye'deki araştırma verileri kentsel ve kırsal bölgelerde 2010 yılının Mayıs ve Haziran aylarında toplanmıştır. 9-16 yaş arası internet kullanan, Türkiye'den 1018 ve 23 ülkeden yaklaşık 23.000 çocuk ve ebeveyni ile yapılan görüşmeler sonucu elde edilen bulgulara göre; çocukların büyük kısmının internet kullanım becerilerinin yeterli olmadığı, birçok çevrimiçi riske maruz kaldığı tespit edilmiştir. Türkiye'deki ebeveynlerin internet kullanım oranlarının diğer ülkelere göre oldukça düşük olduğu ve çocuklarını internet risklerinden uzak tutmayı sağlayacak yeterli bilgiye sahip olmadıkları varılan bir başka sonuçtur.

[17] tarafından yapılan siber zorbalık ölçeğinin Türkçe 'ye uyarlanması çalışmasında İstanbul ilinin Pendik ilçesinde bulunan 633 lise öğrencisi üzerinde siber zorbalık araştırması yürütülmüştür. Bu kapsamda, erkek öğrencilerin kız öğrencilere göre daha fazla siber zorbalık eğilimi gösterdiği ve daha çok mağdur olduğu bulunmuştur. Kişisel internet bağlantısı olan öğrencilerin, kişisel internet bağlantısı olmayan öğrencilere göre daha çok mağdur oldukları tespit edilmiştir. İnternette gün içinde 1 saatten fazla zaman geçiren öğrencilerin, 1 saatten az zaman geçiren öğrencilere göre mağduriyetlerinin arttığı belirlenmiştir. Çalışmaya göre kız öğrencilerin, SMS ve sosyal iletişim ağları aracılığıyla erkeklere oranla daha fazla rahatsız edildiği tespit edilmiştir. Erkek öğrencilerin ise kız öğrencilere göre, e-posta, kişisel video, sanal oyunlar, site/forum aracılığıyla daha fazla rahatsız edildiği ortaya konmuştur. Çocukların % 35,6'sının internete girme süreleri, ebeveynleri ya da bir büyükleri tarafından denetlendiği, diğer % 64,4'lük kısmının denetlenmediği tespit edilmiştir. Yaklaşık olarak her üç öğrenciden ikisinin internete girme süreleri denetlenmediği ortaya çıkmaktadır. Çalışmada, kız öğrencilerin % 91,3'ü, erkek öğrencilerin % 74,3'ü interneti ders çalışmak ve ödev yapmak için kullandığı tespit edilmiştir. Kız öğrencilerin % 82,6'sı, erkek öğrencilerin % 78,8'i interneti sosyal ağlar için kullandıkları tespit edilmiştir.

[18] yaptığı çalışmada, Türkiye'deki çocukların %46'sı sosyal ağlarda kişisel bilgilerini korumaya yönelik kuralları bilmediğini ve bunun sonucu olarak gönderilerini, profil fotoğraflarını ve doğum tarihlerini herkese açık bir biçimde paylaştığını tespit etmiştir.

[19] tarafından Türkiye'deki ergen profilinin araştırıldığı çalışma sonucuna göre, internet üzerinden tanıştığı arkadaşları olan ergen oranı %36 iken bu yolla arkadaş edinmeyenlerin oranı %59'dur. Bu durumu doğru bulmayan ergenlerin oranı ise %4,9'dur.

[20] tarafından yapılan çalışmaya göre, çocuklar, reklam ya da hediye amacıyla isim, adres ve telefon numarası gibi bilgileri isteyen kişilerle paylaşarak hem kendilerini hem de yakınlarını tehlikeye atabilmektedir.

İnternet bağlantısı ve sosyal ağ kullanıcısı çocukların hem siber zorbalık yapma hem de siber zorbalığa maruz kalma eğilimlerinin daha yüksek olduğu [21], teknoloji okuryazarlığı az olan çocukların siber zorbalığa daha çok maruz kaldığı [22] tespit edilmiştir. [23] 'ın Konya'daki 300 ortaokul öğrencisi üzerinde yapmış olduğu araştırma sonuçlarına göre, çocukların %19,6'sı siber zorbalık yapmış, %56,2'si siber zorbalığa bir veya daha fazla kez maruz kalmış, %44,5'i daha önce bir veya daha fazla kez internette kimliğini gizlediği ortaya çıkmıştır.

Bir okulda öğrenim gören öğrenci ebeveynlerinin BTK tarafından başlatılan Güvenli İnternet Hizmeti (İnternet Filtresi) konusundaki görüşlerini araştırdığı çalışmada [1], ebeveynlerin internete bakışı, çocukların internet kullanım alışkanlıkları gibi birçok alana yönelik tespitler yapılmıştır. Bu kapsamda ebeveynlere çocukların evde internete girdiği ortam sorulduğunda aşağıdaki cevaplar alınmıştır (Tablo 2.1). Bu durumda yaklaşık

TABLO 2.1: Çocukların evde internete girdiği ortamlar [1].

Çocukların evde internete girdiği ortam	Sayı	Yüzde
Çocuk Odası	45	26,8
Oturma Odası/Salon	115	68,4
Çocuk Odası/Oturma Odası/Salon	8	4,8
Toplam	168	100

olarak her 4 çocuktan biri kendi odasında yani ebeveyn gözetimi ve müdahalesi olmadan internete erişebilmektedir. Bu durumun özgürlük haricinde çocukların internet üzerinden gelebilecek her türlü tehlikeye açık olduğunu göstermektedir. Bu durumun sebep olduğu birçok problem bulunmaktadır ki bunlar; bilişim yoluyla cinsel istismar, kaçırılma, tehlikeli madde (uyuşturucu, silah vs) ve kişilerin (terör örgütü üyesi, organ kaçakçısı vs) erişimine açık olma şeklinde örneklendirilebilir. Bu problemleri daha gelmeden engellemek ve geldiğinde davranış politikası geliştirebilmek için bilgi güvenliği farkındalığına ve teknoloji kullanım kültürüne sahip olunması önemli bir faktör olarak değerlendirilmektedir.

[2], 2449 temel ve ortaöğretim öğrencisi üzerinde yaptığı bilgi güvenliği farkındalığı araştırmasına göre lise öğrencilerinde, kız öğrencilerde, ilçe merkezindeki öğrencilerde farkındalığın daha yüksek olduğunu tespit etmişlerdir. Ayrıca öğrencilerin evde ve internet kafelerde internet kullanım amaçlarını sorgulamışlardır. Buna göre elde edilen bulgular sunulmuştur (Tablo 2.2).

Bulgularda da görüldüğü üzere ebeveyn kontrolünün daha yoğun olduğu ev ortamında çalışma amaçlı internet kullanım oranı % 15 daha fazla çıkmıştır. Bu durumda ebeveynlerin ev ortamında internet kullanırken çocuklarını daha çok çalışma yapmaya yönlendirdiğini yorumlamak doğru olacaktır.

TABLO 2.2: İnternet kullanım amacı [2].

Öğrencilerin İnternet Kullanım Amacı	Ev Ortamında		İnternet Kafe Ortamında	
	Sayı	Yüzde	Sayı	Yüzde
Oyun	91	14,5	223	32,7
Müzik dinleme	47	7,5	57	8,3
Yazışma	107	17,1	95	13,9
Çalışma	382	60,9	308	45,1
Toplam	627	100,0	683	100,0

[3], Avustralya’da bulunan 3 farklı kamu kuruluşundaki çalışanların bilgi güvenliği farkındalığını toplamda 203 katılımcı ile farkındalığın 3 boyuta (bilgi, tutum ve davranış) ayırarak araştırmışlardır. Araştırmada, personelleri 8 konu üzerinden bilgi güvenliği farkındalığı ölçülmüştür. Bu konular ve araştırma boyutlarına ait toplam ortalama değerler Şekil 4’te sunulmuştur. Ortalama değerler 0 ile 1 arasında değişmekte olup, en çok istenen değer 1 olarak puanlanmıştır. Standart sapma değeri ise parantez içinde gösterilmiştir (Tablo 2.3).

TABLO 2.3: Kamu çalışanlarının 8 odak alanındaki farkındalık seviyeleri [3].

Değişken	Bileşen	Toplam Ortalama Değer (Standart Sapma)
Boyutlar	Bilgi	0.90 (0.09)
	Tutum	0.83 (0.13)
	Davranış	0.83 (0.09)
Odak Alanları	Bilgi güvenliği politikasının önemi	0.90 (0.13)
	Bilgi güvenliği politikasının kuralları	0.85 (0.10)
	Bilgi güvenliği politikasının prensipleri	0.90 (0.14)
	Şifre yönetimi	0.89 (0.11)
	E-posta ve internet kullanımı	0.87 (0.09)
	Güvenlik sorunlarının raporlanması	0.69 (0.21)
	Davranış sonuçları	0.76 (0.16)
	Eğitim	0.78 (0.17)

Araştırmada sunulan bulgulara göre, Avustralya’daki ilgili üç kurum personelinin bilgi güvenliği ile ilgili bilgisi 0.90 değeri ile oldukça yüksek çıkmıştır. Bu bilgiye rağmen çalışanların tutum ve davranışları 0.83 ile bilgi seviyelerine göre daha düşük çıkmıştır. Bu iki değer bizlere, bilgi seviyesi yüksek fakat bunu tutum ve davranışlara çok fazla yansıtmadıklarını göstermektedir. Bilgi güvenliğinde sahip olunan bilginin tutum ve davranışlara yansıtılmaması birçok sorunu beraberinde getirecektir. ‘Güvenlik sorunlarının raporlanması’ değerinin 0.69 olması bilginin tutum ve davranışa yansıtılmamasını destekleyen bir odak alanı olarak ortaya çıkmaktadır. Bilgi seviyesinin yüksek olmasından dolayı bilgi güvenliği politikası, şifre yönetimi, e-posta ve internet kullanım ortalamalarının yüksek çıkması tutarlı bir durum olarak değerlendirilmektedir.

[4], Bartın ilinde 2029 ortaokul öğrencisi üzerinde yaptığı güvenli bilgisayar ve internet kullanım araştırmasında öğrencilere öğrencilerin kullanıcı farkındalıkları ve sosyal mühendislik hakkındaki farkındalıkları bölümünde ailelerin kontrolü ve bilgilendirmesi ile ilgili olarak (Tablo 2.4)'de görüldüğü üzere iki durum hakkında seçim yapmaları istenmiştir.

TABLO 2.4: Çocukların evde internete girdiği ortamlar [4]

Farkındalıklar		Hiçbir zaman	Nadiren	Arada Sırada	Çoğu zaman	Her zaman
Ailem bilgisayarım ve telefon gibi diğer elektronik cihazlarımı kontrol eder.	frekans yüzde	289 14.2	382 18.8	515 25.4	405 20	438 21.6
Ailem bilgisayar ve diğer elektronik cihazları kullanırken güvenli bilgisayar ve internet kullanımını konusunda beni bilgilendirir.	frekans yüzde	252 12.4	408 20.1	415 20.5	514 25.3	440 21.7

Araştırma bulgularına göre öğrencilerin % 58,4'ü elektronik cihazlarının ailesi tarafından kontrol edilmediği görülmektedir. Bu durumda yaklaşık olarak her üç çocuktan ikisi ailesi tarafından kontrol edilmeyerek bilişim ortamları üzerinden birçok tehdiye açık halde günlük hayatını sürdürmektedir. Cihaz kontrolü yapmayan ebeveynlerin sosyal medya ve diğer platformlarda da çocuklarını kontrol etmediklerini söylemek yanlış olmayacaktır. Cihaz, sosyal medya, internet ve uygulama takibinin günümüz çağında fiziksel ve sosyal bir kontrol gibi görülmesi toplumumuz açısından faydalı bulunmaktadır. Bu durumu karşılaştırmalı bir örnek üzerinden açıklamak daha faydalı olacaktır. Eskiden ebeveynler, mahalle ortamında vakit geçiren çocuklarına nereye, kimle, nasıl gittiğini, yabancı biriyle görüşüp görüşmediğini, kısacası neler yaptığını sormaktaydı. Şimdi ise çocuklar ve ergenler sosyal ve fiziksel çevreyi cihazlar üzerinden de takip etmektedir. Artık ebeveynlerin cihazlar üzerinden de çocuklarını kontrol etmeleri oldukça sıradan bir davranış olarak görülmelidir. Sosyal medyada eklenen her arkadaşın fiziksel çevrede olduğu gibi ebeveyn tarafından kontrolü toplumumuz açısından faydalı olacaktır.

Araştırma bulgularına göre, öğrencilerin % 53'ünün ise ailesi tarafından güvenli bilgisayar ve internet kullanımını konusunda bilgilendirilmediği görülmektedir. Her iki çocuktan biri anlamına gelen bu istatistik ise ebeveynlerde bilgi güvenliği farkındalığının oldukça düşük olduğunu ortaya koymaktadır. Çocuklara zarar verme veya onlardan faydalanma niyetinde olan kişilere fırsat veren bu ailelerin önce kendilerini bilgilendirmeleri, ardından da çocuklarını bilgilendirmeleri toplumumuz açısından oldukça önemlidir. Bu yüzden ebeveynlerin, çocuklarının internet kullanımını, internetin riskleri ve güvenli kullanımı konularında yeterli teknik bilgilere sahip olmaları gerekmektedir [24].

[25], Abu Dabi örneğinde okul çocuklarının dijital cihazların ve sosyal medyanın kullanımı ve ebeveyn bilgisi ile ilgili yapmış olduğu çalışmada 8-19 yaşları arasındaki 31.109 öğrenciye ebeveynlerinin kontrolleri ve farkındalıkları ile ilgili çeşitli sorular yöneltilmiştir.

Bunlardan biri, 'Ebeveynleriniz, çevrimiçi sosyal ağ aktivitelerinizin farkında mı?' sorusudur. Bu soruya öğrencilerin % 82.3'ü evet, % 5.76'sı hayır, % 11.9'u emin değilim yanıtını vermiştir. Bir diğeri ise 'Sosyal ağlar üzerinden bir zorbalık mağduru olmanız durumunda ne yapardınız?' sorusudur. Bu soruya öğrencilerin % 26.4'ü ebeveynlerime, % 27.5'i arkadaşlarıma anlatırım yanıtını vermiştir. % 22.4'ü bu durumu kimseye anlatmayacağı yanıtını vermiştir. Geri kalan % 23.7'lik kesim ise bu durumu kardeş, öğretmen veya okuldaki sosyal çalışmacıya anlatacağı yanıtını vermiştir.

Ebeveynlerde çocuk odaklı bilgi güvenliği farkındalığının oluşturulmasına ilaveten kendi güvenliklerini de sağlayacak farkındalık bilgilerine sahip olması önem arz etmektedir. İlk olarak ebeveynler kendi bilgileriyle ilgili güvenlik farkındalığını oluşturmalı daha sonrasında çocuklarını doğru bir şekilde yönlendirmelidir. Ebeveynlerde bilgi güvenliği farkındalığı oluşturulurken değinilmesinin faydalı olacağı konular fiziksel ve bilişim yoluyla gelebilecek tehditler üzerinden anlatılabilir.

Bölüm 3

Uygulama

Bu bölümde, ilk olarak hipotez oluşturmak amacıyla literatür araştırmasına ek olarak mevcut durum araştırması yapılmıştır. Buradan yola çıkılarak hipotezler belirlenmiştir. Sonraki safhada ise hipoteze uyumlu ana kütle ve örneklem seçilmiştir. Bunlara bağlı olarak anket soruları hazırlanmış ve nicel veriler toplanmıştır. Daha sonra nicel veriler frekans ve ki-kare bağımsızlık testi kullanılarak analiz edilmiştir. Analiz sonucunda elde edilen bulgular literatür tartışması kullanılarak yorumlanmıştır. Buna göre bilgi teknolojileri kullanım kültürü ve bilgi güvenliği farkındalık yöntemlerinin geliştirilmesi sağlanmıştır (Şekil 3.1).



ŞEKİL 3.1: Çalışmanın adımları.

3.1 Mevcut Durum Araştırması

Bu bölümde, bilgi teknolojileri kullanım kültürü ve bilgi güvenliği farkındalığını etkileyen unsurlara, ihtiyaçlara ve mevcut durum analizine yer verilmiştir. Bu unsurlar, kuşaklar bağlamında kişisel ve toplumsal çevre, değişen dünyada teknoloji kullanım kültürü ve bilgi güvenliği farkındalığına verilen önem, teknoloji kaynaklı bilgi güvenliği, teknoloji bağımlılığı ve siber zorbalık sorunlarına sebep olan psikolojik nedenler olarak sıralanabilir. Bu konulara ilaven ülkemizdeki teknoloji kullanım kültürü ve bilgi güvenliği farkındalığının doğru oluşturulmasına yönelik ihtiyaç analizinde kullanılacak anket araştırmasının sonuçlarına bu bölümde yer verilmiştir.

3.1.1 Geçmiş Yaşam Analizi

Geçmişte insanlar, sosyal çevrelerini fiziksel dünyada birçok etmen ile birlikte oluşturmaktaydı. Bu fiziksel dünyadaki sosyal çevre, bazen kendi seçtiği insanlardan ve mekanlardan oluşurken bazen de istemediği insanlarla ve ortamlardan oluşurdu. İstemediği insan ve ortamlarla karşı karşıya geldiği zamanlarda nasıl bir davranış biçiminde olması gerektiği tecrübe edebilir, korkularını ve duygularını gözlemleyerek kendini daha iyi tanırdı. İnsanın kendini tanıdığı dönem olarak adlandırılabilen ergenlik döneminde istemediği ortamlara ve insanlara maruz kalması onun birçok açıdan olgunluğa erişmesini de sağladı. Bu istemediği ortam ve insanlar kişilere her şeyle beraber kendisini ve bilgisini nasıl koruması gerektiğini de öğretirdi. Fakat şimdilerde ise özellikle ergenlik döneminde fiziksel çevresini sosyal medya 'fanusu' içinde oluşturan bireyler, istediği kişileri arkadaş olarak ekleyerek mutlu olabileceğini düşündüğü bir dünya kurmasını sağladı. Arkadaşın sosyal medya butonu ile eklenerek veya çıkarılarak oluşacağına kanaat getirdikten sonra oluşan çevre ile dünya hayatını sürdürmeye devam etmektedir. Bu çevre üzerinden geçmişteki gibi istemediği insan ve ortamlarla buluşması mümkün olmayacağı için çoğu kendini ve duygularını tanıyamadan büyüyüp hayata atılmaya çalışmaktadır.

Geçmişte kamera görünce korkan veya ne yapacağını bilemeyen bir nesilden sonra artık hayatını canlı yayın ile yayınlayan bir nesle doğru dönüşen toplumumuzda birçok istenmeyen durum yaşanmaktadır. Sosyal medya ortamlarında birçok bilgisini paylaşan bu nesil kendi bilgisini koruyamadığı gibi çevresindeki insanların da bilgisini ifşa etmektedir. Bu sayede çok da zor olmadan dijital dünya ile fiziksel dünyadaki bilgiyi birleştirip kullanan kişiler tarafından çok sayıda ve türde saldırıya maruz kalmaktadır.

Eskiden farklı sebeplerle de olsa çocuklarını her ortama sokmayan ebeveynler (özellikle anneler), şimdilerde sosyal medya annesi olarak hayatını sürdürmektedir. Popüler olma, reklamlar üzerinden kazanç sağlama gibi sebeplerle kendi ve çocuğunun hayatını herkesin

erişimine açan sosyal medya anneleri günümüzde ve gelecekteki toplumun özü olan aile yapısına oldukça büyük zararlar vermektedir.

Geçmişte eşlerin birbirine olan sevgi ve kırgınlıklarını gizli şekilde yaşamaları makbul görülürken çok fazla zaman geçmeden günümüzde her türlü mecrada açık seçik yaşamaları birçok olumsuz duruma sebep olmaktadır. Bir kaleye benzetilen ailelerimizde içeriden dışarıya ve özellikle dışarıdan içeriye doğru birçok müdahaleye sebep olan bu tür davranış ve teknoloji kullanımının iyileştirilmesi gerekmektedir.

Toplumumuzun büyük kısmı, teknolojiyi özellikle sosyal medya üzerinden keşif ve takip ederek her türlü yönlendirme ve zarara maruz kalmaktadır. Toplumun doğru teknoloji kullanım kültürüne sahip olması amaçlayan bu ve benzer çalışmaların önemi oldukça büyüktür.

3.1.2 Kuşaklar

Bu bölümde geçmiş yaşamı oluşturan kuşak veya nesillerin özelliklerine teknoloji kullanım kültürü ve bilgi güvenliği farkındalığı özelinde yer verilmiştir. Bu sayede teknoloji kullanım kültürünün ve bilgi güvenliği farkındalığına dair ihtiyaçların genel bir bakış açısı üzerinden analiz edilmesi amaçlanmıştır. Kuşakların ağırlıklı olarak pazarlama ve insan kaynakları yönetiminde araştırılmasının yanı sıra bilgi güvenliği farkındalığının geliştirilmesi ve doğru teknoloji kullanım kültürüne sahip olunması açısından da araştırılması birçok açıdan faydalı olacaktır. Bir başka deyişle, kuşakları iyi tanımlamak ve analiz edebilmek doğru bir kültürün oluşmasına katkıda bulunacaktır. Kuşak; 'yaklaşık 25-30 yıllık yaş kümelerini oluşturan bireyler öbeği, nesil, jenerasyon' olarak tanımlanmaktadır [26]. Türk Dil Kurumunun bir başka tanımı ise; 'yaklaşık olarak aynı yıllarda doğmuş, aynı çağın şartlarını, dolayısıyla birbirine benzer sıkıntıları, kaderleri paylaşmış, benzer ödevlerle yükümlü olmuş kişiler topluluğudur' şeklindedir [26]. Farklı araştırmacılar tarafından Kuşakların doğum yılı aralıkları farklı değerler ile açıklanmıştır. Bu değerlerde 4-6 yıllık farklılık gözlemlenmektedir. Günümüz toplumunu oluşturan bireyler, 5 kuşaktan oluşmaktadır. Bunlar;

- 1925-1942 yıllarında doğan sessiz kuşak (Gelenekselciler)
- 1943-1960 yıllarında doğan bebek patlaması kuşağı
- 1961-1981 yıllarında doğan X kuşağı,
- 1982-2005 yıllarında doğan Y kuşağı,
- 2005-2025 yıllarında doğan Z kuşağı olarak sıralanmıştır [27].

Savaşların arasında ve ekonomik buhran döneminde doğan sessiz kuşak, kıtlık ve işsizlik gibi durumlara maruz kaldığı için tasarruf etme, risk almama ve tedbirli davranma gibi davranışları diğer kuşaklara göre daha çok göstermektedir.

Bebek patlaması kuşağı ise, ülkemizde savaş sonrası refah ve barış ortamında doğan nesil olarak bilinir. Özellikle 1950-1960 yıllarında nüfus artış hızı 1940-1950 dönemine göre % 28,5'lere ulaşmasıyla bebek patlaması kuşağı Türkiye'de de nüfusun en fazla artış hızına kavuştuğu dönem olarak karşımıza çıkmaktadır [28].

Ebeveyn ve çocuklardaki teknoloji kullanım kültürü ve bilgi güvenliği farkındalığını araştıran bu çalışmada x, y ve z kuşakları hakkında teorik bilgiler verilerek bunların doğru bir kültür ve farkındalık oluşturmadaki etkisi açıklanmıştır.

3.1.2.1 X Kuşağı

Bebek patlaması kuşağından sonra gelen bu kuşak, bebek patlamasına göre yeteri kadar araştırılmadığı için bilinmeyen kuşak anlamında x kuşağı olarak adlandırılmıştır. X kuşağı bireyleri, teknoloji ve bilgi ile barışık, amaç odaklı ve bağımsız olarak tanımlanmıştır [29]. Teknoloji ve bilgi ile barışık olarak tanımlanan bu kuşak, bilgisayar ve internetin ilk ortaya çıktığı ve yaygınlaşmaya başladığı döneme denk geldiği için, teknolojinin faydalı taraflarını kullanmış veya kullandırmaya çalışmıştır. Bunun etkisi olarak iş ve ev yaşamında kendisinden sonraki Y kuşağına teknolojiyi tavsiye ederek yaygınlaşmasına ve fazlaca kullanılmasına etki etmiştir.

Siyah beyaz televizyon ve merdaneli çamaşır makinesinden akıllı televizyon ve çamaşır makinesinin gelişimine şahit olduğundan bu kuşağı genel anlamda buluşlara ve dönüşümlere tanık olan kuşak olarak tanımlamak yanlış olmayacaktır. Bundan dolayı buluş ve dönüşümlere alışkın hale gelen x kuşağı, yenilikleri takip etmeye alışarak bu duygunun y ve z kuşaklarında kendisini daha baskın biçimde göstermesine neden olmuştur.

Sürekli yenilik takibinde olan x kuşağı, teknolojinin doğru kullanım kültürüyle kullanılmasını y ve z kuşaklarına göre daha fazla önemsemiştir. Bu durumu, cihazların ve buluşların sürekli nitelik değiştirmiş olması sağlamıştır. Bu ifade, tuşlu telefonlardan dokunmatik akıllı telefonlara geçiş sürecinde y ve z kuşağına göre x kuşağının bu cihazların kullanımına verdiği değer ile örneklendirilebilir.

E-posta ve sosyal medya ortamına oranla yüz yüze ve telefon ile görüşmeyi daha çok ön planda tutan x kuşağı, iletişim yönteminde de farklılık göstermektedir.

Otoriteye daha saygılı ve sadık olan x kuşağı, bilgi güvenliği farkındalığının düşük olduğu durumlar ile birleştğinde bazı sorunları daha fazla yaşamaktadır. Bu sorunlar kendisini

telefon yoluyla sosyal mühendislik ve dolandırıcılık örneklerinde daha fazla göstermektedir. Bu örnekler genel olarak kendisini savcı, komiser ve hakim gibi otoriteli sıfatlarla arayan kişilere karşı maddi ve manevi kayıpların yaşandığı durumlar ile sonlanmaktadır.

3.1.2.2 Y Kuşağı

80'lerde çocuk, 90'larda ergen olan Y kuşağı, terimi tarihte ilk kez 1993 yılının Ağustos ayında o zaman ki gençlerin önceki X Kuşağı olarak adlandırılan kuşaktan farklarını ifade etmek amacıyla kullanılmıştır [27]. Başka bir bilgiye göre ise Y kuşağının ismi her şeyi sorgulamaları özelliğinden yola çıkılarak İngilizcede neden anlamına gelen 'why' kelimesindeki Y harfinden geldiği ortaya atılmaktadır.

Y kuşağı bilgi ve iletişim teknolojilerinin yoğun olarak kullanılmaya başlandığı döneme denk geldiği için Milenyum Kuşağı (Millennials), Gelecek Kuşak (Generation Next), Ağ Kuşağı (Net Generation), Kuşak www (www Generation) gibi farklı isimlerle anılmaktadır [30, 31]. Dünya genelinde ise; 'Nükleer olmayan aile kuşağı' (Non-Nuclear Family Generation), 'Hiç bir şeyi kutsal saymayan kuşak' (the Nothing-Is-Sacred Generation), 'Taklitçiler' (the Wannabees), 'İyi hisset kuşağı' (the Feel-Good Generation), 'Siber çocuklar' (CyberKids), Yap yada Öl Kuşağı (the Do-or-Die Generation) ve 'Kimlik arayan kuşak' (the Searching-for-an-Identity Generation) olarak da anılmaktadırlar [32]. [33] kitabında 'Dijital Kuşak' olarak isimlendirdiği Y kuşağını; teknoloji dostu olmanın ötesinde teknoloji, bilgisayar, cep telefonu, internet çocukları olarak tanımlar.

Y kuşağı bireyleri; narsist, bireyci, isteklerini kolaylıkla ortaya koyabilen, girişimci, tatminsiz, otoriteye meydan okuyan, özgürlüklerine düşkün, teknoloji meraklısı, istekleri oldukça fazla, sadakat duyguları az, rahata düşkün, çalışmayı sevmeyen, eğlenceyi kazanmayı seven, hırslı, eleştiriye tahammülü az olan bireylerdir. Genele hitap edeni değil, kişisel olanı severler, standart olanı sevmezler [34].

Y kuşağı bireyleri çoklu görevlerde yüksek adaptasyon gücüne sahip olmaları ile birlikte yaptıkları işlerde çok çabuk sıkılmaktadır. Bu kuşaktakiler ileri düzey düşünebilme ve hızlı bir bilgi edinme sürecine sahiptirler. Değişimi kucaklamak için isteğe ve sürekli yeni yaklaşımlar içinde geleceğe meydan okuyabilme kapasitesine sahiptirler. Ayrıca bu kuşaktakiler yüksek hayat standartlarına sahip olmakla birlikte takım çalışmalarında da ön plana çıkmaktadırlar [35].

Bu kuşakta yer alan kişiler akıllı, özgürlüklerine düşkün, teknoloji tutkunu ve teknoloji kullanımını iyi bilen bir kuşak olarak tanımlanmaktadır. Günlerinin yaklaşık 15 saati medya ve iletişim teknolojileri ile etkileşim halinde geçen bu kuşak için hayatlarını rahat yaşamak çok önemlidir. Bu kuşak için teknoloji, hayatlarındaki pek çok şeyin simgesi olup, Y kuşağının X kuşağına göre en üstün olduğu konulardan birisidir [36].

Türkiye’de özgürlüğüne düşkün, kolay adapte olabilen, çabuk vazgeçen, iyi eğitilmiş, otoriteye meydan okuyan, teknoloji hayranı olan gençlerden oluşan bu nesil; sahip oldukları imkanlar sayesinde küreselleşmenin etkilerinin en iyi şekilde hissedildiği, ekonomi ve kültürlerarası etkileşimin arttığı bir dönemde yaşamaktadır [37]. Türkiye’de yaşayan yaklaşık 76 milyon kişinin % 35’i Y kuşağı üyesidir [38]. Ülkemizde, Avrupa’nın pek çok ülkesindeki toplam nüfustan daha fazla Y kuşağı üyesi yaşamaktadır [39].

Y kuşağına ilişkin olarak ilk akla gelen özellikleri teknolojiye olan yatkınlıklarıdır. Teknoloji becerilerini yaratıcı bir şekilde sahip oldukları görevleri ilerletmek ve sonuçlar elde etmek için kullanırlar. Günlük işlerinin dünyada olumlu bir değişime katkı yapmasını görmek onlar için son derece önemlidir.

Y kuşağının dünyanın en popüler sosyal medya ağı Facebook’u kullanma alışkanlıkları üzerine yapılan bu araştırmada teknoloji ile iç-içe bir hayat sürdüren Y kuşağının % 28,2’sinin günde üç saat Facebook hesaplarını açık tuttuğu tespit edilmiştir. Dört yıldan uzun süredir Facebook hesabı olanların oranı % 58,7’dir. Türkiye’de Facebook’un özellikle son beş yılda büyüme göstermesi ve Türkiye’nin dönem içinde dünyanın en çok Facebook kullanan dördüncü ülkesi konumuna kadar çıkmasında bu kuşağın sosyal ağa gösterdiği talebin bir sonucu olarak yorumlanabilir [40].

Bu sonuçlara göre Y kuşağında her üç kişiden biri günde en az 3 saat Facebook kullanıcısı olup, büyük çoğunluğu ise en az 4 yıldır bu sosyal medya hesabını kullanmaktadır. Görüldüğü üzere X kuşağına göre teknolojiye daha yatkın ve ilgili olmasından dolayı bu kuşakta sosyal medya kullanımını önceki kuşağa göre daha fazladır. Sosyal medyanın bu kadar aktif kullanılması Y kuşağında sosyal medya bağımlısı oranını artıracaktır. Bundan dolayı teknoloji kullanım kültürünün doğru oluşturulmasını amaçlayan çalışmalarda Y kuşağı özelinde sosyal medya ve riskleri üzerine daha fazla özen gösterilmelidir.

Y kuşağının farklı kaynaklarda birçok özelliğine dikkat çekilmiştir. Fakat çoğunun ortak noktası teknolojiye yatkınlığının X kuşağına göre daha fazla olmasıdır. Bu durum kendisini teknolojiye ayrılan zamanın daha fazla olması ile de kendisini göstermektedir. Birçok faaliyetinde ve iş hayatında sürekli teknolojiyle zaman geçirmesi, bu kuşağın bilgi güvenliği farkındalığının daha yüksek olmasını gerektirmektedir. Bu çıkarım ile X kuşağına göre Y kuşağına, bilgi güvenliği farkındalığını daha derin ve teknik detaylarda bilgi sahibi olabilecek şekilde oluşturmak gerekmektedir. Ayrıca bu kuşakta teknoloji kullanımının süre olarak uzaması ve vazgeçilmez hale gelmesinin daha yüksek ihtimalle olabilmesinden dolayı X kuşağına göre teknoloji bağımlılığının konusu üzerine daha fazla düşülmelidir.

3.1.2.3 Z Kuşağı

X ve Y kuşağındaki gibi teknolojik buluş, dönüşüm ve yaygınlaşma evresinden sonra dünyaya gözlerini açan, beşiklerindeyken internet ve teknoloji ile buluşan bu kuşak teknolojiyi bir gereklilik olarak görmektedir. Henüz okullarda bulunan Z kuşağını tanımlayan yüksek özgüven, eğitim ve sosyal statüye önem verme, sabırsızlık, bireyselleşme, çabuk sıkılma ve yalnızlık gibi birçok özellikleri bulunmaktadır. Bunların çoğu ebeveynleri olan X ve Y kuşağının daha zor ulaştığı veya onların katkıları ile sivrilen özelliklerdir.

Önceki kuşaklara göre daha yüksek özgüven bu neslin teknoloji kullanım kültürünün yanlış oluşması ve bilgi güvenliğinde birçok risk ile karşılaşabilmesini sağlamaktadır. Yüksek özgüven ile birçok konuyu sosyal medya platformlarında paylaşımları bu kuşağın bilgi güvenliğini tehdit etmektedir. Yine yüksek özgüven ve statüye verdikleri önem ile siber zorbalık faaliyetlerinin okullarda yaygınlaşmasını sağlayan bir faktör olarak karşımıza çıkmaktadır.

Ayrıca teknoloji bir gereklilik ve her zaman ulaşılması gereken bir ihtiyaç olarak görmeleri bu kuşaktaki teknoloji ve sosyal medya bağımlılığı riskini artırmaktadır. Sosyal medyanın fiziksel yalnızlığı artıran ve mutluluk veren etkisi ile bireyselleşme özellikleri körüklenen bu kuşak, ebeveynleri olan X ve Y kuşağına gittikçe yabancılaşmaktadır. Ayrıca bireyselleşme ve yalnızlık özelliği toplumumuzun yapı taşlarından olan akraba ve eş-dost ilişkilerini zedelediği için bu kuşak üzerinden teknoloji kullanım kültürünün daha hassas oluşturulmasını gerektirmektedir.

Çabuk harekete geçme ve sabırsızlık gibi özellikleri bu neslin, kendisine sosyal medya ve diğer ortamlardan gelen bilgileri teyit etmeden harekete geçmelerini sağlamaktadır. Bundan dolayı geleceğimizi oluşturan Z kuşağının, yanlış yönlendirme ve akabinde yanlış toplumsal olaylara katılım göstermesini engelleyecek çalışmaların yapılması oldukça önemlidir.

Teknoloji ile bu kadar yakından ilgili olan Z kuşağının teknolojiyi tüketen değil üreten ve kendi geleceğini şekillendiren bir nesil haline gelmesi için Z kuşağına daha fazla teknolojik yatırımın yapılması birçok olumsuz durumu engelleyecek ve olumlu birçok gelişmeye neden olacaktır.

3.1.3 Yeni Dünya ve Dijital Yaşam

Bu bölümde, kuşakların yaşayacağı yenedünyadaki dijital yaşamın avantaj, dezavantaj ve riskleri üzerinde durulmuştur. Makinelerin icadı ile başlayan endüstriyel devrimlerin 4.0 ve 5.0 versiyonlarının uygulandığı günümüzde teknoloji, lokomotif bir pozisyonda

dünyanın dijitalleşmesine imkan sağlamaktadır. Teknoloji ile beraber gelişen cihaz ve yazılım ürünleri dünyada daha az emek ile daha fazla ekonomik kazanç getiren bir alan haline gelmiştir. Öyle ki kısa zamanda birçok teknoloji ve sosyal medya şirketi dünyada ciro ve değer bakımından ülkemizin en yüksek değere sahip kuruluşlarından onlarca kat fazla değere sahiptir. Bundan dolayı yenedünyada teknolojiyi tüketen değil üreten ülkeler kazançlı çıkacaktır. Teknolojik gelişmeleri yakından takip eden ülkemizde tüketimin fazla olmasının yanı sıra doğru kullanım ve tüketim kültürüne sahip olması en az teknoloji üretimi kadar önemlidir.

Son 20 yılda yaygınlaşan ve hayatın her alanına nüfuz eden teknoloji ve sayesinde insanlık eskiye oranla daha konforlu ve kolay bir hayat sürmektedir. Teknolojinin yükselişi, hızlı kentleşme ve küreselleşen dünya ile birleşerek insanların birçok hizmet ve ürüne çok hızlı erişmesini sağlamıştır. Akıllı cihazlar, internete ve birbirine bağlı nesnelere üretim maliyetlerinin düşmesi ve yaygınlaşması ile artık birçok birey ve bireylerin yaşadığı konutlarda onlarca teknolojik ürün bir arada bulunmaktadır. Bu ürünler bireylerde akıllı telefon, saat ve diğer giyilebilir teknoloji ürünleri olarak kendini gösterirken konutlarda akıllı ev sistemleri adı altında birçok ürün ile karşımıza çıkmaktadır. Kullanımı ve tüketimi kolaylaşan bu teknoloji ürünlerinin doğru bir teknoloji kullanım kültürüne sahip olunmadan kullanılması toplumumuzun bilgi güvenliğini birçok açıdan tehdit eder hale gelmiştir. Bilindiği üzere birçok teknolojik ürün bir veya daha fazla şifre ile korunmaya çalışılmaktadır. Basit, paylaşılan veya kaptırılan erişim bilgileri ile doğru bir kullanım kültürüne sahip olunmadan kullanılan teknolojik ürünler bireylerin mahremiyetini, maddi ve manevi değerlerini tehdit eder hale gelmiştir.

Dijital ve yenedünyada genç ve ebeveynlerin teknolojik ürünlerin kullanımına adaptasyon hızı ile doğru kullanım kültürüne ve bilgi güvenliği farkındalığına kavuşma hızının aynı olması oldukça önem arz etmektedir.

3.1.4 Gerçekleşmiş Olaylar ve Örnekler

Bu bölümde tezin 2 hedef kitlesi üzerinden BT kullanım kültürü ve bilgi güvenliği farkındalığı hakkında gerçekleşmiş ve olası olaylara yer verilmiştir. Bu sayede hedef kitlelerin riskleri ve önlemler daha iyi açıklanabilecektir.

3.1.4.1 Bilgi Güvenliğine İlişkin Örnekler

İlk olarak bilgi güvenliği farkındalığının önemini vurgulayan örnekler açıklanmıştır. Ortalama, sosyal medya riskleri ve herkese açık bilgiler üzerinden yaşanan örnek olaylara yer verilmiştir. Bunun için öncelikle ortalama örneklerine yer verilmiştir. Ortalama iletileri

daha çok e-posta ve SMS yoluyla maddi değerlerimizi hedef alan konular hakkında kullanıcılara ulaşmaktadır. Neredeyse hepsinde kullanıcıların merak, endişe, korku ve panik gibi duyguları kullanılarak istenilen hamlelerin yaptırılması amaçlanmaktadır. Oltalama örneği olarak geçtiğimiz yıllarda oldukça yaygın bir biçimde yüksek tutarlı faturalar üzerinden kullanıcıların hazırlanan maddi tuzaklara çekilmesi sağlanmıştır (Şekil 3.2).

Inbox - Yerel Dizinler 429336139 Hesap ... x

429336139 Hesap Nolu Kasım 2014 Faturanız

TTNET

HESAP NUMARASI	: 938164975
FATURA DÖNEMİ	: Kasım 2014
SON ÖDEME TARİHİ	: 12 Kasım 2014
ÖDENECEK TUTAR	: 297,25 TL

Rehber Fatura videosu için tıklayınız.

E-Faturamı Görüntüle

E-faturanızı Adobe Reader 8.1.2 (EXE, 22.4MB) ile görüntüleyebilmek için [tıklayınız](#)

Faturanızı hesap numarası ile ödeyebilir, otomatik ödeme talimatı ve diğer tüm ödeme işlemlerinizi bu numara üzerinden takip edebilirsiniz.

Kredi kartınızla hemen ödemek veya otomatik ödeme talimatı vermek için [tıklayınız](#) ya da 444 0375 TTNET Müşteri Hizmetlerini arayınız.

Faturanızın arka sayfasını görmek için [tıklayınız](#).

E-Fatura servisini tercih ettiğiniz ve doğanın korunmasına katkıda bulunduğunuz için teşekkür ederiz.

Bu e-posta'da yer alan hatbn size ait olmadığını düşünüyorsanız veya fatura tercihinizi değiştirmek isterseniz: 444 0 375 TTNET Müşteri Hizmetleri'ni arayabilir, iletisim@ttnet.com.tr e-posta adresine e-posta gönderebilir, **TTNET** adresinde bulunan TTNET E-Fatura Posta Kutunuza girip, fatura ayarlarınızda değişiklik yapabilirsiniz.

If you think that the subscription in this e-mail does not belong to you, or if you want to change your billing preference, you can call 444 0 375 TTNET customer service, you can send an e-mail to iletisim@ttnet.com.tr or you can change your invoice settings from your TTNET E-Billing Postal which is located at **TTNET**

OKUL YOLUNDA, SÜPER LİMİTSİZ İNTERNET İLE TTNET YANINDA!

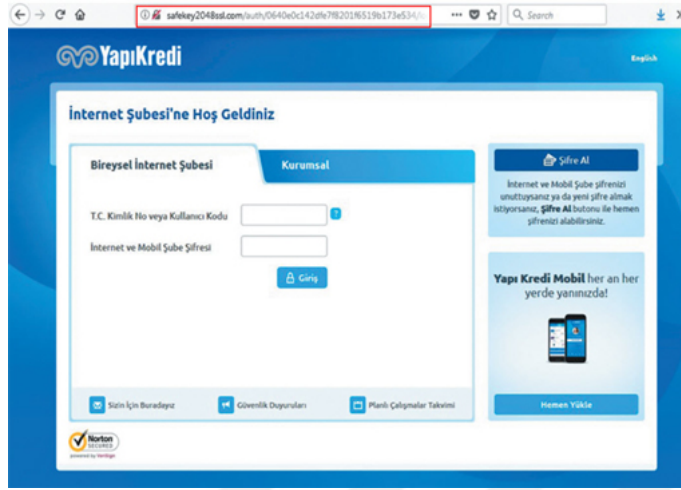
50 TL hediye reki HEDİYE

16 Mbit/s'e kadar hız, 100 GB AKN, 59,9tl

TTNET

ŞEKİL 3.2: Yüksek tutarlı fatura ile oltalama e-postası.

Yüksek faturaların yanı sıra internet bankacılığını da konu edinerek kullanıcılara oltalama saldırıları yapılmaktadır (Şekil 3.3).



ŞEKİL 3.3: Sahte banka web sitesi ile oltalama örneği.

Oltalama saldırılarının temel amacı kullanıcıların bilgilerini ele geçirmektir. Fakat bazı saldırganlar sadece kullanıcı bilgilerini ele geçirmekle kalmayıp aynı zamanda kurbanların cihazlarına farklı türlerde zararlı yazılımlar da bulaştırmaktadır. Buna örnek olarak bir senaryoda; bir kargo şirketinden kargonun doğru adrese ulaşması için adres değişikliği formunu indirilmesi, doldurulması ve bunun bahsedilen adrese geri gönderilmesi istenmektedir (Şekil 3.4). Bu sayede saldırgan hem kişinin güncel adres bilgisine erişmekte, hem de kullanıcıya indirdiği dosya ile kişinin bilgisayarına Cryptolocker gibi zararlı yazılımların bulaşmasını sağlamaktadır.



ŞEKİL 3.4: Kargo firmasından adres değişikliği formu ile adres bilgilerine erişim oltalaması.

Bu tür ortalama e-postaları bazen de şekil değiştirerek SMS yoluyla bireylere ulaştırılmaktadır (Şekil 3.5).



ŞEKİL 3.5: Başlıklı kısa mesaj ile banka bilgileri ortalaması.

Bununla beraber özellikle kamu kuruluşlarındaki son kullanıcıların ve yöneticilerin yaptığı hatalardan olan kişisel bilgilerin açık edilmesi gibi durumlar da söz konusudur. Buna örnek olarak bir personel yerleştirme sonuç bilgisinin tablo olarak herhangi bir bilgi maskelenmeden yayınlandığı görsel sunulmuştur (Şekil 3.6,3.7).



ŞEKİL 3.6: Kamu kuruluşlarının kişisel bilgileri açık etmesi örneği.

14983373334	SELİM	AKIL	İZMİR 2 NOLU F TİPİ YÜKSEK GÜVENLİKLİ KAPALI CEZA İNFAZ KURUMU	TEKNİSYENLİK
	SAHİN		KOCAELİ 1 NOLU F TİPİ YÜKSEK GÜVENLİKLİ KAPALI CEZA İNFAZ KURUMU	TEKNİSYENLİK
				TEKNİSYENLİK
	BERK		ALAYUNT TİPİ KAPALI CEZA İNFAZ KURUMU	TEKNİSYENLİK
	BERK		ALAYUNT TİPİ KAPALI CEZA İNFAZ KURUMU	TEKNİSYENLİK
	SERDAL	YÜKSEL	VAN F TİPİ YÜKSEK GÜVENLİKLİ KAPALI CEZA İNFAZ KURUMU	TEKNİSYENLİK
	SERDAR	KAYA	SİLİFKE ADLİYESİ	TEKNİSYENLİK
	SERDAR	ÇELİK	ANKARA 2 NOLU F TİPİ YÜKSEK GÜVENLİKLİ KAPALI CEZA İNFAZ KURUMU	TEKNİSYENLİK
	SERKAN	YAYLA	KONYA ADLİYESİ	TEKNİSYENLİK
	SERKAN	İNCE	EDİRNE F TİPİ YÜKSEK GÜVENLİKLİ KAPALI CEZA İNFAZ KURUMU	TEKNİSYENLİK
	SERKAN	TABAK	EDİRNE F TİPİ YÜKSEK GÜVENLİKLİ KAPALI CEZA İNFAZ KURUMU	TEKNİSYENLİK
	SERKAN	İREN	SİLİVRİ 7 NOLU L TİPİ KAPALI CEZA İNFAZ KURUMU	TEKNİSYENLİK
	SERKAN	İŞÇİ	KOCAELİ 2 NOLU F TİPİ YÜKSEK GÜVENLİKLİ KAPALI CEZA İNFAZ KURUMU	TEKNİSYENLİK
	SERKAN	KAVACIK	SİLİFKE M TİPİ KAPALI CEZA İNFAZ KURUMU	TEKNİSYENLİK
	SEYİT ALİ	ALPTEKİN	ANKARA 1 NOLU F TİPİ YÜKSEK GÜVENLİKLİ KAPALI CEZA İNFAZ KURUMU	TEKNİSYENLİK
				TEKNİSYENLİK

ŞEKİL 3.7: Kamu kuruluşundan açık edilen kişisel bilgiler.

Görüldüğü üzere saldırganlar, farklı kuruluşları kullanarak kullanıcıların bilgileri ele geçirmeye çalışmaktadır. Bazen bu durumların oluşmasını sağlayan veya kendi eliyle bilgilerini veren/çalıyan birçok birey bulunmaktadır. Bu bilgi kayıpları farkında olarak veya olmayarak özellikle sosyal medya üzerinden karşımıza çıkmaktadır (Şekil 3.8).



ŞEKİL 3.8: Sosyal medyada kişisel bilgilerin açık edilmesi örneği.

3.1.4.2 BT Kullanım Kültürüne İlişkin Örnekler

Bilgi güvenliğinin yanı sıra bilgi teknolojilerinde yanlış kullanım kültürünün oluşması nedeniyle birçok olay gerçekleşmiştir. Bunların temelinde internet ve sosyal medya üzerinden yanlış yönlendirme, siber zorbalık, teknoloji bağımlılığı gibi konular yer almaktadır. İlk olarak internet üzerinden yanlış yönlendirme veya internet yalanları konusu üzerinde durulacaktır. Verilecek örnekler siyasi, milli, dini ve diğer birçok farklı değer üzerinden açıklanacaktır.

İlk örnekte, dini değerler üzerinden toplumu yönlendirmeye ve belirli bir algı oluşturmaya çalışan bir sosyal medya paylaşımı ön plana çıkmaktadır (Şekil 3.9).



ŞEKİL 3.9: Sosyal medyada dini değerler üzerinden yanlış yönlendirme örneği.

(Şekil 3.9)'da görülen, daha sonradan yalan haber olduğu ortaya çıkan bu sosyal medya paylaşımı dini değerler üzerinden insanları yönlendirmiş, çoğu vatandaşımız buna inanarak kin ve nefret dolu bir topluluğa dönüşmüştür. Bu tür gönderilerin hedef aldığı bir diğer unsur algı yönetimidir. Paylaşımında geçen İzmir ifadeleri ile İzmir'li insanları dini değerlere saygısız bir toplum olarak karalamaya çalışmaktadır.

İkinci örnekte ise (Şekil 3.10), birçok değeri ayaklar altına alan görseller sosyal medyada paylaşımına girmiş ve insanların öfke dolu bir hale gelmesine neden olmuştur. Bu paylaşımlar genellikle belirli bir kitleyi hedef alacak şekilde kurgulanmaktadır. Bunları kurgulayanlar, aynı resimleri kullanarak terör örgütü ile ilgili sayfalarda paylaşım örgüt sempaticizliğini yaymaya çalışmakta, bazen de aşırı milliyetçi ortamlarda devreye sokarak insanların arasında ayrılıkçılığın artmasını hedeflemektedir.



ŞEKİL 3.10: Sosyal medyada milli değerler üzerinden yanlış yönlendirme örneği.

Başka bir örnekte ise, gündemde yer tutan evlendirme yetkisi ile ilgili hazırlanmış montajlı görsel aracılığı ile devlet kurumlarına iftira atılarak belirli bir algı oluşturulması amaçlanmıştır (Şekil 3.11).



ŞEKİL 3.11: Sosyal medyada kuruluşları hedef alan yanlış yönlendirme örneği.

Eğlence amaçlı hazırlanan ve iki kurumu hedef alan başka bir örnekte ise hem rahmetli yazarlarımıza saygısızlık yapılmakta, hem de bunu paylaşan insanların aklıyla dalga geçilmektedir (Şekil 3.12).



ŞEKİL 3.12: İki kurumu hedef alan sahte belge ile yanlış yönlendirme örneği.

Son örnekte ise montaj görsel kullanılarak şehitlerimiz üzerinden devlet televizyonuna iftira atılmış ve belirli bir algının oluşması amaçlanmıştır (Şekil 3.13).



ŞEKİL 3.13: Fotoğrafta montaj ile devlet televizyonuna iftira ve algı oluşturma örneği.

İnternet ve sosyal medya sitelerinde dolaşımda bulunan bunun gibi birçok görsel farklı amaçlar doğrultusunda dolaşıma sokularak bilginin güvenilirliği azaltılmaktadır. İnternet yalanları, aslında bilgi güvenliğinin temel prensiplerinden olan bütünlük ilkesini bozmaya yönelik bir hareket veya saldırı olarak nitelendirilebilir.

3.1.4.3 Teknoloji Bağımlılığına ve Siber Zorbaliğa İlişkin Örnekler

Yeni nesil arasında yaygınlaşan akıllı telefon ve sosyal medya kullanımı ile çocuk ve gençler birçok olayı artık kesintisiz yaşamaktadır. İyi olaylarda olduğu gibi kötü olaylarda da bu kesintisiz yaşantı devam etmektedir. Eskiden fiziksel dünyada birlikte olan insanlar iyi veya kötü ne varsa hepsini yüz yüze yaşamaktaydı. Fakat şimdilerde sanal ortamda yaşanan arkadaşlar arası sorunlar fiziksel ortama göre bir anda çok daha kötü bir boyuta geçebilmektedir. Bunun en kötü örneklerinden olan siber zorbalık, zorbalık faaliyetlerinin sanal ortamdan sürekli ve zarar verme bilinci ile yapılan her türlü faaliyet olarak tanımlanmaktadır.

Birçok nedenden dolayı siber zorbalık yapan çocuk ve gençler arasında bazen olaylar ileri boyutlara taşınarak ölümlerle sonuçlanabilmektedir. Dünya'nın farklı yerlerinde özellikle intihar ile adını duyuran siber zorbalık faaliyetlerine rastlanmaktadır. Paylaşılan gönderi veya medyaların başkaları tarafından farklı amaçlar için kullanılabilmesini hesap edemeyen gençler, sosyal medya üzerinden uğradıkları şiddet dolu ifadelerle intihara yönlenebilmektedir. New York/ABD'de Aralık 2017 ayında benzer sebeplerle intihar eden

20 yaşındaki Aliyah Rodriguez siber zorbalık mağduru olarak kayıtlara geçmiştir [41]. Başka bir örnekte ise, küçültücü ve kaba konuşmalardan sonra 10 Ocak 2018 günü intihar eden Florida/ABD’de yaşayan 12 yaşındaki Gabriella Green bir başka siber zorbalık mağdurudur [42].

İnsan ve makine etkileşimi sonucu oluşan ve kimyasal olmayan bağımlılıklar olarak tanımlanan bir çatı isim olan teknoloji bağımlılığı, karşımıza internet, oyun, sosyal medya bağımlılığı gibi farklı türlerle çıkmaktadır. Bozukluk ve bağımlılık olarak farklı kavramlar ile tanımlanmaya çalışılan bu sorunlara, günümüzde daha da sık ve olumsuz örneklerine rastlamaktayız. 2015 yılında Rusya’nın Uchaly bölgesinde yaşayan 17 yaşındaki Rustam, bacağı kırıldığı için evde bir video oyunu günde sadece 6 buçuk saatlik ara vererek 22 gün boyunca oynayarak ölümünü hazırlamıştır [43].

3.2 Hipotezlerin Belirlenmesi

Çalışmanın bu adımında literatür ve kuşaklar, örnekler üzerinden mevcut durum araştırması yapılarak ebeveyn ve çocuklarda teknoloji kullanım kültürü ile bilgi güvenliği farkındalık yöntemlerinin geliştirilmesi doğrultusunda aşağıdaki hipotezler hazırlanmıştır (Tablo 3.1).

TABLO 3.1: Çalışmanın Hipotezleri

Hipotez No	Hipotez İfadesi
Hipotez 1	Çocuğun yaşı ile çocuğun evde internete girdiği ortamlar arasındaki ilişki
Hipotez 2	Çocuğun cinsiyeti ile çocuğun internette geçirdiği süre arasındaki ilişki
Hipotez 3	Çocuğun internette geçirdiği süre ile ebeveynin çocuğuna sosyal medya kullanım yaşı belirleyip belirlememesi arasındaki ilişki
Hipotez 4	Ebeveynin güvenli sosyal medya kullanım bilgisi olup olmaması ile sosyal medyada yapılan paylaşımların gizliliği arasındaki ilişki
Hipotez 5	Ebeveynin güvenli sosyal medya kullanım bilgisi olup olmaması ile ebeveynin daha önceden farkındalık eğitimi alması arasındaki ilişki
Hipotez 6	Ebeveynin sosyal medyada yaptığı paylaşımların gizliliği ile ebeveynin çocuğuna sosyal medya kullanım kuralı belirleyip belirlememesi arasındaki ilişki
Hipotez 7	Ebeveynin çocuğuna sosyal medya kullanım kuralı belirleyip belirlememesi ile ebeveynin çocuğuna sosyal medyada tanımadığını insanlarla iletişim kurmaması konusunda uyarıp uyarmaması arasındaki ilişki

3.3 Ana Kütle ve Örneklem Seçimi

Çalışmanın ana kütlelerini Üsküdar ilçesindeki okullarda okuyan öğrencilerin ebeveynleri oluşturmaktadır. Bu ana kütle içerisinde tüm devlet okullarında (120 adet) okuyan öğrencilerin ebeveynleri örneklem olarak seçilmiştir. Örnekleme, Üsküdar Belediyesi ve

Üsküdar Kaymakamlığı himayesinde gerçekleştirilen 'Ailelerde Bilgi Güvenliği Farkındalığı ve BT Kullanım Kültürü' isimli seminere katılım sağlayan 2118 ebeveyn oluşturulmuştur. Örneklem % 90,8'i kadınlardan, % 9,8'i erkek ebeveynlerden oluşmaktadır. Örneklem %6,9'u 18-30, %48,9'u 31-40, %34'ü 41-50, %6,3'ü 51-65, %0,7'si 66-70 yaş grubundadır. %3,1'i yaş belirtmemiştir. Örneklem % 75,5'i sosyal medya kullanıcısıdır.

3.4 Anket Sorularının Hazırlanması

Anket araştırması için her ebeveyne kağıt ortamda hazırlanmış anket kullanılmıştır. Anket sorularını oluşturmada literatür araştırması, mevcut durum araştırması, bu konuda görev yapan kuruluş ve STK'lara ait kaynaklar incelenmiştir. Anket sorularının hazırlanmasında literatür araştırmasında verilen çalışmalara ek olarak [8, 16, 44, 45] çalışmalarından yararlanılmıştır. Ebeveynlere özel hazırlanan, ihtiyaç tespitini ve farkındalık oluşturma yöntemini belirlemede kullanılacak anket soruları EK-1'de bulunmaktadır.

3.5 Nicel Verilerin Toplanması

'Ailelerde Bilgi Güvenliği Farkındalığı ve BT Kullanım Kültürü' isimli seminere katılan 2118 ebeveyne, seminer sonrası kağıt ortamda yapılan anket çalışması daha sonra bilgisayar ortamına aktarılmıştır.

3.6 Anket Sonuçlarının Analizi

Ebeveynlere yapılan anketin sonuçları frekans analizi ve ki-kare bağımsızlık testi ile değerlendirilmiştir. Üsküdar'daki 120 devlet okulunda çocuğu olan 2118 veli anketleri yanıtlamıştır. Frekans analizi için birbirine bağlı olabilecek sorular birlikte analiz edilmiştir. Frekans analizi ile bazı sorulara cevap aranmıştır (Tablo 3.2,3.3,3.4).

TABLO 3.2: Frekans analizi sonuçları.

Cevap Aranan Soru	İlk Anket Sorusu ve Cevabı	İkinci Anket Sorusu ve Cevabı	Cevap
Sosyal medya kullanan velilerin cinsiyeti nedir?	Ankete katılan velilerin %75,5'i sosyal medya kullanıcısıdır.	Ankete katılan velilerin %90,8'i kadınlardan, %9,8'i erkeklerden oluşmaktadır.	Ankete katılan kadın velilerin %75,3'ü, erkek velilerin %71,5'i, sosyal medya kullanıcısıdır. 18-30 yaş grubundaki velilerin %77,5'i, 31-40 yaş grubundaki velilerin %80,9'u, 41-50 yaş grubundaki velilerin %73,2'si, 51-65 yaş grubundaki velilerin %67,9'u, 66-70 yaş grubundaki velilerin %35,7'si sosyal medya kullanıcısıdır. Yaş belirtmeyen velilerin ise %42,4'ü sosyal medya kullanıcısıdır.
Sosyal medya kullanan velilerin yaş dağılımı nasıldır?	Ankete katılan velilerin %75,5'i sosyal medya kullanıcısıdır.	Ankete katılan velilerin %6,9'u 18-30, %48,9'u 31-40, %34'ü 41-50, %6,3'ü 51-65, %0,7'si 66-70 yaş grubundadır. %3,1'i yaş belirtmemiştir.	Ankete katılan sosyal medya kullanıcıları; %31'i 1 saatten az, %44,7'si 1-3 saat arasında, %7,6'sı 4-6 saat arasında, %1,8'i 6 saatten fazla internette vakit geçiriyor. Çocukların %11,6'sı internette hiç vakit geçirmiyor.
Sosyal medya kullanan velilerin çocukları internette ne kadar vakit geçiriyor?	Ankete katılan velilerin %75,5'i sosyal medya kullanıcısıdır.	Ankete katılan tüm velilerin çocukları; %31,5'i 1 saatten az, %41,4'ü 1-3 saat arasında, %7,2'si 4-6 saat arasında, %1,7'si 6 saatten fazla internette vakit geçiriyor. Çocukların %14,3'ü internette hiç vakit geçirmiyor.	Ankete katılan sosyal medya kullanıcıları; %31'i 1 saatten az, %44,7'si 1-3 saat arasında, %7,6'sı 4-6 saat arasında, %1,8'i 6 saatten fazla internette vakit geçiriyor. Çocukların %11,6'sı internette hiç vakit geçirmiyor.

TABLO 3.3: Frekans analizi sonuçları (devam).

Cevap Aranan Soru	İlk Anket Sorusu ve Cevabı	İkinci Anket Sorusu ve Cevabı	Cevap
Sosyal medya kullanan velilerin cinsiyeti nedir?	Ankete katılan velilerin %75,5'i sosyal medya kullanıcısıdır.	Ankete katılan velilerin %90,8'i kadınlardan, %9,8'i erkeklerden oluşmaktadır.	Ankete katılan kadın velilerin %75,3'ü, erkek velilerin %71,5'i, sosyal medya kullanıcısıdır.
Sosyal medya kullanan veliler, güvenli sosyal medya kullanım bilgisine sahip mi?	Ankete katılan velilerin %75,5'i sosyal medya kullanıcısıdır.	Ankete katılan tüm velilerin; %38,8'i evet, %54,1'i hayır, %7,2'si belirtmek istemiyorum seçeneğini işaretlemiştir.	Ankete katılan sosyal medya kullanıcısı olan velilerin; %42,3'ü evet, %58,5'i hayır, %7,2'si belirtmek istemiyorum seçeneğini işaretlemiştir.
Sosyal medya kullanan veliler, çocukları için sosyal medya kullanım yaşı belirlemiş mi?	Ankete katılan velilerin %75,5'i sosyal medya kullanıcısıdır.	Ankete katılan tüm velilerin; %43,5'i çocuklarına sosyal medya kullanım yaşı belirlemiş, %45,6'sı belirlememiştir. %6,1'i çocuğum ne zaman isterse kullanabilir seçeneğini işaretlemiştir.	Ankete katılan sosyal medya kullanıcısı olan velilerin; %47,5'i çocuklarına sosyal medya kullanım yaşı belirlemiş, %43,1'i belirlememiştir. %4,5'i çocuğum ne zaman isterse kullanabilir seçeneğini işaretlemiştir.
Sosyal medya kullanan veliler, çocuğuna sosyal medya kullanım kuralları belirlemiş mi?	Ankete katılan velilerin %75,5'i sosyal medya kullanıcısıdır.	Ankete katılan tüm velilerin; %67,3'ü evet, %16,5'i hayır, %16,2'si belirtmek istemiyorum seçeneğini işaretlemiştir.	Ankete katılan sosyal medya kullanıcısı olan velilerin; %70'i evet, %14,4'ü hayır, %15,6'sı belirtmek istemiyorum seçeneğini işaretlemiştir.

TABLO 3.4: Frekans analizi sonuçları (devam).

Cevap Aranan Soru	İlk Anket Sorusu ve Cevabı	İkinci Anket Sorusu ve Cevabı	Cevap
Sosyal medya kullanan veliler, çocuklarını sosyal medyada tanımadığı kişilerle iletişim kurmaması konusunda uyarı yapmış mı?	Ankete katılan velilerin %75,5'i sosyal medya kullanıcısıdır.	Ankete katılan tüm velilerin; %92,1'i evet, %7,9'u hayır seçeneğini işaretlemiştir.	Ankete katılan sosyal medya kullanıcısı olan velilerin; %79,7'si evet, %6,1'i hayır, %14,2'si belirtmek istemiyor seçeneğini işaretlemiştir.
Sosyal medya kullanan veliler, çocuğunu sosyal medya kullanımındaki herhangi bir nedenden dolayı cezalandırmış mı?	Ankete katılan velilerin %75,5'i sosyal medya kullanıcısıdır.	Ankete katılan tüm velilerin; %21,6'sı evet, %63,6'sı hayır, %14,8'i belirtmek istemiyor seçeneğini işaretlemiştir.	Ankete katılan sosyal medya kullanıcısı olan velilerin; %23,1'i evet, %62,7'si hayır, %14,2'si belirtmek istemiyor seçeneğini işaretlemiştir.
Hangi yaş grubundaki öğrenciler internette ne kadar vakit geçiriyor?	Ankete katılan velilerin çocuklarının yaş gruplarına göre dağılışı şöyledir: %7,7'si 3-6 Yaş Grubu (Anaokulu), %47,7'si 7-10 Yaş Grubu (İlkokul), %28,4'ü 11-14 Yaş Grubu (Ortaokul), %11,6'sı 15-18 Yaş Grubu (Lise), %4,3'ü 18-25 Yaş Gruplarıdır.	Ankete katılan tüm velilerin çocukları; %31,5'i 1 saatten az, %41,4'ü 1-3 saat arasında, %7,2'si 4-6 saat arasında, %1,7'si 6 saatten fazla internette vakit geçiriyor. Çocukların %14,3'ü internette hiç vakit geçirmiyor.	

Ki-kare için hipotezler belirlenmiş ve ki-kare bağımsızlık testi uygulanmıştır. Ki-kare testi, ilk olarak 1900'lü yıllarda Pearson tarafından ortaya atılmıştır. Ki-kare; aritmetik ortalaması sıfır ve varyansı bir olan normal bölünmeli bir ana kütlede her biri diğerinden bağımsız olarak seçilen n birimli bir örnekleme ait değerlerin karelerinin toplamı demektir [46]. Ki-kare dağılımı; uygunluk, bağımsızlık, varyans, homojenlik ve bağımlı grup testinde oldukça sık kullanılır [47]. Ki-kare testi; iki veya daha fazla değişken grubu arasındaki ilişkinin bulunup bulunmadığını sorgulamak amacıyla kullanılmaktadır [34, 48]. Bu kapsamda çalışmada uygulanan ki-kare bağımsızlık testi ile bilgi güvenliği farkındalığı ve teknoloji kullanım kültürü arasındaki ilişki araştırılmıştır.

Ki-kare bağımsızlık testi, iki veya daha fazla değişken arasında ilişki olup olmadığını test etmek amacıyla kullanılmıştır. Ki-kare bağımsızlık testinde kategorik değişken olarak hazırlanan anket soruları çapraz tablo olarak aşağıda sunulmuştur [49]. Bu bölümde arasında ilişki olan ve farkındalık geliştirme yöntemlerine katkı sağlayan 7 hipotez hakkında detaylı bilgiler verilmiştir.

3.6.1 Çocuğun yaşı ile çocuğun evde internete girdiği ortamlar arasındaki ilişki (Hipotez 1)

Ankete katılan ebeveynlerin çocuğunun yaşı ile çocuğun evde internete girdiği ortamlar arasında bir ilişki olup olmadığını tespit etmek amacıyla ki-kare testi uygulanmıştır. Bu test sonuçlarına göre ki-kare değeri 268.1 serbestlik derecesi (df) 228, anlamlılık (p) 0.035 olarak çıkmış ve bu iki durum arasında pozitif ve anlamlı bir ilişki vardır (Tablo 3.5). Buna göre, sadece çocuk odasında internete giren çocukların tüm çocuklara oranı % 13'tür. Çocuk odasında internete giren çoğu çocuk gözetim ve kontrolden uzak olacağı için riskli grupta yer almaktadır. Bu % 13'lük riskli grubun büyük çoğunluğu (% 74) 6-14 yaş grubundadır. Özellikle istismar gibi sorunlarla karşılaşan çocukların yaş aralıklarının bu kitleyle aynı yaşlarda olması daha fazla dikkatli olunması gerektirmektedir. Çocuk odasında internete erişen çocukların % 36,9'u, 11-14 yaş grubundakilerden oluşmaktadır. Elde edilen bulgular, [50] resmi kuruluşunun sonuçları ile örtüşmektedir. 2016 yılında İngiltere'de yürüttüğü çalışmada, yatak odasında internete erişen çocukların % 40'ı erkek, % 31'i kız olan 12-15 yaşındaki çocuklardan oluşmaktadır [50].

TABLO 3.5: Çocuğun yaşı ile çocuğun evde internete girdiği oda arasındaki ilişki.

Çocuğunuz evde iken internete hangi odada/odalarda giriyor?	Çocuğunuzun yaş aralığını seçiniz.				Toplam
	Okul Öncesi (3-5)	İlkokul (6-10)	Ortaokul (11-14)	Lise (15-18)	
Çocuk Odasında	5	90	89	57	241
Çocuk Odasında, Oturma Odasında	1	5	6	5	17
Evin Her Yerinde	7	214	175	96	509
Oturma Odasında	12	361	171	40	584
Oturma Odasında, Evin Her Yerinde	0	4	0	0	4
Salonda	8	304	135	37	484
Salonda, Çocuk Odasında	0	10	9	6	25
Toplam	33	988	585	241	1852

Ki-Kare Testi			
	Değer	df	p
χ^2	268.1	228	0.035
N	1852		

3.6.2 Çocuğun cinsiyeti ile çocuğun internette geçirdiği süre arasındaki ilişki (Hipotez 2)

Ebeveynlerin çocuğunun cinsiyeti ile çocuğun internette geçirdiği süre arasında bir ilişki olup olmadığını tespit etmek amacıyla ki-kare testi uygulanmıştır. Bu test sonuçlarına göre ki-kare değeri 50.31 serbestlik derecesi (df) 8, anlamlılık (p) 0.001'den küçük olarak çıkmış ve bu iki durum arasında pozitif ve anlamlı bir ilişki vardır (Tablo 3.6). Buna göre, günde 4 saat ve üzeri bir sürede internet kullanan çocukların toplama oranı % 9.2'dir. Günde 1 saatten fazla olan tüm internet kullanım sürelerinde erkeklerin oranı kızlara göre daha fazladır. Bu bulgular, [51] tarafından yapılan çalışmayla örtüşmektedir. Erkek öğrencilerde günde 5 saat ve daha fazla internet kullanım süresinin % 16,8, kız öğrencilerde % 4,5 olduğu tespit edilmiştir [51]. Elde edilen bulgular, Ofcom (2016) resmi kuruluşunun sonuçları ile kısmen örtüşmektedir. Bu çalışmada cinsiyet ayırmaksızın yıllara bağlı internet kullanım araştırmasına göre 2007 yılından 2016 yılına kadar 3-15 yaş aralığındaki tüm yaş gruplarında haftalık internet kullanım süresi sürekli artmaktadır. Aynı çalışmada, 12-15 yaş grubunda internet kullanımı 2007 yılında haftalık 13 saat 42 dakika, 2016 yılında 20 saat 6 dakikaya ulaşmıştır [50].

TABLO 3.6: Çocuğun cinsiyeti ile çocuğun internette geçirdiği süre arasındaki ilişki.

Çocuğunuz internette ne kadar vakit geçiriyor?	Çocuğunuzun cinsiyetini seçiniz.		
	Erkek	Kız	Toplam
1 Saatten Az	295	351	646
1-3 Saat	482	368	850
4-6 Saat	101	45	146
6+	29	7	36
Hiç Geçirmiyor	139	152	291
Toplam	1046	923	1969

Ki-Kare Testi			
	Değer	df	p
x^2	50.31	8	«.001
N	1969		

3.6.3 Çocuğun internette geçirdiği süre ile ebeveynin çocuğuna sosyal medya kullanım yaşı belirleyip belirlememesi arasındaki ilişki (Hipotez 3)

Ebeveynlerin çocuğunun internette geçirdiği süre ile ebeveynin çocuğuna sosyal medya yaşı belirleyip belirlememesi arasında bir ilişki olup olmadığını tespit etmek amacıyla ki-kare testi uygulanmıştır. Bu test sonuçlarına göre ki-kare değeri 40.46 serbestlik derecesi (df) 16, anlamlılık (p) 0.001'den küçük olarak çıkmış ve bu iki durum arasında pozitif ve anlamlı bir ilişki vardır (Tablo 3.7). Buna göre, 4 saat ve üzeri bir sürede internet kullanan çocukların % 65'ine sosyal medya kullanım yaşı belirlenmemiştir. [45] çalışmasına göre ebeveynlerin % 55'i çocuklarına sosyal medya kullanım yaşı belirlememiştir. % 17'si ise bunu çocuğunun isteğine bırakmıştır.

TABLO 3.7: Çocuğun internette geçirdiği süre ile ebeveynin çocuğuna sosyal medya kullanım yaşı belirlemesi arasındaki ilişki.

Çocuğunuz internette ne kadar vakit geçiriyor?	Çocuğunuz için sosyal medya kullanmaya başlama yaşı belirlediniz mi?			
	Çocuğum ne zaman isterse	Evet	Hayır	Toplam
1 Saatten Az	31	329	287	647
1-3 Saat	46	412	391	849
4-6 Saat	9	51	87	147
6+	5	13	19	37
Hiç Geçirmiyor	11	110	172	293
Toplam	102	915	956	1973

Ki-Kare Testi			
	Değer	df	p
x^2	40.46	16	<.001
N	1973		

3.6.4 Ebeveynin güvenli sosyal medya kullanım bilgisi olup olmaması ile sosyal medyada yapılan paylaşımların gizliliği arasındaki ilişki (Hipotez 4)

beveynin güvenli sosyal medya kullanım bilgisi olup olmaması ile çocuğun evde internete girdiği ortamlar arasında ilişki olup olmadığını tespit etmek amacıyla ki-kare testi uygulanmıştır. Bu test sonuçlarına göre ki-kare değeri 32.24 serbestlik derecesi (df) 4, anlamlılık (p) 0.001'den küçük olarak çıkmış ve bu iki durum arasında pozitif ve anlamlı bir ilişki vardır (Tablo 3.8). Buna göre, sosyal medyada herkese açık paylaşım yapan ebeveynlerin % 66'sı güvenli sosyal medya kullanım bilgisine sahip olmadığını beyan etmiştir. [45] çalışmasına göre ebeveynlerin % 44'ü güvenli sosyal medya kullanım bilgisine sahip olmadığını beyan etmiştir.

TABLO 3.8: Ebeveynin güvenli sosyal medya kullanım bilgisi olup olmaması ile sosyal medyada yapılan paylaşımların gizliliği arasındaki ilişki.

Sosyal medyada yaptığınız paylaşımları kimlerin görmesine izin verdiniz?	Güvenli sosyal medya kullanımı konusunda yeterli bilgiye sahip misiniz?		
	Evet	Hayır	Toplam
Arkadaşlarımın arkadaşları	19	37	56
Arkadaşlarım	578	665	1243
Sosyal medya kullanmıyorum.	81	109	190
Herkes	41	81	122
Hiç kimse	109	241	350
Toplam	828	1133	1961

Ki-Kare Testi			
	Değer	df	p
x^2	32.24	4	«.001
N	1961		

3.6.5 Ebeveynin güvenli sosyal medya kullanım bilgisi olup olmaması ile ebeveynin daha önceden farkındalık eğitimi alması arasındaki ilişki (Hipotez 5)

Ebeveynin güvenli sosyal medya kullanım bilgisi olup olmaması ile ebeveynin daha önceden farkındalık eğitimi alması arasında ilişki olup olmadığını tespit etmek amacıyla ki-kare testi uygulanmıştır. Bu test sonuçlarına göre ki-kare değeri 52.82 serbestlik derecesi (df) 1, anlamlılık (p) 0.001'den küçük olarak çıkmış ve bu iki durum arasında pozitif ve anlamlı bir ilişki vardır (Tablo 3.9). Buna göre, daha önceden farkındalık eğitimi almamış ebeveyn oranı %83.6'dır. Farkındalık eğitimi almamış ebeveynlerde güvenli sosyal medya kullanım bilgisine sahip olma durumu %38.5'tir.

TABLO 3.9: Ebeveynin güvenli sosyal medya kullanım bilgisi olup olmaması ile ebeveynin daha önceden farkındalık eğitimi alması arasındaki ilişki.

Daha önce bu konuda farkındalık eğitimi aldınız mı?	Güvenli sosyal medya kullanımı konusunda yeterli bilgiye sahip misiniz?		
	Evet	Hayır	Toplam
Evet	196	129	325
Hayır	641	1022	1663
Toplam	837	1151	1988

Ki-Kare Testi			
	Değer	df	p
x^2	52.82	1	«.001
N	1988		

3.6.6 Ebeveynin sosyal medyada yaptığı paylaşımların gizliliği ile ebeveynin çocuğuna sosyal medya kullanım kuralı belirleyip belirlememesi arasındaki ilişki (Hipotez 6)

Ebeveynin sosyal medyada yaptığı paylaşımların gizliliği ile ebeveynin çocuğuna sosyal medya kullanım kuralı belirleyip belirlememesi arasında ilişki olup olmadığını tespit etmek amacıyla ki-kare testi uygulanmıştır. Bu test sonuçlarına göre ki-kare değeri 42.01 serbestlik derecesi (df) 4, anlamlılık (p) 0.001'den küçük olarak çıkmış ve bu iki durum arasında pozitif ve anlamlı bir ilişki vardır (Tablo 3.10). Buna göre, herkese açık paylaşım yapan ebeveynlerin % 31'i çocuklarına sosyal medya kullanım kuralı belirlememiştir. [45] çalışmasına göre, ebeveynlerin % 86'sı çocuğuna sosyal medya kullanım kuralı belirlememiştir.

TABLO 3.10: Ebeveynin sosyal medyada yaptığı paylaşımların gizliliği ile ebeveynin çocuğuna sosyal medya kullanım kuralı belirleyip belirlememesi arasındaki ilişki.

Sosyal medyada yaptığınız paylaşımları kimlerin görmesine izin verdiniz?	Çocuğunuzun sosyal medya kullanırken uyması gereken kuralları belirlediniz mi?		
	Evet	Hayır	Toplam
Arkadaşlarımın arkadaşları	46	12	58
Arkadaşlarım	1004	177	1181
Sosyal medya kullanmıyorum.	117	47	164
Herkes	84	38	122
Hiç kimse	252	85	337
Toplam	1503	359	1862

Ki-Kare Testi			
	Değer	df	p
χ^2	42.01	4	«.001
N	1862		

3.6.7 Ebeveynin çocuğuna sosyal medya kullanım kuralı belirleyip belirlememesi ile ebeveynin çocuğuna sosyal medyada tanımadığı insanlarla iletişim kurmaması konusunda uyarıp uyarmaması arasındaki ilişki (Hipotez 7)

Ebeveynin çocuğuna sosyal medya kullanım kuralı belirleyip belirlememesi ile ebeveynin çocuğuna sosyal medyada tanımadığı insanlarla iletişim kurmaması konusunda uyarıp uyarmaması arasında ilişki olup olmadığını tespit etmek amacıyla ki-kare testi uygulanmıştır. Bu test sonuçlarına göre ki-kare değeri 122.3 serbestlik derecesi (df) 1, anlamlılık (p) 0.001'den küçük olarak çıkmış ve bu iki durum arasında pozitif ve anlamlı

bir ilişki vardır (Tablo 3.11). Buna göre, çocuğuna sosyal medya kullanım kuralı belirlemeyen ebeveynlerin % 53'ü (79 ebeveyn) çocuklarını sosyal medyada tanımadığı insanlarla iletişim kurmaması konusunda uyarı yapmamıştır. [45] çalışmasına göre, ebeveynlerin % 89'u çocuğuna sosyal medyada tanımadığı insanlarla iletişim kurması konusunda uyarı yapmıştır.

TABLO 3.11: Ebeveynin çocuğuna sosyal medya kullanım kuralı belirleyip belirlememesi ile ebeveynin çocuğuna sosyal medyada tanımadığı insanlarla iletişim kurmaması konusunda uyarı yapmaması arasındaki ilişki.

Çocuğunuzu sosyal medyada tanımadığı insanlarla iletişim kurmaması konusunda uyardınız mı?	Çocuğunuzun sosyal medya kullanırken uyması gereken kuralları belirlediniz mi?		
	Evet	Hayır	Toplam
Evet	1466	280	1746
Hayır	70	79	149
Toplam	1536	359	1895
Ki-Kare Testi			
	Değer	df	p
χ^2	122.3	1	«.001
N	1895		

3.7 Bulguların Yorumlanması: Bilgi Teknolojileri Kullanım Kültürü ve Farkındalık Yöntemlerinin Geliştirilmesi

Tezin bu bölümünde, toplumun 2 farklı kesimine (ebeveyn ve genç) ilişkin BT kullanım kültürü farkındalık yöntemlerinin nasıl geliştirilebileceği, bunun faydaları ve etkilerine yer verilmiştir. Ebeveyn ve gençlerin çalışmaya dahil edilmesindeki temel neden, teknolojinin bu hızlı gelişimine ayak uydurmakta zorlanmaları ve edindikleri teknolojinin kullanım kültürüne genel olarak sahip olmayışlarıdır. Bugünün ergeni olan gençlerimizin gelecek 5-10 yıl içinde aile kuracak olmaları hem kendi neslini hem çocuklarının neslini etkileyebilecek olmalarındandır. Ebeveynler ise teknoloji kullanım kültürüne ve bilgi güvenliği farkındalığına ergenlere göre daha zor ve geç sahip olabileceği için bu kitle de çalışma kapsamına alınmıştır.

Çalışmanın devam eden bölümlerinde bu 2 farklı kitle üzerinde bilgi teknolojileri kullanım kültürü ve bilgi güvenliği farkındalığının geliştirilmesi ayrı ayrı yer verilmiştir.

3.7.1 Çocuklarda BT Kullanım Kültürü ve Farkındalık Yöntemlerinin Geliştirilmesi

Çocuklarda BT kullanım kültürü ve bilgi güvenliği farkındalık yöntemlerinin geliştirilmesi, tezin önceki bölümlerinde tespit edilen riskler üzerinden anlatılarak gençlerimizin değerlerimize daha uygun bir nesil olarak yetiştirilmesine katkı sağlanması amaçlanmıştır.

3.7.1.1 BT ve sosyal medya kullanım kültürü

Çocuklarda BT ve sosyal medya ortamlarında bir kullanım kültürünün olmayışı veya yanlış yerleşmesi ile birçok toplumsal sorun ve bozukluk meydana gelmektedir. Bunların temel nedenleri aşağıda sıralanan maddelerden oluşturmaktadır.

- Ergen bireyler, sanal dünyada yaptıklarının gerçek dünyada bir karşılığı olduğunu çoğu zaman unutmakta ve buna göre bazı zararlı davranışlar sergilemektedir. Bundan dolayı siber zorbalık faaliyetleri meydana gelmektedir.
- Ergen bireyler, ebeveynleri kadar olmasa da günümüzün sosyal ortamı haline gelen sosyal medya platformlarında görüp duydukları birçok bilgiyi teyit etmeden sanal ve gerçek dünyada faaliyetler gösterip birçok olumsuz durumun oluşmasına sebep olmaktadır.
- Ergen bireyler, gerçek dünyadaki birçok durumdan uzaklaşmak, sanal dünyada farklı ve istediği/hayal ettiği gibi bir birey olmak için teknoloji ve bunun en yaygın kullanılan sosyal medya, oyun, internet bileşenlerine bağımlı hale gelebilmektedir.

Siber zorbalık Siber zorbalık, bilgisayar, telefon veya diğer elektronik araçların ısrarlı ve başkalarına zarar veya rahatsızlık verme amacıyla kullanılmasıdır. Siber zorbalığın kapsamını oluşturan konular; şiddet, taciz, siber gözdağı, iftira, kimlik değiştirme, açığa vurma, komplo, dışlama olarak sıralanmış ve bu konular aşağıda kısaca açıklanmıştır.

- Şiddet, kısaca kaba ve kızgın bir dil kullanarak elektronik mesaj göndermek olarak açıklanabilir.
- Taciz, sürekli olarak incitici ve kaba mesajlar göndermek olarak açıklanabilir.
- Siber gözdağı, sürekli olarak zarar verme tehdidi veya onur kırıcı sözler içeren mesajlar göndermektir. Kişinin kendisini güvenlik tehdidi altında hissettiği çevrim-içi etkinliklerde yer almasıdır.

- İftira, bir kişi hakkında arkadaşlıklarını veya saygınlığını zedeleyebilecek asılsız dedikodu ve söylentileri yayma yada bu tür içerikte mesajlar göndermektir.
- Kimlik değiştirme, başka biri gibi davranarak kurban kişiyi kötü gösteren, saygınlığını zedeleyen ve tehlikeye atan mesajlar gönderme yada yayınlamaktır.
- Açığa vurma, kişinin özel yaşamına dair utandırıcı olabilecek bilgileri çevrimiçi ortamda yaymaktadır.
- Komplo, bir kişi hakkında özellikle utandırıcı bilgileri hileyle elde etmektir.
- Dışlama, kurban seçilen kişiyi kasıtlı olarak çevrimiçi grupların dışına itme veya bunu sağlamaktır [52].

Yukarıda bahsedilen bileşenlerden en az birini kullanan kişiler siber zorba, buna maruz kalan kişi ise siber zorbalık mağduru/kurbanı olarak adlandırılabilir. Bu bilgiler ışığında siber zorbalığın nedenleri 8 başlıkta aşağıda toplanmıştır.

- Öç alma duygusu ile gerçek veya sanal dünyada zarar gören özellikle kindar ergen bireyler, oluşan öç alma isteği ile sanal alemde zorbalık yapmaktadır.
- Eğlence ve dalga geçme arzusu ile fiziksel özellikleri veya yaptığı bir davranış yüzünden sanal ortamda ısrarlı biçimde dalga geçerek ve eğlenerek ergen bireyler siber zorbalık yapmaktadır.
- Farklı görünüş ve görüşlerden olan kişileri cezalandırma arzusu ile daha çok aile ortamından örnek alarak ergen bireyler kendisinden farklı görünüş ve görüşlerden olan kişileri cezalandırma eğiliminde olan ergen bireyler din, dil, ırk veya farklı siyasi görüşlerde olanlara karşı siber zorbalık yapmaktadır.
- Fiziksel dünyada elde edemediği başarıyı sanal ortamda yakalama arzusu ile özellikle içe kapanık ve içten pazarlıklı bireylerde karşımıza çıkabilecektir. Bu istekle çok istediği bir spor dalında gerçek dünyada başarılı olamayan ergen bireyler sanal ortamda başarılı bireylere karşı siber zorbalık faaliyetleri yürütmektedir.
- Popüler olma ve güç arzusu ile birçok ergen birey arkadaş gruplarındaki en zayıf bireylere karşı güç gösterisini gerçek dünya ile siber ortamda yapabilmektedir. Bu durum sosyal statüsünü yükseltme isteyen ergenlerde de karşımıza çıkabilir.
- Düşük özgüven ve özsaygısı bulunan ergen bireyler, kendilerine çok fazla saygıları olmadığı için başkalarına da saygısız bir dil kullanarak siber zorbalık faaliyetleri yapmaktadır.

- Aile içinde yaşanan sorunları etrafına yansıtan ve genellikle saldırgan, başına buyruk davranan ergen bireyler aynı davranışları sanal ortamda da göstererek siber zorbalık faaliyetleri yapmaktadır.
- Akıl sağlığı sorunları olan ergen bireyler ise gerçek dünyadaki sorunlu davranışları sanal ortamda da göstererek siber zorbalık yapabilmektedir [53].

Zorbalık, geçmiş yıllarda ergen bireylerde daha çok bir araya geldikleri ortam olan okullarda veya sokakta yapılmakta ve insanların hafızalarına göre kayıtlı kalmaktaydı. Eskiden yapılan zorbalık faaliyetleri araya çeşitli nedenlerle zaman girmesi ile kesintiye uğramakta ve zorbalığı devam ettirecek kişi veya çevrelerin hafızası kadar gün yüzüne çıkmaktaydı. Bu şekilde mağdur olan birey daha seyrek ve kısa süreyle zorbalığa maruz kalmaktaydı. Fakat artık yaygınlaşan elektronik mesajlaşma ve sosyal medya platformları üzerinden yapılan siber zorbalık mağduru/kurbanı olan bireyler eskiye nazaran daha sık, daha uzun süre ve daha yaygın çevre ile zorbalığa maruz kalmaktadır.

Bu bilgiler ışığında ergen bireylerin siber zorbalık faaliyetleri hakkında farkındalık yöntemlerini geliştirmek için aşağıda sıralanan maddeler tespit edilmiştir.

- Ergen bireyler, kendisi ve sevdikleri ilgili sosyal medya ve yazışma ortamlarında bir şey paylaşmadan önce iki kez düşünmelidir. Bu düşünme sırasında paylaşılan materyalin daha sonra kendi ve sevdikleri aleyhinde defalarca ve farklı amaçlarla çarpıtılarak kullanılabilceğinden emin olmalıdır. Mümkünse güven ilişkisinin olmadığı ortamlarda riskli paylaşımlar yapmamalıdır.
- Ergen bireyler, hayatlarında her olup biteni paylaşmamalıdır. Buna sebep olan fazla egodan kaynaklanan ön planda ve gündemde olma arzusu olarak tahmin edilmektedir.
- Ergen bireylerin elektronik ortamdaki tüm erişim şifrelerini sadece kendisi ve ailesi bilmelidir. Okul notlarının görüntülediği sistemin şifresinden sosyal medya hesaplarının şifresine kadar tüm şifrelerin saklı kalması gerekmektedir. Aksi durumda kötü niyetli kişiler tarafında ele geçirilen şifreler ile birçok zorbalık faaliyeti yapılabilmektedir.
- Ergen bireyler, sosyal medyada paylaştığı gönderilerin kimler tarafından görülebileceğini ayarlamalıdır. Aksi durumda herkese açık şekilde paylaşılan bilgi, görsel ve videolar sahte hesaplarda kullanılarak iftiradan dolandırıcılığa kadar birçok farklı kötü emel için kullanılabilir.
- Ergen bireyler, sosyal medyada yaptığı faaliyetleri ebeveynleri ile paylaşmalı, ebeveyn ve sevenlerinin kendisini sosyal medyada takip etmesine izin vermelidir. Bu sayede

olası bir zorbalık faaliyetine maruz kalma durumunda ebeveynlerin alabileceği önlemlerle daha etkili sonuçlar alınabilecektir.

- Ergen bireyler, başka bir arkadaşı hakkında zorbalık faaliyetine tanık olduğu andan itibaren ebeveyn, öğretmen veya güvenilir başka birine durumdan bahsetmelidir.
- Son olarak ergen bireyler, zorbalık mağduru olan başka birine karşı nazik olmalı, tüm ortamlarda onların yanında olmalı ve yalnız olmadığını bilmesine yardımcı olmalıdır.

Yukarıda bahsedilen farkındalık oluşturma yöntemleri uygulanmadığı takdirde, sosyal çevreden uzaklaşan, başka sorunlu çevrelerle irtibata geçen ergenlerin çoğalması sağlanacaktır. Özellikle aşırıya giden siber zorbalık faaliyetlerinde veya içe kapanık bireylerin siber zorbalık mağduru olması durumunda intiharla sonuçlanan vakalar ortaya çıkabilmektedir.

Ergenlerde siber zorbalık hakkında farkındalık yöntemlerinin geliştirilmesini sağlamak ve bunu sürekli hale getirmek için aşağıdaki çalışmaların yürütülmesi faydalı olacaktır.

- Ergenlerin en çok zamanlarını geçirdiği okuldaki yönetici ve öğretmenlerin tümü siber zorbalık faaliyetlerini önlemek, doğru müdahale ve diğer süreçleri doğru yönetmek için bilinçlendirilmelidir.
- Ergenlerin ebeveynleri kendi çocuklarının siber zorbalık yapmaması veya mağdur olmaması için bilinçlendirilmelidir.
- STK, kamu kuruluşu, hukuksal altyapı desteği ile toplumun tüm kesimleri siber zorbalık faaliyetlerini azaltıcı ve bilinçlendirici fiziksel veya sanal ortamda çalışmalar yapmalıdır.
- Siber zorbalık faaliyetlerinin ihbar edilebileceği bir web sitesi kurularak, bu sitede yaş gruplarına göre zorbalığa müdahale yöntemlerinin anlatılması, ebeveynlere ve ergenlere her türlü danışmanlık faaliyetlerinin verilmesi gün geçtikçe daha önemli hale gelmektedir.

Sosyal medya üzerinden yanlış yönlendirme Ergen bireyler, özellikle tecrübesizlikleri ve idol edindikleri tam olarak tanımadığı kişilerin sosyal medyadaki aleni ve üstü kapalı yönlendirmelerine maruz kalabilmektedir. Bu durumun temel sebebi olarak ebeveynlerinden kopup birey olma arzusu ile başka insanlara daha fazla değer vermesinin sonucunda daha ileri boyutlara taşınmaktadır. Aşağıda iki ana grupta toplanmış yanlış yönlendirme türlerine yer verilmiştir. İlk kısa vadede ikincisi ise uzun vadeli yanlış yönlendirme olarak düşünülebilir.

- Din, dil, ırk, siyasi görüş gibi farklılıklara sahip insanlara karşı sosyal medyada yönlendirmeler ile sanal ve fiziksel dünyada linç girişimleri yapabilmektedir.
- Belirli bir sorun üzerine toplumsal galeyamı tetikleyecek paylaşımlara itibar ederek çeşitli çevreler tarafından ekilen öfke tohumlarını bünyesine katıp onunla büyüyen ergen bireyler günümüzde ve gelecekte farklı amaçlar için kullanılabilir.

Bu bölüm için Hipotez 7'den faydalanılmıştır. Hipotez 7'de, çocuğuna sosyal medya kullanım kuralı belirleme ile sosyal medyada tanımadığı kişilerle iletişim kurup kurmaması arasındaki ilişki test edilmiştir. Buna göre çocuğuna sosyal medya kullanım kuralı belirlemeyen ebeveynlerin % 22'si aynı zamanda çocuğunu sosyal medyada tanımadığı kişilerle iletişim kurmaması için uyarınmıştır. Sosyal medya kullanım kuralı belirlenmeyen çocukların ve herkesle iletişim kurabilen çocukların sosyal medya üzerinden yanlış yönlendirilmesi ve diğer riskler açısından dikkate alınması gerekmektedir. Bu bilgileri ışığında ergen bireylerin sosyal medya üzerinde yanlış yönlendirme hakkında farkındalık geliştirilmesi için aşağıdaki durum tespit edilmiştir.

- Ergen bireylerde oldukça yaygın olan sosyal medya kullanımının toplumsal değerlerimizi merkeze alacak şekilde kullanım kültürünün fiziksel ve sanal ortamlarda anlatılması gerekmektedir. Bunun için bakanlık ve diğer merkezi kuruluşlar, GSM operatörleri, yerel yönetimler, STK ve aile ölçeğinde sosyal medya kullanım kültürü ergen bireylere farklı ortamlarda farklı konular üzerinden anlatılmalı ve onların farkındalık kazanması sağlanmalıdır.

Teknoloji bağımlılığı Ergen bireyler üzerinde teknoloji bağımlılığına karşı farkındalık geliştirmek için teknoloji bağımlılığı kapsamına giren konuların ortaya konması gerekmektedir. Teknoloji bağımlılığı bir çatı ifade olarak internet, oyun ve sosyal medya bağımlılığı olmak üzere 3 bağımlılığı kapsamaktadır. Özellikle teknoloji ve internet bağımlılığı birbirine fazla karıştırılan iki farklı terimdir. Teknoloji bağımlılığı; insan-makine etkileşimini içeren ve kimyasal olmayan (davranışsal) bağımlılıklar olarak tanımlanır [54]. Kimyasal bir bağımlılık olmayan bu 3 bağımlılık türü aslında kimyasal ve organik madde bağımlılığına göre daha tehlikeli ve yaygınlaşma ihtimali kolay olan bağımlılıklardır. Çünkü bir madde bağımlısının maddeye ulaşma ihtimali teknoloji bağımlısının ilgili materyale ulaşmasına göre daha zordur. İkinci durum ise teknoloji bağımlısı olan birey madde bağımlısına göre daha uzun süreli mutluluğa erişebilmektedir. Son ve en önemli fark olan konu ise madde bağımlılığında her birey aynı madde ile bağımlı olurken teknoloji bağımlılığı ise kişiye özel bir uyuşturucu olarak nitelendirilebilir. Bu durumu oyun ve sosyal medya bağımlılığı üzerinden açıklamak daha iyi olacaktır. Birey sosyal medyada veya oyunda kendi oluşturduğu bir karaktere veya profilin dünyasına bağımlı

hale gelmektedir. Bu da aslında madde bağımlılığına göre kurtulması daha zor bir bağımlılık olarak ortaya çıkmaktadır.

Teknoloji bağımlılığı sadece uzun süre teknolojik cihaz ve yazılım kullanımı ile ortaya çıkan bir bağımlılık değildir. Henüz teknoloji bağımlılığı ile ilgili olarak tanı koyma bileşenlerine rastlanmamıştır. Bundan dolayı internet bağımlılığı için oluşturulan bileşenlere yer verilecektir.

Bireylerde internet bağımlılığı tanısı koyabilmek için Amerikan Psikiyatri Birliği mental bozuklukların tanısal ve istatistiksel rehberinde (Diagnostic and Statistical Manual of Mental Disorders-DSM) bazı bileşenler tespit etmiştir. Öte yandan başka bir çalışmada aşağıdaki 6 bileşen tespit edilmiştir.

- Dikkat çekme (saliency); Gerçekte internete bağlı (çevrim içi) olmasalar bile internete bağlı olacakları zamanı düşünme
- Duygu durum değişikliği (mood modification); internete bağlandıklarında duygusal olarak kendilerini iyi hissetme
- Zamanda uzama (tolerance); başlangıçta kısa süreli internette kalma ile aldığı hazzı sonraları daha uzun zamanda elde etmesi
- Geri çekilme belirtileri (withdrawal symptoms); internette kalması engellendiğinde titreme, karamsarlık ve sinirlenme gibi davranışlara yol açma
- Çatışma (conflict); çeşitli aktivitelerde başkaları ile ya da kişinin kendisi ile içsel çatışmalara girmesini konu alma
- Nüksetme (relapse); belli bir süre uzak durulduktan sonra tekrar çevrim içi olduğunda hastalığın uç seviyeye ulaşmasını konu almak olarak sıralanmıştır [54].

Buna ek olarak ülkemizde, Yeşilay tarafından teknoloji bağımlılığının belirtileri aşağıdaki 8 başlıkta toplanmıştır.

- Yalnızca birkaç dakika diyerek saatler harcamak,
- Çevrenizdekilere ekran karşısında geçirdiğiniz zaman hakkında yalan söylemek,
- Uzun süre bilgisayar kullanmaktan dolayı fiziksel sorunlardan şikayet etmek,
- Anonim bir kişiliğe bürünmek, insanlarla internet üzerinden konuşmayı yüz yüze konuşmaya tercih etmek,
- İnternete girmek için yemek öğünlerinden, derslerden ya da randevulardan ödün vermek,

- Bilgisayarınızın başında çok fazla zaman geçirdiğiniz için suçluluk duyuyorken bir yandan da büyük bir zevk almak ve bu iki duygular arasında gidip gelmek,
- Bilgisayarınızdan uzak kaldığınız zaman gergin ve boşluktaymış gibi hissetmek,
- Gece geç saatlere kadar bilgisayar başında kalmak olarak sıralanmıştır [55, 56].

Bu bölümde Hipotez 3'den faydalanılmıştır. Bu hipotezde, çocuğun internette geçirdiği süre ile ebeveynin çocuğuna sosyal medya kullanım yaşı belirleyip belirlememesi test edilmiş ve arasında ilişki olduğu ortaya çıkmıştır. Buna göre 3 saatten fazla internet kullanan çocukların % 65'ine sosyal medya kullanım yaşı belirlenmediği beyan edilmiştir. Bu durum teknoloji bağımlılığı için riskli bir durum olarak değerlendirilmektedir. Bu bilgiler ışığında teknoloji bağımlılığının kapsamına giren 3 bağımlılığın özellikleri üzerinde durularak bunlara karşı farkındalık geliştirme yöntemlerine yer verilmiştir.

Ergen bireylerde internet bağımlılığına karşı farkındalık geliştirmek için merkezi kuruluşlar, yerel yönetim, STK ve okul ve ebeveyn tarafından internetin gerçek dünyanın bir alternatifi olmadığı ve internetin daha çok faydalı taraflarına odaklanılması gerektiği anlatılmalıdır. Burada özellikle ebeveynlerin üzerine bu politika ile ters düşecek davranışlardan kaçınması gerekmektedir. Diğer kuruluşların ise merak duygusunu giderme, araştırma geliştirme ve inovasyon kültürünün aşılmasında internetin faydalı taraflarını kullanırmaya yönlendirmesi oldukça önemlidir.

Oyun bağımlılığı ise daha çok çevrim içi oyunlarda oluşturulan karakterler üzerinden oluşmakta ve ergen bireylerde yukarıda bahsedilen belirtileri taşımaktadır. Oyun bağımlılığı en çok gerçek dünyadaki zayıf yanlarını sanal oyunlarla kapatmak isteyen, orada başarılı olmak isteyen, gerçek dünya sorunlarından kaçınmak isteyen ergen bireylerde ortaya çıkmaktadır. Bu bağımlılık türüne karşı farkındalık oluşturmak için kuruluşlar ve aile üyelerine yine birtakım görevler düşmektedir. Kuruluşlar ve ebeveynler, ilk olarak ergen bireyleri sanal oyun yerine gerçek dünya oyunlarına ve sporlarına yönlendirmelidir. Sanal ortamda oynanan oyunları şiddetten müstehcenliğe ve bağımlılık yapma durumuna göre değerlendiren bağımsız kuruluşlar olmalı ve buna göre sanal ortamdaki oyunlar kontrol altına alınmalıdır. Oyunlardan doğrudan koparmak yerine bunların diğer aile üyeleri ile oynanabilir oyunlara yönlendirilebilir. Özellikle STK, şirket ve kamu eliyle oyun bağımlılığına meyilli ergen bireyleri oyun yazılımı üretecek nesillere dönüştürme yatırımları yapılabilir.

Son olarak sosyal medya bağımlılığı, günümüzde diğer iki bağımlılığa göre daha önemli hale gelmiştir. Sosyal medyada ergen bireylerin oluşturduğu hesaplar ile kendilerini mutlu hissedecekleri arkadaş, grup ve sayfaları seçerek kendilerine gerçek dünyadan bağımsız bir dünya yaratabilmektedir. Sosyal medya bağımlılığı, sürekli son gelişmeleri takip etme

bozukluğunun haricinde kendisine oluşturdukları dünyada mutlu olmaya bağımlı olmaları olarak da yorumlanabilir. Sosyal medya bağımlılığı ayrıca kendini sürekli iyi ve mutlu gösterme bağımlılığı haline de gelmektedir. Ergen bireylerde sosyal medya bağımlılığına karşı farkındalık oluşturmak için ilk olarak sosyal medyada yapılan her faaliyeti gerçek dünyada yapmasının bireyselleşme eğiliminde olan z kuşağının idrak etmesi gerekmektedir. Bu durum ancak toplumsal olarak sosyal medyadan gerçek dünyaya göç ile mümkün hale gelecektir. Özel hayatın ifşası, aile mahremiyeti, her olup biteni paylaşan kullanıcılar ile sosyal medyayı günümüzde özellikle manevi değerlerimizle çelişen bir yapıda kullandığı için buna karşı manevi değerlerimize daha fazla ağırlık verilmesi gerekmektedir.

3.7.1.2 Bilgi güvenliği farkındalığı

Bilgi, günümüz ve gelecekte daha da önemli bir varlık haline gelecektir. Tecrübesizliğin yanı sıra her şeyi daha aleni yaşayan, vurdumduymaz ve keyfine daha düşkün bir genç nesil özellikle sosyal medya üzerinden kendisine ve yakınlarına ait birçok bilgiyi paylaşabilmektedir. Sosyal medya üzerinden kaptırılan bilgiler fiziksel dünyada yapılacak kısa bir araştırma ile desteklendiğinde maddi ve manevi birçok soruna sebep olmaktadır.

Günümüz gençliğinde bilgi güvenliği farkındalık yöntemi geliştirmek için z kuşağının özelliklerini dikkate alarak sık karşılaşılan riskler göz önünde bulundurulmuştur. Buna göre aşağıda sıralanan konular farkındalık geliştirme yöntemi olarak kullanılabilir.

- İlk olarak sosyal medya üzerinde birçok bilgisini paylaşan gençlerin bunun fiziksel dünyada ne anlama geldiği idrak ettirecek çalışmaların yapılması gençlerde bilgi güvenliği farkındalığını geliştirecektir. Bunu bir örnek üzerinden açıklamak gerekirse; sosyal medya biyografisinde hangi okula gittiğini, neleri sevdiğini, yaklaşıklık konumunu paylaşmanın, sokakta üzerinde bir tabelaya veya kıyafetine basılı şekilde gezme ile aynı olduğunu idrak ettirmek farkındalığın gelişmesini sağlayacaktır.
- Özellikle sosyal medya ortamında yakınlarının iznini istemeden birlikte çekilmiş görsel materyali veya konumu paylaşan gençler siber suçların yanında fiziksel suçlarda kullanılacak bilgilerin kaybedilmesini sağlamaktadır. İzin istemeksizin sosyal medyada paylaşılan her bilginin başkaları için çok değerli bilgiler olabileceğini idrak ettirecek çalışmaların yapılması bilgi güvenliği farkındalığını geliştirecektir.
- Sosyal medya profilinin ve gönderilerin herkese açık biçimde paylaşılması veya her takipçi isteğinin kabul edilmesi gibi güvenlik önlemlerinin alınmadığı durumlarda ortaya çıkabilecek sorunları idrak ettirecek çalışmalar üzerinden bilgi güvenliği farkındalığının geliştirilmesini sağlayacaktır. Bu durum önceki maddeler ile aynı

senaryoda kullanılarak farkındalığın daha kalıcı ve etkili hale gelmesini sağlayacaktır.

- Fiziksel dünyada aleni yapılan her aktivitenin sosyal medyadaki bilgiler ile birleştirilerek birçok olumsuz duruma neden olabileceğini idrak ettirecek çalışmaların yapılması bilgi güvenliği farkındalığını geliştirecektir. Örnek olarak bir toplu taşımada, çağrı merkezinden arayan kişiye bazı anahtar bilgilerin verilmesi veya çok yakın arkadaşı ile detaylı ve anahtar bilgilerin konuşulması ortamdaki kötü niyetli kişilerin faaliyetlerini kolaylaştırabilecektir.
- Özellikle siber zorbalık faaliyetlerinde kullanılan birçok bilginin, herkese açık paylaşılan gönderilerden elde edilerek zorbalık faaliyetlerinde kullanıldığını idrak ettirecek çalışmalar bilgi güvenliği farkındalığını geliştirecektir.
- Sosyal medya üzerinden bir gönderiye yorum yaptırarak, kişilik testi, fal gibi paravan materyaller üzerinden toplanan bilgilerin gençlerin aleyhinde kullanılabilceğini idrak ettirecek çalışmaların yapılması bilgi güvenliği farkındalığını geliştirecektir.
- Son olarak şirketler tarafından ücretsiz olarak sunulan tüm mobil ve web uygulamalar (sosyal medya gibi) üzerinden alınan bilgilerin karşılıklı kişisel bilgi paylaşımı ve işlenmesi anlaşmaları ile pazarlamadan kötü niyetli taraflarca kullanılmasına kadar birçok alanda kullanılabilceğinin idrak ettirilmesi bilgi güvenliği farkındalığını geliştirecektir.
- Özellikle bankacılık işlemlerinde ortalama yöntemi ile bilgilerin çalınmaması için teyit mekanizmasını kullandıracak çalışmaların yapılması ile bilgi güvenliği farkındalığı geliştirilebilecektir.

3.7.2 Ebeveynlerde BT Kullanım Kültürü ve Farkındalık Yöntemlerinin Geliştirilmesi

Ebeveynlerde BT kullanım kültürü ve bilgi güvenliği farkındalık yöntemlerinin geliştirilmesi, tezin önceki bölümlerinde tespit edilen riskler üzerinden açıklanarak ebeveynlerimizin değerlerimizi kaybetmemesi ve çocuklarını daha iyi bir nesil olarak yetiştirmesine katkı sağlanması amaçlanmıştır.

3.7.2.1 BT ve sosyal medya kullanım kültürü

Ebeveynlerde, BT ve sosyal medya kullanım kültürünün olmayışı veya yanlış yerleşmesi ile kendilerinde ve çocuklarında birçok toplumsal sorun ve bozukluk meydana gelmektedir. Bunların temel nedenleri aşağıda sıralanan maddelerden oluşturmaktadır.

- Ebeveynler, günümüzün sosyal ortamı haline gelen sosyal medya platformlarında görüp duydukları birçok bilgiyi teyit etmeden sanal ve gerçek dünyada faaliyetler gösterip birçok olumsuz durumun oluşmasına sebep olmaktadır.
- Ebeveynler, çocuklarının erken yaşlarda meşgul olmaları ve kendilerini rahatsız etmemeleri için ellerine verdiği her teknolojik aletin aslında ileride davranış bozukluklarından teknoloji bağımlılığına kadar birçok sorunun oluşmasına neden olmaktadır.
- Ebeveynler, tam olarak olgun bir birey haline gelmemiş çocuklarına, bireyselleşme ve ben duygusunu ön plana çıkaracak davranış ve imkanları ile (kendi odasını verme ve o odada internet erişim imkanı vermeleri gibi) siber zorbalık, cinsel istismar ve teknoloji bağımlılığı gibi birçok sorunun oluşmasına ortam hazırlayabilmektedir.
- Ebeveynler, yetişmiş oldukları mahrem aile hayatını bazen kendi elleri ile bazen de çocuklarına bir teknoloji kullanım kültürü vermemiş olmaları nedeniyle aile mahremiyetinin ve bilgi güvenliğinin zarar görmesine neden olmaktadır.
- Ebeveynler, sosyal medya üzerinden kendilerinin ve çocuklarının aynı saniyeler içerisinde duygusal karışıklığa sürüklenmektedir. Sonuç olarak ruhsal bozuklukların ve umursamazlığın aile bireylerinde kalıcı hale gelmesine neden olmaktadır.

İnternet yalanları İnternet yalanı; internet üzerinden belirli bir kitleyi hedeflenen amaca göre direkt veya dolaylı olarak yönlendirmek için hazırlanmış teyidi zor olan kısmen veya tümüyle yanlış bilgilerdir. Bu bilgiler, bazen sanal bazen de fiziksel dünyada aksiyona dönüşebilmektedir. Aksiyona dönüşmeyen birçok internet yalanı da kitleler üzerinde algı oluşturmak amacıyla yayımlanmaktadır. Günümüze kadar taraflı basın-yayın organları üzerinden gelen haberler artık internet siteleri ve özellikle sosyal medya üzerinden çok çeşitli şekillerde kitlelere ulaşmaktadır. Bu bilgiler, kitlelerin ilgi alanlarına göre hazırlanmış sosyal medya ortamlarında veya web sitelerinde yayına alan kötü niyetli kişi veya kuruluşlarca toplumun hassas değerlerine saldırı yapılmaktadır.

İnternet ve sosyal medya kullanımının son 10 yılda birçok yaş grubunda bir kullanım kültürüne sahip olmadan yaygınlaşması kötü niyetli kişilerin amaçlarını gerçekleştirebilmesine olanak sağlamaktadır. İnternet ve sosyal medya sitelerinde karşısına çıkan fikir, içerik ve yönlendirmelere sorgulamaksızın ve teyit etmeden inanıp istenen şeyi yapan birçok ebeveyn, hem kendisinin yanlış bir fikre kapılmasına hem de yanlış bilginin yayılmasına sebep olmaktadır. İnternet yalanlarının amacına ulaşmasını sağlayan temel faktör, toplumumuzda bir teknoloji kültürünün olmaması veya yanlış oluşturulmasıdır. Ciddi bir toplumsal sorun haline gelen internet yalanlarının oluşma sebepleri,

yaygınlaşma sebepleri ve farkındalık geliştirme yöntemlerine bu bölümde yer verilmiştir. İnternet yalanlarının oluşmasını sağlayan sebepler aşağıda sıralanmıştır.

- İlk olarak eğlence amaçlı hazırlanan internet yalanları, takipçi sayılarının çok olduğu internet ve sosyal medya sayfalarında dolaşıma sokulmaktadır. Özellikle önemli ve faydalı bir içerikmiş gibi hazırlanan bu yalanlar bazen bir kurumu hedef alırken bazen de bir değeri hedef alabilmektedir.
- Paylaşıldığı sayfayı takip eden insanları tahrik etmek ve öfke tohumlarını ekmek için internet yalanları hazırlanmaktadır. Örnek olarak, dini değerlere bakışı daha hassas kişilerin toplandığı sayfalarda dini değerleri hedef alan ve belirli bir amaca göre yönlendirmek için hazırlanmış birçok içerik bulunmaktadır. Bu sayede içerikte hedef gösterilen kişi, grup, düşünceye karşı öfkeyi körüklemektedirler.
- Bir kişiye, kuruma veya topluluğa iftira atmak ve istenen amaçta algı oluşturmak, topluma buna karşı harekete geçirmek için internet yalanları hazırlanmaktadır.

İnternet yalanlarının etkili olabilmesi için büyük kitlelere ulaştırılması gerekmektedir. İnternet yalanlarını hazırlayan kişiler bu yaygınlaşmayı da sağlamaktadır. İnternet yalanlarının yaygınlaşma sebeplerine aşağıda yer verilmiştir.

- Teknoloji kullanım kültürünün olmadığı veya yanlış olduğu bireyler, internet ve sosyal medya sitelerinde karşılaştığı içerikleri tam olarak okumadan ve teyit etmeden hem sanal hem de gerçek dünyada yaygınlaştırmaktadır. Özellikle içeriğin faydalı olduğu kanısına hemen kapılan ebeveynlerimiz gönderiyi tam olarak okumadan paylaşım asılsız içeriğin yayılmasına katkıda bulunmaktadır.
- Siyasi, dini, milli bir algı oluşturmak için hazırlanan asılsız içerikler iki farklı görüşe sahip bireylerce paylaşarak yaygınlaşmaktadır. İlk görüşe sahip olan bireyler, haberin yalan olduğunu yazarak, ikinci gruptakiler de muhalif görüş bildirmek suretiyle aynı içeriği yaygınlaşmasına sebep olmaktadır.

İnternet yalanlarının sebepleri ve yaygınlaşmaya etki etken faktörler ışığında farkındalık geliştirme yöntemleri aşağıda sıralanmıştır.

- Ebeveynler öncelikle internet ve sosyal medya sitelerinde karşılaştığı içeriği tam olarak okuyup anlamalıdır. Bu açıdan sosyal medya okuryazarlığı eğitimleri ebeveynler için faydalı olacaktır.
- Okunan ve anlaşılan içerikler paylaşmadan veya gerçek dünyada harekete geçmeden önce iki kez düşünülmelidir. Sosyal medyada yapılan her hareketin gerçek

dünyayla özdeşleştirilmesi gerekmektedir. Paylaşılan her içeriğin altına imza atıldığı bir kağıt olduğunu idrak edilmesi oldukça önemlidir. Bu sayede daha sağlıklı bir sanal dünyaya sahip olunacaktır. Aksi takdirde sosyal medya üzerinden suça karışma ihtimali artacaktır.

- Çocuklarını ne tür insan ve bilgilerin bulunduğu sosyal medyaya teslim etmeden önce ebeveynlerin hem kendisi hem de çocukları için sosyal medya risklerine karşı tedbirli olmaları gerekmektedir.
- Sosyal medyada asılsız içeriği yayan her ebeveynin başkalarının tetikçisi ve algı kurbanı olduğunu idrak ettirecek çalışmaların yapılması gerekmektedir.

İnternet yalanlarına inanma potansiyeli olabilen ebeveynler yani güvenli sosyal medya kullanım bilgisine sahip olmayan ebeveyn oranı % 57'dir (Hipotez 5). Ayrıca ankete katılan ebeveynlerin % 83'ü daha önce bilgi güvenliği farkındalığı eğitimi almadığını beyan etmiştir. Ebeveynlerin büyük kesiminin bu şekilde olduğu varsayıldığında internet yalanlarından zarar görme riski artabilir.

Çocukların erken yaşta yanlış kullanım ile teknolojiye teslim edilmesi Çocuklarının erken yaşta meşgul olması, mutlu olması gibi amaçlarla bir kullanım kültürü olmadan verilen teknolojik aletin çocuklarının gelecekte de o aletlerle mutlu olmayı öğrenmesini sağlamaktadır. Erken yaşta bir çocuk neye teslim edilirse ileri yaşlarda da aynı şeyden koparılmak için uğraşılacaktır. Bu durum kendisini bazen teknoloji bağımlılığı bazen de içe kapanıklık ve bunların getirileri ile karşımıza çıkmaktadır. Bunları engellemek için aşağıda sıralanan farkındalık yöntemlerinin geliştirilmesi oldukça önemlidir.

- Kuralsız her kullanımda olduğu gibi teknolojik aletlerin de erken yaşlarda kuralsız bir biçimde çocuklara teslim edilmemelidir. Çocuğa teknoloji alet ve diğer bileşenleri teslim edilmeden önce ebeveynler kendilerini bu konuda geliştirmeli ve eğitmelidir. Daha sonra çocuğuna en uygun kullanımı belirleyerek çocuklara teknolojiyi vermelidir.
- Ebeveynlerin yanlış teknoloji kullanım politikaları sonrası teknoloji bağımlılığına doğru ilerleyen süreci kontrol altında tutabilmesi için teknoloji bağımlılığının kapsamı, bileşenleri ve çözüm önerileri hakkında gerekli bilgilendirme ve eğitimlerin yapılması gerekmektedir. Günümüzde çoğu ebeveyn teknoloji bağımlılığı uzun süreli teknoloji kullanımı olarak idrak etmektedir. Teknoloji bağımlılığına karşı yapılması gerekenleri ilgili STK, yerel yönetim ve merkezi kuruluşlardan talep etmelidir.

Bu bölümde, hipotez olarak belirlenmemiş fakat Ki-kare analizi sonucunda çıkan iki değişken arasında ilişki olduğu tespit edilmiştir. Buna göre çocuğun yaşı ile cep telefonunda internet varlığı arasında bir ilişki olduğu tespit edilmiştir. Ankete göre ankete katılan ebeveynlerin % 31'inin çocuğunda internet olduğu tespit edilmiştir. İnternete sahip olan çocukların % 27'si 10 yaşından daha küçüktür. Bu kesimin erken yaşta teknoloji ve internet erişiminin getirebileceği birçok risk bulunmaktadır. Ayrıca bu bölümde Hipotez 2'den faydalanılmıştır. Buna göre bir günde erkek öğrencilerin % 12'si, kız öğrencilerin % 5'i 3 saatten daha fazla internette vakit geçirmektedir. Bu oranlar özellikle erkek öğrencilerin yanlış teknoloji kullanımında daha riskli olduğu anlamına gelebilir.

Ayrıca Bakırköy Ruh Sağlığı ve Sinir Hastalıkları Hastanesi İnternet Bağımlılığı Polikliniği'ne başvurmak teknoloji bağımlılığını kontrol altına almak için değerlendirilmelidir. Özellikle ebeveynlerin teknoloji bağımlılığı hakkında en çok ihtiyaç duyduğu bağımlılığı kontrol altına alma yöntemleri Yeşilay tarafından 13 başlıkta toplanmıştır.

- Günlük teknoloji kullanımını tam zıt saatlere kaydırmak,
- Dış durdurucular kullanmak,
- Teknoloji kullanımı ile ilgili hedefler belirlemek,
- Çok kullanılan belli işlevlerden uzak durmak,
- Hatırlatıcı kartlar kullanmak,
- Kişisel defter oluşturmak,
- Aile terapisine başvurmak,
- Hedefler koymak,
- Kullanılan teknolojik cihazı ailece toplu kullanmak,
- Spor yapmak,
- Düşünceleri kontrol etmek,
- Yeni sosyal becerilerin kazanılması,
- Yardım istemek olarak sıralanmıştır [55, 56].

Ayrıca bireylerin internet bağımlısı olma riskini kontrol etmek için internet bağımlılığı testi hazırlanmıştır [55, 56].

Bireyselleşen internet kuşağını bekleyen teknolojik tehditler Günümüz çocuk ve gençleri, tezin 'Kuşaklar' bölümünde de yer verildiği üzere Z kuşağı/internet kuşağı gibi farklı isimlerle adlandırılan, ebeveynlerinden oldukça farklı özelliklere sahip olan bir nesil olarak yetişmektedir. Y ve Z kuşağı mensubu olan birçok ebeveyn, kendilerine oranla daha az sayıda ama daha iyi yetişmiş bir çocuk hayali ile aile yapısını şekillendirmektedir. Bu sayede Z kuşağı, proje çocukların yetiştiği bir nesil olarak da adlandırılmaktadır. Çocuğunun isteklerini azami derecede yerine getiren daha o talep etmeden birçok imkanı elinde bulan Z kuşağı çocukları dolayısı ile daha fazla ben duygusunu sivrilen, yüksek özgüven sahibi bir kuşak olarak yetişmektedir. Bu duygu, davranış ve imkanlarla yetişen Z kuşağı, yanlış veya olmayan teknoloji kullanım kültürü ile teknolojinin faydasından çok zararından etkilenir hale gelmektedir. Ebeveynler üzerinden bu tür zararları engellemek için geliştirilen farkındalık yöntemleri aşağıda sıralanmıştır.

Ebeveynlerin Z kuşağı mensubu çocuklarına gösterdiği davranış, tutum ve imkanlar onların daha fazla bireyselleşmesini, yüksek özgüvene sahip olmasını ve sosyal statüye, popüleriteye önem vermesi sağlamaktadır. Bu durumlar ile yanlış veya hiç olmayan teknoloji kullanım kültürü, Z kuşağında bazı önemli durumlarda çok daha kötü sonuçlarla karşılaşılmasını sağlamaktadır. Bu durumlardan ilki siber zorbalık faaliyetlerinin yaygınlaşması ve bu zorbalığa karşı daha kötü sonuçların ortaya çıkmasını sağlamaktadır. Yüksek özgüven sahibi ve sosyal statüye önem veren Z kuşağı kesimi siber zorbalığa daha yatkın olabilmekte ve zorbalık içeren davranışlarını sanal ortamlarda çekinmeden ortaya koyabilmektedir. Z kuşağının diğer özelliklerinden olan bireyselleşme ve buna bağlı daha fazla yalnızlık, zorbalığa maruz kalan çocukları daha fazla etkilemekte ve sonuç olarak intihara kadar vakaların oluşmasını sağlamaktadır. Bunları engellemek için ilk önce Z kuşağında zorbalığı tetikleyen yüksek özgüven ve sosyal statüye önem verme özelliklerinin ebeveynler tarafından kontrol altına alınması, her insanın hatalarına karşı hoşgörülü davranmanın gerektiği aşılmalıdır. Öte yandan bireyselleşme özelliği ağır basan Z kuşağı mensubu çocuklarda, fiziksel dünyada olduğu gibi sanal dünyada da yaşadıklarını paylaşmanın önemi ebeveynleri tarafından vurgulanmalıdır.

- Çocuklarına teknoloji dahil birçok imkanı sağladıklarında görevini yerine getirdiğini varsayan ve doğru teknoloji kullanım kültürüne sahip olmayan ebeveynler ile bireyselleşme özelliği daha ağır basan Z kuşağı bireyleri teknoloji bağımlılığına daha yatkın olabilmektedir. Teknoloji bağımlılığının diğer bağımlılıklar gibi bir sonuç olduğunun bilinmesi gerekmektedir. Bundan dolayı ebeveynlerin öncelikle doğru teknoloji kullanım kültürüne sahip olması, çocukları ile daha kaliteli zaman geçirmesi gerekmektedir. Çocuklarını herkesten iyi tanıyan ebeveynlerin, bireyselleşen ve

ailesiyle-yakınlarıyla iyi zaman geçirmeyen çocuklarında teknoloji bağımlılığı riskine karşı onları daha doğru yetiştirmesi gerekmektedir.

Aile mahremiyeti Ailenin temelini oluşturan bileşenler; birlikte bir şeyler yaşama, paylaşma, sevgi, saygı, sadakat, merhamet ve mahremiyettir. Mahremiyet, kişinin kendisini var eden her türlü bilgi veya gizlilik olarak tanımlanabilir. İnsanların teknoloji aracılığı ile azar azar ve kısmi olarak verdiği izinler veya paylaştığı bilgiler mahremiyetinin zarar görmesine ve bir süre sonra gizlilikten mahrum kalmasına sebep olmaktadır. Mahremiyetin zarar görmesini kolaylaştıran bir başka faktör ise, herkesin mahrem bilgisini veya durumunu paylaşarak bunu normalleştirmesidir. Bu normalleşme sayesinde kişisel, ailevi ve toplumsal birçok sorunun ortaya çıkmaktadır. Bunlardan en kötüsü ise mahremiyet mahrumu olmaktır. X ve Y kuşağına mensup olan günümüz ebeveynleri, kendi yetiştikleri aile hayatını ve bunun bir parçası olan mahremiyetinin zarar görmesini sağlamaktadır. Bu durum özellikle sanal dünyada bazen kendileri bazen de çocukları eliyle oluşmaktadır.

Bu bölümde Hipotez 6 ve 7'den faydalanılmıştır. Hipotez 7'de, çocuğuna sosyal medya kullanım kuralı belirleme ile sosyal medyada tanımadığı kişilerle iletişim kurup kurmaması arasındaki ilişki test edilmiştir. Buna göre çocuğuna sosyal medya kullanım kuralı belirlemeyen ebeveynlerin % 22'si aynı zamanda çocuğunu sosyal medyada tanımadığı kişilerle iletişim kurmaması için uyarınmamıştır. Sosyal medya kullanım kuralı belirlenmeyen çocukların ve herkesle iletişim kurabilen çocukların aile mahremiyeti ve diğer riskler açısından dikkate alınması gerekmektedir. Bazen de aile mahremiyetini ebeveynler direkt kendileri bozabilmektedir. Hipotez 6'da ebeveynin sosyal medyada yaptığı paylaşımların gizliliği ve çocuğuna sosyal medya kullanım kuralı belirleyip belirlememesi arasındaki ilişki olumlu çıkmıştır. Buna göre çocuklarına sosyal medya kullanım kuralı belirlemeyen ebeveynlerin % 10'u sosyal medya sitelerinde herkese açık bir şekilde paylaşım yaptığını beyan etmiştir. Aile mahremiyeti ve bilgi güvenliğinin yanlış teknoloji kullanım kültürü ile zarar görmemesi için aşağıdaki farkındalık yöntemleri geliştirilmiştir.

- Günümüz ebeveynleri, öncelikle kendileri iyi toplumu oluşturacak aile hayatının kapsamını çocuklarının idrak etmesini sağlamalıdır.
- Ebeveynler, aile mahremiyetinin bileşenlerini çocuklarına anlatmalıdır. Aile mahremiyetinin zarar görmesine sebep olacak riskleri her ebeveyn kendi ailesi için tespit etmeli ve buna göre önlemler almalıdır.
- Ebeveynler hem kendileri hem de çocukları için teknoloji kullanımında aile mahremiyetini ön planda tutarak eğitim almalıdır. Eğitimler ebeveynlere ayrı, çocuklara ayrı bir içerikle anlatılmalıdır.

- Ebeveynler, en az çocukları kadar teknoloji ve sosyal medya kullanım bilgisine sahip olmalı ve buna göre mahrem durumların ifşa edilmemesi konusunda çocuklarına çeşitli uyarılarda bulunmalıdır. Bu yöntemin geliştirilmesi için hipotez olarak belirlenmemiş iki çapraz tablodan yararlanılmıştır. İlk çapraz tablo sonucuna göre, ebeveynlerin % 28.6'sı (535 ebeveyn) çocuklarını sosyal medyada takip etmediğini beyan etmiştir. Çocuklarını sosyal medyada takip etmeyen ebeveynlerin % 73.4'ü güvenli sosyal medya kullanım bilgisine sahip olmadığını beyan etmiştir. Bundan dolayı ebeveynler, çocukları kadar sosyal medya kullanım bilgisine sahip olmalı, onları takip etmelidir. İkinci çapraz tablo sonucuna göre, çocuklarını sosyal medyada takip etmeyen ebeveynlerin % 35.4'ü çocuğuna sosyal medya kullanım kuralı belirlemediğini beyan etmiştir. Çocuğa sosyal medya kuralı belirlenmemişse mahrem durumların ifşa edilme olasılığı artabilir, bundan dolayı çocuklara sosyal medya kullanım kuralı belirlenmesi önem arz etmektedir.
- Mahremiyete zarar veren bilgi ve durumların paylaşılması aynı zamanda siber zorbalığı tetiklemektedir. Mahrem bilgilerin başka kişilerin eline geçmesi ile zorbalığa maruz kalma ihtimali de ortaya çıkmaktadır. Bundan dolayı bireysel ve aile mahremiyeti iyi korunmalıdır. Bu yöntemin geliştirilmesi için, hipotez olarak belirlenmemiş bir çapraz tablo kullanılmıştır. Buna göre, çocuklarını sosyal medyada takip etmeyen ebeveynlerin % 13'ü çocuklarını sosyal medyada tanımadığını kişilerle iletişim kurmaması için uyarınmıştır. Çocuğun tanımadığı kişilerle iletişim kurması mahremiyet, zorbalık, istismar ve bilgi güvenliği alanında birçok soruna yol açacağı için çocukların ve ebeveynlerin sosyal medya üzerinden iletişim konusunda bilinçlendirilmesi önem arz etmektedir.

Duygusal karışıklık ve umursamazlık İnsanı insan yapan bileşenlerden olan duygu, vicdan ve duyarlılık ile daha iyi bir aile ve toplum yapısı kurulabilir. Fakat sosyal medyada gezinti esnasında aynı saniyeler içerisinde farklı içerikler ile karşılaşan kullanıcılar, çok farklı duygulara kapılabilmektedir. Bu durum sürekli bir hal aldığı için insanlar duygusal karışıklık olarak adlandırılan mental bozukluğa maruz kalmaktadır. Bu durum kişiden kişiye değişmekle beraber çoğu kişide bir süre sonra umursamazlığın yaygınlaşmasını sağlayabilir. Bu iki durumdan korunmak için aşağıda ifade edilen farkındalık yöntemleri geliştirilmiştir.

- Ebeveynler, önce kendisi sonra çocukları için sosyal medya platformlarında haber kaynağını uygulama bazlı özelleştirebilir. Akraba ve arkadaşlık için farklı, iş ve haber alma amaçlı farklı bir sosyal medya platformu kullanabilir.
- Sosyal medyadan gelen paylaşımları filtrelemek, özellikle travmatik paylaşımlar yapan kişi, sayfaları akıştan çıkarılabilir.

Ebeveynler, çocuklarına yeterince kaliteli ve model olacak zamanları ayırmadıkları için çocukların kendilerinden teknolojik ortamlarla uzaklaşmalarını önemsememektedir.

3.7.2.2 Bilgi güvenliği farkındalığı

Ebeveynlerde, bilgi güvenliği farkındalığının olmaması, eksik veya yanlış yerleşmiş olması hem kendilerini hem de çocuklarında birçok sorunun ortaya çıkmasına neden olmaktadır. Aşağıda ebeveynler için tespit edilen sorunlar ve farkındalık geliştirme yöntemlerine yer verilmiştir.

Sosyal mühendislik Ebeveynlerin günlük yaşamda bilgi güvenliğini riske atan yöntemlerden biri sosyal mühendisliktir. Özellikle fiziksel yakınlık sağlanarak yapılan sosyal mühendislik saldırıları orta yaş ve üzeri yaş grubundaki ebeveynlerin daha sık maruz kaldığı bir durumdur. Sosyal mühendislik saldırıları sanal dünyadan elde edilen bilgiler ile birleştirilerek ebeveynlerin daha fazla zarar görmesini sağlamaktadır. Sosyal mühendisliğin ebeveynlere en çok uygulanan hali eve ulaşan saldırganın öncesinde ve kapıda öğrendiği bilgiler ile ebeveyni dolandırması durumu ile sonuçlanmaktadır. Ebeveynlerde sosyal mühendislik saldırılarına karşı farkındalık yöntemi oluşturmak için Hipotez 4'den faydalanılmıştır. Sosyal mühendisliğin bir kısmını oluşturan bilgi, günümüzde kolaylıkla sosyal medya platformlarından toplanabilmektedir. Sosyal medyada herkese açık paylaşım yapan ebeveynlerin % 66'sı güvenli sosyal medya kullanım bilgisine sahip olmayan ebeveynlerden oluşmaktadır. Ebeveynlerde sosyal mühendisliğe karşı farkındalık oluşturmak için aşağıdaki yöntemler geliştirilmiştir.

- Ebeveynlere; sosyal mühendislik ve çeşitli örnekleri eğitim, kamu spotu, basılı ve dijital medya araçları kullanılarak kamu, STK ve yerel yönetim eliyle aktarılmalıdır. Bu sayede fiziksel, telefon veya sanal ortamlardan gelen sosyal mühendislik saldırılarına karşı koyulabilecektir.
- Sosyal mühendislik faaliyetlerinin bir kısmı doğru bilgiler üzerine inşa edilmiş senaryolar üzerinden kurban kişiye uygulanır. Burada ebeveynlerin kendisine yöneltilen soruları, istenen şeyleri ve kaybedeceği konuları düşünmesi karşı taraftan gelen yönlendirmeleri analiz etmesi gerekmektedir. Sosyal mühendislik yapmaya çalışan kişinin hangi kuruluşu temsil ettiğini iyi anlamalı ve buna göre kuruluşun güvenilirliğini test etmelidir. Örnek olarak kendisini adli veya güvenlik personeli olarak tanıtan personeli geri arama yöntemini kullanarak çalıştığı yerin gerçek kuruluştan kontrol ederek görüşmeye devam etmelidir.

- Sosyal mühendisler, güven vererek, baskıcı veya aceleci, yardımsever ve çeşitli senaryolar kullanarak yaklaşırlar. Sosyal mühendisin isteklerinin yanında bir telefon, adres bilgisi istendiğinde, acele etme, kötü sonuçlar doğacağı ve iltifat etme gibi yöntemler kullanarak konuyu geçiştirmeye çalışıldığında tüm iletişimin kesilmesi ve gerekli yerlere haber verilmesi gerekmektedir.
- Sosyal mühendislik saldırılarına karşı farkındalık yöntemi geliştirmek için en önemli nokta, sosyal mühendislik yöntemlerinin her zaman değişebileceği fakat amacının her zaman aynı olduğudur. Bunun da çözümü için bireylerin bu tür saldırılara karşı her zaman uyanık olması sağlayacak aktivitelerin yapılması gerekmektedir. Sosyal mühendislik farkındalığı için sadece bir veya daha fazla eğitim yeterli olmayıp, bu konunun bir programa dönüşmesi önem arz etmektedir.

Siber saldırılar Ebeveynler ve aileleri farkında olarak veya olmayarak farklı yöntemlerden oluşan siber saldırıların hedefi olmaktadır. Bu yöntemlerden ilki ve yaygın görüleni oltalama saldırılarıdır. Telefon veya e-mail aracılığı ile fayda veya zarar getirebilecek konular üzerinden gelen talepleri dinleyen ebeveynler ve ailesi birçok olumsuz durumla karşılaşmaktadır. Öncelikle telefon ile gelen oltalama ve dolandırıcılık olayları üzerinden farkındalık yöntemlerinin geliştirilmesi üzerinde durulacaktır. Özellikle çok bilinmeyen terimler kullanarak, banka çağrı merkezi, karakol gibi arka plan seslerini kullanarak arayan saldırganlara karşı hangi bilgiyi neden istediğini sormak ve verilen cevabı teyit edebilmek önemlidir. Normal bir durumda banka veya güvenlik görevlisinin isteyebileceği bilgileri öncesinde öğrenmek gerekmektedir. Arayan saldırganın her söylediğine şüphe ile yaklaşarak, geri arama yöntemi kullanılmalıdır. Geri arama yöntemi için karşı tarafın verdiği iletişim-web adresi bilgilerini kullanmadan doğrudan bankanın veya ilgili kurumun gerçek numarası aranarak durum teyit edilebilir. Oltalama sırasında kullanılan bir diğer araç e-mail ve kısa mesajdır. Bu yöntemle gelen oltalama saldırılarına karşı ilk olarak gönderici etiketinde bulunan isimleri kontrol ederek doğruluğunu teyit etmek oldukça önemlidir. Daha sonra istenen bilgilerin normal durumlarda istenip istenmediğini analiz edebilmek gerekmektedir. Banka veya birçok kuruluş sms ve e-mail ile herhangi bir bilgi istemeyeceğini düşünerek şüphe ile yaklaşmak her durumda uyanık olmaya çalışmak gerekmektedir. E-mail'de gelen bağlantılara tıklayarak ilgili siteye gitmek birçok sorunu beraberinde getireceği için arama motorunda çıkan ilgili kuruluşun adresine gitmek veya mobil uygulama ile gerekli işlemi yapmak doğru bir yöntem olacaktır. Zararlı yazılım bulaştırma ve fidye yazılımları oltalama saldırıları ile beraber gelebileceği için bu saldırılar için de ayrı bir yer açılmalıdır. Her zaman bilgi toplama amaçlı yapılmayan oltalama saldırıları ile bir e-mail ekinden fatura, ekstre, lisansız yazılım indirme gibi yöntemlerle cihazlara zararlı yazılımlar bulaşmaktadır. Bu tür durumlara karşı da temel olarak şüpheli yaklaşım ve uyanık olmak gerekmektedir.

Tüm cihaz ve uygulamalarda kullanılan şifreler ve onların güvenliği de saldırıların kolayca yapılabilmesine imkan vermektedir. Sosyal medya hesaplarına farklı site ve uygulamaların erişmesine izin vermek, kişilik testleri ve diğer fark ettirmeden şifre tahmini yapılabilmesini sağlayan her duruma karşı uyanık olmak oldukça önemlidir. Öte yandan her cihaz ve uygulama için farklı ve karmaşık şifreler kullanmak gerekmektedir. Ek olarak şifrelerin bir yerde yazılı olmaması, paylaşılmaması gerekmektedir. Ebeveynlerin, bu ve benzeri önlemleri öğrenebileceği çalışmaların kamu, STK ve vatandaşların temas ettiği her yerde bir program dahilinde yürütülmesi önem arz etmektedir.

Sosyal medya platformlarında irtibat kurmaya çalışan kişilere karşı sürekli şüphe ile yaklaşmak, fiziksel ortamda tanışılmamış kişilerin takip ve arkadaşlık isteklerini kabul etmemek ebeveynler ve ailesi açısından oldukça önemlidir.

Bu yöntemlerin geliştirilmesinde Hipotez 5 kullanılmıştır. Güvenli sosyal medya kullanım bilgisine sahip olmayan ebeveynlerin oranı % 57'dir (1151 ebeveyn). Bu kitlenin % 88'i (1022 ebeveyn) daha önce bilgi güvenliği farkındalığı eğitimi almadığını beyan etmiştir. Genel siber saldırıların haricinde bireysel saldırılara maruz kalabilen ebeveynlerde bu oranlar oldukça kritik olarak değerlendirilmekte ve siber saldırılara karşı farkındalık yöntemlerinden haberdar edilmesi gerekmektedir.

Kişisel verilerin korunması Ebeveynler, tüm aile bireyleri için kişisel verilerin hangi durumlarda saklanabileceği, izne tabi olan ve olmayan durumlara ilişkin herhangi bir olay yaşamadan önce bilinçli olması gerekmektedir. Ebeveynlerin, kişisel verilerin nasıl korunabileceği hakkında yasal durumu öğrenmesi gerekmektedir. Hangi bilgilerin kişisel olup olmadığı, hangi durumlarda hangi kuruluş ve şirketlerde kalmaması gerektiğini önce kendilerinin öğrenmesi sonra da aile bireylerine bunu aktarması gereklidir.

Bölüm 4

Tartışma ve Sonuç

Hemen hemen herkesin teknoloji kullanıcısı olduğu günümüz dünyasında bilgi güvenliği farkındalığı ve onunla bütünleşen teknoloji kullanım kültürü oldukça önem kazanmaktadır. Her geçen gün internet üzerinde kullanılan hesap bilgileri ile ilgili sızan ve sızdırılan veriler artmaktadır. Gizli kalması gereken kişisel ve hassas kişisel veriler açığa çıkmaktadır. Kişisel verileri koruma için hem Avrupa'da (General Data Protection Regulation-GDPR), hem ülkemizde (Kişisel Verilerin Korunması Kanunu-KVKK) yasal düzenlemeler yapılmış olsa da henüz yeterli bilinç yoktur.

Çalışmada, Üsküdar ilçesindeki çocuk ve ebeveynlerde teknoloji kullanım kültürü ve bilgi güvenliği farkındalık durumunu tespit etmeyi ve buradan yola çıkılarak farkındalık oluşturma yöntemleri geliştirilmiştir. Bu aşamada, ebeveynlere yapılan anketler mevcut durum tespitinde ve yöntem geliştirmede kullanılmıştır. Ayrıca ebeveyn ve diğer hedef kitleler için literatür araştırması, gerçekleşmiş olaylar ve nesil özellikleri kullanılarak farkındalık yöntemleri geliştirilmiştir.

Bu çalışma kapsamında; çocuk ve ebeveynler olmak üzere belirlenen kitlerde bilgi güvenliği farkındalık yöntemlerinin nasıl geliştirilebileceği ve doğru teknoloji kullanım kültürünün nasıl oluşacağı üzerinde durulmuştur. Bunun için toplumun karakteristiğini ortaya koyan kuşaklar, geçmiş yaşam, önceki benzer çalışmalar ve mevcut durum analizinden yola çıkmıştır. Ardından ebeveynler üzerinde uygulanan farkındalık eğitimlerinden sonra yapılan anketler analiz edilerek elde edilen bulgulara yer verilmiştir. Daha sonra da biriken bu bilgilere ve topluma göre teknoloji kullanım kültürünün doğru biçimde oluşması ve bilgi güvenliği farkındalık yöntemlerinin geliştirilmesi sağlanmıştır.

Çalışmada bilgi güvenliği farkındalığı ve teknoloji kullanım kültürünün oluşturulması konuları ailenin farklı özelliklerinde olan ebeveyn ve ergenlerde birlikte ele alınmıştır. Yapılan anket çalışması ebeveynin cinsiyetinin, yaşının, internet kullanıp kullanmamasının,

internette geçirdiği sürenin; çocuğun internet kullanımı, bilgi güvenliği farkındalığı, siber zorbalık yaşaması-yaşatması gibi konularda etkili olduğunu göstermiştir. Bu da farklı ailelere farklı şekilde farkındalık çalışması yapılması gerektiğini göstermektedir.

Çalışmanın hedef kitlesini oluşturan çocuk ve ebeveynlerde teknoloji kullanım kültürünün ve bilgi güvenliği farkındalığının doğru yerleşmesi için bundan sonraki çalışmalara ışık tutacak gereklilik ve öneriler aşağıda sıralanmıştır.

- Ülkemizde ebeveyn ve çocuklarda bilgi güvenliği farkındalığı konusu birlikte araştırılarak ebeveyn farkındalık seviyesine göre farkındalık çalışmasının yapılması planlanmalıdır. Ebeveynlerde bilgi güvenliği farkındalığı; çocuk ve ergen yaşlarda çocuk sahibi olan ve çocuk sahibi olmayan ebeveynlerde ayrı ayrı araştırılarak ebeveyn modelleri belirlenmeli ve buna göre farkındalık oluşturma çalışması yapılmalıdır.
- Sadece gençlerin ve çocukların değil, ebeveynlerin de sosyal medya, oyun ve internet bağımlısı olduğu görülmüştür. Ebeveynler ailelerine ayırmadığı vakitlerini sosyal medya, oyun ve internete ayırmakta, bu da aile içi iletişimi ve çocukları olumsuz etkilemektedir. Ebeveynlerin bilinçlendirilmesi için yapılacak çalışmalara öncelik verilmelidir.
- Donanımlara ve yazılımlara yüksek bedeller ödenen ülkemizde bu donanım ve yazılımlar için gerekli eğitimlere bütçe ayrılmamaktadır. Bu da donanım ve yazılımların doğru konfigure edilmemesini, yanlış ve güvensiz kullanılmasını ve güvenlik zaafalarının oluşmasını sağlamaktadır. Eğitime daha fazla önem verilerek her türlü donanım ve yazılım alımları ile eğitimlerinin de alınması sağlanmalıdır.
- Toplum olarak geçmişimize, manevi değerlerimize ve hedeflerimize uygun nitelikli teknoloji kullanım kültürü ve bilgi güvenliği farkındalığını oluşturmayı hedefleyen kamu ve STK kuruluşlarının sayısı ve niteliği artmalıdır. Bu iki konu güdümünde yapılan projeleri teşvik edecek çalışmalar yapılmalıdır.
- Ergen bireylerde oluşan teknoloji kullanım bozukluğu neticesinde ortaya çıkan siber zorbalık, sosyal medya riskleri, internet, oyun, sosyal medya bağımlılığına karşı ebeveynlere rehberlik edecek bir yapı kurulmalıdır. Bu yapı STK, okul, üniversite, özel ve kamu sektörü destekleri alınarak bilinçlendirme, farkındalık kazandırma, önleme ve müdahale etme amaçlarına hizmet edecek bir bilimsel araştırma merkezi, web sitesi, çağrı merkezi bileşenlerinden oluşmalıdır.
- Teknoloji sadece zarar üreten bir kavram değildir. Ayrıca günümüz dünyasında teknoloji kullanımı, internet, sosyal medya artık kaçınılmazdır. Bu nedenle yasaklayan değil; izleyen, sınırlandıran ve bilinçlendiren yöntemler geliştirilmelidir.

- Ülkemiz toplum ve kültür yapısına uygun içerikteki dijital oyunların yerli üreticiler tarafından daha çok üretilmesine, bu yapıya uygun bir derecelendirme ve sınıflandırma sisteminin oluşturulmasına ihtiyaç duyulmaktadır.
- Öğrenciler için diğer tatbikat ve testler gibi okulda bilgi güvenliği ve teknoloji kullanım kültürü ile ilgili testler yapılmalıdır. Bu testler e-okul sistemi üzerinden de uygulanabilir.
- Ebeveynler için e-devlet sistemi gibi kamu web siteleri üzerinden bilgi güvenliği testleri yapılabilir.
- Gençlerin bilgisayar ve telefon dışında etkinliklere katılım sağlanması için çalışmalar yapılmalıdır. Özellikle çocukların tekrardan sokak oyunları ve aktiviteleri ile ilgilenmeleri sağlanarak sokaklar tekrardan kazanılmalı, birebir iletişim ile sosyal medya ve internet zararları azaltılmalıdır.

Sonuç olarak, bilgi güvenliği farkındalığının sadece çalışanlarda değil bilgiyi üreten, bilginin asıl sahibi olan toplumun tüm bireylerinde oluşturulması gerekmektedir. Bilgi güvenliğini tamamlayan doğru teknoloji kullanım kültürü de bu oluşuma dahil edilmelidir. Bu oluşum, gelişen ve aktif tutulması gereken dinamik bir süreç olarak kurgulanması gerekmektedir.

Ek A

Anket

TABLO A.1: Ebeveynlerde Teknoloji Kullanım Kültürü ve Bilgi Güvenliği Farkındalık Anketi.

- 1) Lütfen cinsiyetinizi belirtiniz. (Ebeveynler)
 Kadın
 Erkek
- 2) Lütfen yaşınızı belirtiniz. (Ebeveynler)
.....
- 3) Sosyal medyayı kullanıyor musunuz? (Facebook, Twitter, Instagram vb.)
 Evet
 Hayır
- 4) Lütfen çocuğunuzun yaşını belirtiniz. (Bu okulda eğitim gören çocuğunuz.)
.....
- 5) Lütfen çocuğunuzun cinsiyetini işaretleyiniz.
 Kız
 Erkek
- 6) Çocuğunuz bir günde internette ne kadar vakit geçiriyor?
 Hiç Geçirmiyor
 1 Saatten Az
 1 - 3 Saat
 4 - 6 Saat
 6 Saatten Fazla
- 7) Çocuğunuz için sosyal medya kullanmaya başlama yaşı belirlediniz mi?
 Evet
 Hayır
 Çocuğum Ne Zaman İsterse
- 8) Sosyal medyada çocuğunuzu aşağıdaki yöntemlerden hangisi ile takip ediyorsunuz?
 Hesap Şifreleri Bende var
 Kendi Hesabımla
Takip Ediyorum
 Yazılanlar Aracılığı ile Takip Ediyorum
 Takip Etmiyorum

TABLO A.2: Ebeveynlerde teknoloji kullanım kültürü ve bilgi güvenliği farkındalık anketi (devam).

- 9) Güvenli sosyal medya kullanımı hakkında yeterli bilgiye sahip olduğunuzu düşünüyor musunuz?
 Evet
 Hayır
- 10) Çocuğunuz evde iken internete hangi odada/odalarda giriyor?
 Salonda
 Çocuk Odasında
 Oturma Odasında
 Evin Her Yerinde
- 11) Facebookda yaptığımız paylaşımları kimlerin görmesine izin verdiniz?
 Herkes
 Arkadaşlarım
 Arkadaşlarımın Arkadaşları
 Hiçkimse
- 12) Çocuğunuzun sosyal medya kullanırken uyması gereken kuralları belirlediniz mi?
 Evet
 Hayır
- 13) Çocuğunuzun sosyal medyada tanımadığı insanlarla iletişim kurmaması konusunda uyardınız mı?
 Evet
 Hayır
- 14) Herhangi bir tanıdığımız siber zorbalığa maruz kaldı mı?
 Evet
 Hayır
- 15) Çocuğunuzun sosyal medya kullanımıyla ilgili herhangi bir nedenden dolayı cezalandırdınız mı?
 Evet
 Hayır
- 16) Daha önce bu konuda farkındalık eğitimi aldınız mı?
 Evet
 Hayır
- 17) Evdeki internetiniz için ücretsiz aile veya çocuk profili hizmeti kullanıyor musunuz?
 Evet
 Hayır
- 18) Çocuğunuzun kullandığı cep telefonunda internet var mı?
 Telefonu Yok
 İnterneti Var
 Telefonu Var ama İnterneti Yok
- 19) Bu seminer sizin için faydalı oldu mu?
 Evet
 Hayır

Ek B

Hipotezler

TABLO B.1: Çalışmanın Hipotezleri

Hipotez No	Hipotez İfadesi
Hipotez 1	Çocuğun yaşı ile çocuğun evde internete girdiği ortamlar arasındaki ilişki
Hipotez 2	Çocuğun cinsiyeti ile çocuğun internette geçirdiği süre arasındaki ilişki
Hipotez 3	Çocuğun internette geçirdiği süre ile ebeveynin çocuğuna sosyal medya kullanım yaşı belirleyip belirlememesi arasındaki ilişki
Hipotez 4	Ebeveynin güvenli sosyal medya kullanım bilgisi olup olmaması ile sosyal medyada yapılan paylaşımların gizliliği arasındaki ilişki
Hipotez 5	Ebeveynin güvenli sosyal medya kullanım bilgisi olup olmaması ile ebeveynin daha önceden farkındalık eğitimi alması arasındaki ilişki
Hipotez 6	Ebeveynin sosyal medyada yaptığı paylaşımların gizliliği ile ebeveynin çocuğuna sosyal medya kullanım kuralı belirleyip belirlememesi arasındaki ilişki
Hipotez 7	Ebeveynin çocuğuna sosyal medya kullanım kuralı belirleyip belirlememesi ile ebeveynin çocuğuna sosyal medyada tanımadığını insanlarla iletişim kurmaması konusunda uyarıp uyardırması arasındaki ilişki

Kaynaklar

- [1] M. Demirel and O. Ózkan M. Yórúk. Çocuklar İçin güvenli İnternet: Güvenli İnternet hizmeti ve ebeveyn görüşleri üzerine bir araştırma. Technical report, 2012.
- [2] Mehmet Tekerek and Adem Tekerek. A research on studentsâ information security awareness. *Turkish Journal of Education*, 2(3), 2013.
- [3] Kathryn Parsons, Agata McCormac, Malcolm Pattinson, Marcus Butavicius, and Cate Jerram. A study of information security awareness in australian government organisations. *Information Management & Computer Security*, 22(4):334–345, 2014.
- [4] Ramazan Yilmaz, F Gizem Karaoglan Yilmaz, H Tugba Özturk, and Tugra Karademir. Examining secondary school students’ safe computer and internet usage awareness: An example from bartin province= lise öğrencilerinin güvenli bilgisayar ve internet kullanım farkındaliklarinin incelenmesi: Bartin ili örneđi. *Online Submission*, 7(1):83–114, 2017.
- [5] PCI Security Standard Council. Security Awareness Program Special Interest Group. Information supplement: Best practices for implementing a security awareness program. Technical report, <https://www.pcisecuritystandards.org>, September 2017.
- [6] J. L. Grama and E. Dahlstrom. Higher education information security awareness programs. Research bulletin., ECAR., Louisville, 2016.
- [7] Z. Avinç. 0-8 yaş arasındaki Çocukların İnternet ve mobil teknoloji alışkanlıkları ve güvenli İnternet kullanımını. Master’s thesis, Atatürk Üniversitesi, Erzurum, Turkey, 2017.
- [8] F. G. Karaođlan Yilmaz and Ç. Çavuş Ezin. *Ebeveynlerin Bilgi Güvenliđi Farkındaliklarının İncelenmesi*. Eğitim Teknolojisi Kuram ve Uygulama Cilt 7, Sayı 2., 2017.
- [9] H. Yelci. Ortaokul öğrencilerinde siber zorbalık ile saldırganlık İlişkinin İncelenmesi. Master’s thesis, İstanbul Üniversitesi., İstanbul, Turkey, 2018.

- [10] H. Gencer. Ortaokul öğrencilerinde İnternet bağımlılığı ve siber zorbalık davranışları ile İlişkili değişkenlerin İncelenmesi. Master's thesis, Sivas, Cumhuriyet Üniversitesi., Sivas, Turkey, 2017.
- [11] E. S. Erbiçer. Üniversite öğrencilerinin siber zorbalık ve siber mağduriyet düzeylerinin sosyal uyuma ve bazı kişisel değişkenlere göre İncelenmesi. Master's thesis, İstanbul, Yıldız Teknik Üniversitesi., İstanbul, Turkey, 2017.
- [12] G. Metli. Ortaokul öğrencilerinin siber zorbalık, siber mağduriyet ve İnsani değerleri arasındaki İlişkinin İncelenmesi. Master's thesis, İstanbul Sabahattin Zaim Üniversitesi., İstanbul, Turkey, 2017.
- [13] A. Ümmetler İlhan. Ortaöğretim öğrencilerinin siber zorbalık ve İnternet salgırganlık düzeyleri ile sosyal medyaya İlişkin tutumlarının İncelenmesi (Çekmeköy örneği). Master's thesis, İstanbul, Yeditepe Üniversitesi., İstanbul, Turkey, 2016.
- [14] F. Baykal. Lise öğrencilerinde siber zorbalık ve mağduriyetin ailedeki koruyucu etmenlerle İlişkisi: Afyonkarahisar İli örneği. Master's thesis, Afyon Kocatepe Üniversitesi, Afyonkarahisar, Turkey, 2016.
- [15] G. Güçlü. Yaşam boyu öğrenme argümanı olarak teknoloji bağımlılığı ve yaşama yansımaları. Master's thesis, Sivas, Cumhuriyet Üniversitesi., Sivas, Turkey, 2016.
- [16] T. Karakuş E. Kurşun D. N. Kaşıkçı, K. Çağıltay and C. Ogan. Türkiye ve avrupa'daki Çocukların İnternet alışkanlıkları ve güvenli İnternet kullanımı. Technical report, Education Science/Eğitim Ve Bilim, 2014.
- [17] S. Kúçük. Siber zorbalık ölçeği türkçe uyarlaması. Master's thesis, İstanbul, İstanbul Üniversitesi., İstanbul, Turkey, 2016.
- [18] E. Kurşun D. N. Kaşıkçı I. Cankar K. Çağıltay, T. Karakuş and S. Bayzan. The use of social networks among children in turkey. Technical report, EU Kids Online II Final Conference, London, UK, 22-23 September, 2011.
- [19] ASAGEM. İnternet kullanımı ve aile. Technical report, ASAGEM - T.C. Başbakanlık Aile ve Sosyal Araştırmalar Genel Múdürlüğü., Ankara, 2008.
- [20] ASAGEM. Türkiye'de ergen profili. Technical report, ASAGEM - T.C. Başbakanlık Aile ve Sosyal Araştırmalar Genel Múdürlüğü., Ankara, 2008.
- [21] B.E. Başak J.B. Salı and E.B. Akca. Türkiye'de ortaokul öğrencileri arasında siber zorbalık,. *Anadolu Journal of Education Sciences International*, 5(2), july 2015.
- [22] Y. L. Şahin Y. Akbulut and B. Erişti. Cyberbullying victimization among turkish online social utility members. *Educational Technology Society*, 13(4):192â-201, 2010.

- [23] B. Dilmaç and D. Aydođan. Values as a predictor of cyber-bullying among secondary school students. *International Journal of Social Sciences*, 5(3):185–188, 2010.
- [24] S. Livingstone and E. J. Helsper. Parental mediation and children’s internet use. *Broadcasting and Electronic Media*, 52(4):581–599, 2008.
- [25] Masood Badri, Ali Alnuaimi, Asma Al Rashedi, Guang Yang, and Khaled Temsah. School children’s use of digital devices, social media and parental knowledge and involvement—the case of abu dhabi. *Education and Information Technologies*, 22(5): 2645–2664, 2017.
- [26] Trk Dil Kurumu. Technical report, <http://www.tdk.gov.tr>, 2018.
- [27] W. Strauss and N. Howe. *The History of America’s Future, 1584 to 2069*. 1991.
- [28] R. Kasarcı. Trkiye’de nfus geliřimi. Technical report, TUCAUM V. Cođrafya Sempozyumu., Ankara, 2015.
- [29] J. Jianrui. The y factor: Managing the new generation of soldiers. *The Singapore Armed Forces*, 139(4):53–59, 2011.
- [30] C. Raines R. Zemke and R. Filipczak. Generations at work: Managing the clash of veterans, boomers, xers and nexters in your workplace. Technical report, New York: Amacom, 1999.
- [31] A. Tolbize. Generational differences in the workplace, [elektronik srm]. Technical report, Research and Training Center on Community Living, Minnesota: University of Minnesota., August 2008.
- [32] B. Ycebalkan and B. Aksu. Potansiyel İř gc olarak y kuřađının transformasyonel liderlerle Çalıřabilirliđine ynelik bir arařtırma. *Organizasyon ve Ynetim bilimleri Dergisi*, 5(1):16–32, 2013.
- [33] H. Senbir. *Z Son İnsan mı? Z Kuřađı ve Sonrasına Dair Dřnceler*. İstanbul: O kitaplar., İstanbul, 2004.
- [34] ř. Kalaycı. *SPSS Uygulamalı Çok Deđiřkenli İstatistik Teknikleri*. Asil Yayın Dađıtım, Ankara, 2010.
- [35] J. Lower. Brace yourself here comes generation y. Technical report, <http://ccn.aacnjournals.org/content/28/5/80.short>, 2008.
- [36] Z. Mengi. İř bařarisında kuřak farkı. Technical report, <http://www.kigem.com/is-basarisinda-kusak-farki.html>, 2013.
- [37] A. Turk. *Y Kuřađı*. Kafekultur Yayıncılık, 2013.

- [38] TUIK. Technical report, www.tuik.gov.tr, 2013.
- [39] Hatice Toruntay. Takım rolleri çalışması: X ve y kuşağı üzerinde karşılaştırmalı bir araştırma. 2018.
- [40] M. Kuyucu. Y kuşağı ve facebook: Y kuşağının facebook kullanım alışkanlıkları üzerine bir İnceleme. *Elektronik Sosyal Bilimler Dergisi*, 13(49):55–83, 2014.
- [41] Wric. Technical report, <http://wric.com/2017/12/20/mother-says-her-daughter-committed-suicide-over-cyber-bullying/>, 2018.
- [42] Cnn. Technical report, <https://edition.cnn.com/2018/01/23/us/florida-cyberstalking-charges-girl-suicide/index.html>, 2018.
- [43] mirror. Technical report, www.mirror.co.uk/news/world-news/tragic-teen-gamer-dies-after-6373887, 2018.
- [44] Z. Genç. Parents' perception about the mobile technology use of preschool aged children. *Third Annual International Conference: Early Childhood Care and Education.*, 146:55–60, 2014.
- [45] A. Ulusoy and M. Bostancı. Çocuklarda sosyal medya kullanımı ve ebeveyn rolü. *International Journal of Social Sciences*, (28):559–572, 2014.
- [46] M. Aytaç. *Matematiksel İstatistik*. Uludağ Üniversitesi Basımevi, Bursa, 1998.
- [47] M. Kartal. *Hipotez Testleri*. Şafak Yayınevi, Erzurum, 1998.
- [48] K. Özdamar. *Paket Programlar ile İstatistik Veri Analizi*. Kaan Kitabevi1. Cilt (2. Baskı), Eskişehir., 2010. 335s.
- [49] M. Akyol Z. Akkuş, S.Y. Sanisoğlu and M.Y. Çelik. Değişken yapılarına göre İstatistiksel yaklaşım. *Dicle Tıp Dergisi*, 33(2):101–104, 2006.
- [50] Ofcom. Children and parents: Media use and attitudes report. Technical report, <https://www.ofcom.org.uk>, January 2016.
- [51] H. Sezer M. Kelleci, N. Güler and Z. Gölbaşı. Lise öğrencilerinde İnternet kullanma süresinin cinsiyet ve psikiyatrik belirtiler ile İlişkisi. *TAF Prev Med Bull*, 8(3): 223–230, 2009.
- [52] C. Hanel B. Trolley and L. Shields. Demystifying deescalating cyber bullying in the schools: A resource guide for counselors, educators and parents. Technical report, Booklocker.com, Inc., Booklocker.com, Inc., January 2014.
- [53] Dianne L Hoff and Sidney N Mitchell. Cyberbullying: Causes, effects, and remedies. *Journal of Educational Administration*, 47(5):652–665, 2009.

- [54] Mark Griffiths. Towards a risk factor model of fruit machine addiction: A brief note. *Journal of Gambling Studies*, 11(3):343–346, 1995.
- [55] Yeşilay. Technical report, www.yesilay.org.tr, 2018.
- [56] Yeşilay. Technical report, www.yesilay.org.tr/documents/file/yesilay/kitap/tbm/internet-bagimliligi.pdf, 2018.

