T.C.

HİTİT ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

ADLİ BİLİMLER ANABİLİM DALI

ÜNİVERSİTE ÖĞRENCİLERİNİN BİLGİ GÜVENLİĞİ FARKINDALIK DÜZEYLERİNİN BELİRLENMESİ: HİTİT ÜNİVERSİTESİ ÖRNEĞİ

Yüksek Lisans Tezi

Sinan DÖNER

Çorum - 2022

ÜNİVERSİTE ÖĞRENCİLERİNİN BİLGİ GÜVENLİĞİ FARKINDALIK DÜZEYLERİNİN BELİRLENMESİ: HİTİT ÜNİVERSİTESİ ÖRNEĞİ

Sinan DÖNER

Lisansüstü Eğitim Enstitüsü

Adli Bilimler Anabilim Dalı

Yüksek Lisans Tezi

TEZ DANIŞMANI

Doç. Dr. Emre DEMİR

Çorum 2022

Sinan DÖNER tarafından hazırlanan "Üniversite Öğrencilerinin Bilgi Güvenliği Farkındalık Düzeylerinin Belirlenmesi: Hitit Üniversitesi Örneği" adlı tez çalışması 14/06/2022 tarihinde aşağıdaki jüri üyeleri tarafından oy birliği ile Hitit Üniversitesi Lisansüstü Eğitim Enstitüsü Adli Bilimler Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir.

Doç. Dr. Mustafa Tolga ÇIRAK .....

Doç. Dr. Emre DEMİR .....

Doç. Dr. Engin YILDIRIM .....

Hitit Üniversitesi Lisansüstü Eğitim Enstitüsü Yönetim Kurulunun .../.../..... tarih ve ..... sayılı kararı ile Sinan DÖNER'in Adli Bilimler Anabilim Dalında Yüksek Lisans derecesi alması onanmıştır.

(İmza)

Prof. Dr. Muhammed Asıf YOLDAŞ

Lisansüstü Eğitim Enstitüsü Müdürü

TEZ BİLDİRİMİ

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

Sinan DÖNER

ÜNİVERSİTE ÖĞRENCİLERİNİN BİLGİ GÜVENLİĞİ FARKINDALIK DÜZEYLERİNİN BELİRLENMESİ: HİTİT ÜNİVERSİTESİ ÖRNEĞİ

Sinan DÖNER

ORCID: 0000-0002-3049-3729

HİTİT ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Yüksek Lisans Tezi

Haziran 2022

ÖZET

İnsanoğlu yaratılışından itibaren üzerinde yaşadığı dünyayı ve daha geniş tabirle evreni anlama çabası içindedir. Çabası sonucu elde ettiği bilgileri ilk çağlarda sözlü olarak kuşaktan kuşağa aktaran insan, bu bilgilerin aktarımı konusunda önce yazının icadı ile bir çağ atlamış, sonra teknolojik gelişmeler ile gerek bilgi aktarımını kolaylaştırmış gerekse de bilginin aktarım süresi kısalmıştır. İnsanlar elde ettikleri bilgileri kısa zamanda geniş kitlelere ulaştırır hale gelmiş, yani bilginin küreselleşmesi sağlanmıştır. Bunda en büyük pay tabiki de teknolojik gelişmelere aittir.

Bilginin hızlı aktarımıyla toplumların gelişmesi hız kazandığı gibi teknolojinin gelişmesi de hız kazanmıştır. Gelişen teknoloji bilginin aktarımında olduğu kadar, saklanmasında da önemli bir rol üstlenmektedir. Diğer bir açıdan ise teknolojik ortamlarda sakladığımız kişisel, ulusal ve uluslararası öneme haiz gizli kalması gereken bilgilerin güvenliğinin sağlanması son derece önemli hale geldiğinden bilginin güvenliğinin sağlanması zorunluluğu oraya çıkmıştır.

Teknolojik gelişmeler nasıl bilginin kısa zamanda geniş kitlelere ulaşmasını sağlayıp toplumların gelişmesini sağlıyorsa aynı zamanda bilginin güvenliğinin sağlanması açısından en büyük tehdit olarak kendini göstermektedir. Bu tehditler çoğunlukla farkındalık düzeyi düşük ve savunmasız kullanıcıları hedef almaktadır. Bu durum kişilerin bilgi güvenliği kazanımları ve farkındalıklarının artırılması zorunluluğunu doğurmuştur.

Bu çalışmada bilgi, bilgi güvenliği, bilgi güvenliği farkındalığı ve bunların unsurları hakkında yapılan araştırma ile Hitit Üniversitesi öğrencilerinin bilgi güvenliği farkındalıkları belirlenerek çözüm yolları açısından bir değerlendirme yapılması amaçlanmıştır.

Çalışmamızda Hitit Üniversitesi öğrencilerinin bilgi güvenliği farkındalıklarını ölçmek için bu konuda geliştirilmiş olan bir ölçek kullanılmış ve elde edilen veriler istatistiksel olarak analiz edilmiştir.

Anahtar Kelimeler: Bilgi, Bilgi Güvenliği, Bilgi Güvenliği Farkındalığı

Bilim Kodu: 20101

DETERMINING THE INFORMATION SECURITY AWARENESS LEVELS OF UNIVERSITY STUDENTS: HİTİT UNIVERSITY SAMPLE

Sinan DÖNER

ORCID: 0000-0002-3049-3729

HITIT UNIVERSITY

GRADUATE SCHOOL

Master of Science Thesis

June 2022

ABSTRACT

Since its creation, human beings have been trying to understand the world they live on and, in a broader sense, the universe. In the first ages, the human being orally transferring the information he obtained because of his efforts, passed a new age with the invention of writing in the transfer of this information, and then, with the technological developments, both the transfer of information was facilitated, and the transfer time of the information was shortened. People have become able to convey the information they have obtained to large masses in a short time, that is, the globalization of information has been achieved. The biggest share in this, of course, belongs to technological developments.

With the rapid transfer of information, the development of societies has accelerated, as well as the development of technology. Developing technology plays an important role not only in the transfer of information, but also in its storage. On the other hand, since it has become extremely important to ensure the security of the personal, national, and international information that we keep in technological environments, which should be kept confidential, the necessity of ensuring the security of the information has arisen.

Just as technological developments enable information to reach large masses in a short time and ensure the development of societies, it also presents itself as the biggest threat in terms of ensuring the security of information. These threats generally target vulnerable, unconscious users, in this case, the information security gains, and awareness of the society have to be increased.

In this study, it is aimed to make an evaluation in terms of solutions by determining the information security awareness of Hitit University students with the research on information, information security, information security awareness and their elements. In our study, a scale developed on this subject was used to measure the information security awareness of Hitit University students and the obtained data were analyzed statistically.

Keywords: Information, Information Security, Information Security Awareness

Science Code: 20101

TEŞEKKÜR

Çalışma sürecinde desteklerini ve emeklerini eksik etmeyen başta danışman hocam Doç. Dr. Emre DEMİR ve Hitit Üniversitesi Lisanüstü Eğitim Enstitüsü Adli Bilimler Ana Bilim Dalı Başkanı Prof. Dr. Faruk GÖKMEŞE'ye, çalışmamda yardımları ile bana yol gösteren, Tıp Fakültesi Biyoistatistik Anabilim Dalında Arş. Gör. Gülçin AYDOĞDU'ya, lisans eğitimimde ve sonrasında dostluğunu hiçbir zaman esirgemeyen, örnek insan Prof. Dr. Mehmet TEYFUR hocama, iş ve sosyal hayatımda desteğini esirgemeyen, her zaman yanımda olduğunu bildiğim eşim Aslıhan AKTAŞ DÖNER'e ve kimi zamanlar ilgisiz bıraktığım ve bu durumu hiçbir zaman bana karşı sorun etmeyen canım oğlum Ali DÖNER'e, ayrıca yaptığımız anket/ölçek araştırmasına katılarak bu çalışmanın bir parçası olan Hitit Üniversitesi öğrencilerine sonsuz teşekkürü borç bilirim.

Sinan DÖNER

İÇİNDEKİLER

Sayfa

Sayfa

3. BÖLÜM

ARAŞTIRMA SONUÇLARI VE TARTIŞMA

TABLOLAR DİZİNİ

Tablo **Sayfa**

ŞEKİLLER DİZİNİ

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Simgeler

A	Alfa
X	Ki

Kısaltmalar

BİT	Bilgi ve İletişim Teknojileri
TDK	Türk Dil Kurumu
MÖ	Milattan Önce
FATİH	Fırsatları Arttırma ve Teknolojiyi İyileştirme Hareketi

GİRİŞ

Bilgi; insanlığın varoluşundan bugüne kadar insanların düşüncesini, davranışını ve gelişim sürecini belirleyen en önemli unsurlardan biri olmuştur (Taner ve Kılıç, 2019). Bilgi, insanları ve toplumları güç ve başarı sahibi yapmıştır. Bilgi bu haliyle güç ve başarıya ulaşmanın en büyük anahtarı olmuştur. Bilginin bu denli önemli oluşu onun titizlikle saklama ve korunması zorunluluğunu doğurmuştur. Zamanla bilgi miktarındaki artış, verilerin saklanması, erişimi, analizi, paylaşımı ve güvenliğini zorlaştırmıştır. Daha fazla bilgiyi daha kolay saklamak, korumak, paylaşmak için teknolojik sistemler geliştirilmiştir.

Bilginin üretilmesi, saklanması, korunması, muhafaza edilmesi, yararlanılması, paylaşılması tamamen teknolojinin etkisi ile bilginin hızlı işlenişi ve iletişim araçlarıyla kısa zamanda geniş kitlelere ulaşır hale gelmiştir. Teknolojinin hızlı gelişmesi ile internet ve akılllı cihazların hayatımızdaki yerini alması ile insanların bilgiye erişimi hız kazanmış, insanlar istedikleri zamanda ve yerde istedikleri bilgiye kolayca ulaşır hale gelmiştir. Teknoloji çağıda denilen bu dönemde insanlar teknoloji ile yaşama zorunluluğu içine girmiş, teknoloji insan hayatının bir parçası olmuştur. Tabi ki bundan bilgi olgusu da nasibini almış, bilginin kullanılması, muhafaza edilmesi, aktarılması daha basit hale gelmiş, insanların bilgiye ulaşımı kolaylaşmıştır.

İnsanlar bilişim teknolojilerini kullanarak günlük hayatta yapmaları gereken işleri daha hızlı ve daha kolay yapabilmektedirler (Seferoğlu ve ark., 2018). Teknoloji günlük hayatımızda çok büyük kolaylıklar getirse de zamanla bu teknoloji bilgi güvenliği açısından çeşitli tehlikeler ve tehditler oluşturur hale gelmiştir. İşte tam bu noktada bilgi güvenliği kavramı ortaya çıkmıştır.

Günümüz bilgi toplumlarında bilişim yani bilgi teknolojileri sürekli gelişmekte ve değişmektedir. Bu gelişim ve değişim kullanıcı sayısında da hızlı bir artışa neden olmaktadır. Kullanıcı sayısındaki artış bilgi güvenliği açısından risk ve tehdit altında bulunan insan sayısını da her geçen gün artırmaktadır. İnsanlar bilgiden olumlu bir şekilde faydalanabilmek ve bilgi teknolojilerinin risk ve tehditlerinden korunabilmek için bu teknolojileri kullanırken iyi bilmek zorundadırlar. İnsanların teknolojiyi iyi bilmelerinin yanında bilgi güvenliğini nasıl sağlayacağı yönünde farkındalık düzeyinin yüksek olması gerekmektedir.

Bilginin güç sembolü olması ve önemli bir rekabet aracı olması, aynı zamanda teknolojinin gelişimi ile bilgiye istenilen zamanda istenilen yerde kolaylıkla ulaşılması bilgi güvenliğinin sağlanmasını da zorunluluk haline getirmiştir. İnsanların kişisel ve kurumsal bilgilerinin korunması yönünde çalışmalar yapılması, insanların bilinçlendirilmesi, eğitilmesi, bilgi güvenliği için yeni teknolojilerin geliştirilmesi artık bir mecburiyettir.

Bilgi teknolojileri bilginin nasıl hızlı yayılmasını sağlıyor ise olumsuz yanları da kesinlikle vardır. Özellikle bu teknolojiye bağımlı hale gelen insanlar iletişim becerileri açısından çok büyük sorunlar yaşar hale gelmişlerdir. Bu sorunların başında, sanal dünya bağımlısı gençlerin ortaya çıkması ve bu bireylerin gerçek yaşamdan uzak, antisosyal bir yaşam benimsemeleri gelmektedir. Antisosyal bireyler sanal ile gerçeklik arasında bilişsel bir karmaşa yaşamaktadır.

Aynı zamanda bu bireyler internet üzerindeki yararlı içeriklerin yanında yer alan zararlı içeriklere de kolayca ulaşabildiğinden her yaştaki birey bilgi teknolojilerinden kişisel gelişim yönünden olumsuz yönde etkilenmektedir. Bu insanlar kötü alışkanlıklar edinmekte, kişilik bozuklukları yaşamakta ve yasal olmayan faaliyetler içerisine girebilmektedir.

Bilgi teknolojilerindeki çeşit fazlalığı daha fazla insanın bu teknolojileri kullanmasını sağlamaktadır. Bu durum da insanların etkilenebileceği risk ve tehdit sayısını da artırmaktadır (Erdoğmuş, 2017). Hızla gelişen teknoloji dünyanın dört bir tarafına etki etmekte, teknolojiyi kullanan insan sayısı arttıkça insanların maruz kalabileceği tehdit ve saldırı yöntemlerinin de sayısı arttığından bilgi güvenliği açısından alınacak tedbirleri zorlaştırmaktadır.

Elindeki bilgiyi korumak isteyen insanlar ve kurumlar bilgi güvenliğini sağlamanın yolunu hep teknolojide aramış olsalarda asıl çözüm unsuru insanı hep ikinci plana atmışlardır. Bilgi güvenliği sorunları teknoloji ön plana alınarak çözüm arandığında hem para hem de zaman kayıplarına neden olmuştur. Ayrıca teknoloji temelli çözümler tehdit ve riskleri de tamamen önleyememiştir. Burada dikkat edilmesi gereken asıl nokta bu teknolojiyi kullanan, yöneten, üretenin insan olduğudur. Bilgi güvenliği yatırımının teknolojiden önce insana yapılması ile bilgi güvenliği üzerindeki risk faktörü minimum seviyeye indirilebilecektir. Diğer yandan ne kadar büyük miktarlarda harcamalar yapılsada insan faktörünün soyutlandığı bir bilgi güvenliği çalışması maksimum başarıyı hiçbir zaman sağlayamayacaktır.

Bilgi güvenliği risklerinden korunmanın temelinde insanların bilinçlendirilmesi ve bilgi güvenliği teknolojilerini yerinde ve zamanında kullanmaları yatmaktadır. Bu teknolojilere çok fazla harcama yapmanın ve koruma amaçlı teknolojileri fazlasıyla kullanmanın ikinci planda olması gerekmektedir (Güldüren ve Keser, 2015).

Bilgi güvenliğini sağlamanın çok harcama yapmaktan öte insan faktörünün dikkate alınarak önce insanların bilinçlendirilmesi, farkındalıklarının sağlanmasından geçtiği açıkça görülmektedir.

Bilgi güvenliği farkındalığı gelişmemiş insanlar internet ortamında birçok kişisel ve kurumsal bilgilerinin paylaşımında sakınca görmemektedir. Bu bilgiler kötü niyetli kişiler tarafından farklı amaçlarla kolayca kullanılabilecektir. Son yıllarda dolandırıcılık olaylarının artmasındaki en temel faktörlerden biride bilgi güvenliği farkındalığı gelişmemiş insanların kişisel veya kurumsal bilgilerini internet ortamında paylaşmalarıdır. Unutmayalım ki dolandırıcılarda bizler gibi birer insandır ve bu teknolojiyi onlarda kullanmaktadır. İnternet üzerinde sosyal medya olsun, iletişim teknolojisinin diğer uygulamaları olsun bu tür suç meyili olan insanların işlerini kolaylaştırmaktadır. Bizlerin facebook, instagram gibi sosyal paylaşım sitelerinde akraba, eş dost bilgilerimizi paylaşmamız veya WhatsApp üzerinden görev belgemiz, öğrenci belgemiz, banka kartımızın bilgilerini veya fotoğrafını birilerine göndermemiz veya paylaşmamız bu insanların işini kolaylaştırmaktadır.

Dijital teknolojinin hayatımızın her noktasında yer alması ile birlikte bu teknolojileri kullanan insanlar kötü niyetli teknoloji kullanıcılarının hedefi haline gelmiş ve gün geçtikçe siber saldırı sayıları artmıştır (Taner ve Kılıç, 2019). Görüldüğü gibi bilgi güvenliği konusunda farkındalık geliştirmediğimiz zaman kötü niyetli kişiler kişisel ve kurumsal bilgilerimize kolayca ulaşıp bizi bir suçun mağduru edebilmektedir. Bu açıdan bilgi güvenliği konusunda bir farkındalığımızın olması gerekmektedir. Bilgi güvenliği farkındalığının sağlanması görevi ise eğitim kurumlarımıza düşmektedir.

Değişim ve gelişimi çok hızlı olan teknolojinin bilişim alanı içerisinde, bu teknolojileri günümüzde en çok kullanarak olumlu ve olumsuz yanlarına en fazla maruz kalan gençler bilgi güvenliği konusunda bilinçlendirilerek gelecek nesillere bilgi güvenliği açısından daha güvenli bir dünya bırakılabilir. Bu açıdan bakıldığında bu gençlerin mesleklerinde artık uzmanlaşma aşamasında oldukları üniversite ortamında bulundukları dikkate alındığında bu durum daha da önemlidir. Çünkü üniversitede eğitim gören gençler hem kendi bilgi güvenliklerinden, hem çalışacakları kurumların bilgi güvenliğinden hem de belkide eğitecekleri öğrencileri ve çocuklarının bilgi güvenliğinden sorumlu olacakları için üniversite öğrencisi olan gençlerin bilgi güvenliği farkındalıkları çok önemlidir. Tez çalışmamızda üniversite öğrencilerinin bilgi güvenliğine yönelik farkındalıklarının belirlenmesi, bilgi güvenliği farkındalıklarının hangi derecede olduğunun tespit edilmesi ve demografik özelliklerine göre farklılık gösterip göstermediğinin araştırılması amaçlanmıştır.

1. BÖLÜM

BİLGİ GÜVENLİĞİ FARKINDALIĞI

1.1. Temel Kavramlar

TDK da bilgi, "insan aklının erebileceği olgu, gerçek ve ilkelerin bütününe verilen ad. Öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek, malumat, öğrenerek, araştırarak, deney yaparak elde edilen gerçek" olarak tanımlanmıştır (Yıldız, 2016).

Kişilerin korkusuzca yaşayabilmesi durumu ve toplum yaşamında yasal düzenin aksamandan yürütülmesi güvenlik olarak tanımlanır (Yıldız, 2016).

Farkındalık, bir canlının çevresinde gelişen olayları bilme, algılama ve duyumsama becerisidir.

Bilginin korunması, bütünlüğünün bozulmadan yalnızca yetkili kişilerce ulaşılabilir olmasına bilgi güvenliği denir (Hacımustafaoğlu, 2019). Bilgi güvenliği, bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamaya yönelik metotları içeren işlemler bütünüdür.

Bilgi güvenliği tehditlerinden ve alınacak tedbirlerden haberdar olunması durumuna bilgi güvenliği farkındalığı denir. Bu kişisel ve kurumsal tedbirlerle ilgili bilinçli olunması, geliştirilebilecek stratejilerle ilgili bilgi sahibi olunması durumudur.

Bilginin toplanmasını, işlenmesini ve saklanmasını, herhangi bir yere iletilmesini, herhangi bir yerden bu bilgiye erişilmesini, elektronik vb. yollarla sağlayan teknolojiler bütününe bilgi teknolojileri denir. Akkoyunlu (1998), bilgi teknolojilerini "bilginin yaratılması, toplanması, biriktirilmesi, islenmesi, yeniden elde edilmesi, yayılması, korunması ve bunlara yardımcı olan araçlar" olarak tanımlarken, Uzay (2001), "Bir bilginin toplanmasını, islenmesini, saklanmasını ve gerektiğinde herhangi bir yere iletilmesini ya da herhangi bir yerden bu bilgilere erişilmesini otomatik olarak sağlayan teknolojiler bütünü" olarak ifade etmiştir (Hacımustafaoğlu, 2019).

Üstün olan kişinin kendi isteklerinin olması için zayıf kişiyi ezmesi, gözünü korkutması, sözlü veya fiziksel şiddet uygulamasına zorbalık denir. Gücünü kullanarak başkalarını rahatsız etme durumudur (Yıldız, 2016). Zorbalık bir insan yada grup tarafından yapılabilir. Ayrıca fiziksel ve psikolojik olabilir ve süreklilik arz eden bir şiddet unsurudur. Teknoloji çağıda denilen bu dönemde dijital teknolojiler üzerinden insanların başka insanlar tarafından korkutulması, kızdırılması, suçlanması ve utandırılması gibi yapılan eylemlere siber zorbalık denir. Bu eylemler sosyal medya hesapları mesaj platformları ve cep telefonları üzerinden gerçekleştirilebilmektedir. Bu eylemler bir kişi yada gruba, özel yada tüzel kişiliğe yapılabilir. Bunlar kasıtlı tekrarlayan ve zarar verici etkisi olan eylemlerdir (Hacımustafaoğlu, 2019). Siber zorbalık davranışlarına maruz kalan ve bu davranışlar sonucunda maddi ve manevi zarara uğrayan insanlara ise siber mağdur denilmektedir (Hacımustafaoğlu, 2019). Siber mağduriyet, bilgi ve iletişim teknolojileri üzerinden tehdit, hakaret, taciz, şantaj gibi davranışlar ile zorba

kişinin mağduru ruhen ve bedenen rahatsız etmesi durumudur. Bu davranışlar sonucunda mağdurun yaşamı olumsuz etkilenir (Karaca ve ark., 2021).

Dijital okuryazarlık, teknoloji üzerinden bilgiyi bulma, kullanma ve dağıtma yeteneğinin oluşmasıdır. Bu bilgiler farklı formatlarda, farklı türlerde, farklı bakış açılarında olabilir. İnsan bu farklılıklar içinde doğru bilgileri bulup kullanabiliyor ise dijital okuryazarlık bilgisine sahiptir demektir. İnsanların dijital teknolojileri tanıması, erişmesi, yönetmesi bu teknolojiler üzerinden değerlendirme yaparak çeşitli çıkarımlarda bulunma becerisi dijital okur yazarlık olarak tanımlanmaktadır (Göldağ, 2021).

Bir kişinin özel hayatının, özel hayatı ile ilgili bilgilerin sadece ona gizli, ona özel olmasına kişisel mahremiyet denir. Teknolojinin güzel yönlerini kullanırken bilgi güvenliği farkındalığı gelişmemiş şeklide bu özel bilgilerin bu teknolojiler üzerinden paylaşılması kişisel mahremiyeti olumsuz etkilemektedir.

Sosyal mühendislik saldırı türünde saldırgan bizim onun istediği şekilde davranmanızı sağlamaktadır. Çünkü saldırgan, tanımadığı bir insanı kendi çıkarları doğrultusunda yönlendirmektedir. Teknoloji üzerinden insanların hileli davranışlarla kandırılması ve zarara uğratılması sosyal mühendisliğin özetidir. Sosyal mühendislik psikolojik bir saldırı türüdür.

1.2. Bilgi ve Tarihçesi

Bilginin ne olduğu konusu uzun yıllardır tartışma konusu olmuştur. Özellikle felsefe içerisinde yer alan düşünürler bilgiye farklı zamanlarda farklı anlamlar yüklemiş ve bilgi ile ilgili farklı tanımlar ortaya koymuşlardır. Ancak günümüzde artık bilgiyle ilgili tüm insanların kabul ettiği tanımlar bulunmaktadır.

Bilgi, genellikle, geçerliliği veya doğruluğu varsayılacak şekilde mümkün olan en yüksek kesinlik derecesi ile karakterize edilen, kişiler veya gruplar için mevcut olan bir dizi gerçektir. Bilgi kullanıldığı alana ve bakış açılarına göre farklı tanımlanmaktadır. Öğrenme, araştırma ve gözlemle elde edilen gerçekler, malumatlar ve bireyin bunlara yüklediği anlamlara bilgi diyebiliriz. İnsanın beynini çalıştırarak elde ettiği düşünsel, kurgusal ürünlerdir.

TDK'da bilgi kavramı; "kişi zihninin kavrayabileceği öge, hakikat ve kuralların tümünü, ilim, malumat, anlama, inceleme ve izlemeyle erişilen her çeşit hakikat, edinç, birey aklının işlemesi neticesinde meydana gelen fikir ürünüdür. Genellikle ve ilk sezgi durumunda zihinde kavranan ana fikirler" şeklinde ifade edilmektedir (Altunsaban Yerlikaya, 2019). Bilgi; öğrenilerek, araştırılarak ve gözlem yöntemiyle ortaya konulan gerçeklerdir.

Bilginin oluşması için deneyim gibi kültür gibi birçok faktörün bir araya gelmesi gerekmektedir. Mesleğe yeni başlamış bir Polis Memuru ile meslekte 20 yılını geçirmiş bir Polis Memurunun meslek bilgisinin aynı olduğunu söylememiz çok yanlış olur. Aynı şekilde Avrupa'da herhangi bir ülkede yetişmiş bir insan ile Afrika'da zorlu şartlarda yetişen bir

insanın bilgi düzeylerinin aynı olduğunu söyleyemeyiz. Afrika'daki insan daha çok doğa ile mücadele yönünden üstün bilgiye sahipken, Avrupa'daki insan ise rahat yaşam, teknolojinin gelişmesi açısından daha fazla bilgiye sahip olur. Bunun temelinde deneyim ve kültür gibi bilgi öğeleri yer almaktadır.

Çoban (1996) bilgiyi; "belirli şekilde yoğurulmuş ve alan bakımından anlamı bulunan, şimdiki ve ileride alınacak kararlar adına önemli olan, kavranan ya da reel değeri bulunan veri" biçiminde ifade etmiştir (Altunsaban Yerlikaya, 2019). Bilginin temelinde deneyim yani tecrübenin en başta yer aldığını görüyoruz. Mesleğine yıllarını vermiş bir hakimin, karşısına getirilen şüphelinin doğruyu söyleyip söylemediğini, şahsın hal ve hareketlerinden anlaması tecrübeyle elde edilmiş bir bilgidir.

Günümüzde bilgi, gerek üretim, gerek tüketim gerekse de hizmet safhasında en değerli, vazgeçilmez başarı ve rekabet unsuru olmuştur. Kısacası bilgi sahibi insanlar gücüde, başarıyı da elinde tutmaktadır.

Tüm bu tanımlamalara baktığımızda bütün tanımların ortak noktasının bilginin özne ve nesne arasındaki etkileşim sonrası insan üzerinde bıraktığı olgu, birikim, etki olduğu; gücün ve başarının bir numaralı anahtarı olduğu dikkatimizi çekmektedir.

Bilgi latince kökenli bir sözcük olmakla birlikte, bu sözcüğün ne anlama geldiği ve nasıl bir tarihsel süreçten geçtiği araştırmacılar tarafından incelenmiştir. Kökeni Hellenistik döneme kadar uzanan bilgi kavramı günümüze gelinceye kadar çok çeşitli anlamlar yüklenerek günümüze ulaşmıştır. Tarihsel süreç içerisinde biyoloji, ahlak ve pedagoji gibi farklı alanlarda eğitim, öğretim, zihnin veya karakterin şekillendirilmesi, kalıba sokulması gibi tanımlamaların yapıldığı görülmektedir Zaman içerisinde sözcüğe yüklenen anlamlarda değişmeler olmuş örneğin, Orta çağda bilgi "şekil vermek" anlamında kullanılmış sonrasında ise "herhangi bir şeyin bir başkasına iletilmesi" haline dönüşmüştür. 20. Yüzyılla birlikte bilgi kuramı kavramı ortaya çıkmış ve bilgi kavramı tekrar hareketlilik kazanmıştır (Sancak, 2013). Görüldüğü üzere bilgi, insanların sürekli aklını kurcalayan bir kavram olarak tarih boyunca aktifliğini devam ettirmiştir. Bilgiye farklı dönemlerde farklı anlamlar yüklendiği de açıkça görülmektedir.

Antik zamanlardan günümüze kadar bilgi, felsefe ile bir arada yer almıştır. Filozoflar bilgiyi bulmaya, açıklamaya ve yorumlamaya çalışmışlardır. Zaten merak etme duygusu insanın yapısında olan bir durum olduğu için insan çevresini tanımak ve bunları diğer kuşaklara aktarmak için sürekli bir uğraş içinde olmuştur.

1.2.1. Bilgi türleri

Bilgi gündelik hayatta ne kadar çok kullanılan bir kavram olsa da net bir tanımının yapılması oldukça zordur. Bilgi, farklı disiplinlerce, kendi alanlarına uygun olarak farklı tanımlamalara maruz kalmıştır. Bunun yanında bilgi zamana göre de farklı tanımlamalar görmüştür. Bilgi, oluşum şekline, etki alanına, uygulama alanına ve niteliğine göre farklı başlıklar altında gruplandırılmıştır (Uçak, 2010).

Bilginin sınıflandırılması açısından çok çeşitli ayrımlar yapılsa da günümüzde en çok kabul gören tanımlama Mengüşoğlu'nun yaptığı sınıflandırmadır. Mengüşoğlu bilgiyi niteliğine göre beş türe ayırmıştır (Uçak, 2010). Bunların doğal bilgi, bilimsel bilgi, felsefi bilgi, sanat bilgisi ve din bilgisi olduğunu görüyoruz.

Mengüşoğlu'nun bilgi sınıflandırmasına daha sonra bir çok ek sınıflandırma yapılmış olsa da bunların içinde genel kabul gören bilgi türü ise "teknik bilgi" türüdür. Bunun yanında "Politik" bilgi türü gibi türlerde bulunmaktadır. Ancak bu bilgi türü de kaynaklarda yer alsada bu bilgi türü üzerinde tam da bir uzlaşı olmadığı dikkatimizi çekmektedir. Yapılan araştırmada "Politik bilgi" haricindeki tüm bilgi türlerinin genel kabul gördüğü dikkatimizi çekmiştir. Genel kabul gören bilgi türleri kısaca şunlardır.

1.2.1.1. Gündelik (Doğal) Bilgi

Gündelik bilgi, temelinde neden sonuç ilişkisi ve yöntem bulunmayan, insanların yaşantıları esnasındaki deney, gözlem ve tecrübelerine dayanarak elde ettikleri bilgilerdir. Bu bilgiler insanların algı, sezgi ve gözlemlerine göre farklılık gösterebilir. Gündelik bilginin oluşumunda gözlem, tecrübe ve denemelerin etkisi oldukça fazladır (Hakkoymaz, 2022).

1.2.1.2. Teknik Bilgi

Bireylerin el ve zihin becerisine dayalı olarak temel ihtiyaçlarını karşılamak amacıyla araç ve gereç yapımı için gerekli olan bilgiye teknik bilgi denir. Teknik bilgi insanlara yaşamları esnasında fayda ve kolaylık sağlamaktadır. Örneğin demirin nasıl eritileceği, nasıl şekil verileceğini bilmek teknik bir bilgidir (Hakkoymaz, 2022).

1.2.1.3. Sanatsal Bilgi (Sanat Bilgisi)

Sanatçının elinde bulunan malzemeler üzerinde kendi bakış açısını yansıttığı güzelliklerin ortaya konulması sırasında oluşan bilgisidir. İnsan doğal malzemeleri kullansa da doğada olmayan bir güzellik ortaya çıkarabilir (Hakkoymaz, 2022).

1.2.1.4. Dini Bilgi

Bireylerin dini inançlarını ve dine ait olan tüm kavramlarını içeren bilgiye dini bilgi denir . Örneğin bir çok dinde insanların öldükten sonra tekrar bir yaşamın olacağı, yani ahiret inancı bir dini bilgidir (Hakkoymaz, 2022).

1.2.1.5. Felsefi Bilgi

Evreni, dünyayı, toplumu ve bireyleri kısacası insanın aklı ile ortaya koyduğu her şeyi sorgulayabilen evrensel bir bilgi türüne felsefi bilgi denir. Şüphe ile başlar şüphesizlik ile son halini alır (Hakkoymaz, 2022).

1.2.1.6. Bilimsel Bilgi

Toplumdan topluma veya kişiden kişiye değişmeyen kanıtlanır ve denetlenir nitelikte olan nesnel bilgi türüne bilimsel bilgi denir (Hakkoymaz, 2022).

1.3. Güvenlik ve Tarihçesi

Güvenlik, odak noktasında insanın kendisinin bulunduğu, aile, ülke, evren şeklinde halkalanmış, insanların herhangi bir saldırıya maruz kalmama durumunun genel adıdır. Temelinde insanın güvende olması vardır. Bu gerek aile içinde, gerekse toplum içinde, gerek uluslararası, gerekse de evrenin korunması şeklinde olabilir. Dünyamıza yaklaşan meteor nasıl dünyamızda yaşayan tüm canlıların güvenliğini ilgilendiriyor ise, ülkeler arası savaşlar, ülke içi savaşlar, ailenin içinde yaşanan olaylar da insanları güvenlik açısından etkilemektedir. Günümüzün en büyük sorunlarından olan güvenlik ile ilgili birçok çalışma yapılmış olsa da güvenliğin ne olduğu yönünde ortak bir tanım ortaya konulamamıştır.

TDK'da güvenlik; "Toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet, asayiş" şeklinde tanımlamıştır (Yıldız, 2016).

Güvenlik kavramı kelime kökeni olarak Latince "se-curus" kelimesinden gelirken bu kelime İngilizce de "security" olarak isimlendirilmiştir. Birçok araştırmacı güvenliğin ne olduğu konusunda farklı farklı tanımlar ortaya koymuşlar ortak bir tanım ortaya konulamamıştır. Genel olarak güvenliği riskin endişenin olmadığı bir durum şeklinde tanımlamışlardır. Güvenliğin tanımı, insanlara, konulara, adetlere, tarihsel şartlara göre değişik tanımları yapılmıştır.

İnsanların herhangi bir saldırı, kaza tehlikesi olmadan, endişesiz bir şekilde rahatça yaşamalarına güvenlik denilmektedir. Güvenlik kelimesi çoğu zaman "Emniyet" ve "Asayiş" kelimeleriyle eş anlamlı olarak kullanılsa da bu kelimeler tam olarak birbirinin karşılığı kesinlikle değildir.

Güvenliği sağlama görevi öncelikle kolluk kuvvetlerine aittir. Güvenliğin amacı, toplumun huzur ve refah içerisinde varlığının korunması ve kamu düzeninin sağlanmasıdır. İnsan, güvenliğin sağlayıcısı, mağduru, şüphelisi, tanığı, öznesi, nesnesi kısacası her türlü aktörü olabilir yani güvenliğin her noktasında yer alabilir.

Genel anlamda bu tanımlarda güvenliği sağlama görevi sadece kolluk kuvvetlerine verilmiş gibi görünmektedir. Her ne kadar bu görev kolluk kuvvetlerine ait olsa da bireylere de güvenliklerini sağlama konusunda büyük sorumluluklar düşmektedir. İnsanlar önce kendi güvenliklerini sağlamakla mükelleftirler. Bu durumu sağlamayan insanlarda yani güvenlik kaygısı yaşayan insanlarda depresyon, kişilik bozuklukları, panik atak gibi hastalıklar ortaya çıkmakta, bu nedenle güvenliğin sağlanması oldukça önemli hale gelmektedir.

Güvenlik aileden başlayarak, ulusal ve uluslararası hatta evren üzerine bir boyut kazanabilir. Dietrich Fischer'ın güvenliği şu şekilde tanımladığını görüyoruz. Dietrich Fischer'e göre güvenlik "sadece savaştan korunmak yada savaşı engellemek demek değildir. Aynı zamanda hayatta kalabilmemizi ve refahı etkileyen muhtemel tehlikelerden korunmayı da içerir. Savaştan korunmanın tek yolu askeri tehditlere karşı koymaktan geçmez. Muhtemel savaş nedenlerine dikkat etmek ve muhtemel çatışmaları öngörebilmek ve bunları bir savaşa yol açmadan önce çözebilmek, güvenliği sağlamak için doğru yaklaşımlardır" (Küçükşahin, 2006).

Yukarıda güvenlik ile ilgili farklı tanımlar verilmiştir. Bu tanımların hepsinin bakış açısı farklıdır, ancak sağlanmak istenen hedef aynıdır; insanların kişisel veya ulusal açıdan huzur içinde korkusuz bir yaşam sürmeleridir.

İnsan varoluşundan bu güne değin üç temel ihtiyaç üzerine yaşamını sürdürmüştür. Bunlar beslenme, barınma, giyinmedir. Barınma ihtiyacı temelinde insanın güvenlik ihtiyacı vardır. Çünkü insan her an güvende olmak ister. İşte tam bu noktada insanlar istirahat ettikleri yani her türlü dış faktöre açık kaldıkları dönemlerde kendilerini koruyacak bir kalkan oluşturmak istemişlerdir. Bu nedenle önce ağaç kovukları, mağaralar gibi doğal korunma alanlarını kullanmışlar, daha sonra kendilerine evler inşaa etmişlerdir. Ayrıca barınakları dışında da kendilerini koruyabilecek aletler geliştirmişlerdir.

İlkel çağlarda insanoğlu dış tehditlere karşı kendisini savunma amacıyla ateş, orak, taş gibi savnma malzemelerini kullanırken zaman içerisinde gelişen teknolojinin getirdiği tehdit ve risklere ve karşı yeni savunma araçları ve stratejiler geliştirmiştir (Bakan ve Şahin, 2018).

İnsanların zamanla bir arada yaşama zorunluluğu ortaya çıkmış, bir arada yaşayan insanlar toplumları, toplumlar da devletleri oluşturmuşlardır. Devletler oluştuğunda ise güvenlik kavramının kapsamında değişmeler olmuştur. Güvenlik uluslararası bir boyut kazanmıştır. Güvenliğin uluslararası boyutuna bakıldığında güvenlik, antik dönemlerde M.Ö. Sümer site devletlerine kadar gitmektedir. Güvenlik endişesinin ilk örneği, M.Ö. 16. yüzyılda Hititler'e aittir. M.Ö. 1340'lı yıllarda Hititlerin Mısırlılar ile yaşadıkları anlaşmazlık sonucu önce Kadeş

Savaşı yaşanmış, sonrasında ise iki devlet arasında dünyanın ilk yazılı anlaşması olan "Kadeş Antlaşması" yapılarak sınır güvenliği sağlanmıştır (Bakan ve Şahin, 2018).

Ülkelerin farklı coğrafyalarda yer almaları ve coğrafyanın her yerde aynı bonkörlükte olmaması, yine insanların farklı dini ve kültürel inançlarının olması vb. durumlar nedeniyle güvenliğin uluslararası olan boyutu çok büyük önem kazanmıştır. Tarihsel süreçte gerçekleşen tüm bu olaylar yeni tehditlerin ortaya çıkmasına neden olmuştur. Küreselleşme, teknolojinin gelişmesi gibi etmenler devletler arası sınırları, iletişim sınırlarını ortadan kaldırmış, bu durum çözülmesi oldukça zor uluslararası bir durum haline gelmiştir. İnsanlar savaş meydanlarında silahlarla savaşmak yerine artık bilgisayar başında yani masa başı dediğimiz şekilde oturdukları yerden savaşmaktadır. Bu şekilde güvenlik riskleri artarak günümüze kadar gelmiştir.

Teknolojik gelişmeler ile güvenlik olgusu artık küresel hale gelmiştir. Çünkü insanlar dünyanın bir çok noktasından anlık bilgi sahibi olabilmekte, kıtalar arası alışveriş yapabilmekte, kısacası her türlü etkileşim sağlayabilmektedir. Bu durum da yeni güvenlik sorunlarını ortaya çıkarmaktadır.

1.3.1. Güvenlik türleri

Güvenliği, devlet, sistem ve birey düzeyinde ele alan yaklaşımlarla iç ve dış güvenlik olarak ya da askeri, siyasi, sosyal, ekonomik, çevre güvenliği ve müşterek güvenlik olmak üzere farklı kategorilere ayırarak inceleyen yaklaşımlar bulunmaktadır. Güvenliğin farklı alanlarına ortak bir tanım bulunamayacağı gibi farklı alanları da ortadan kadırarak yani birbirinden soyutlayarak bağımsız bir inceleme yapılamamaktadır (Sancak, 2013).

Güvenlik çok kapsamlı bir kavram, bir alan olması nedeniyle çalışılması, anlaşılması, yeni sistemlerin ortaya konulması açısından birçok alt kategoriye ayrılmıştır.

1.3.1.1. İç Güvenlik

Ülkenin siyasi sınırları içerisinde, insanların huzurlu bir şekilde yaşaması, devletin devamı için alınan tedbirlerdir. İç güvenliği sağlamada öncelikli yetkili birim kolluk kuvvetleridir (Küçükşahin, 2006).

1.3.1.2. Dış Güvenlik

Dış güvenlik kavramı, bir ülkenin siyasi sınırlarının dışından o ülkeye yönelen tehditlere karşı alınan tedbirler olarak tanımlanır. Bu tehditlere karşı devletler başta silahlı kuvvetler olmak üzere, istihbarat, diplomasi ve uluslararası örgütleri kullanırlar (Küçükşahin, 2006).

1.3.1.3. Siyasi Güvenlik

Bir ülke içinde devlet tarafından çıkarılan yasaların o ülkede yaşayan insanlara uygun olup olmadığı ve rejimin o ülkede yaşayan insanları temel alıp almadığını ifade eden güvenlik çeşididir (Küçükşahin, 2006).

1.3.1.4. Sosyal güvenlik

İnsanın insan olduğu için hakkı olan, bulunulan dönemin şartlarına göre insanların ihtiyaçlarının asgari düzeyde de olsa sağlanması durumudur (Küçükşahin, 2006).

1.3.1.5. Ekonomik güvenlik

Üretim ve tüketim arasındaki yani arz ile talep arasındaki ekonomik sistemin düzenli şekilde, aksamadan, yine insanların ihtiyaçlarını asgari düzeydede olsa karşılanması durumudur. Her insan maddi açıdan kendini güvende hissetmek ister. Bu amaçla ihtiyaç fazlalılığı biriktirir (Küçükşahin, 2006).

1.3.1.6. Askeri güvenlik

İç ve dış güvenliğin hazırlanan askeri tedbirler ile sağlanması durumudur. Askeri güvenliğin ülkeler açısından en temel unsuru ülkelerin ordularıdır (Küçükşahin, 2006).

1.3.1.7. Çevresel güvenlik

Doğal ortamın, çevrenin korunması; insanların bu konuda duyarlı hale getirilerek çevresel düzenin devamlılığını, doğanın sağlıklı bir şekilde varlığını devam ettirmesi için yapılan çalışmalarıdır (Küçükşahin, 2006).

1.3.1.8. Ulusal güvenlik

Bir devletin millî menfaatlerini gerçekleştirilme, iç ve dış tehditlere karşı bu menfaatleri koruma ve kollaması durumudur (Küçükşahin, 2006).

1.3.1.9 Bölgesel güvenlik

Ülkelerin belli bir bölge içerisinde güvenliklerini sağlamak amacıyla birlikte hareket etme birlikte tedbir uygulama durumudur (Küçükşahin, 2006).

1.3.1.10. Uluslararası güvenlik

Ortak çıkarlar etrafında ikiden fazla devlettin bir araya gelerek oluşturduğu güvenlik yapılanmasıdır (Küçükşahin, 2006).

1.3.1.11. Küresel Güvenlik

Dünyanın tamamın da birlikte hareket edilmediği zaman, insanların tamamına olumsuz etki edebilecek güvenlik türüdür (Küçükşahin, 2006). Örneğin dünyamıza yaklaşan bir meteor, asit yağmuru gibi.

1.3.1.12. Fiziki olmayan güvenlik

Geçmişten gelen ve daha çok fiziki tedbirlere dayanan güvenlik tedbirleri dışında yeni bir güvenlik yaklaşımı gerekmektedir. Fiziki olmayan güvenlik bağlamında bilgi güvenliği, teknolojik güvenlik, sanal güvenlik ve siber uzayda güvenlik kavramlarını sıralayabiliriz. Örneğin dolandırıcıların en çok kullandığı güvenlik türü fiziki olmayan güvenlik türüdür. Çünkü fiziki herhangi bir unsur ortamda yoktur, tüm işlemler sanal ortamlarda yapılır (Küçükşahin, 2006).

1.4. Bilgi Güvenliği

Bilgisayarların hayatımıza yoğun bir şekilde girdiği son 20-30 yıl ve buna ek son 10-15 yıldır cep telefonları, tabletlerimiz ile bilgisayarın artık yanımızda (cebimizde) taşınır hale gelmesi; bizlerin birçok işimizi bu cep bilgisayarları üzerinden halletmemiz bilgi güvenliği kavramının daha çok ön plana çıkmasına sebep olmuştur.

İnsanlar arasındaki bilgi paylaşımı ve iletişim süreçleri artık sanal ortam dediğimiz bilgi ve iletişim teknolojileri üzerine taşınmış, gerçek ortamdan uzaklaşmıştır (Güldüren ve ark., 2017). Bilginin hızlı aktarımı toplumlarında çağa ayak uydurabilmesi için gereklidir.

Toplumların hızlı gelişmeleri için bilginin de hızlı aktarımı çok önemlidir. Bu nedenle tüm ülkeler bilgiye ulaşmak, onu kullanmak ve bilgiye sahip olmak için çok büyük emekler harcamaktadır. Bunun sonucunda bilginin elde edildiği, depolandığı, kullanıldığı, aktarıldığı bilgi teknolojileri hızlı bir gelişme göstermiştir (Hacımustafaoğlu, 2019).

Zamanla bilginin hızlı bir şekilde artışı ve teknolojinin gelişmesinin de etkisiyle eldeki bilgilerin dijital ortama aktarılması gerekli hale gelmiştir. bilgi ne kadar fazla olursa olsun, az yer kaplar bir şekilde dijital ortama taşınmış, bu bilgilerin buradan başka bir yere aktarılması, taşınması kullanılması kolaylaşmıştır. Teknolojinin bilgiye böyle bir kolaylık sağlaması, teknolojinin günlük hayatta iletişim kurma ve bilgi paylaşmada daha çok istifade edilmesini sağlamıştır. Bilgi aktarımında bu kolaylığı sağlayan teknoloji aynı zamanda gerekli farkındalık oluşturulmadığında bilgi için bir tehlike unsuruna da dönüşebilmektedir.

Güvenliğinin sağlanması beklenen bilgi; dijital ortama aktarılmış, düzenlenmesi, saklanması, başka bir yere nakledilmesi yine dijital ortam üzerinden olan bilgilerdir. Bu bilgiler ile ilgili gerekli farkındalık oluşturulmaz ise en kolay erişilebilen bilgiler olma özelliği de vardır.

Dünya üzerinde internet kullanımının yaygınlaşması ile insanların bilgiye ulaşımı kolaylaşmıştır. Ancak bu durum beraberinde getirdiği riskler sebebiyle eldeki bilgiye başkaları tarafından kolayca erişilmesine, değiştirilmesine, bilginin kaybolmasına da gerekli tedbirler alınmadığı zaman uygun bir ortam hazırlamıştır (Çam ve ark., 2019).

Bilginin çok boyutlu oluşu araştırmacıların bilgi güvenliğinin ne olduğu konusunda bir çok tanım yapmalarına neden olmuştur.

Bilgi güvenliği özünde bilginin kendisine zarar verebilecek oluşumlardan uzak tutulması, gerekli yerlerde yetkili kişilerce kullanımının sağlanması, bilgiye zarar verebilecek ve bilgiyi kötü amaçları için kullanabilecek kişilerin engellenmesi olarak tanımlayabiliriz (Canbek ve Sağıroğlu, 2006). Bilginin göndericiden alıcıya ulaşıncaya kadar gizli, zarar verilmeden, değiştirilmeden, başka insanlar bu bilgiye ulaşmadan, korunarak güvenli bir şekilde naklinin sağlanması sürecini bilgi güvenliği olarak tanımlayabiliriz.

Bilgi güvenliği, izni ve yetkisi olmayan kişilerin bilgiye ulaşmasını, kullanmasını, bu kişilerin bu bilgileri değiştirmesini, açığa çıkarmasını, ortadan kaldırmasını, başkalarına aktarmasını veya bu bilgiye zarar vermesini engellemektir. Gizlilik, bütünlük ve erişebilirlik olarak üç temel unsurdan meydana gelir (Güldüren ve ark., 2017).

Bilgi güvenliği, bilginin üç temel unsuru olan gizlilik (sadece yetkili kişilerin erişebilmesi), bütünlük (bilginin ilk haliyle değiştirilmeden, zarar görmeden korunması) ve kullanılabilirlik/erişilebilirlik (yetkisi olan kişilerin gerek görüldüğünde bilgiye ulaşma durumu) unsurlarının var olması halinde sağlanabilecektir. Çünkü yetkisi olmayan kişilerin bilgiye ulaşımını engelleyemezseniz o bilginin güvenliğinden söz edemeyiz. Aynı şekilde bilginin bütünlüğünü temin edemezseniz o bilginin güvenliğinden bahsedemezsiniz.

Bilgi dijital ortamda da olsa, kâğıt üzerinde de olsa bilginin korunması için aşırı bir çaba gerekir. İnsanların bilgiyi nasıl koruyacaklarını, bu bilginin güvenliğini nasıl sağlayacaklarını bilmeleri gerekir. Bir bilginin ne kadar güvende olduğu o bilgiye erişim yetkisi bulunan kişinin bilgi güvenliği farkındalığı seviyesi ile doğru orantılıdır. Kişinin bilgi güvenliği farkındalığı gelişmişse bilginin güvenlik yüzdeside o derecede artar. Kısacası bilgi güvenliğindeki temel etken insandır.

Öztemiz ve Yılmaz 2013 yılında yaptıkları çalışmada, bilgi güvenliğinin, bilginin bozulma, silinme, tahribat gibi zarar verici unsurlara ve olası saldırılara karşı korunmasını sağlayan birtakım uygulamalar olduğunu ifade etmişlerdir.

Kısaca bilgi güvenliğini bilginin kullanım hakkı bulunan kişiler dışında herhangi bir kişinin müdahalesi olmaması durumudur. Yani bilgiye sadece yetkili kişiler ulaşabilmelidir. Bu kişilerde bu bilgiyi nasıl koruyacaklarını, nasıl aktaracaklarını, nasıl kullanacaklarını iyi bilmelidirler.

Ortaya çıkabilecek olası tehditlere karşı bilginin korunmasına bilgi güvenliği denir. Bu açıdan bilgi güvenliği bilgiyi güvenli bir şekilde saklamak için gerekli sistemlerin oluşturulması, istenmeyen kişilerce erişiminin engellenmesi için gerekli tedbirlerin alınması durumudur. Kurumlar açısından bilgi güvenliği kurumların devamı, başarısı, kar elde etmesi açısından önemlidir. Kurumlar iş hayatında sadece fiziki olarak rekabet etmezler, ayrıca dijital ortamda da bir rekabet halindedirler.

Bilgi güvenliği, "biz gereken tedbirleri aldık, bu dakikadan itiaren bu bilgilere bir şey olmaz" diyebileceğimiz bir durum değildir. Çünkü bilgi güvenliği bir anda başlayıp bitmez. Bilgi güvenliği sürekli değişmesi, geliştirilmesi, gerekli denetimlerinin yapılması gereken bir olgudur. Bilgi güvenliğinin sürekliliği vardır. Bilgi güvenliği; teknoloji, insan ve sürecin birlikte uyumlu bir şekilde çalışmasını gerektiren bir kavramdır (Eminağaoğlu ve Gökşen, 2009). Bilgi güvenliği süreklilik arz eden bir durumdur. Bilgi güvenliğinin sonu var mıdır? diye soracak olursak insanlığın yok oluşu cevabını vermemiz en doğrusu olacaktır. İnsan var olduğu sürece bilgi de var olacak ve bu bilgi mutlak surette korunma ihtiyacı duyacaktır.

Bilgi güvenliği sürekli değişimlere ve gelişimlere açık bir olgudur. Bilgi güvenliğini, sadece teknoloji güvenliği yada sadece bilgisayar güvenliği olarak algılamamız yanlış olur. Çünkü bilgi güvenliğinin sağlanmasında; insan, süreç ve teknoloji üçlüsünün birbirleriyle uyumlu olduğu bir süreç vardır. Bu bilgilerden de anlaşılacağı gibi bilgi güvenliği, gerek kişisel hayatımızda ve gerekse de kamusal hayatımızda öğrenilmesi, içselleştirilmesi, en önemlisi varlığının kabul edilmesi gereken bir süreçtir (Eminağaoğlu ve Gökşen, 2009). Bilgi güvenliği varlığını kabul etmek önemlidir. Çünkü bilgi güvenliği olgusunu yok saymak bilinçsiz insanların yetişmesine ve risklerin daha çok artmasına neden olacaktır.

Bilgi güvenliği farkındalığının geçici olduğu düşünülse de bir kurum çalışanlarının güvenlik farkındalığını periyodik olarak ölçmeli ve uygun iyileştirmeleri sağlamalıdır (Al-Shanfari ve ark., 2020).

Bilginin paylaşımı noktasında başta kişisel bilgilerimiz olmak üzere bize ait tük özel bilgilerimiz teknoloji sayesinde sanal dünyada yani teknolojik cihazlardaki uygulamalarda saklanmaktadır (Güldüren ve ark., 2016). Kişisel veya kurumsal bilgilerimizin kötü niyetli şahısların ellerine geçmemesi, geçse de kullanılamaması bizim bilgi güvenliğimiz açısından önemlidir. Çünkü bilgilerimiz kötü niyetli kişilerin ellerine geçtiğinde biz maddi ve manevi kayba uğrayabiliriz. Yıllardır fabrikalarda işçi olarak çalışarak veya tarlalarda alın teri dökerek elde edilen birikimler bilgi güvenliğine dikkat edilmediğinde saniyeler içinde kötü niyetli kişilerin hesabına geçebilir. Henüz okuma yazma bilmeden dijital ortamlarla tanışan insanlar bilgi güvenliği açısından en büyük risklerdir. Bu kişilerin gerek eğitim ile gerekse de ailelerinin koruması ile bilgi güvenliklerinin sağlanması bir zaruriyettir. Bu açıdan bilgi güvenliğinin ne olduğunu iyi bilmemiz gerekir.

Bilginin saklanması esnasında gerekli tedbirler alınmaz, gerekli hassasiyet gösterilmez ise insanlar iş kaybı, ekonomik kayıplar, manevi kayıplar yaşayabilir, hatta ölümde dahil olmak üzere çok ağır sonuçlar ortaya çıkabilir. Bunların hepsi birer bilgi güvenliği sorunudur.

1.4.1. Bilgi güvenliğinin unsurları

Bilgiye yetkisiz veya izinsiz ulaşılması, kullanılması, değiştirilmesi ve ortadan kaldırılması, başka kişilerin eline geçmesinin önlenmesi olarak tanımlanan bilgi güvenliğinin olmazsa olmaz unsurları bulunmaktadır.

Bilgi güvenliği erişilebilirlik, gizlilik ve bütünlük olmak üzere üç temel faktörden oluşmaktadır (Çam ve ark., 2019). Bu üç unsur temel kabul edilse de araştırmacılar bilgi güvenliğine zamanla farklı unsurlarda eklemişlerdir. Örneğin; Güvenlik, giriş denetimi, inkâr edememe, kimlik tespiti, kayıt altına alma, güven duyulması gibi. Bunlarda aslında bu üç temel unsurun alt dallarıdır diyebiliriz. Bu unsurlara dikkat edilmesi tabiki de bilginin daha da güvenli hale gelmesini sağlamaktadır (Altunsaban Yerlikaya, 2019).

1.4.1.1. Gizlilik

Gizlilik, bilginin yetkisiz kişilerce erişiminin engellenmesine yönelik çalışmalardır. Amaç, kötü niyetli kişilerce bilgilere ulaşılsa dahi onların bu bilgilere müdahalesini, bu bilgileri kullanmalarını, bu bilgileri nakletmelerini engelleyici çalışmalar yapmaktır. Bu durum genellikle şifreleme yöntemleri ile sağlanmaktadır. Bunun yanında yüz tanıma, parmak izi algılama sistemleride kullanılmaktadır.

Kurumsal açıdan bilgi güvenliğinde ise bu bilgilerin korunması için gerekli tedbirler kurum tarafından alınır. Yine korunması gereken bilgilerin gizlilik seviyeleri kurum tarafından belirlenir. Örneğin bir kamu kurumuna gittiğiniz zaman evrak dolaplarında "yangında ilk kurtarılacak" ibaresini görürsünüz. Bu o evrakların önemli bilgiler içerdiğini göstermektedir.

1.4.1.2. Bütünlük

Bilginin göndericiden alıcıya zarar görmeden ulaşmasının sağlanması bütünlük ilkesidir. Bilginin göndericideki haliyle alıcıya ulaşması durumudur. Bu aktarım esnasında bilgide değişme, bozulma vb. olursa bilgi bütünlüğünü yitirmiş olur ve bilgi güvenliği zaafiyeti ortaya çıkar.

1.4.1.3. Erişebilirlik

Erişilebilirlik ilkesi ise bilginin kişilerin yetkileri dahilinde ihtiyaç duyulan her anda ulaşılabilir olmasını sağlayan uygulamaları kapsar. Kısacası yetkisi olmayan kişinin bilgiye ulaşamamasını ifade eder.

Bu üç unsurun tamamı gerçekleştirildiği takdirde bilgi güvenliği sağlanmıştır, diyebiliriz. Bu unsurlardan birinde eksiklik olması halinde bilginin güvenliğinden söz etmemiz mümkün olmayacaktır. Bu unsurlardan herhangi birinin olmaması güvenlik zafiyetine neden olur ve bilgi güvenliği açığı ortaya çıkar (Güldüren ve ark., 2017).

Verilen üç temel güvenlik unsurlarından herhangi biri zarar görürse güvenlik zafiyeti oluşur. Bilgi güvenliği bireyler ve kurumlar için çok değerli bir varlık olan bilginin korunması için gereklidir (Güldüren ve Keser, 2015).

1.4.2. Bilgi güvenliğinde teknoloji, tehlike ve tehdit ilişkisi

Biz insanlar günümüzde artık tüm bilgilerimizi (değerli olsun olmasın) dijital ortamda tutmaktayız. Bu durumu da kendimiz için bir tehlike olarak görmemekteyiz. İnsanlar interneti günlük yaşamlarını tüm noktalarında kullanmaktadır. Arkadaş ve ailelerle bağlantı kurmak için, banka işlemleri için, sağlık, eğitim için birçok internet hizmetinden faydalanmaktadırlar. Böylece teknoloji ile olan bağlantı artmaktadır. Bu durum teknolojinin bize sunduğu riskleride artırmakdadır (Senthilkumar and Easwaramoorthy, 2017).

Banka bilgileri, iş hayatı bilgileri, kişisel bilgiler dijital ortamlarda bilinçsizce paylaşılabilmektedir. Bu paylaşımlara kötü niyetli kişiler yine aynı teknolojiyi kullanarak rahatça ulaşabilmektedir. Bizim için değersiz olan bilgilerimiz kötü niyetli kişiler için çok büyük değer taşıyabilir.

İnternetin ortaya çıkması sonrasında çevrimiçi uygulamaların kullanılması ve her gün gelişen sosyal medyayı kullanan öğrenciler birçok riskede maruz kalmaktadır. Dolandırıcılık, siber zorbalık, kimlik avı gibi risklere maruz kalabilmektedirler. Bilgi güvenliği bilinci sağlanarak bu risklere çözüm bulunabilir (Garba ve ark., 2020)

Bilgi teknolojilerini, interneti en çok kullanan yaş grubu gençlerdir. Bu gençlerin çoğunluğu eğitim hayatına devam etmektedir. Öğrenciler yaşamlarının her noktasında teknoloji ve internetle adeta birlikte yaşamaktadır. Bu nedenle çoğunluğu öğrenci olan gençlerin internet ve teknoloji kullanımı noktasında eğitilmedikleri zaman zarar görme riski en fazla olan insanlarda onladır (Avcı ve Oruç, 2019).

İnternet yani dijital teknoloji kullanımı arttıkça insanların maruz kalabilecekleri risklerde çeşit ve sayı olarakta artmaktadır. İletişim noktasında çevrimiçi cihazlarla çok büyük kolaylık sağlayan teknoloji beraberinde insanları çeşitli tehlikelerle de açık hale getirmektedir. İnsanların özel bilgilerin paylaşımı, gerçek ve sanal dünya arasındaki sınırı çizememesi en büyük tehlikeler olarak kendini göstermektedir (Güldüren ve ark., 2017).

İnsanlar internet ortamında gerçek yaşamdan çok farklı davrandıkları için sonuçlarını düşünmeden gerçek yaşamdan bağımsızmış gibi bilgi paylaşımı yapmakta, kişisel bilgilerini, resimlerini paylaşmaktadırlar. Bu durum kötü niyetli kişilerce suistimal edilerek paylaşımda bulunan kişilerin mağdur olmalarına sebep olabilmektedir.

Teknoloji bilgi güvenliği için çok önemli bir unsur ve aynı zamanda çok önemli bir tehdittir. Tehdit kavramı, bilginin gizlilik, bütünlük ve erişilebilirliğine olumsuz etki edebilecek tehlikelerdir.

Bilgi ve bilişim teknolojisi ne kadar gelişir ise bizim de bilgi güvenliği açısından o kadar kendimizi geliştirmemiz gerekmektedir. Bu açıdan uzmanların geliştirdikleri güvenlik tedbirlerini de iyi takip etmemiz gerekmektedir. Teknoloji geliştikçe kötü niyetli kişiler insanlara yeni tehlikeler oluşturmak için çaba sarf etmektedir. Ayrıca teknolojiyi kullanan insan sayısının kontrolsüz olarak hızlı bir şekilde artması insanların tehlikeler ile karşı karşıya kaldıklarının açıkça göstergesidir (Arslan ve Bal, 2013).

Bilişim teknolojileri geliştikçe güvenlik sorunlarıda daha fazla ortaya çıkmaya başlamıştır. Bir çoğumuz günlük yaşantımızda kredi kartımız ile ilgili, cep telefonumuza virüs bulaşıp bulaşmadığı ile ilgili, banka hesabımızın güvenliği ile ilgili aklımızı meşgul eden sorularla baş başa kalmışızdır (Öztezcan ve Çetinkaya, 2017). Tüm bu sorunları yaşamamak için bilgi güvenliği konusunda bilinçli olmamız artık bir zorunluluktur. İnsanlar ve kurumlar bu konuda daha dikkatli olmalıdır.

Kuruluşlar önleyici tedbirlerini başlarına bir iş geldiğinde kullanmaktadır. Olay meydana geldiğinde çok geç olabilir. Bu nedenle üzgün olmaktansa güvende olmak daha iyidir (Chan and Mübarek, 2012).

Kısacası gelişen teknoloji bizlere birçok kolaylık sağladığı gibi bizler gerekli teknolojik donanıma, bilgiye sahip olmazsak aynı teknolojiyi kullanan kötü niyetli kişiler bu teknolojiyi bize karşı kullanabilir, bizim açımızdan bir tehlike ve tehdit unrusu olabilirler.

1.4.2.1. Teknolojik Açıdan Maruz Kalabileceğimiz (Tehdit) Saldırı Çeşitleri

Bilgi teknolojilerini kullandığımızda maruz kalabileceğimiz saldırı çeşitlerinin temelinde birincisi insan faktörü, ikincisi teknoloji faktörü yer almaktadır. İnsan faktöründen kaynaklı saldırılar genellikle vurdumduymazlık, önemsememe, eğitimsizlik gibi unsurlar üzerine şekillenirler.

Saldırganlar aynı zamanda bilgi güvenliği farkındalığı olmayan ve güvenlik uygulamalarını görmezden gelen kullanıcıları hedef almaktadırlar (Ramalingam ve ark., 2015).

Burada en önemli faktör insandır ve bilgi güvenliğinde insan aktif bir rol oynar. İnsanlar daha çok sosyal ağlar üzerinden bilgi güvenliği açıkları vermektedir. Bu açıkların temel nedenleri; mahremiyet ilkelerine uymama, sosyal ağın kontrolünün nasıl yapıldığını, bilgi güvenliğinin nasıl sağlanacağını bilmeme, bilinçsizlikten kaynaklı olarak kişisel bilgilerin bu ortamlarda paylaşılmasıdır. Bu durum bu tür bilgi paylaşımı yapan insanları kötü niyetli kişilerin birinci hedefi haline getirmektedir (Yavanoğlu, ve ark., 2012).

Diğer yandan teknoloji kaynaklı (zararlı yazılımlara dayalı tehditler) saldırılarda ise insan pasif durumdadır. Kötü niyetli kişiler yazılımsal boşluklardan, kötü niyetli programlardan faydalanarak insanların bilgilerine ulaşmakta ve onları mağdur etmektedirler. Bu saldırı çeşitleri ise şunlardır;

1.4.2.2. İnsan Faktöründen Kaynaklı Tehditler

İnsan faktörü, güvenliğin diğer alanlarında olduğu gibi bilgi güvenliği alanında da en önemli noktada yer almaktadır. Saldırganlar insanların zafiyetlerinden faydalanarak sistemlere zarar verebilir, bilgileri ele geçirebilir, bozabilir veya değiştirebilir. Bunun soncunda da birtakım çıkarlar elde ederler.

1.4.2.2.1. Sosyal Mühendislik

Sosyal mühendislik, saldırganın insanları kandırmak suretiyle kişilerin ve kurumların bilgilerine ulaşması durumudur. Bu duruma örnek olarak herhangibir kurumda çalışan personelin o kurumun bilgi işlem sorumlusu olduğunu söyleyerek şifrelerinin ele geçirilmesi gösterilebilir. (Öztezcan ve Çetinkaya, 2017). Bu saldırı çeşidi günümüzde en çok dolandırıcılar

tarafından kullanılmaktadır. Telefon veya başka bir iletişim aracı ile hedef şahısları ikna ederek, elde ettikleri bilgiler ile büyük miktarda maddi kazanç elde etmektedirler.

1.4.2.2.2. Oltalama

Bu teknik daha çok sahte web siteleri üzerinden gerçekleştirilmektedir. Mağdur kendisine gönderilen e-postadaki bağlantıyı kullanmış olduğu bankadan veya alışveriş yapmış olduğu bir siteden geldiğini düşünür. Sonrasında linki tıkladığında linkin kendisini yönlendirmesi ile banka bilgilerini, iletişim bilgilerini, kimlik bilgilerini bu link üzerinden paylaşır. Bu şekilde kötü niyetli insanlar mağdurun tüm bilgilerini oltalama tekniği ile elde etmiş olur (Öztezcan ve Çetinkaya, 2017). Oltalama tekniği zararlı yazılımlar kullanılarak insanların yönlendirilmesi şeklinde kullanılır.

1.4.2.3. Zararlı Yazılımlara Dayalı Tehditler

Bilgisayar sistemlerine bulaşarak zarar verme, bilgiyi çalma ya da kullanıcıları rahatsız etme amacı ile hazırlanmış kötü niyetli yazılımlardır. Bu yazılımlar bulaştığı sistemin çalışmasını aksatmaktadır (Öztezcan ve Çetinkaya, 2017).

Bu yazılımlar, farkındalık düzeyi düşük ve yeterli güvenlik bilincine sahip olmayan kişileri hedef alarak bu kişilerin bilgisayarlarına ve sistemlerine bulaşmaktadır. Sosyal mühendislik ile inka edilen mağdurun bilgisayarına zararlı yazılım kolayca yüklenmekte ve buradan bilgiler kolayca temin edilmektedir. Bazı bilgisayarlarda da sosyal mühendisliğe gerek kalmadan etkileşim sağlanabilmektedir (Öztezcan ve Çetinkaya, 2017).

İndirilen programların, zararlı yazılımların, oltalama tekniğinin, sahte içerikli e-postaların, bilgi sızdırmanın ve fiziksel zarar vermenin saldırı çeşidi olarak en fazla zararı verdiğini Merinos (2013) yaptığı araştırma ile belirlemiştir (Karaoğlan Yılmaz ve Çavuş Ezin, 2017).

Teknoloji çağında olduğumuz için kimlik hırsızlığı, kimlik avı, veri sızıntısı gibi yenilikçi tehditler sürekli gelişmektedir (Al-Shanfari ve ark., 2020)

1.4.2.3.1. Casus/Köstebek Yazılımlar

Casus yazılım, kullanıcının bilgisi olmadan, kullanıcıya ait bilgileri ve yaptığı işlemleri kötü niyetli kişilere ulaştıran yazılımlardır. Bu yazılımlar kişilere ait bilgileri kişiler farketmeden, gizli bir şekilde başka bir bilişim teknolojisi cihazına aktarır. Örneğin internet üzerinden alışveriş yaptınız ve burada kredi kartı bilgilerinizi bu sitede kullandınız. Zararlı yazılım kredi kartı bilgilerinizi anında kötü niyetli kişinin bilgisayarına ulaştıracaktır. Kişiler kredi kartı bilgilerinin çalındığını kredi kartı ödeme tarihi geldiğinde fark etmektedir.

Casus yazılımlar virüs ve solucanlardan kendi kopyasını oluşturarak çoğalmazlar. Amaçları mağdurun yani kullanıcının e-posta adresi, telefon numarası, şifreleri, kredi kartı numaraları gibi birçok özel bilgisini elde ederek kötü niyetli kişinin bilgisayarına ulaştırmaktır. Kötü niyetli kişi de bu bilgileri en başta maddi kazanç elde etmek olmak üzere farklı amaçlarda kullanabilir (Arslan ve Bal, 2013).

1.4.2.3.2. Bilgisayar Virüsleri (Computer Viruses)

Adını organizmalardaki hücrelere buşalarak zarar veren virüslerden almışlardır. Virüsler, en çok zarar verebilecek ve en tehlikeli yazılımlardır. Bulaştığı yazılımdaki bilgilerin kopyasını oluşturur, kedi kodlarını bu bilgilere entegre eder, hızlı bir şekilde yayılır ve çoğalır.

1.4.2.3.3. Bilgisayar Solucanı (Computer Worms)

Solucanlar da bilgisayar virüslerine benzerler. Virüsler gibi bir programa kendisini iliştirmez ve bu programın bir parçası olmazlar. Yayılmaları için insan etkileşimine de ihtiyaçları yoktur. Kendi kendilerine çoğalırlar (Canbek ve Sağıroğlu, 2006).

1.4.2.3.4. Truva Atları (Trojan Horses)

Truva atları, kendi kendine çoğalmayan yazılımlardır. Kendisini faydalı bir programa inşa eder. Sonrasında kullanıcıya kendisinin faydalı bir program olduğunu, faydalı işlevlerinin olduğunu inandırarak onu ikna eder ve kullanıcının kendisini çalıştırmasını sağlayıp etkin hale gelir (Canbek ve Sağıroğlu, 2006).

1.4.2.3.5. Arka Kapılar (Backdoor)

Arka kapılar sıradan bilgisayar incelemeleri esnasında bulunamayan, uzaktan erişim sağlayabilen yöntemlerdir. Kötü niyetli kişiler mağdurun bilgisayar sistemine sızdıktan sonra daha sonrada bilgilere erişebilmek için bu yazılımları kullanırlar (Canbek ve Sağıroğlu, 2006).

1.4.2.3.6. Mesaj Sağanakları (Spams)

Mesaj sağanakları, belki de insanların en çok karşılaştıkları ve sorun yaşadıkları kötü niyetli yazılımlardır. Sağanak şeklinde reklam, ürün tanıtımı, ürün satma, e-postalara gelen

istenmedik mesajların kullanıcıyı meşgul etmesidir (Canbek ve Sağıroğlu, 2006). Bilgisarımızı açtığımızda ekranımıza arka arkaya çok sayıda reklam, tanıtım fotoğrafları, arkadaşlık istekleri geldiğinde artık mesaj sağanakları kötücül yazılımlarına maruz kalmışsınız demektir. Bundan kurtulmanın yonu bilgisayarınızı formatlayarak bu kötücül yazılımları ortadan kaldırmaktır.

1.4.3. Bilgi güvenliğinde insan faktörü

Bilgi güvenliğinin sağlanmasındaki en önemli rol yine bu bilgiyi kullanacak insandır. Bilgi güvenliğinde başarılı olmanın yolu, insanların bu konuda eğitilmesi, bilgilendirilmesi ve bilinçlendirilmesi, bu şekilde farkındalıklarının artırılmasından geçmektedir.

İnsan faktörüne bağlı bilgi güvenliği riskleri bilgi güvenliğinin sağlanması açısından ortaya konulan güvenlik tedbirleri içerisinde en önemli noktada yer almaktadır (Güldüren ve Keser, 2015). Çünkü bilgi güvenliği tedbirlerini uygulayacak, bu bilgileri kullancak insandır. Bilgi güvenliğinin sağlanması için alınan teknik önlemlerin temelinde yine insan faktörü dikkate alınmalıdır. Geliştirilen güvenlik önlemlerini yöneten, kullanan, öğreten insandır. Bu nedenle insan teknik boyutun önünde değerlendirilmelidir.

Güvenlik önlemlerinin başarısı son kullanıcıların o konu hakkındaki bilgisine bağlıdır. Bu durum altı çizilmesi gereken önemli bir noktadır (Stanciu and Tinca, 2016).

Bilgi güvenliğini sağlamanın sadece güvenlikle uğraşan kişilerin ve kurumların görevi olmadığını, bu teknolojileri kullanan herkesin bu göreve sahip olduğunu Vural ve Sağıroğlu (2007) yaptıkları araştırmada belirtmişlerdir (Hacımustafaoğlu, 2019). Bilgi ve iletişim teknolojilerinin, internetin hızla gelişmesi ve yaygınlaşması güvenlik açıklarının da artmasına neden olmaktadır. Bu açıdan bakıldığında bilgi güvenliği sağlama görevi teknolojiyi ve interneti kullanan herkesin görevidir (Güldüren ve ark., 2017).

Bilgi güvenliğinde başarılı olabilmek için insanların istekli, bilinçli ve bilgili olması gerekmektedir. Aksi takdirde verilen eğitimlerin hiçbir faydası olmayacaktır.

Günümüzde bilgi güvenliği farkındalığı çok önemli bir konu haline gelmiştir. Kuruluşlar bilgilerini güvenli hale getirmek için çok para harcasalar da tehditler hala büyük ölçüde devam etmektedir (Al-Jerbie ve ark., 2014)

Bilgi güvenliğini sağlamak için, bilgi güvenliği risklerinden korunmak için ne kadar para harcanırsa harcansın % 100 güvenlik sağlamak mümkün değildir. Bunun sebebi bu teknolojileri kullanacak olanların yine insan faktörü olmasıdır. Kurumlar isterlerse milyar dolarlık, milyarlarca avroluk harcama yapsınlar, bu teknolojiyi kulnanan insanın bilgi güvenliği açısından bu teknolojiyi kullanmada yeterli bilgisi yok ise yapılan harcamaların hiç bir değeri yoktur.

Bilgi güvenliğinin sağlanması için insan faktörü dikkate alınarak teknolojik önlenler alınabilir. Bilgi güvenliği açısından gerekli farkındalık sağlanarak riskler en aza indirilebilir. İnsan faktörünün olduğu bir bilgi güvenliği tedbirinde riskleri tamamen ortadan kaldırmak imkansızdır. Ancak bu riskler minimum seviyeye indirilebilir (Güldüren ve Keser, 2015).

Kurumların, teknik güvenlik önlemlerini insan faktörünü de dikkate alarak dijital veri güvenliğini sağlamaları gerekmektedir. Yapılan çalışmalar kurumlardaki bilgi güvenliğinin en zayıf halkasının yine kurum çalışanları olduğunu ortaya çıkarmıştır (Çam ve ark., 2019).

Bilgi güvenliğinde insan faktörü, güvenliğin teknik yönü kadar dikkate alınmalıdır. Bu amaçla güvenlik sağlanmak isteniyor ise öncelikle insanların bilinçlendirilmesi ve farkındalıklarının artırılması gerekmektedir. Teknoloji önde tutulur insan faktörü geri plana itilir ise en güçlü güvenlik tedbirleri dahi bilginin korunmasında yetersiz kalacaktır. Bazı insanlarda bilgi güvenliğinin sağlanması açısından teknolojik çalışmaların yeterli olacağı düşüncesi insan faktörünü ikinci plana itmektedir.

Bilgi güvenliğinin sağlanmasındaki en temel faktör olan insanın, ilk olarak bu konuya gerekli duyarlılığı göstermesi, yaşayabileceği tehlikelerin ne tür olumsuz sonuçlar doğurabileceğini bilmesi önemlidir (Sağır ve ark., 2018).

1.5. Bilgi Güvenliği Farkındalığı ve Eğitimi

Bir bilgiye yetkisi ve izni olmayan bir kişinin erişimi, bu bilgiyi kullanması, değiştirmesi, yok etmesi ve başka kişiler tarafından ele geçirilmesini önlemek bilgi güvenliğidir. İşte bu güvenlik önlemlerinden haberdar olma, güvenlik önlemleri hakkında bilgi sahibi olma, bilgi güvenliğine ait yeni teknolojileri takip etme durumu da bilgi güvenliği farkındalığını oluşturmaktadır.

Bilgi güvenliği farkındalığı, bilgi güvenliğini tehdit eden durumlara karşı ne gibi önlemler, güvenlik tedbirleri alınacağını bilmek olarakta tanımlanabilir.

İnsanlar nasıl ki herhangi bir sağlık sorunu yaşamadan hastaneye gitmiyorlarsa bilgi güvenliği konusunda da bir tehlike ile karşı karşıya kalmadıkları sürece bilgi güvenliği farkındalığına eğilim göstermediklerini Siponen (2001) ortaya koymuştur (Öztemiz ve Yılmaz, 2013). Yani bilgi güvenliği farkındalığı hasta olmadan önce düzenli kan tahlili yaptırmak, sağlık taramasından geçmesi neticesinde hasta olmamak için gerekli sağlık tedbirlerini alması gibidir. Herhangi bir saldırıya maruz kalmadan önce kendini nasıl koruyacağını bilmek bilgi güvenliği farkındalığıdır.

İnsanların kişisel ve kurumsal bilgilerini sorumsuzca paylaşmaları ve bu duruma dikkat etmemeleri bilgi güvenliği farkındalığını bir zorunluluk haline getirmiştir. Aynı zamanda gelişen teknoloji ile bilgi güvenliğine yönelik tehdit çeşitlerinin de artması insanları daha fazla risk altına sokmaktadır. Bu açıdan bakıldığında bilgi güvenliği farkındalığı önemini her geçen gün artırmaktadır.

Yeni koronavirüs Covid 19'un ortaya çıkması ile dünya genelinde her türlü etkinliğin yapılmasında zorluklar ve engeller ortaya çıkmıştır. Eğitim sektörüde bu zorluklardan ve engellerden nasibini almıştır. Sokağa çıkma yasakları ve sosyal mesafe kuralları ile birlikte iletişim ve etkileşimlerde dijital alanlara kaymıştır. Bu yasaklamalardan nasibini alan eğitim sektöründe de yüzyüze eğitim yerine uzaktan eğitime geçilmiştir. Bu durum da öğrencilerin dijital öğrenme ortamındaki güvenlik farkındalığını daha önemli hale getirmiştir (Mai and Tick, 2021). Aslında koronavirüs salgını döneminin bu şekilde yasaklar getirmesi ile bilgi güvenliği noktasında, dijital teknolojilerde kişiler bir çok eksiklerinin olduğunu, bu alanda eğitim almaları gerektiğini uygulamalı olarak öğrendiler.

Bilgi güvenliği farkındalığını sağlamanın en iyi yolu eğitimdir. Çünkü eğitimde bilgi güvenliği gibi sürekli kendini yenileyen, geliştiren bir alandır. Tüm teknolojik gelişmeleri yakından takip ederek, toplumların değişim ve gelişimine öncülük eden eğitim kurumları, nasıl teknolojik gelişmeleri takip ediyor ise bunların insanlara sunumunu, güvenli kullanımını da öğretmekle mükelleftir.

Bilgi güvenliği farkındalığının sağlanması açısından sorumluluğun en büyüğü eğitim alanına aittir. Bilgi güvenliği noktasında bilgiyi ele geçirmek isteyen kötü niyetli kişilerin kullandığı yöntemler ve bilgi üzerindeki tehditlerin fazlalağı, bizleri aynı oranda tedbir alma zaruriyetinde bırakmaktadır (Canbek ve Sağıroğlu, 2007).

İnsanların gerek iş hayatında gerekse toplumsal yaşamda bilgi güvenliği farkındalıklarının sağlanması için gerekli eğitim programları, seminerler, toplantılar düzenlenmelidir.

Her ne kadar insan hatası temelli bilgi güvenliği tehditlerini tamamen ortadan kaldırmak imkansız olsa da iyi planlanmış bilgi güvenliği farkındalığı eğitimi ile bu tehditler minimum seviyeye indirilebilir ve bu seviyede tutulabilir (Güldüren, 2021). Bilgi güvenliği risklerini % 0 seviyesine indirmek imkansız olsa da bilgi güvenliği farkındalığı eğitimlerinin temel amacı zaten hataları en aza indirmektir.

Bilgi güvenliği eğitimlerinde gençlerin bulunması hem onların bu tehditlerden korunması açısından gereklidir hem de bu eğitimler ile farkındalık düzeylerinin artmasının sağlanarak gençlerde bir sorumluluk bilinci oluşturmak için önemlidir (Güldüren ve ark., 2017). Özellikle gençlerin bu sürece dahil olmaları çok önemlidir. Çünkü birçok genç üniversite eğitiminde olduğundan hem kendi güvenlikleri, hem meslek hayatına atıldıklarında eğitecekleri kişilerin bilgi güvenliği açısından farkındalık kazanma faaliyetlerinde aktif rol oynayacaklardır. Aynı zamanda bu gençler geleceğin anne, baba adayları olmaları nedeniyle bilgi güvenliği farkındalığı sahibi olmaları bu açıdan da çok önemlidir.

Bilgi güvenliği farkındalığı oluşturmada diğer bir aktörde öğretmenlerdir. Çünkü öğretmenlerin öncelikle kendilerinin bilgi güvenliği açısından farkındalık sahibi olması gerekir. Öğretmenlerin kendilerinden sonra bilgi güvenliği farkındalığı açısından sorumlu

oldukları diğer iki kitle ise birincisi yetiştirdikleri öğrencileri, ikincisi ise anne, babası oldukları çocuklarıdır.

Dijital teknolojinin artık günümüzde, eğitim öğretim sürecinde hızlı ve aktif bir şekilde yerini alması ile öğretmenle bu teknolojilerdeki uygulamaları öğrenme açısından sorumluluk yüklemektedir. Bu da öğretmenlerin bilgi güvenliği farkındalığının önemini arttırmaktadır (Güldüren ve ark., 2017).

Bilgi güvenliği farkındalığına çocuklar ve aileler açısından baktığımızda ise küçük yaşta bilgisayar gibi teknolojik aletlerle tanışan çocukların bilgi güvenliği farkındalığı açısından koruma kalkanı aileleridir.

Güvenli internet kullanımı farkındalığı henüz gelişmemiş olan çocuklar kullandıkları sosyal ağlar üzerinden bir takım tehditlere maruz kalabilmektedir. Bu açıdan bakıldığında çocukların farkındalık düzeylerinin arttırılması güvenli internet kullanımı davranışları açısından oldukça önemlidir. Çocuklar anne babalarından bu konuda yardım alabilmelidir. Anne babalarında çocuklarına doğru bilgi verebilmeleri, çocuklarını bu risklerden korumaları için kendilerininde yeterli farkındalık düzeyine ulaşmış olması gerekmektedir. (Karaoğlan Yılmaz ve Çavuş Ezin, 2017).

1.6. Literatür Taraması

Güldüren ve Keser (2015) ülkemizde farklı yükseköğretim kurumlarında görev yapan 363 öğretim elemanıyla gerçekleştirdikleri çalışma ile öğretim elamanlarının bilgi güvenliği farkındalık seviyelerini belirlemek için bir ölçek geliştirmişlerdir. Yüksek öğretim çalışanı öğretim elemanlarının bu şekilde bilgi güvenliği farkındalıklarını kolayca belirlemeyi amaçlamışlardır.

Güldüren ve ark. (2017), öğretmenlerin bilgi güvenliği farkındalık düzeylerinin gelecek nesiller açısından önemli olduğu düşüncesinden hareketle yaptıkları çalışmada öğretmenlerin bilgi güvenliği farkındalık düzeylerini belirleyebilecek güvenilir ve geçerli bir ölçek geliştirmişlerdir.

Güldüren (2021) yaptığı çalışma ile üniversite öğrencilerinin bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik bir ölçek geliştirmiştir.

Akgün ve Topal (2015), eğitim fakültesinde eğitim gören öğrencilerinin bilgi güvenliği farkındalık seviyelerini tespit etmek için bir araştırma yapmışlardır. Araştırma sonucunda öğrencilerin farklı değişkenler üzerinden bilgi güvenlği farkındalık düzeylerini belirlemişlerdir. Araştırma sonucunda bilgi güvenliği farkındalık düzeyinin yetersiz olduğunu tespit etmişlerdir. Ayrıca daha önceden bilgi güvenliği farkındalığı eğitimi almış kişilerin farkındalık düzeylerinin daha yüksek olduğunu tespit etmişlerdir.

Canbek ve Sağıroğlu (2006), bilgi olgusu geniş bir açıdan irdelemiş, bilişim teknolojilerinin bilgi üzerindeki etkilerini ve boyutlarını ortaya koymuşlardır. Bilginin korunması ihtiyacından doğan bilgi güvenliğini incelemişler ve bilgi güvenliğini oluşturan ana unsurların neler olduğu üzerine durmuşlardır. Bilgi güvenliğine yönelik saldırıların, sayı ve çeşitlilik açısından değerlendirmesini yapmışlardır.

Tekerek ve Tekerek (2013) yaptıkları araştırma ile ilkokul, ortaokul ve lise öğrencilerinin bilgi ve bilgisayar güvenliği farkındalık seviyelerini ölçmeye çalışmışlardır. Araştırma için Kahramanmaraş ilinde, 2449 öğrenciye, bilgi ve bilgisayar güvenliği farkındalık ölçeği uygulamışlardır. Öğrencilerin güvenliği farkındalık düzeylerinin etik konularda yeterli olduğunu ortaya koymuşlardır. Ancak öğrencilerin kurallar ve bilgi gerektiren konularda farkındalık düzeylerinin düşük olduğunu tespit etmişlerdir. Bu durumu farkındalık eğitim ve etkinliklerinin yetersiz olması ile açıklamışlardır.

Talan ve Aktürk (2021) araştırmalarında, Kilis ve Gaziantep illerinde eğitim gören ortaöğretim öğrencilerini bilgi güvenliği farkındalığı ve dijital okuryazarlık açısından araştırılarak öğrencilerin cinsiyet, , internet ve sosyal medya kullanım süreleri, sınıf düzeyleri gibi farklı değişkenleri kullanarak bilgi güvenliği farkındalık durumlarının düzeylerini incelenmişlerdir. Araştırma ile öğrencilerin dijital okuryazarlık düzeylerinin genel olarak orta seviyenin üzerinde olduğunu, dijital teknoloji kullanımında öğrencilerin genel olarak yeterli düzeyde olduğunu ortaya koymuşlardır. Ancak öğrencilerin bilgi güvenliği açısından aynı seviyede olmadıklarını tespit etmişlerdir.

Keser ve Yayla (2021) yaptıkları çalışmada FATİH Projesini kullanan eğitim kurumlarında görevli öğretmenlerin bilgi güvenliği farkındalık seviyelerini tespit etmek amacıyla bu projeyi kullanan ve kullanmayan okullarda görev yapan öğretmenlerin bilgi güvenliği farkındalık seviyeleri karşılaştırarak, FATİH projesini kullanan eğitim kurumlarındaki öğretmenlerin bilgi güvenliği farkındalıklarının daha fazla olduğunu ortaya koymuşlardır. Ayrıca öğretmenlerin önceden bilgi güvenliği farkındalığı eğitimi alıp almama durumlarını değerlendirdiklerinde daha önce bu eğitimi alan öğretmenlerin farkındalık düzeylerinin daha yüksek olduğunu tespit etmişlerdir.

Ünver ve ark. (2009) yaptıkları çalışmada bilgi güvenliği zafiyetlerine vurgu yaparak, Siber Güvenlik, siber saldırı çeşitleri, ne tür önlemler alınabileceği üzerine bilgiler ortaya koymuşlardır.

Karaoğlan Yılmaz ve ark. (2014) tarafından yapılan çalışmada üniversite öğrencilerinin güvenli BİT kullanım davranışları belirlenmeye çalışılmıştır. Araştırmada öğrencilerin güvenli BİT kullanım davranışları sergilediği sonucuna ulaşılmıştır. Bununla beraber sergilenen davranışların hızla gelişen teknoloji karşısında yeni gelişmelere karşı yetersiz olduğunu ortaya koymuşlardır. Araştırma sonucunda ise öğrencilerin, bilgisayara erişimi, zararlı yazılımlar ve bunlardan korunma, parola, sosyal mühendislik, dosyalara erişme ve dosyaları paylaşma gibi

konularda temel seviyede ve herkesçe bilinen güvenlik tedbirlerinden sadece birini veya birkaçını kullandıklarını, diğer güvenlik önlemlerini ise almadıklarını tespit etmişlerdir.

Akgün ve Gökmen (2015) bilgisayar ve öğretim teknolojileri bölümünde öğrenim gören öğrenciler üzerinden yaptıkları araştırma da geleceğin eğitimcileri olan öğrencilerin bilişim güvenliği bilgilerinin seviyesini belirlemeye çalışmışlardır. Sonuçta bu öğrencilerin bilişim güvenliği bilgilerinin düşük seviyede olduğunu, cinsiyet ve öğrenim görülen üniversitenin bilişim güvenliğine etki ettiğini tespit etmişlerdir. Ayrıca bilişim güvenliğinin; bazı farklı değişkenlere göre farklılık göstermediğini ortaya koymuşlardır.

Rençber ve Mete (2016) çalışmalarında bilgi güvenliği farkındalığını etkileyen faktörleri ve bu faktörlerin bilgi güvenliği farkındalığına etki düzeylerini yüksekokul düzeyinde incelemişlerdir. Çalışmaları neticesinde bilgi güvenliği farkındalık düzeylerini etkileyen etkenleri tespit etmişlerdir. Bunların şifre yönetimi, mobil internet kullanımı, e-posta kullanımı, internet kullanımı ve sosyal ağ sitelerinin kullanımı olduğunu ortaya koymuşlardır.

Sağır ve ark. (2018) yılında yaptıkları çalışma ile meslek yüksekokulunda eğitim gören öğrencilerin eğitim gördükleri bölümler ile bilgi güvenliği farkındalıkları arasında anlamlı bir farklılaşma olmadığını ortaya koymuşlardır. Yine bu öğrencilerin bilgi güvenliği farkındalığı açısından daha önceden herhangi bir eğitim alıp almamalarının bilgi güvenliği farkındalığına anlamlı bir etki etmediğini tespit etmişlelerdir.

Çavuş Ezin ve Karaoğlan Yılmaz (2017), anne babaların bilgi güvenliği farkındalık seviyelerini incelemişlerdir. Çalışma sonucunda anne babaların belli bir seviyeye kadar bilgi güvenliği farkındalıklarının bulunduğunu ancak bilginin depolama yerleri ve depolama süreleri gibi konularda bilgi güvenliği farkındalık düzeylerinin beklenen seviyede olmadığı sonucuna varmışlardır. Yine aynı araştırma sonucunda anne babaların bilgi güvenliği açısından çocuklarına sadece uyarıda bulundukları, somut bir bilgi veremediklerini tespit etmişlerdir.

Erdoğmuş (2017), üniversitede eğitim gören öğrencilerin bilgi güvenliği farkındalıkları üzerine bir anket çalışması yapmıştır. Üniversite öğrencilerinin bilgi güvenliği farkındalık seviyelerinin beş alt boyutta değerlendirilebileceği ortaya koymuş ve bunların internet güvenliği, sosyal medya kullanımı, ağ güvenliği, şifre oluşturma ve sosyal medya tuzakları olduğunu belirtmiştir.

Abuhanoğlu ve Karadağ (2015), Gülhane Askeri Tıp Fakültesi Hastanesi personeli üzerinden yaptıkları bilgi güvenliği farkındalık seviyelerinin belirlenmesine yönelik yaptıkları çalışmada bir ölçek geliştirmişlerdir. Ölçeği bilgi güvenliği farkındalığı açısından, politika güvenliği, sistem güvenliği ve çalışan güvenliği olmak üzere üç alt bölüm oluşturmuşlardır. Sonuç olarak ise ilgi güvenliği farkındalık düzeylerinin yüksek olduğu, yaş ve unvan değişkenlerinin de bilgi güvenliği farkındalığı üzerinde etkili olduğunu belirlemişlerdir.

Çam, ve ark. (2019), Gümüşhane Üniversitesi'nde eğitim gören öğrenci, üniversite çalışanları ve üniversitede görev yapan akademisyenlerin İnternet kullanımları ve kişisel bilişim güvenliği davranışlarını inceleyerek yaptıkları araştırma sonucunda üniversite e üzeri eğitim kurumlarında bilgi güvenliği farkındalık seviyelerinin yükseltilmesine yönelik çalışmaların yapılması gerektiği sonucuna ulaşmışlardır.

Mai and Tick (2021) Macaristan'daki Obuda Üniversitesi ve Vietnam'daki Danang Üniversitesinde eğitim gören 313 öğrenciye yaptıkları anket çalışması ile siber güvenlik farkındalığı, bilgi ve davranış düzeylerini ölçmeye çalışmışlardır. Yaptıkları araştırma sonucunda katılımcıların siber güvenlik açısından bilgi eksiklerinin olduğu sonucuna varmışlardır. Ülkeler karşılaştırması yaptıklarında siber güvenlik açısından küçük farklılıklar olduğunu ortaya koymuşlardır.

Stanciu and Tinca (2016), Romanya Bükreş Ekonomik Araştırmalar Üniversitesi Muhasebe ve Yönetim Bilişim Sistemleri Fakültesi öğrencilerinin bilgi güvenliği tehditlerine karşı ne kadar eğitimli olduklarını, farkındalık düzeylerini ortaya koyma amaçlı olarak bir çalışma yapmışlardır. Araştırma sonucunda fakültede verilen derslerin iyileştirilmesi gerektiği sonucuna varmışlardır.

2. BÖLÜM

MATERYAL VE YÖNTEM

2.1. Araştırmanın yeri ve zamanı

Anket araştırması 5 Nisan 2022 ve 20 Nisan 2022 tarihleri arasında Hitit Üniversitesinde öğrenim gören ve ankete katılmayı gönüllü olarak kabul eden öğrenciler ile yapılmıştır.

2.2. Araştırmanın evreni

Araştırmanın evreni Hitit Üniversitesinde öğrenim gören 16905 öğrenci olarak belirlenmiştir. Evren sayısı Hitit Üniversitesi'nin resmi web sitesinden elde edilmiştir.

2.3. Araştırmanın örneklemi

Araştırma öncesi örneklem büyüklüğünü belirlemek için güç (power) analizi yapılmıştır. Güç analizi sonucunda anket araştırmasına minimum 376 gönüllü öğrencinin katılmasının yeterli olacağı belirlenmiştir. Çalışma öncesinde örneklem büyüklüğünü hesaplayabilmek amacıyla 0,05 anlamlılık düzeyinde (%95 güven aralığı ile) yapılan güç analizi sonucunda elde edilen minimum katılımcı sayısı olan 376 öğrenci sayısı aşılarak toplam 476 öğrenciye anket uygulatılarak anket araştırması tamamlanmıştır. Araştırma öncesinde örneklem büyüklüğü aşağıda gösterilen formül ve değerler kullanılarak hesaplanmıştır.

n: Örneklem büyüklüğü

N: Evren birim sayısı = 16905

P: Evrendeki X'in gözlenme oranı = 0.5

Q (1-P): X'in gözlenmeme oranı = 0.5

Zα : α=0.05 için kritik tablo değeri = 1.96

d= Örneklem hatası = 0.05

$$n = \frac{N * Z_{\alpha}^{2} * P * Q}{d^{2} * (N-1) + Z_{\alpha}^{2} * P * Q}$$

$$n = \frac{16905 * 1.96^{2} * 0.5 * 0.5}{(0.05)^{2} * (16905-1) + 1.96^{2} * 0.5 * 0.5} = 376$$

Araştırma öncesi yapılan örneklem büyüklüğü belirleme analizi sonucuda elde edilen bulgulara göre Hitit Üniversitesinde öğrenim gören öğrencilerden anket araştırmasına katılmayı kabul eden 476 gönüllü öğrenci araştırmanın örneklemini oluşturmuştur.

Öğrencilerin anket araştırmasına dâhil edilme kriterleri:

Anket araştırmasına Hitit Üniversitesinde öğrenim gören gönüllü 18 yaş ve üzeri tüm öğrenciler alınmıştır.

Öğrencilerin anket araştırmasından dışlanma kriterleri:

Anket araştırmasında Hitit Üniversitesi öğrencisi olmayan, gönüllü olarak çalışmaya katılmak istemeyen ve 18 yaş altında bulunan öğrenciler araştırma dışı bırakılmıştır.

2.4. Veri toplama araçları

Veri toplama aracı olarak "kişisel bilgi formu" ve "Üniversite Öğrencileri için Bilgi Güvenliği Farkındalık Ölçeği"nin kullanılmasına karar verilmiştir (Güldüren, 2021). Araştırmaya başlamadan önce araştırmada kullanılan anket formu uzman görüşlerinden faydalanılarak oluşturulmuştur. Araştırma ile ilgili ankete katılan öğrencilere bilgi verilerek gönüllü onamları alındıktan sonra "Kişisel bilgi formu" ve "Üniversite Öğrencileri için Bilgi Güvenliği Farkındalık Ölçeği" aracılığıyla veriler elde edilmiştir. Tez çalışmamızda anket araştırması online olarak Google anket ile yapılmıştır.

Üniversite Öğrencileri İçin Bilgi Güvenliği Farkındalığına ilişkin Anket ve Ölçekler

Öğrencilere uygulanan anket/ölçek iki bölümden oluşur. Birinci bölümde anket uygulaması ile öğrencilerin demografik özelliklerine yönelik bilgilere yer verilmiştir. "Kişisel bilgi formu" cinsiyet, yaş, eğitim durumu, fakülte/yüksek okul, sınıf, ailenin gelir düzeyi, aile ile yaşanılan yer/ikametgah, günlük internet kullanım sıklığı, günlük sosyal medya kullanım sıklığı, sosyal medya kullanım süresi (yıl ve sosyal medya hesaplarının herkese açık veya gizli olma durumu olmak üzere toplam 11 sosyo-demografik tanımlayıcı sorudan oluşmuştur. İkinci bölümde ise ölçek uygulaması ile öğrencilerin bilgi güvenliği farkındalığı düzeylerinin değerlendirilmesi amacıyla 34 maddelik ölçek kullanılmıştır. Can Güldüren tarafından 2021 yılında üniversite öğrencileri üzerinde geliştirilen ölçek 34 madde ve 4 alt boyuttan ('mahremiyet ve güvenli gezinme (MGG)', 'saldırı ve tehditler (ST)', 'genel güvenlik (GG)' ve 'siber güvenlik (SG)') oluşmaktadır (15). Ölçek 5 li likert olarak belirlenmiş ve yanıtlar "Hiç Katılmıyorum", "Katılmıyorum", "Kararsızım", "Katılıyorum" ve "Tamamen Katılıyorum" olarak sunulmuştur. Ölçekte ters kodlanmış madde bulunmamaktadır. Ölçek toplam puanı ve alt faktörlere ilişkin puanlar arttıkça, katılımcıların bilgi güvenliği farkındalığı artmaktadır.

2.5. Araştırma hipotezleri

1. Öğrencilerin dijital veri güvenliği farkındalık düzeyleri nedir?

2. Öğrencilerin cinsiyetine göre dijital veri güvenliği farkındalık düzeyleri arasında istatistiksel olarak anlamlı bir farklılık var mı?

3. Öğrencilerin yaşları ile dijital veri güvenliği farkındalık düzeyleri arasında istatistiksel olarak anlamlı bir ilişki var mı?

4. Öğrencilerin eğitim düzeylerine göre dijital veri güvenliği farkındalık düzeyleri arasında istatistiksel olarak anlamlı bir farklılık var mı?

5. Öğrencilerin Fakültelerine/Yüksek okullarına göre dijital veri güvenliği farkındalık düzeyleri arasında istatistiksel olarak anlamlı bir farklılık var mı?

6. Öğrencilerin sınıflarına göre dijital veri güvenliği farkındalık düzeyleri arasında istatistiksel olarak anlamlı bir farklılık var mı?

7. Öğrencilerin ailelerinin gelir düzeylerine göre dijital veri güvenliği farkındalık düzeyleri arasında istatistiksel olarak anlamlı bir farklılık var mı?

8. Öğrencilerin aileleri ile birlikte yaşadıkları yerlere göre dijital veri güvenliği farkındalık düzeyleri arasında istatistiksel olarak anlamlı bir farklılık var mı?

9. Öğrencilerin günlük internet kullanım süresine göre dijital veri güvenliği farkındalık düzeyleri arasında istatistiksel olarak anlamlı bir farklılık var mı?

10. Öğrencilerin sosyal medya kullanım süresine göre dijital veri güvenliği farkındalık düzeyleri arasında istatistiksel olarak anlamlı bir farklılık var mı?

11. Öğrencilerin sosyal medya kullanım biçimine göre dijital veri güvenliği farkındalık düzeyleri arasında istatistiksel olarak anlamlı bir farklılık var mı?

2.6. İstatistiksel analizler

Tez çalışmamızda kurulan hipotezler doğrultusunda hipotezleri test etmek için anket/ölçek aracılığıyla elde edilen verilerin istatistiksel analizleri SPSS (Versiyon 22.0, SPSS Inc., Chicago, IL, USA, Lisans: Hitit Üniversitesi) paket programı ile yapılmıştır. Anket ve ölçek ile elde edilecek değişkenler sayısal olduğu durumda tanımlayıcı istatistikleri veri dağılımına uygun olarak ortalama ± standart sapma ya da ortanca (en küçük-en büyük) olarak raporlanmıştır. Değişkenler kategorik olduğu durumda ise tanımlayıcı istatistikleri sayı ve yüzde (%) olarak sunulmuştur. Verilerin normal dağılım sınaması Kolmogorov–Smirnov testi ile yapılmıştır. Sosyo-demografik özelliklere göre sayısal ölçümlerin karşılaştırılması veri dağılımına uygun olarak bağımsız iki grup karşılaştırması için Mann Whitney U testi kullanılmıştır. İkiden fazla

grup karşılaştırmaları ise veri dağılımına uygun olarak ANOVA veya Kruskal Wallis testi ile gerçekleştirilmiştir. Farklılığın hangi gruptan kaynaklandığını belirlemek amacıyla Varyans analizi sonrasında Tukey veya Bonferroni düzeltmeli post-hoc ikişerli karşılaştırma testleri kullanılmıştır. Sosyo-demografik özellikler ile ölçek puanı arasındaki ilişkiler veri dağılımına uygun olarak Spearman korelasyon katsayısı kullanılarak hesaplanmıştır. İstatistiksel analizlerde anlamlılık düzeyi $p<0.05$ olarak kabul edilmiştir.

2.7. Etik kurul onayı

Anket araştırmasına başlayabilmek için öncelikle Hitit Üniversitesi Girişimsel olmayan Araştırmalar Etik Kurulu'ndan 30.03.2022 tarihli 2022-07 sayılı kararıyla etik kurul onayı alınmıştır (Ek 3). Araştırmaya başlamadan önce araştırmaya katılacak gönüllü öğrencilere araştırmanın amacı ve anket katılımı için yapmaları gerekenler açıklanmıştır (Aydınlatılmış Onam ilkesi). Katılımcılara araştırmaya katılma ya da katılmama konusunda özgür oldukları bildirilmiştir (Özerkliğe Saygı ilkesi) ve bireysel bilgilerinin üçüncü kişilerle paylaşılmayacağı konusunda güvence verilmiştir (Gizlilik ve Gizliliğin Korunması ilkesi).

3. BÖLÜM

ARAŞTIRMA SONUÇLARI VE TARTIŞMA

3.1. Anket sonuçlarına ilişkin tanımlayıcı istatistikler

Anket araştırmasına katılan toplam öğrenci sayısı 476'dır. Araştırmaya katılan öğrencilerin %58 (n=276)'i kadın ve %42 (n=200)'si erkektir. Katılımcıların yaş ortalaması 21,4±3,053 (18-56) olarak hesaplanmıştır. Katılımcılarının sosyo-demografik özellikleri Tablo 3.1'de sunulmuştur.

Tablo 3.1. Anket katılımcılarının sosyo-demografik özelliklerine ilişkin tanımlayıcı istatistikler

		n	%
Cinsiyetiniz	Erkek	200	42
	Kadın	276	58
Eğitim durumunuz	Ön lisans	60	12,6
	Lisans	403	84,7
	Yüksek lisans	12	2,5
	Doktora	1	0,2
Fakülteniz/Yüksek okulunuz	Tıp Fakültesi	132	27,7
	Fen Edebiyat Fakültesi	19	4
	İktisadi ve İdari Bilimler Fakültesi	1	0,2
	Mühendislik Fakültesi	36	7,6
	Sağlık Bilimleri Fakültesi	105	22,1
	Spor Bilimleri Fakültesi	117	24,6
	Güzel Sanatlar, Tasarım Ve Mimarlık Fakültesi	5	1,1
	İlahiyat Fakültesi	8	1,7
	Meslek Yüksekokulu	49	10,2
	Lisansüstü Eğitim Enstitüsü	4	0,8
Sınıfınız	1	186	39,1
	2	139	29,2
	3	92	19,3
	4	55	11,6
	5	1	0,2
	6	3	0,6

Ailenin Gelir Düzeyiniz	0 – 5000 TL	216	45,4
	5001 – 10000 TL	170	35,7
	10001– 15000 TL	44	9,2
	15001TL – üzeri	46	9,7
Aileniz ile yaşadığınız yer / İkametgah	Köy / Kasaba	57	12
	İlçe Merkezi	135	28,3
	İl Merkezi	284	59,7
Toplam		476	100

Anket araştırmasına katılan üniversite öğrencilerinin günlük internet kullanım sıklığı, günlük sosyal medya kullanım sıklığı ve kaç yıldır sosyal medya kullandığına ilişkin tanımlayıcı istatistikleri Tablo 3.2'de verilmiştir.

Tablo 3.2 . Anket katılımcılarının günlük internet kullanım sıklığı, günlük sosyal medya kullanım sıklığı ve kaç yıldır sosyal medya kullandığına ilişkin tanımlayıcı istatistikler

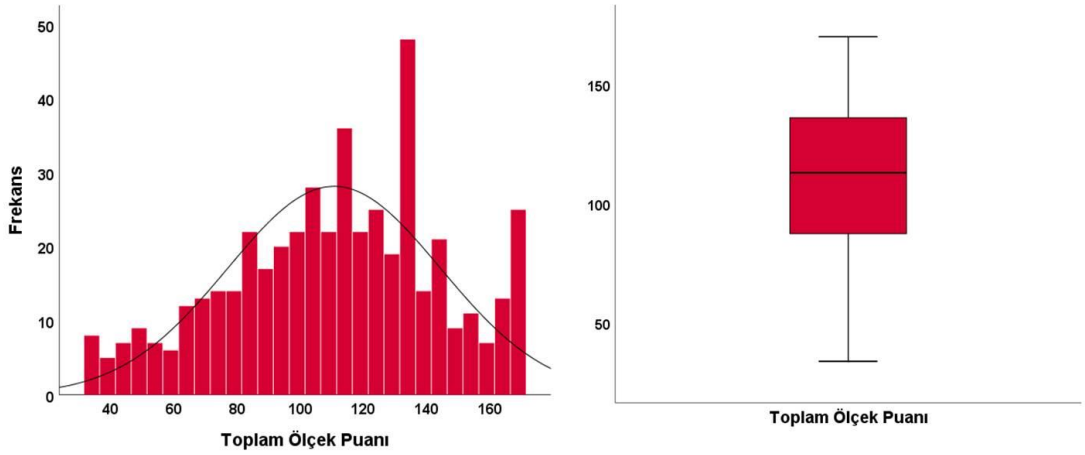
		n	**%**
Günlük internet kullanım sıklığınız (Eğitim, Haber, Youtube, Sosyal medya, Facebook, Instagram, Twitter vb.)	1 saatten az	14	2,9
	1-3 saat	128	26,9
	3-5 saat	217	45,6
	5-10 saat	101	21,2
	10 saatten fazla	16	3,4
Günlük sosyal medya kullanım sıklığınız (Facebook, Instagram, Twitter vb)	1 saatten az	69	14,5
	1-3 saat	220	46,2
	3-5 saat	145	30,5
	5-10 saat	34	7,1
	10 saatten fazla	8	1,7
Kaç yıldır sosyal medya (Facebook, Instagram, Twitter vb.) kullanıyorsunuz?	1 yıldan az	26	5,5
	1-3 yıl	49	10,3
	3-5 yıl	121	25,4
	5-10 yıl	203	42,6
	10 yıldan fazla	77	16,2
Sosyal medya hesaplarınızı herkese açık mı yoksa gizli mi kullanıyorsunuz	Herkese açık	59	12,4
	Gizli	417	87,6
Toplam		476	100

Toplam Ölçek puanları

Üniversite öğrencileri için bilgi güvenliği farkındalık ölçek puanlarının normal dağılımına ilişkin istatistiksel sonuçları Tablo 3.3'te verilmiştir. Ölçek puanlarına ilişkin normal dağılım analizi kullanılarak üniversite öğrencilerinin bilgi güvenliği farkındalık ölçek puanlarının normal dağılıma uygun olmadığı sonucuna ulaşılmıştır (*P*=0,010; Tablo 3.3).

Tablo 3.3 Üniversite Öğrencileri için Bilgi Güvenliği Farkındalık Ölçek puanının normal dağılım sınamasında kullanılan Kolmogorov-Smirnov test sonuçları (n=476)

	Kolmogorov-Smirnov		
	Test istatistik değeri	**Serbestlik derecesi**	***P* değeri**
Üniversite Öğrencileri için Bilgi Güvenliği Farkındalık Ölçek Puanı	0,048	476	0,010



Şekil 3.1 Üniversite Öğrencileri için Bilgi Güvenliği Farkındalık Ölçek puanları arasındaki normal dağılıma ilişkin histogram ve kutu grafiği

Üniversite öğrencileri için bilgi güvenliği farkındalık ölçek puanlarına ilişkin tanımlayıcı istatistikler Tablo 3.4' te raporlanmıştır. Üniversite öğrencilerinin bilgi güvenliği farkındalığı toplam ölçek puan ortalamaları 110,6±33,71 olarak hesaplanmıştır. Ölçek 5 li likert olarak belirlenmiş olup yanıtlar "Hiç Katılmıyorum", "Katılmıyorum", "Kararsızım", "Katılıyorum" ve "Tamamen Katılıyorum" olarak verilmiştir. Ölçekte ters kodlanmış madde bulunmamaktadır. Ölçek toplam puanı ve alt faktörlere ilişkin puanlar arttıkça, katılımcıların bilgi güvenliği farkındalığı artmaktadır.

Tablo 3.4. Üniversite Öğrencileri için Bilgi Güvenliği Farkındalık Ölçek puanlarının tanımlayıcı istatistikleri

	Ortalama±SS	Ortanca (EK-EB)
Üniversite Öğrencileri için Bilgi Güvenliği Farkındalık Ölçek Puanı	110,6±33,71	113 (34-170)

EK: En küçük

EB: En büyük

3.2. Sosyo-demografik Özelliklere Göre Üniversite Öğrencileri İçin Bilgi Güvenliği Farkındalık Ölçek Puanları Arasındaki İlişkiler

Sosyo-demografik özelliklere göre üniversite öğrencileri için bilgi güvenliği farkındalık ölçek puanları arasındaki ilişkiler Tablo 3.5'te sunulmuştur. Anket katılımcılarının günlük internet kullanım sıklığına, günlük sosyal medya kullanım sıklığına ve kaç yıldır sosyal medya kullandığına göre üniversite öğrencileri için bilgi güvenliği farkındalık ölçek puanları arasındaki ilişkiler Tablo 3.6'dasunulmuştur. Cinsiyet grupları arasında bilgi güvenliği farkındalık ölçek puanlarının istatistiksel olarak anlamlı farklı olduğu belirlenmiştir (P<0,001). Eğitim düzeyleri arasında bilgi güvenliği farkındalık ölçek puanları istatistiksel olarak anlamlı farklı bulunamamıştır (P=0,572). Katılımcıların bulundukları Fakülte/Yüksek okullar arasında bilgi güvenliği farkındalık ölçek puanları istatistiksel olarak anlamlı farklı bulunmuştur (P=0.001). Post-hoc çoklu karşılaştırma test sonucuna göre Mühendislik fakültesinde öğrenim gören öğrencilerin bilgi güvenliği farkındalık düzeylerinin Tıp fakültesinde öğrenim gören öğrencilerin bilgi güvenliği farkındalık düzeylerinden anlamlı daha yüksek olduğu belirlenmiştir. Katılımcıların ailelerinin gelir düzeyleri arasında bilgi güvenliği farkındalık ölçek puanları istatistiksel olarak anlamlı farklı bulunamamıştır (P=0,708). Katılımcıların ailelerinin yaşadıkları yerler arasında bilgi güvenliği farkındalık ölçek puanları istatistiksel olarak anlamlı farklı bulunamamıştır (P=0,307). Katılımcıların günlük internet kullanım sıklıkları arasında bilgi güvenliği farkındalık ölçek puanları istatistiksel olarak anlamlı farklı bulunmuştur (P=0,032). Post-hoc çoklu karşılaştırma test sonucuna göre günlük 10 saatten fazla internet kullanan öğrencilerin bilgi güvenliği farkındalık düzeylerinin günlük 5-10 saat internet kullanan öğrencilerin bilgi güvenliği farkındalık düzeylerinden anlamlı daha yüksek olduğu belirlenmiştir. Katılımcıların günlük sosyal medya kullanım sıklıkları arasında bilgi güvenliği farkındalık ölçek puanları arasında istatistiksel olarak anlamlı farklı bulunmuştur (P=0,028). Post-hoc çoklu karşılaştırma test sonucuna göre günlük 10 saatten fazla sosyal medya kullanan öğrencilerin bilgi güvenliği farkındalık düzeylerinin günlük 1-3 saat , 3-5 saat ve 5-10 saat sosyal medya kullanan öğrencilerin bilgi güvenliği farkındalık düzeylerinden anlamlı daha yüksek olduğu belirlenmiştir. Katılımcıların sosyal medya kullanım süreleri (yıl) arasında ölçek puanları istatistiksel olarak anlamlı farklı bulunamamıştır (P=0,439). Katılımcıların sosyal medya hesaplarını herkese açık ve gizli kullanma durumları arasında bilgi

güvenliği farkındalık ölçek puanları istatistiksel olarak anlamlı farklı bulunamamıştır (*P*=0,805).

Tablo 3.5. Sosyo-demografik özelliklere göre üniversite öğrencileri için bilgi güvenliği farkındalık ölçek puanları arasındaki ilişkiler

			Bilgi Güvenliği		
		n	**Ortalama±SS Ortanca (EK-EB)**	***P* değeri**	**Post-hoc *P* değeri**
Cinsiyetiniz	Erkek	200	125 (34-170) (117,8±34,9)	**<0,001[a]**	-
	Kadın	276	106 (34-170) (105,5±31,89)		
Eğitim durumunuz	Ön lisans	60	116 (34-166) (112,1±33,97)	0,572[c]	-
	Lisans	403	112 (34-170) (110,2±33,66)		
	Yüksek lisans	13	115 (59-170) (119,5±35,18)		
Fakülteniz/Yüksek okulunuz	Tıp Fakültesi (1)	132	102,5 (38-170) (104,1±29,42)	**0.001[c]**	**1-2:0.002**
	Mühendislik Fakültesi (2)	36	130,5 (34-170) (125,1±30,99)		
	Sağlık Bilimleri Fakültesi (3)	105	113 (34-170) (109,8±32,63)		
	Spor Bilimleri Fakültesi (4)	117	122 (34-170) (111,9±37,80)		
	Meslek Yüksekokulu (5)	49	119 (34-166) (115,5±34,18)		
	Diğer (6)	37	117 (37-170) (112,6±35,50)		
Ailenin Gelir Düzeyiniz	0 – 5000 TL	216	108,89±34,61	0,708[b]	-
	5001 – 10000 TL	170	111,6±33,08		
	10001– 15000 TL	44	114,5±32,75		
	15001TL - üzeri	46	111,8±33,18		
Aileniz ile yaşadığınız yer / İkametgah	Köy / Kasaba	57	104,2±36,16	0,307[b]	
	İlçe Merkezi	135	111,1±34,72		
	İl Merkezi	284	111,7±32,68		

[a]Mann-Whitney U testi

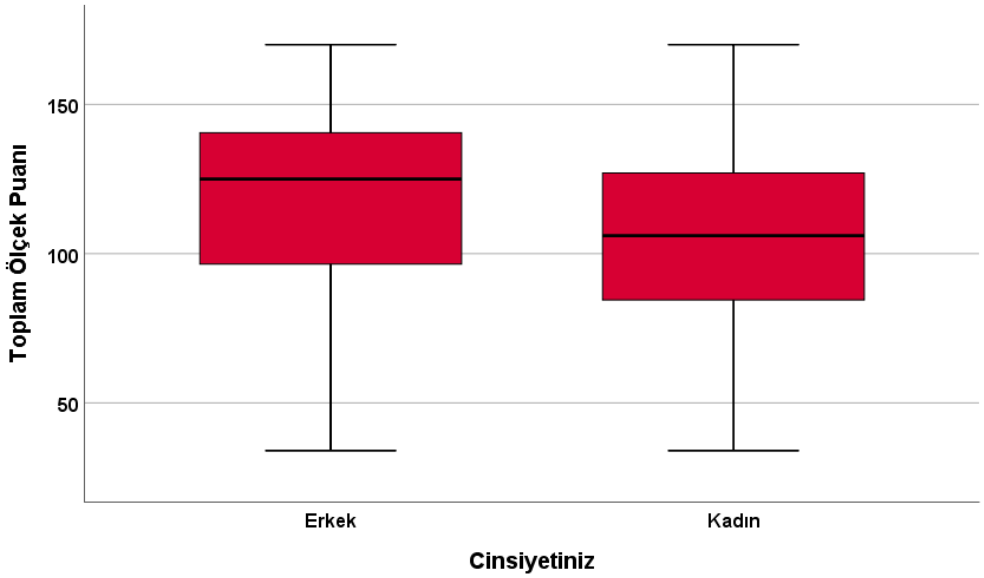
[b]One-Way ANOVA testi

[c]Kruskal Wallis testi

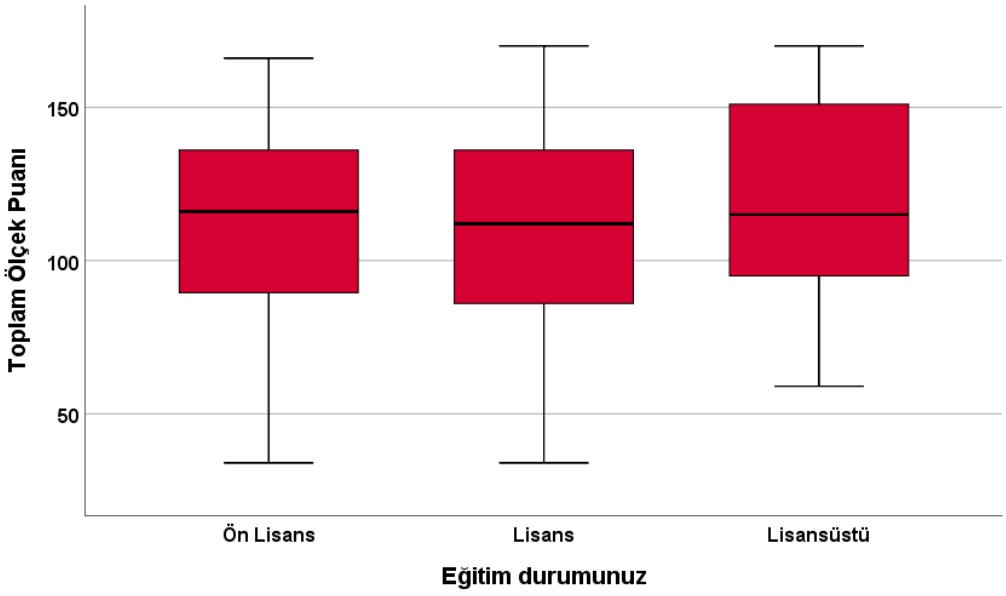
EK:En küçük

EB:En büyük

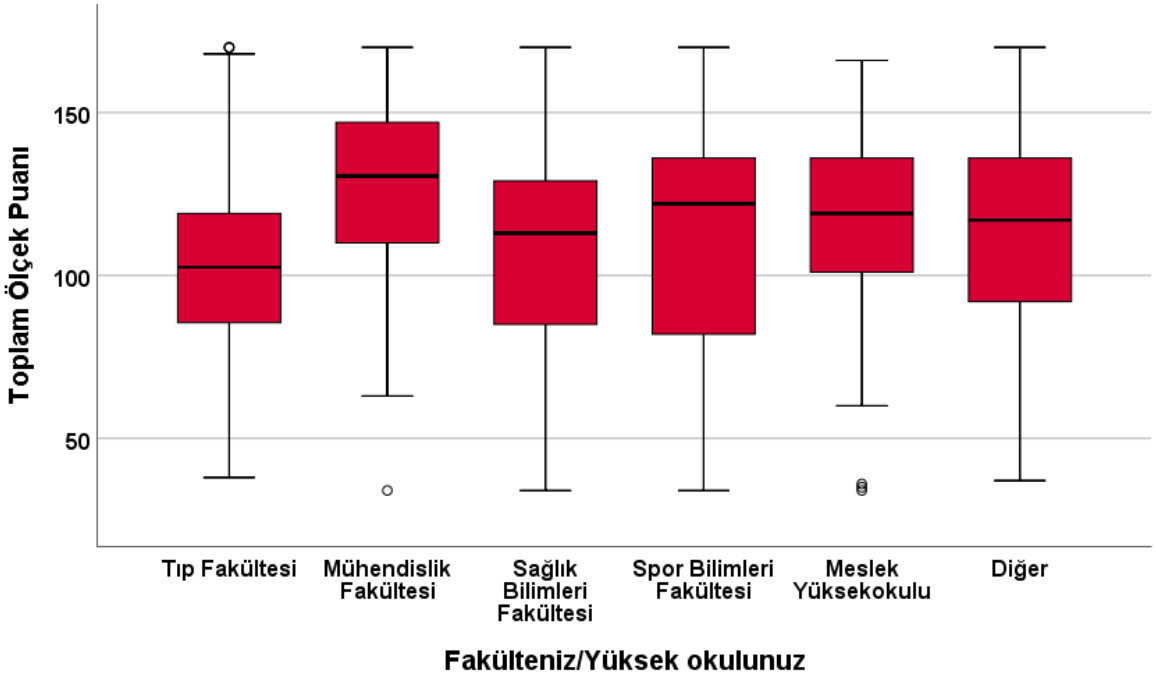
Katılımcıların cinsiyetine, eğitim durumuna, fakülte/yüksekokuluna, ailelerinin gelir düzeyine, aileleri ile birlikte yaşadıkları yere göre üniversite öğrencilerinin bilgi güvenliği farkındalık ölçek puanlarının değişimlerine ilişkin kutu grafikleri şekil 2, şekil 3, şekil 4, şekil 5 ve şekil 6'da verilmiştir.



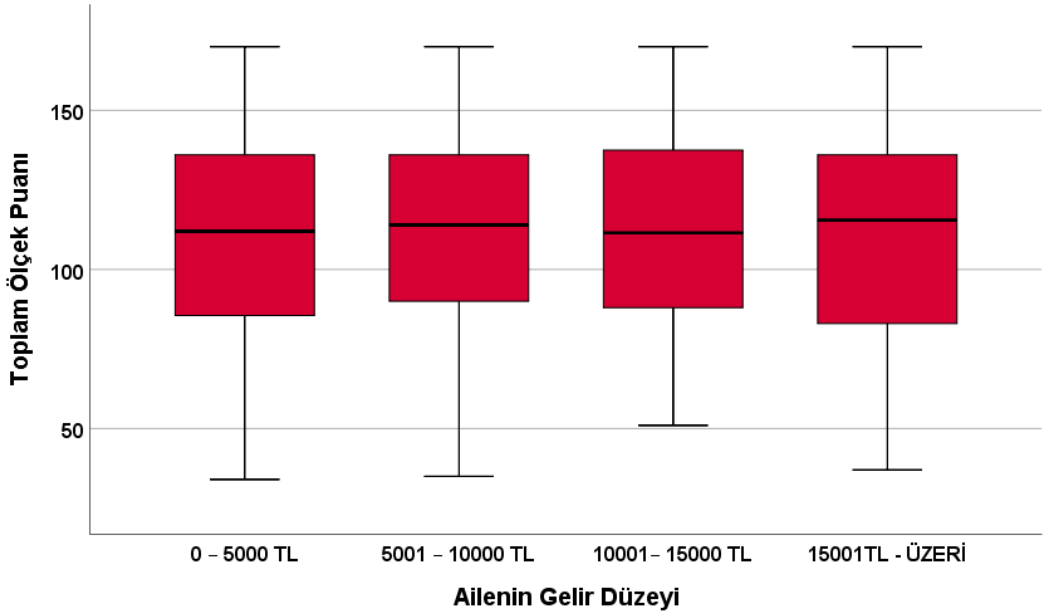
Şekil 3.2. Cinsiyet grupları arasında üniversite öğrencilerinin bilgi güvenliği farkındalık ölçek puanlarının değişimlerine ilişkin kutu grafiği (box-plot)



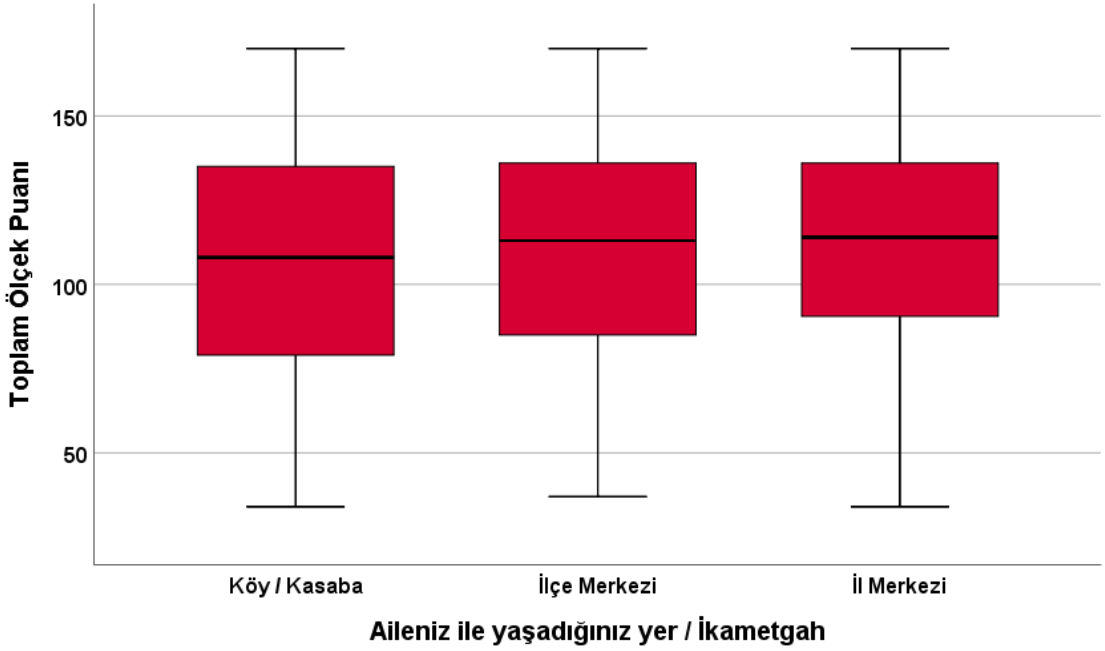
Şekil 3.3. Eğitim düzeyleri arasında üniversite öğrencilerinin bilgi güvenliği farkındalık ölçek puanlarının değişimlerine ilişkin kutu grafiği (box-plot)



Şekil 3.4. Katılımcıların bulunduğu Fakülte/Yüksek okullar arasında üniversite öğrencilerinin bilgi güvenliği farkındalık ölçek puanlarının değişimlerine ilişkin kutu grafiği (box-plot)



Şekil 3.5. Katılımcıların ailelerinin gelir düzeyleri arasında üniversite öğrencilerinin bilgi güvenliği farkındalık ölçek puanlarının değişimlerine ilişkin kutu grafiği (box-plot)



Şekil 3.6. Katılımcıların aileleri ile birlikte yaşadıkları yerler arasında üniversite öğrencilerinin bilgi güvenliği farkındalık ölçek puanlarının değişimlerine ilişkin kutu grafiği (box-plot)

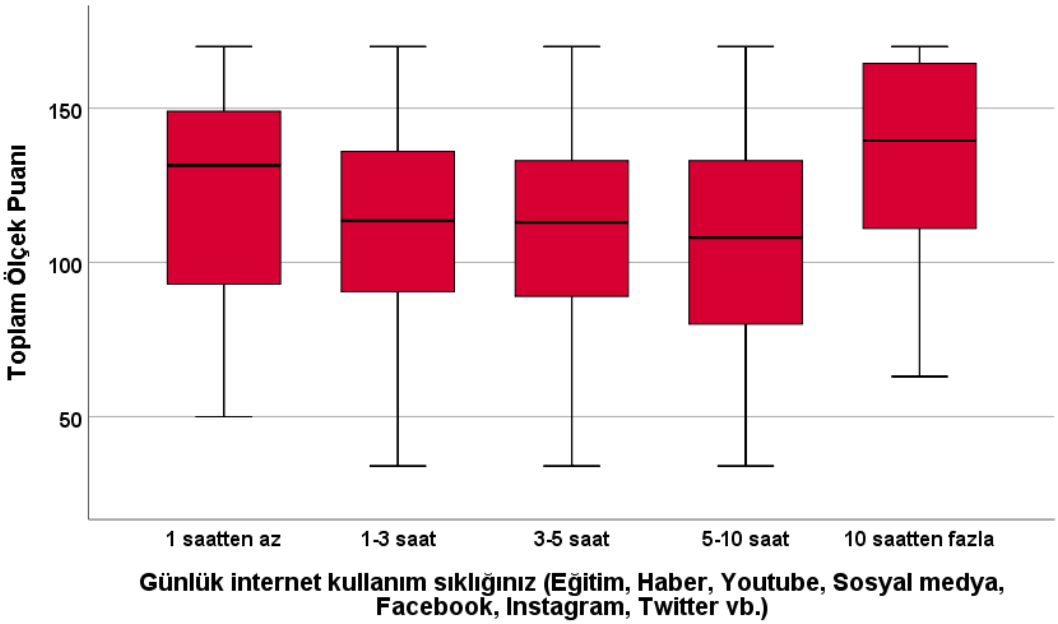
Tablo 3.6. Anket katılımcılarının günlük internet kullanım sıklığına, günlük sosyal medya kullanım sıklığına ve kaç yıldır sosyal medya kullandığına göre üniversite öğrencileri için bilgi güvenliği farkındalık ölçek puanları arasındaki ilişkiler

		n	Bilgi Güvenliği Ortalama±SS Ortanca (EK-EB)	*P* değeri	*Post-hoc P değeri*
Günlük internet kullanım sıklığınız (Eğitim, Haber, Youtube, Sosyal medya, Facebook, Instagram, Twitter vb.)	1 saatten az (1)	14	131,5 (50-170) (121,1±38,19)	**0,032[c]**	**4-5: 0,031**
	1-3 saat (2)	128	113,5 (34-170) (110,9±31,67)		
	3-5 saat (3)	217	113 (34-170) (110,3±32,93)		
	5-10 saat (4)	101	108 (34-170) (106,1±36,05)		
	10 saatten fazla (5)	16	139,5 (63-170) (133,1±34,16)		
Günlük sosyal medya kullanım sıklığınız (Facebook, Instagram, Twitter vb)	1 saatten az (1)	69	117 (50-170) (115,4±29,4)	**0,028[c]**	**2-5:0,021 3-5:0,036 4-5:0,033**
	1-3 saat (2)	220	111 (34-170) (108,9±32,29)		
	3-5 saat (3)	145	114 (34-170) (109,9±34,9)		
	5-10 saat (4)	34	104 (34-170) (107,4±42,46)		
	10 saatten fazla (5)	8	152,5 (103-170) (146,6±25,01)		
Kaç yıldır sosyal medya (Facebook, Instagram, Twitter vb.) kullanıyorsunuz?	1 yıldan az	26	114 (49-170) (115,1±33,31)	0,439[c]	-
	1-3 yıl	49	104 (36-170) (105,7±34,91)		
	3-5 yıl	121	111 (34-170) (107,1±32,6)		
	5-10 yıl	203	115 (34-170) (111,9±32,92)		
	10 yıldan fazla	77	120 (34-170) (114,5±36,68)		
Sosyal medya hesaplarınızı herkese açık mı yoksa gizli mi kullanıyorsunuz	Herkese açık	59	117 (34-170) (111,1±37,48)	0,805[a]	-
	Gizli	417	113 (34-170) 110,6±33,19		

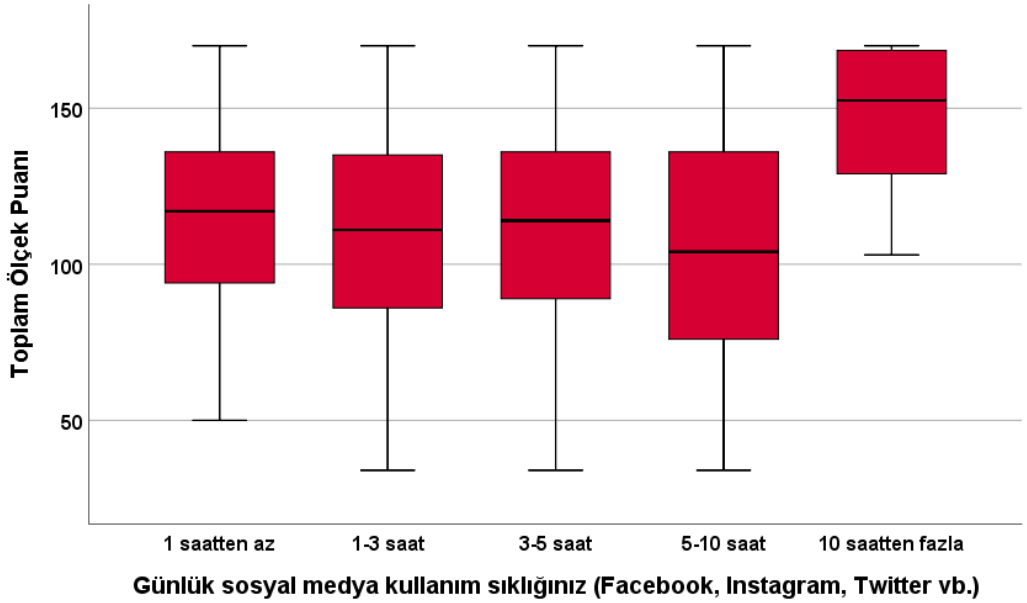
[a]Mann-Whitney U testi

[c]Kruskal Wallis testi

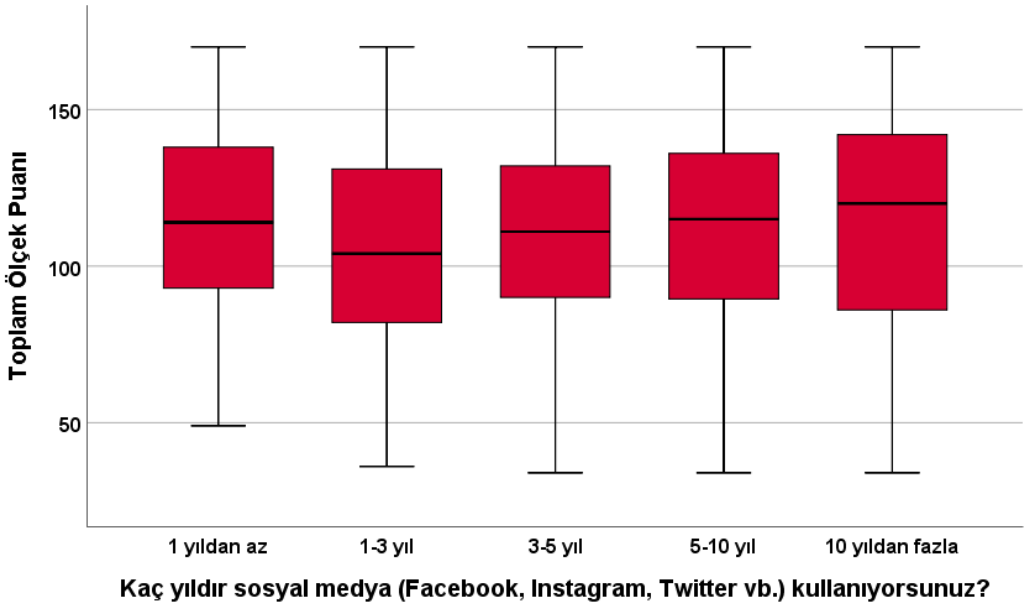
Katılımcıların Günlük internet kullanım sıklığına, Günlük sosyal medya kullanım sıklığına, Sosyal medya kullanım sürelerine (yıl) ve sosyal medya hesaplarını herkese açık ve gizli kullanma durumları göre üniversite öğrencilerinin bilgi güvenliği farkındalık ölçek puanlarının değişimlerine ilişkin kutu grafikleri şekil 7, şekil 8, şekil 9 ve şekil 10' da verilmiştir.



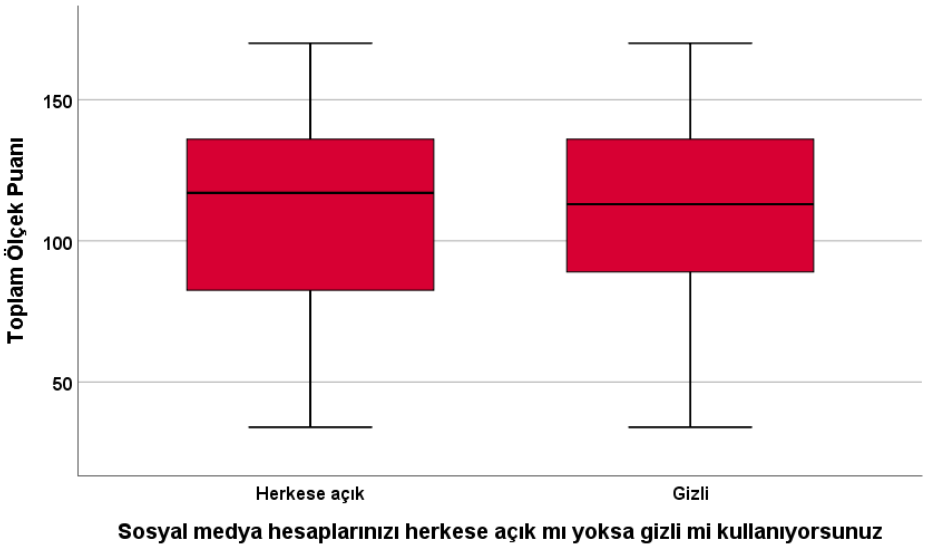
Şekil 3.7. Günlük internet kullanım sıklığı arasında üniversite öğrencilerinin bilgi güvenliği farkındalık ölçek puanlarının değişimlerine ilişkin kutu grafiği (box-plot)



Şekil 3.8. Günlük sosyal medya kullanım sıklığı arasında üniversite öğrencilerinin bilgi güvenliği farkındalık ölçek puanlarının değişimlerine ilişkin kutu grafiği (box-plot)



Şekil 3.9. Sosyal medya kullanım süreleri (yıl) arasında üniversite öğrencilerinin bilgi güvenliği farkındalık ölçek puanlarının değişimlerine ilişkin kutu grafiği (box-plot)



Şekil 3.10. Sosyal medya hesaplarını herkese açık ve gizli kullanma durumları arasında üniversite öğrencilerinin bilgi güvenliği farkındalık ölçek puanlarının değişimlerine ilişkin kutu grafiği (box-plot)

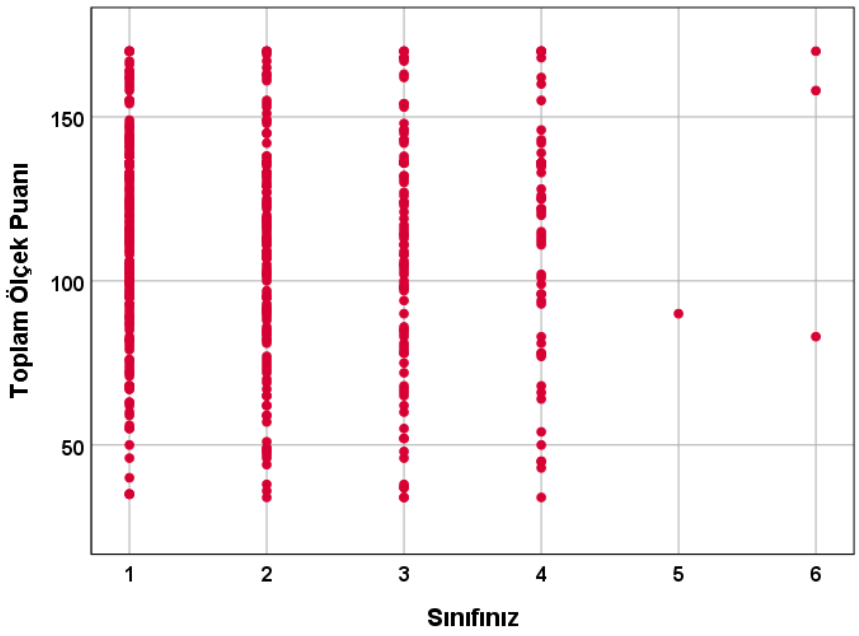
Katılımcıların bulundukları sınıfları ve yaşları ile üniversite öğrencileri için bilgi güvenliği farkındalık ölçek puanları arasındaki ilişki Tablo 3.7'de sunulmuştur. Katılımcıların bulundukları sınıfları ve yaşları ile bilgi güvenliği farkındalık ölçek puanları arasında istatistiksel olarak anlamlı bir ilişki bulunamamıştır (*P*=0,832, *P*=0,495).

Tablo 3.7. Katılımcıların bulundukları sınıfları ve yaşları ile üniversite öğrencileri için bilgi güvenliği farkındalık ölçek puanları arasındaki ilişki

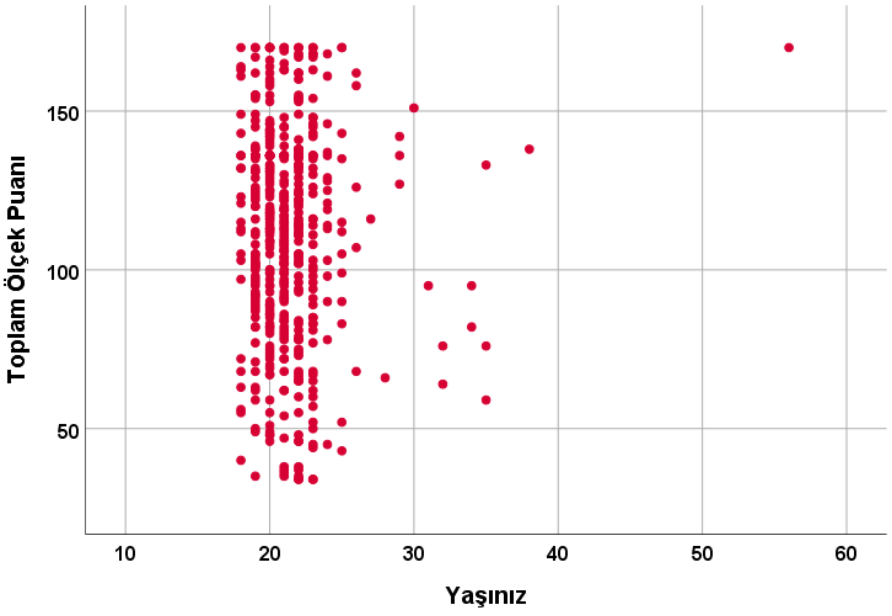
		Bilgi güvenliği farkındalık ölçek puanı
Sınıf	r	-0,010
	p	0,832
	N	476
Yaş	r	-0,031
	p	0,495
	N	476

Spearman korelasyon katsayısı

Katılımcıların bulundukları sınıfları ve yaşları ile bilgi güvenliği farkındalık ölçek puanları arasındaki ilişkiye ilişkin saçılım grafikleri şekil 11 ve şekil 12'de verilmiştir.



Şekil 3.11. Katılımcıların bulundukları sınıfları ile bilgi güvenliği farkındalık ölçek puanları arasındaki ilişkiye ilişkin saçılım grafiği



Şekil 3.12. Yaş ile bilgi güvenliği farkındalık ölçek puanları arasındaki ilişkiye ilişkin saçılım grafiği

3.3. Tartışma

Tez çalışmamızda Hitit Üniversitesinde eğitim gören 476 öğrenciye ölçek araştırması gerçekleştirilmiştir. Katılanların %58'i kadın, %42'si erkektir. Araştırmaya katılan öğrencilerin %84,7'sinin lisans eğitimi gören öğrenciler olduğu, katılımın %39,1 ile birinci sınıf öğrencilerince gerçekleştirildiği tespit edilmiştir. Ayrıca katılımcıların gelir durumları dikkate alındığında 0-5000 TL arası gelir durumundaki katılımcıların %45,4 ile en fazla katılımı sağladığı görülmüştür. Katılımcıların %59,7'si il merkezinde yaşadıklarını beyan etmişlerdir.

Yapılan ölçek araştırmasının sonuçlarına göre katılımcıların %42,6'sı 5 ila 10 yıl arasında sosyal medya kullandığı tespit edilirken, günlük internet kullanım sıklığında ölçeğe katılanların %45,6'sı 3-5 saat, %26,9'u ise 1-3 saat internet kullandığı, ayrıca ölçeğe katılanların %46,2'sinin 1-3 saat aralığında günlük sosyal medya kullandığı ölçek sonucuna göre belirlenmiştir. Veriler üzerinden değerlendirme yapıldığında ölçek çalışmasında yer alan katılımcıların internet kullanım sürelerinin çoğunluğunun sosyal medya kullanımı olduğu görülmektedir.

"Sosyal medya hesaplarınızı herkese açık mı yoksa gizli mi kullanıyorsunuz" sorusuna katılımcıların %87,6'sının gizli ve %12,4'ünün ise herkese açık cevabını verdiği görülmektedir.

Sosyo-demografik özelliklere göre üniversite öğrencileri için bilgi güvenliği farkındılık ölçek puanları kontrol edildiğinde katılımcılarının günlük internet kullanım sıklığına, günlük sosyal medya kullanım sıklığına ve kaç yıldır sosyal medya kullandığına göre üniversite öğrencileri için bilgi güvenliği farkındalık ölçek puanları arasındaki ilişkiler şu şekilde ortaya çıkmıştır.

Cinsiyet grupları arasındaki bilgi güvenliği farkındalık ölçek puanlarında erkeklerin ortalama 125 (EK:34- EB:170) olduğu kadınlarda ise bu oranın 106 (EK:34- EB:170) olduğu dikkate alındığında cinsiyet grupları arasında bilgi güvenliği farkındalık ölçek puanlarının istatistiksel olarak anlamlı bir fark olduğu belirlenmiştir (P<0,001). Erkeklerin bilgi güvenliği farkındalıklarının daha yüksek olduğu dikkat çekmektedir.

Eğitim durumları arasındaki bilgi güvenliği farkındalık ölçek puanları ön lisans 116 (EK:34- EB:170), lisans 112 (EK:34- EB:170) ve yüksek lisans 115 (EK:34- EB:170) olduğu dikkate alındığında eğitim düzeyleri arasında bilgi güvenliği farkındalık ölçek puanları istatistiksel olarak anlamlı bir fark bulunamamıştır (P=0,572).

Katılımcıların eğitim gördükleri Fakülte/Yüksek okullar arasında bilgi güvenliği farkındalık ölçek puanları dikkate alındığında ise istatistiksel olarak anlamlı bir fark olduğu tespit edilmiştir (P=0.001). Ölçek test sonucuna göre Mühendislik fakültesinde eğitim alan öğrencilerin bilgi güvenliği farkındalık düzeylerinin 130,5 (EK:34- EB:170) oranı ile en yüksek, buna karşılık Tıp fakültesinde eğitim alan öğrencilerin bilgi güvenliği farkındalık düzeylerinin 102,5 (EK:38- EB:170) oran ile en düşük seviyede olduğu, yani mühendislik fakültesi öğrencilerinin bilgi güvenliği farkındalık düzeylerinin Tıp fakültesi öğrencilerinin bilgi

güvenliği farkındılık düzeylerine göre daha yüksek olduğu görülmektedir. Bu da bize katılımcıların eğitim gördükleri Fakülte/Yüksek okullar arasında bilgi güvenliği farkındalığı açısından anlamlı bir fark bulunduğunu göstermektedir.

Katılımcıların ailelerinin gelir düzeyleri arasında bilgi güvenliği farkındalık ölçek puanları istatistiksel olarak anlamlı bir fark tespit edilememiştir (*P*=0,708). Yine katılımcıların ailelerinin yaşadıkları yerler arasında bilgi güvenliği farkındalık ölçek puanları istatistiksel olarak anlamlı bir fark bulunamamıştır (*P*=0,307).

Katılımcıların günlük internet kullanım sıklıkları arasında bilgi güvenliği farkındalık ölçek puanları arasında istatistiksel olarak anlamlı bir fark bulunmuştur (*P*=0,032). Ölçek test sonucuna göre günlük 10 saatten fazla internetten faydalanan öğrencilerin bilgi güvenliği farkındalık düzeylerinin günlük 5-10 saat internetten faydalanan öğrencilerin bilgi güvenliği farkındalık düzeylerinden anlamlı bir şekilde daha yüksek olduğu tespit edilmiştir. Ayrıca diğer bir dikkat çekici nokta ise günde bir saatten az internet kullanan katılımcıların da bilgi güvenliği farkındalık düzeyleri yüksek çıkmasıdır.

Ölçek çalışmasına katılanların günlük sosyal medya kullanım süreleri ile bilgi güvenliği farkındalık ölçek puanları arasında istatistiksel olarak anlamlı bir fark olduğu tespit edilmiştir (*P*=0,028). Ölçek test sonucuna göre günlük 10 saatten fazla sosyal medya kullanımı olan öğrencilerin bilgi güvenliği farkındalık seviyelerinin günlük 1-3 saat, 3-5 saat ve 5-10 saat sosyal medya kullanan öğrencilerin bilgi güvenliği farkındalık düzeylerinden anlamlı bir şekilde daha yüksek olduğu ortaya çıkarılmıştır.

Katılımcıların bilgi güvenliği farkındalığı açısından sosyal medya kullanım sürelerinin (yıl) arasında ölçek puanlarının anlamlı bir farklı tespit edilememiştir (*P*=0,439). Katılımcıların sosyal medya hesaplarını herkese açık ve gizli kullanma durumları arasında bilgi güvenliği farkındalık ölçek puanları arasında anlamlı fark olmadığı görülmüştür (*P*=0,805).

Tüm bu elde edilen veriler ışığında literatürde üniversite öğrencilerinin bilgi güvenliği farkındalık düzeylerinin belirlenmesi: Hitit Üniversitesi örneği ölçek sonuçları değerlendirildiğinde; Yayla ve Keser (2021) ülkemizde FATİH Projesinin kullanıldığı okullardaki öğretmenlerin bilgi güvenliği farkındalık seviyesini belirlemek için bir çalışma yapmışlardır. Yaptıkları çalışma ile FATİH projesinin kullanıldığı okullardaki öğretmenler ile FATİH projesini kullanmayan okullardaki öğretmenlerin karşılaştırmasını bilgi güvenliği farkındalığı yönünden değerlendirmişlerdir. Sonuçta FATİH projesini kullanan okullardaki öğretmenlerin bilgi güvenliği farkındalık seviyeleri daha yüksek çıkmışır. Bu durumun Hitit Üniversitesinde yapmış olduğumuz çalışmamızdaki daha fazla internet kullanan ve daha fazla sosyal medya kullanımı olan bireylerin bilgi güvenliği farkındalığının daha yüksek olduğu yönündeki çıkarım ile benzer bir sonuç olduğu görülmektedir. Bu iki çalışma sonucu da bizlere teknoloji ortamında daha fazla bulunan bireylerin farkındalıklarının daha yüksek olduğu,

bireylerin teknolojiyi kullandıkça gereken önlemleri de öğrendiklerini göstermektedir. Ancak bu öğrenme durumunun yeterli bir öğrenme durumu olmadığını düşünmekteyiz.

Rençber ve Mete (2016) yaptıkları çalışmalarında Çukurova Üniversitesi Kozan Meslek Yüksekokulu öğrencilerinin bilgi güvenliği farkındalığını etkileyen faktörleri ve bu faktörlerin etki düzeylerini incelemişlerdir. İnternet kullanımı, şifre yönetimi, e-posta kullanımı ve sosyal ağ sitelerinin kullanımı gibi faktörlerin bilgi güvenliği farkındalık düzeyini etkilediğini tespit etmişlerdir. Araştırmalarında öğrencilerin %57,6'sının 1 saat ile 3 saat arasında internete girdiğini ve sosyal medya sitelerinde 1 saatten fazla zaman geçirdiklerini tespit etmişlerdir. Bu durum bizim araştırmamız sonuçları ile farklılaşmaktadır. Araştırmamızda internet kullanım sıklığında ölçeğe katılanların %45,6'sı 3-5 saat, %26,9'u ise 1-3 saat internet kullandığını belirledik. Geçen süre yıl bazında değerlendirildiğinde öğrenciler arasında internet kullanım süresinin geçen 6 yıllık süre içerisinde arttığı görülmektedir.

Sağır ve ark. (2018) yaptıkları çalışmada Kahramanmaraş Sütçü İmam Üniversitesi Göksun Meslek Yüksekokulunda öğrenim gören 240 öğrencinin bilgi güvenliği farkındalık seviyeleri ile öğrenim gördükleri bölümler arasında bağlantı olmadığını tespit etmişlerdir. Ancak çalışmamızdaki bulgular bilgi güvenligi farkındalığı konusunda katılımcıların eğitim gördükleri fakülte/yüksekokullar arasında anlamlı bir fark olduğu yönündedir. Her iki araştırma sonucu incelendiğinde birinci araştırmanın sadece yüksekokul içindeki bölümleri kapsadığı, araştırmamızın ise tüm üniversite fakültelerini kapsadığı noktası önemlidir. Bu sonuçlar bize fakülteler arası fark olduğu ortaya çıksa bile fakülteler içerisindeki bölümler arasında fark oluşmayabilir sonucunu vermektedir. Ayrıca araştırmacılar bu araştırmalarında internet kullanım süresi arttıkça bilgi güvenliği farkındalığının da artığı sonucunu ortaya koymuşlar, bu sonuç bizim araştırmamız ile benzer doğrultudadır.

Üner, B. (2019) yaptığı Türkiye'de bilgi güvenliği algısının istatistiksel analizi üzerine yaptığı çalışmasında katılımcıların eğitim durumunun bilgi güvenlgi farkındalığına herhangi bir etkisinin olmadığını ve daha fazla, örneğin 11 yıl ve üzeri internet kullanımının bilgi güvenliği farkındalığının oluşumunda etkili olduğunu tespit etmiştir. Biz de araştırmamızda daha fazla internet ve sosyal medya kullanımının bilgi güvenliği farkındalığının oluşumunda olumlu etkiye sahip olduğunu gözlemledik.

Taner ve Kılıç (2019) yaptıkları çalışmada güvenlik güçlerinin bilgi güvenliği farkındalık düzeylerini belirlemeye çalışmışlardır. Araştırmalarında öğrenim durumunu ve yaşın (18 yaş ve üzeri gruplarda) bilgi güvenliği farkındalığında herhangi bir etkilerinin olmadığını ortaya koymuşlardır. Bu sonuçlar araştırmamız ile benzerlik göstermektedir.

Erdoğmuş, A. (2017) Afyon Kocatepe Üniversitesinde öğrencilerin bilgi güvenliği farkındalık düzeylerini etkileyen etmenleri analiz çalışmasında cinsiyetin, yaşın, eğitim görülen bölümün, sınıfın, internet kullanım süresinin bilgi güvenliği farkındalığında anlamlı bir etkisinin olmadığını ortaya koymuştur. Bunun yanında biz araştırmamızda eğitim görülen fakültenin,

cinsiyetin, internet kullanım süresinin bilgi güvenliği farkındalığının düzeyine etki ettiğini belirledik. Bu sonuç bizim elde ettiğimiz bulgular ve Topal ve Akgün'ün yaptıkları çalışma bulguları ile farklılaşmaktadır.

Altunsaban Yerlikaya (2019) öğretmen, öğrenci, veli ve okul yöneticilerinin bilgi güvenliği açısından farkındalıklarını tespit etmek için yaptığı araştırmada erkeklerin bilgi güvenliği farkındalık düzeylerinin kadın katılımcılara göre daha yüksek olduğunu ortaya koymuştur. Eğitim durumunun bilgi güvenliği farkındalığında anlamlı bir etkisinin olmadığını ortaya koymuş, ancak özel okul devlet okulu ayrımında özel okulda okumanın bilgi güvenliği farkındalığında devlet okuluna göre daha önde olduğunu tespit etmiştir. İnternet kullanım süresinin bilgi güvenliği farkındalık düzeyinde etkili olduğunu ortaya koymuş ve ayrıca günde 2-4 saat internet kullanan katılımcıların bilgi güvenliği farkındalık düzeylerinin daha fazla olduğunu belirtmiştir. Çalışmamızda fazla internet kullananların bilgi güvenliği farkındalık düzeylerinin daha fazla olduğunu ortaya çıkardık. Bu sonuçlar Altunsaban Yerlikaya (2019)'nın bulguları ile benzerlik gösterse de çalışmamızda 10 saatten fazla internet kullanan katılımcıların bilgi güvenliği farkındalık düzeylerinin en yüksek olarak bulunması bu çalışmadan farklılaşmaktadır.

SONUÇ VE ÖNERİLER

Günümüzde artık ilkokul düzeyindeki çocukların dahi akıllı telefon sahibi olduğundan hareketle bilgi güvenliği farkındalığının önem kazanması dikkatimizi çekmiş ve bu farkındalık düzeyinin Hitit Üniversitesi öğrencilerin de hangi seviyede olduğunu belirlemek amacıyla Hitit

Üniversitesinde eğitim gören 476 katılımcıya ölçek çalışması uygulanmıştır. Ölçek çalışması sonucu elde edilen veriler istatiksel yöntemler ile analiz edilmiştir. Ölçek sonucunda ortaya çıkan sorunların nedenleri tartışılmış ve sorunlara çözüm yolları belirlenmeye çalışılmıştır.

Güldüren ve Keser (2015) yılanda yaptıkları çalışmada ülkemizde yükseköğretim kurumlarında çalışan öğretim elamanlarının bilgi güvenliği farkındalık düzeylerini tespit amacıyla bir ölçek ortaya koymuşlardır. Sonrasında Güldüren ve ark. (2017), yaptıkları çalışmada öğretmenlerin bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik bir ölçek geliştirmişler, en sonunda Güldüren (2020) yaptığı çalışma ile üniversite öğrencilerinin bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik bir ölçek geliştirmiştir.

Yapılan ölçek çalışması sonucunda üniversite öğrencilerinin bilgi güvenliği farkındalık düzeyleri katılımcıların günlük internet kullanım sıklığına, günlük sosyal medya kullanım sıklığına ve kaç yıldır sosyal medya kullandığına göre farklılaşmaktadır. Cinsiyet grupları arasında bilgi güvenliği farkındalık ölçek puanlarının istatistiksel olarak anlamlı farklı olduğu belirlenmiştir. Erkeklerin bilgi güvenliği farkındalıklarının daha fazla olduğu dikkat çekmektedir.

Eğitim durumlarına göre bilgi güvenliği farkındalık ölçek puanları arasında istatistiksel olarak anlamlı bir fark tespit edilememiştir. Katılımcıların eğitim gördükleri Fakülte/Yüksek okullar arasında bilgi güvenliği farkındalık ölçek puanları dikkate alındığında ise istatistiksel olarak anlamlı farklılık bulunmuştur. Mühendislik fakültesi öğrencilerinin bilgi güvenliği farkındalık düzeylerinin Tıp fakültesi öğrencilerinin bilgi güvenliği farkındılık düzeylerine göre daha yüksek olduğu görülmektedir.

Ölçeğe katılan öğrencilerin ailelerinin gelir düzeylerine göre bilgi güvenliği farkındalık ölçek puanları arasında istatistiksel olarak anlamlı fark tespit edilememiştir. Yine ailelerinin yaşadıkları yerlere göre bilgi güvenliği farkındalık ölçek puanları arasında istatistiksel olarak anlamlı fark tespit edilememiştir.

Günlük internet kullanımı en fazla olan katılımcıların bilgi güvenliği farkındalık ölçek puanlarıda yüksek çıkmıştır. Günlük 10 saatten fazla internet kullanan katılımcıların bilgi güvenliği farkındalık düzeylerinin günlük 5-10 saat internet kullanan katılımcıların bilgi güvenliği farkındalık düzeylerinden daha yüksek olduğu belirlenmiştir. Ayrıca diğer bir dikkat çekici nokta ise günde bir saatten az internet kullanan katılımcıların da bilgi güvenliği farkındalık düzeylerinin yüksek çıkmasıdır.

Katılımcıların günlük sosyal medya kullanım sıklıklarına göre bilgi güvenliği farkındalık ölçek puanları arasında istatistiksel olarak anlamlı fark olduğu belirlenmiştir.

Katılımcıların yıl bazında sosyal medya kullanım sürelerinin ve katılımcıların sosyal medya hesaplarının herkese açık veya gizli olmasının bilgi güvenliği farkındalık düzeyi üzerinde bir etkisi tespit edilememiştir.

Sonuç olarak; teknolojinin hızla gelişmesi, bilgisayarların cebimize girmesini sağlamış, cebimize giren bilgisayarlar bizim bilgiyi kısa sürede elde etmemizi, iletişimin kolaylaşmasını sağlamıştır. Buna karşılık gelişen teknoloji bilinçsizce yani farkındalık sahibi olunmadan kullanıldığında gerek kurumsal gerekse de kişisel bilgilerimizin kötü niyetli kişilerin ellerine geçmesine aracılık etmektedir.

İnternet ortamı her yaşta, her ırktan, her meslekten diğer bir ifade ile her kesimden insanın bulunduğu sanal bir ortamdır. Bu sanal ortam masum insanları barındırdığı gibi suç potansiyeli olan insanları da barındırmaktadır. Suç potansiyeli olan kötü niyetli insanlar internetin bulunduğu bu teknolojik cihazları suç işleme amaçlı olarak uzman seviyesinde kullanmakta ve bilgi güvenliği zafiyetlerini çok iyi bilmektedirler.

Suç mağduru olmamak için öncelikle bilgi güvenliği farkındalığımızı geliştirmemiz gerektiğini düşünmekteyiz. Bu amaç uğrunda en başta insanlara, eğitim kurumlarına ve insanların çalıştığı meslek kuruluşlarına çok büyük görev düşmektedir. Her yaştan insan bilgi güvenliği mağduru olmaya aday olduğu için her yaşta insanın bu farkındalık düzeyini geliştirmesi önemlidir. Burada en hassas noktada olan örneklemin ise üniversite öğrencileri olduğunu söyleyebiliriz.

Üniversite öğrencilerimizin bilgi güvenliği farkındalığının geliştirilmesi amacıyla başta üniversite yönetimimiz ve teknoloji temelli öğrenci klüplerimiz olmak üzere bilgi güvenliği konusunda gerekli eğitim planlaması yapılarak öğrencilerimizin bu konuda bilinçlenmesinin sağlanabileceğini önerebiliriz.

Unutulmamalıdır ki bilgi güvenliği öncelikle teknolojiye değil, kişiye yapılan yatırımla sağlanabilir. Bilgi güvenliği tehditlerinin en aza indirilmesinin birinci yolu insanların bu konuda farkındalıklarının ve bilgi düzeylerinin arttırılması ile sağlanabilir.

Tüm bunlara ek olarak araştırma, geliştirme merkezleri olan üniversitelerimizde bu konuda daha çok araştırma yapılması, konunun hassasiyetinin anlaşılması açısından oldukça önemli olduğu kanaatindeyiz.

KAYNAKÇA

Al-Jerbie S.I., Jali M.Z., (2014). A Second Look at the Information Security Awareness among Secondary School Students. *Proceedings of the International Conference on Information Security and Cyber Forensics*, 88-97.

Al-Shanfari I., Yassin W., Abdullah R., (2020). Identify of Factors Affecting Information Security Awareness and Weight Analysis Process. *International Journal of Engineering and Advanced Technology*, *9*(3), 534-542.

Altunsaban Yerlikaya, C. (2019). *Bilgi Güvenliğine Yönelik Öğrenci, Öğretmen, Veli ve Okul Yöneticilerinin Farkındalıklarının Incelenmesi.* (Tez No. 586587) [Yüksek Lisans Tezi, Ege Üniversitesi]. YÖK Ulusal Tez Merkezi.

Arslan, M., ve Bal, I. (2013). İnternet Ortamında Karşılaşılan Olası Tehditlere Karşı Üniversite Öğrencilerinin Farkındalık Düzeylerinin Ölçülmesi. *1st International Symposium on Digital Forensics and Security.* 277-280.

Avcı, Ü., Oruç, O. (2019). Üniversite Öğrencilerinin Kişisel Siber Güvenlik Davranışları ve Bilgi Güvenliği Farkındalıklarının İncelenmesi. *İnönü Üniversitesi Eğitim Fakültesi Dergisi, 21*(1), 284-303.

Bakan, S., ve Şahin, S. (2018). Uluslararası Güvenlik Yaklaşımlarının Tarihsel Dönüşümü ve Yeni Tehditler. *The Journal of International Lingual, Social and Educational Sciences*, *4*(2), 135-152.

Canbek, G. ve Sağıroğlu, Ş. (2006). Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, *22*(1), 121-136

Canbek, G. ve Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir. İnceleme. Politeknik Dergisi, *9*(3), 165-174.

Canoğulları, E. (2021). Öğretmenlerin Bilgi Güvenliği Farkındalıklarının İncelenmesi. *Kalem Eğitim ve İnsan Bilimleri Dergisi*, *11*(2), 651-679.

Ceylan, H. (2019). Türkiye'de Bilgi Güvenliği Algısının İstatistiksel Analizi. (*Yüksek Lisans Tezi*). İstanbul Üniversitesi, İstanbul.

Chan H., Mübarek S., (2012). Significance of Information Security Awareness in the Higher Education Sector. *International Journal of Computer Applications (0975 – 8887)* 60(10), 23-31.

Çam, H., Aslay, F., ve Özen, Ü. (2019). Yükseköğretim Kurumlarında Bilgi Güvenliği Farkındalık Düzeylerinin Ölçülmesi. *Yönetim Bilişim Sistemleri Dergisi*, *5*(2), 1-11.

Eminağaoğlu, M., ve Gökşen, Y. (2009). Bilgi Güvenliği Nedir, Ne Değildir, Türkiye' de Bilgi Güvenliği Sorunları ve Çözüm Önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *11*(4), 01-15.

Erdoğmuş, A. (2017). *Üniversite Öğrencilerinin Bilgi Güvenliği Kazanimlarinin, Farkindaliklari Üzerindeki Etkilerinin Analizi: Afyon Kocatepe Üniversitesi Örneği.* (Tez No. 472920) [Yüksek Lisans Tezi, Afyon Kocatepe Üniversitesi]. YÖK Ulusal Tez Merkezi.

Fadi A. Aloul, (2012). The Need for Effective Information Security Awareness. *Journal of Advances in Informatıon Technology,* 3(3), 176-183.

Garba, A.A., Siraj, M.M., Othman, S.H., Musa, M.A., (2020). A Study on Cybersecurity Awareness Among Students in Yobe State University, Nigeria: A Quantitative Approach. *International Journal on Emerging Technologies*, *11*(5), 41-49

Gökmen, Ö. F., Akgün, Ö. E. (2015). Bilgisayar ve Öğretim Teknolojileri Eğitimi Öğretmen Adaylarının Bilişim Güvenliği Bilgilerinin Çeşitli Değişkenlere Göre İncelenmesi. *Çukurova Üniversitesi Eğitim Fakültesi Dergisi*, *44*(1), 61-84.

Göldağ, B. (2021). Üniversite Öğrencilerinin Dijital Okuryazarlık Düzeyleri İle Dijital Veri Güvenliği Farkındalık Düzeyleri Arasındaki İlişkinin İncelenmesi. *E-Uluslararası Eğitim Araştırmaları Dergisi*, *12*(3), 82-100.

Güldüren, C. (2021). Üniversite Öğrencileri İçin Bilgi Güvenliği Farkındalık Ölçeği (ISAS) Geçerlilik ve Güvenirlik Çalışması. *Akademik Sosyal Bilimler Araştırmaları Dergisi, 14*(85), 309-326.

Güldüren, C., Çetinkaya, L., Keser, H. (2017). Öğretmenler için Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması. *Milli Eğitim*, *46*(216), 33-52.

Hacımustafaoğlu, R. (2019). *Ortaöğretim Öğrencilerinin Bilgi Güvenliği Farkındalık Düzeylerinin Siber Mağdur Olma Durumlarına Etkisinin İncelenmesi (Üsküdar Örneği).* (Tez No. 586385) [Yüksek Lisans Tezi, Sakarya Üniversitesi]. YÖK Ulusal Tez Merkezi.

Hadlington L., Chivers S., (2018). Segmentation Analysis of Susceptibility to Cybercrime: Exploring Individual Differences in Information Security Awareness and Personality Factors. *Policing*, *14*(2), 479–492.

Hakkoymaz, S. (2022) Animasyon filmlerinde kullanilan bilgi türlerinin dağilimi üzerine bir araştirma. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi*, *19*(1), 62-76.

Karaca, M., Mutlu, T. ve Gencer, G. (2021). Siber Mağduriyet: Kavramsal Bir Bilgi. *Anadolu Akademi Sosyal Bilimler Dergisi*, *3*(1), 177-191.

Karadağ, M. ve Abuhanoğlu, H. (2015). Sosyo-Kültürel Özelliklerin Bilgi Güvenliği Farkındalığı Üzerine Etkisi: Gülhane Askeri Tıp Fakültesi Eğitim Hastanesi'nde Bir Çalışma. *The Journal of Academic Social Science Studies*, *36*, 379-386.

Karaoğlan Yılmaz, F. G., ve Çavuş Ezin, Ç. (2017). Ebeveynlerin Bilgi Güvenliği Farkındalıklarının İncelenmesi. *Eğitim Teknolojisi Kuram ve Uygulama*, *7*(2), 41-57

Karaoğlan Yılmaz, F. G., Yılmaz, R., ve Sezer, B. (2014). Üniversite Öğrencilerinin Güvenli Bilgi ve İletişim Teknolojisi Kullanım Davranışları ve Bilgi Güvenliği Eğitimine Genel Bir Bakış. *Bartın Üniversitesi Eğitim Fakültesi Dergisi, 3(*1), 176-199

Keser, H. ve Güldüren, C. (2015). Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme. *Kastamonu Eğitim Dergisi*, *23*(3), 1167-1184

Keser, H. ve Yayla, H. G. (2021). Fatih Projesi Uygulanan Okullardaki Öğretmenlerin Bilgi Güvenliği Farkındalık Düzeylerinin İncelenmesi. *Millî Eğitim*, *50*(229), 9-40.

Küçükşahin, A. (2006). Güvenlik Bağlamında, Risk ve Tehdit Kavramları Arasındaki Farklar Nelerdir ve Nasıl Belirlenmelidir?. *Güvenlik Stratejileri Dergisi*, *2*(4), 7-40.

Mai, P.T., Tick A., (2021). Cyber Security Awareness and Behavior of Youth in Smartphone Usage: A Comparative Study between University Students in Hungary and Vietnam. *Acta Polytechnica Hungarica, 18*(8), 67-87.

Öztezcan, B.A., ve Çetinkaya, A. (2017). Bilgi Güvenliği Farkındalığı Üzerine Bir Araştırma: Marmara Üniversitesi Örneği. *Ulusal Multidisipliner Hakemli Sosyal Bilimler ve Araştırmalar Dergisi*, *1*, 56-69.

Öztemiz, S. ve Yılmaz, B. (2013). Bilgi Merkezinde Bilgi Güvenliği Farkındalığı: Ankara'daki Üniversite Kütüphaneleri Örneği. *Bilgi Dünyası*, *14*(1), 87-100.

Ramalingam, R., Khan S., Mohammed S., (2015). The Need for Effectıve Informatıon Security Awareness Practıces in Oman Hıgher Educatıonal Instıtutıons*. Information Technology and Biotechnology,* 1-6.

Rençber, Ö. F., Mete, S (2016). Bilgi Güvenlik Farkındalığını Etkileyen Faktörlerin Belirlenmesi: Yüksekokul Öğrencileri Üzerine Bir İnceleme. *Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *18*(3), 800-823.

Sağır, M., Doğruluk, S., Mutluay, Y., ve Emlik, H. (2018). Meslek Yüksekokulu Öğrencilerinin Bilgi Güvenliği Farkındalık Düzeylerinin İncelenmesi. *Akademik Sosyal Araştırmalar Dergisi, 6*(74), 566-582.

Sancak, K. (2013). Güvenlik Kavramı Etrafındaki Tartışmalar ve Uluslararası Güvenliğin Dönüşümü. *Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *6*, 123-134.

Seferoğlu, S.S., Yıldız Durak, H., Karaoğlan Yılmaz, F.G., ve Yılmaz, R. (2018). Bilgi Güvenliği Farkındalığı ve Bilgi Güvenliği Politikalarıyla İlgili Bir İnceleme. *Eğitim Teknoloji Okumaları,* 29-43.

Senthilkumar, K., Easwaramoorthy, S., (2017). A Survey on Cyber Security awareness among college students in Tamil Nadu. *Materials Science and Engineering,* (263), 1-10

Sivaslıoğlu, A. ve Türkmen, A. (2017). *Türkçe Sözlük*. İstanbul: Özyürek Yayınevi.

Stanciu, V., Tinca, A., (2016). Students' awareness on information security between own perception and reality – an empirical study. *Accounting and Management Information Systems*, *15*(1), 112-130.

Talan, T. & Aktürk C. (2021). Ortaöğretim Öğrencilerinin Dijital Okuryazarlık ve Bilgi Güvenliği Farkındalığı Seviyelerinin İncelenmesi. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi, 18*(1), 158-180.

Taner, E. ve Kılıç, İ. (2019). Güvenlik Güçlerinin Bilgi Güvenliği Farkındalığını Belirlemeye Yönelik Bir Araştırma. *Güvenlik Bilimleri Dergisi*, *8*(2), 253-269.

Tekerek, M. ve Tekerek, A. (2013). Öğrencilerin Bilgi Güvenliği Farkındalığı Üzerine Bir Araştırma. *Turkish Journal of Education*, *2*(3), 61-70.

Topal, M. ve Akgün, Ö. E. (2014). Eğitim Fakültesinde Okuyan Öğretmen Adaylarının Eğitim Amaçlı İnternet Kullanımı Öz-yeterlik Algılarının İncelenmesi: Sakarya Üniversitesi Örneği. *Kastamonu Eğitim Dergisi*, *23*(1), 343-364.

Uçak, N. Ö. (2010). Bilgi: Çok Yüzlü Bir Kavram. *Türk Kütüphaneciliği*, *24*(4), 705-722.

Ünver, M., Canbay, C., & Mirzaoğlu, A. G. (2009). *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler.* Ankara: Bilgi Teknolojileri ve İletişim Kurumu (BTK).

Yavanoğlu, U., Sağıroğlu, Ş., ve Çolak, İ. (2012). Sosyal Ağlarda Bilgi Güvenliği Tehditleri ve Alınması Gereken Önlemler. *Politeknik Dergisi*, *15*(1), 15-27.

Yıldız, H.E., (2016). *Türkçe Sözlük*, Ankara: Karatay Yayınları.

Yılmaz, F. G., ve Ezin, Ç. (2017). Ebeveynlerin Bilgi Güvenliği Farkındalıklarının İncelenmesi. *Eğitim Teknolojisi Kuram ve Uygulama Dergisi*, *7*(2), 41-57.

EKLER

EK-1. Kişisel Bilgi Formu

Değerli Katılımcılar; Bu araştırmayı, Hitit Üniversitesi Lisansüstü Eğitim Enstitüsü-Adli Bilimler Ana Bilim Dalında yürütmekte olduğum yüksek lisans tezi kapsamında yapmaktayım. Çalışma; ''Üniversite Öğrencilerinin Bilgi Güvenliği Farkındalık Düzeylerinin Belirlenmesi: Hitit Üniversitesi Örneği (Determining the Information Security Awareness Level of University Students: Hitit University Sample)'' incelemeyi amaçlamaktadır. Araştırma sonuçlarının güvenilir olması açısından sorulara içten ve gerçeği yansıtan yanıtlar vermeniz çok önemlidir. Yanıtlarınız tamamen gizli kalacak ve yalnızca bu araştırma için kullanılacaktır. Hiçbir maddeyi boş bırakmamanız sonuçların daha sağlıklı değerlendirilmesini sağlayacaktır.

Çalışmamıza gösterdiğiniz ilgiden dolayı teşekkür ederiz.

Doç. Dr. Emre DEMİR
Hitit Üniversitesi Tıp Fakültesi
(Tez Danışmanı)

Sinan DÖNER
Hitit Üniversitesi Adli Bilimler

KİŞİSEL BİLGİ FORMU

KİŞİSEL BİLGİLER		
1	**Cinsiyetiniz**	( ) Erkek ( ) Kadın
2	**Yaşınız**	……
3	**Eğitim durumunuz**	( ) Ön-Lisans ( ) Lisans ( ) Yüksek Lisans ( ) Doktora
4	**Fakülteniz/Yüksek okulunuz**	( ) Tıp Fakültesi ( ) Fen Edebiyat Fakültesi ( ) İktisadi ve İdari Bilimler Fakültesi ( ) Mühendislik Fakültesi ( ) Sağlık Bilimleri Fakültesi ( ) Spor Bilimleri Fakültesi ( ) Güzel Sanatlar, Tasarım Ve Mimarlık Fakültesi ( ) İlahiyat Fakültesi ( ) Meslek Yüksekokulu

		( ) Lisansüstü Eğitim Enstitüsü
5	**Sınıfınız**	( ) 1 ( ) 2 ( ) 3 ( ) 4 ( ) 5 ( ) 6
6	**Ailenin Gelir Düzeyi**	( ) 0 – 5000 TL ( ) 5001 – 10000 TL ( ) 10001 – 15000 TL ( ) 15001 TL ÜZERİ
7	**Aileniz ile yaşadığınız yer / İkametgah**	( ) Köy / Kasaba ( ) İlçe Merkezi ( ) İl Merkezi
8	**Günlük internet kullanım sıklığınız (Eğitim, Haber, Youtube, Sosyal medya, Facebook, Instagram, Twitter vb.)**	( ) 1 saatten az ( ) 1-3 saat ( ) 3-5 saat ( ) 5-10 saat ( ) 10 saatten fazla
9	**Günlük sosyal medya kullanım sıklığınız (Facebook, Instagram, Twitter vb.)**	( ) 1 saatten az ( ) 1-3 saat ( ) 3-5 saat ( ) 5-10 saat ( ) 10 saatten fazla
10	**Kaç yıldır sosyal medya (Facebook, Instagram, Twitter vb.) kullanıyorsunuz?**	( ) 1 yıldan az ( ) 1-3 yıl ( ) 3-5 yıl ( ) 5-10 yıl ( ) 10 yıldan fazla
11	**Sosyal medya hesaplarınızı herkese açık mı yoksa gizli mi kullanıyorsunuz?**	( ) Herkese açık ( ) Gizli

EK-2. Üniversite Öğrencileri İçin Bilgi Güvenliği Farkındalık Ölçeği

ÜNİVERSİTE ÖĞRENCİLERİ İÇİN BİLGİ GÜVENLİĞİ FARKINDALIK ÖLÇEĞİ

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

	Maddeler	Hiç Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Tamamen
1	Kablosuz ağların (wireless networks) güvenliği ile ilgili alınması gereken tedbirleri biliyorum.					
2	İnternete bağlanabilen cihazlarla (internet-enabled devices) seyahat ederken dikkat edilmesi gereken konuları biliyorum.					
3	Kişisel mahremiyet nedir biliyorum.					
4	Bilgi güvenliği konusunda yasal sorumluluklarımı biliyorum.					
5	Bilgi güvenliği konusunda sorun yaşadığımda kime ve nereye başvuracağımı biliyorum.					
6	İnternette gezinirken mahremiyetimi korumak için alınması gereken tedbirleri biliyorum.					
7	İnternette gezinirken hakkımda toplanan bilgi miktarının nasıl sınırlandırılacağını biliyorum.					
8	Kritik bilgilerin güvenli olarak nasıl silinmesi gerektiğini biliyorum.					
9	Şifre kullanımına ilave olarak alınması gereken tedbirlerin neler olduğunu biliyorum.					
10	Web sayfalarında kullanılan aktif içeriğin (active content) ne işe yaradığını biliyorum.					
11	Web sayfalarında kullanılan çerezlerin (cookies) ne işe yaradığını biliyorum.					
(EK-2 DEVAMI)						
12	Web Sitesi sertifikasının (web site certificate) ne işe yaradığını biliyorum.					
13	Son kullanıcı lisans sözleşmesi (end-user license agreement) nedir biliyorum.					
14	Dosya paylaşımı teknolojisi (file-sharing technology) nedir biliyorum.					

15	Dosya paylaşım teknolojilerinin (file-sharing technology) taşıdığı riskleri biliyorum.					
16	Aldatmaca (hoax) nedir biliyorum.					
17	Bilgisayarımda casus yazılım (spyware) olup olmadığını anlayabilirim.					
18	Bilgisayarıma casus yazılım (spyware) yüklenmesinin engelleme yöntemlerini biliyorum.					
19	Kimlik hırsızlığı (identity theft) nedir biliyorum.					
20	Kimlik hırsızlığına (identity theft) karşı alınması gereken güvenlik tedbirlerini biliyorum.					
21	Sahte virüs koruma yazılımının ne olduğunu biliyorum.					
22	Hizmet aksatrma (Denial of Service - DoS) saldırısı nedir biliyorum.					
23	Kimlik avı (phishing) saldırısı nedir biliyorum.					
24	Sosyal mühendislik (social engineering) saldırısı nedir biliyorum.					
25	Sosyal mühendislik (social engineering) saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum.					
26	Bilgisayarın başından ayrılırken ekranın kilitlenmesi gerektiğini biliyorum.					
27	Çocukların bilgisayar başında iken ne tür tehditlere maruz kalabileceğini biliyorum.					
28	Çocukların bilgisayarı güvenli kullanmaları için yapılması gerekenleri biliyorum.					
29	Kişisel verilerimi nasıl korumam gerektiğini biliyorum.					
30	Okul ile ilgili verilerimi nasıl korumam gerektiğini biliyorum.					
(EK-2- DEVAMI)						
31	USB sürücülerini (USB drives) kullanırken dikkat edilmesi gereken hususları biliyorum.					
32	Siber zorbalık (cyberbullying) nedir biliyorum.					
33	Siber zorbalığa (cyberbullying) karşı kendimi nasıl koruyacağımı biliyorum.					

34	Siber zorbalığa (cyberbullying) karşı çocukları nasıl koruyacağımı biliyorum.					

Teşekkürler…

EK-3. Etik Kurul Onayi

T.C.
HİTİT ÜNİVERSİTESİ
GİRİŞİMSEL OLMAYAN ARAŞTIRMALAR ETİK KURULU

Sayı : 2022-95 08/04/2022
Konu: Başvuru Değerlendirme Sonucu

Sayın Doç. Dr. Emre DEMİR

Etik Kurulumuza yapmış olduğunuz başvurunuzla ilgili kurul kararımız ve ilgili bilgiler aşağıda yer almaktadır.

Bilgilerinize rica ederim.

Başvuru Numarası	2022-69
Sorumlu Araştırmacı	Doç. Dr. Emre DEMİR
Araştırma Başlığı	Üniversite Öğrencilerinin Bilgi Güvenliği Farkındalık Düzeylerinin Belirlenmesi Hitit Üniversitesi Örneği
Toplantı Tarihi	30.03.2022
Karar Numarası	2022-07

☒ Araştırma başvurunuz etik açıdan uygun bulunmuştur.

☐ Araştırmaya Kurum İzni/İzinleri alındıktan sonra başlanması uygun bulunmuştur.

☐ Başvurunun, ekte belirtilen düzeltmelerin yapılması halinde tekrar değerlendirilmesine karar verilmiştir.*

☐ Araştırma projesi etik açıdan uygun olmadığından başvurunun reddine karar verilmiştir.