2022

4(1), 66-86

Önlisans Öğrencilerinin Bilgi Güvenliği Kazanımı ve Farkındalık Düzeylerinin Belirlenmesi: Kırıkhan Meslek Yüksekokulu Örneği

Fidan Hakkari*[1]

Anahtar Sözcükler

Bilgi güvenliği
Farkındalık
Kazanım
Önlisans

Makale Hakkında

Gönderim Tarihi
25 Mayıs 2022
Kabul Tarihi
26 Haziran 2022
Yayın Tarihi
29 Haziran 2022

Makale Türü
Araştırma Makalesi

Öz

Bu çalışmanın amacı, önlisans öğrencilerinin bilgi güvenliği konusundaki kazanım ve farkındalık düzeylerinin belirlenmesidir. Çalışma tarama modelinde tasarlanmıştır. Örneklem seçiminde kolayda örnekleme yöntemi kullanılmıştır. Bu bağlamda, araştırmanın örneklemini Kırıkhan Meslek Yüksekokulu'nda çeşitli bölümlerde öğrenim gören 161 önlisans öğrencisi oluşturmaktadır. Çalışmada Bilgi Güvenliği Kazanımları (BGK) ve Bilgi Güvenliği Farkındalığı (BGF) ölçekleri kullanılmıştır. Demografik bilgiler için betimsel istatistikler kullanılırken, araştırmaya katılanların yaş ve bölüm değişkenleri için tek yönlü ANOVA testi, sınıf düzeyi için bağımsız örneklem t-testi uygulanmıştır. Bu çalışmanın sonucunda, önlisans öğrencilerinin bilgi güvenliği farkındalık düzeylerinin yüksek, bilgi güvenliği kazanım düzeylerinin orta düzeyde olduğu belirlenmiştir. Öğrencilerin BGK ortalama puanlarının öğrenim gördükleri programlara göre istatistiksel olarak önemli ölçüde farklılık gösterdiği tespit edilmiştir. Aynı zamanda öğrencilerin BGF alt boyutlarından olan İnternet Tarayıcısı ve Ağ Güvenliği puanlarının öğrencilerin yaşlarına göre önemli ölçüde farklılık gösterdiği bulunmuştur. Bununla birlikte önlisans öğrencilerinin bilgi güvenliği kazanımları ve alt boyutları ile bilgi güvenliği farkındalığı internet güvenliği, internet tarayıcısı ve ağ güvenliği alt boyutlarına göre bilgi güvenliğine ilişkin bilişim suçlarını bilme durumuna göre de önemli ölçüde farklılık gösterdiği bulunmuştur. Öğrencilerin bilgi güvenliği farkındalığı (BGF) ortalama puanları ile bilgi güvenliği kazanımları (BGK) ve tüm BGK alt boyutlarına ait ortalama puanlarının öğrencilerin sınıf düzeylerine göre istatistiksel olarak önemli ölçüde bir farklılık göstermediği tespit edilmiştir.

Determination of Information Security Acquisition and Awareness Levels of Associate Degree Students: Kırıkhan Vocational School Sample

Keywords

Acquisition
Associate degree
Awareness
Information security

Article Info

Received
May 25, 2022
Accepted
June 26, 2022
Published
June 29, 2022
Article Type
Research Paper

Abstract

The aim of this paper is to determine the information security acquisition and awareness levels of associate degree students. The sample group of this paper consists of 161 associate degree students studying in various departments at Kırıkhan Vocational School. Information Security Acquisition and Information Security Awareness were used as data collection tools in this paper. The data were evaluated in terms of normal distribution and it was determined that they were normally distributed. Descriptive statistics, independent samples t-test and one-way ANOVA were used to analyze the data. Research findings show that the information security awareness level of the associate degree students was high, and their information security acquisition level was medium. It was found that the Information Security Acquisition mean of the students differ according to the programs they studied, and the Information Security Awareness Internet Browser and Network Security sub-dimension scores differ according to the age of the students. It was found that the information security acquisition of the students and all its sub-dimensions, Internet Security, Internet Browser and Network Security scores which are sub-dimensions of Information Security Awareness scale differ according to students' state of knowing information crimes related to information security. The students' scores of Information Security Awareness, Information Security Acquisition and their sub-dimensions scores weren't differ according to their grade level.

Atıf: Hakkari, F. (2022). Önlisans öğrencilerinin bilgi güvenliği kazanımı ve farkındalık düzeylerinin belirlenmesi: Kırıkhan Meslek Yüksekokulu örneği. *Bilgi ve İletişim Teknolojileri Dergisi*, *4*(1), 66-86. https://doi.org/10.53694/bited.1121085

Cite: Hakkari, F. (2022). Determination of information security acquisition and awareness levels of associate degree students: Kırıkhan Vocational School sample. *Journal of Information and Communication Technologies*, *4*(1), 66-86. https://doi.org/10.53694/bited.1121085

* **Sorumlu Yazar/Corresponding Author:** fhakkari@mku.edu.tr

[1] Phd, Hatay Mustafa Kemal Üniversitesi, Kırıkhan Meslek Yüksekokulu, Hatay/Türkiye, fhakkari@mku.edu.tr, https://orcid.org/0000-0003-3238-6510

Extended Abstract

Introduction

The term information security awareness is used to denote a situation where users in an organization are aware of their security mission. In other words, it can be expressed as users' prevention of threats to information security, their knowledge of relevant personal and corporate information security policies, and their conscious behavior against these threats.

The acquisition (target) is defined as the desired characteristics that are planned to be observed in the individual. It is stated that these are characteristics such as knowledge, interest, skill, and attitude. In this context, information security acquisition can be defined as students gaining the desired knowledge, skills, and behaviors about information security.

Information Security includes three principles; integrity, confidentiality, and accessibility. Confidentiality indicates the prevention of access to information by unauthorized persons. Integrity refers to the verification that there is no change or loss with information processing methods during the transmission of information. The accessibility principle refers to the accessibility of information without harming individuals from within or outside the institution. In case of threats, the behavior of individuals is expected to guide the provision of information security. Nowadays, universities are of the institutions that have a computer network and technology infrastructure. Moreover, universities are institutions where many strategic scientific information is produced and distributed. One of the system user groups in universities is students. In matters of confidentiality and security, it is stated that the protection of information sources is based on action rather than intent. The main purpose of information security is to make positive changes in the behavior of the end user or to correct the existing behavior to make it compatible with the desired behavior. For that reason it is important for the end users to be aware of the threats in question and the damage they will cause, in ensuring information security.

In order to create a strong infrastructure in ensuring information security, administrative measures, technology applications, education and awareness-raising processes should be considered as a whole. So, it is very important to ensure that all users understand the existing risks and how to protect the computing and information resources- which they use, develop, support, or protect- from multiple threats. This study is important in terms of contributing to the information security awareness studies conducted for associate degree students. The aim of this study is to determine the information security acquisition and awareness levels of associate degree students.

Method

This study conducted in the 2019-2020 academic year. The survey model, one of the quantitative research designs, was applied. This study was conducted with 161 students from Hatay Mustafa Kemal University, Kırıkhan Vocational School. The data were collected with Information Security Acquisition and Information Security Awareness Scales. In order to determine the reliability of the collected data, the Cronbach's alpha internal consistency coefficient was calculated. The Cronbach's alpha internal consistency coefficient for Information Security Acquisition was calculated as .939 and for Information Security Awareness as .961. According to these results, it can be said that the scales are reliable.

Findings, Discussion and Conclusion

As a result of this research, it is seen that the information security awareness level of the associate degree students is high. The findings of similar studies also support this finding. Information security acquisition level, on the other hand, is moderate according to obtained results. However, as far as we know, there is no observation involving the similar context in previous studies to conduct a comparative phrase.

It was found that the means of Information Security Acquisition of the students differ according to the programs they studied. The difference between the Information Security Program and Office Management and Executive Assistantship was in favor of the Information Security Program students. Information Security Acquisition levels of the students are higher in favor of Information Security Program students against Office Management and Executive Assistant Program students. This is because the courses that Information Security Program students take about information and communication technologies and security.

Only Internet Browser and Network Security sub-dimensions scores differ according to the age of the students. It was determined that the difference was between the 20-21 age group and the 24+ group, in favor of the students in the 20-21 age group. Furthermore, Information Security Awareness, Information Security Acquisition and their sub-dimensions scores of the students was not differ according to their grade level. In a similar study, it was found that the Information Security Awareness levels of undergraduate students studying in upper grades were higher, on the contrary to this finding.

At the same time, it was found that the scores of Information Security Acquisition scale and its all sub-dimensions, scores of Information Security Awareness and some of its sub-dimensions -which are Internet Security, Internet Browser and Network Security- differ in favor of the students who previously have knowledge about information (cyber) crimes related to information security. According to this result, it can be said that students who are aware of cybercrimes related to information security have higher awareness and gains about internet networks and security, except for social media and password creation, compared to those who do not. The fact that students are aware of such criminal elements also supports the finding that their awareness is at a high level.

Giriş

Bilgi ve iletişim teknolojileri (BIT), bireylere haberleşme, reklamcılık, bankacılık, ticaret, eğlence, sosyal ve kültürel ilişkilerde, bilgiye erişim ve paylaşım gibi konularda sağladıkları olanak ve kolaylıklar nedeniyle hayatın vazgeçilmez bir parçası halini almıştır. Bilgi ve iletişim teknolojilerindeki bu gelişmelerin ve hayatımıza kısa sürede girmesinin temel nedenlerinden biri de internettir. İnternet, öğrencilerin bilişsel ve sosyal gelişimini destekleyen, dünyayı öğrenmeleri ve keşfetmelerini sağlayan zengin bir öğrenme ortamıdır. TÜİK (2020) verilerine göre, hanelerin %90.7'sinin evden internete erişim imkânı olduğu belirtilmektedir. Bu oranın büyük bir bölümünü özellikle uzaktan eğitimlere katılım amacıyla öğrencilerin oluşturduğu söylenebilir (Kahraman, 2020). Öğrenciler interneti genellikle derslerini takip etme, oyun oynama, sosyal medya ve ödev yapma gibi amaçlar için kullanmaktadırlar (Çağlar & Savaşer, 2010; Ersoy & Ersoy, 2008; Yurttaş, 2013). Bilgisayar, tablet ve akıllı telefonlar gibi araçlarla birlikte internetin eğitim ve öğretim ortamlarına girmesiyle öğrenciler arasında yaygın olarak kullanılmaktadır (Taylan, 2020). Söz konusu araçların sağladığı faydaların yanı sıra bazen de güvenlik zafiyetleri nedeniyle öğrencilerin birtakım tehditlerle karşı karşıya kalmaları mümkün olabilmektedir (Akgün & Topal, 2015, Markelj & Berniki, 2015). Hanus ve Wu (2016)'ya göre dünya genelinde bilgisayar kullanıcılarının %40'ından fazlası kimlik avı, kötü amaçlı yazılım saldırıları, solucan, sosyal mühendislik gibi siber suçların kurbanı olmaktadır. Bu tip saldırıları düzenleyenler güvenlik duvarı, antivirüs yazılımlar, şifreleme teknikleri gibi yazılımsal ve donanımsal engelleri aşmada dahi sosyal mühendislik yöntemleriyle insan faktörünü kullanmaktadırlar (Van Bavel, Rodríguez-Priego, Vila, & Briggs, 2018; Kraemer, Carayon, & Clem , 2009; Taha & Dahabiyeh, 2020). Yapılan bir anket çalışmasına göre, organizasyon içindeki bireylerin neden olduğu güvenlik olaylarının oranı %34'tür (Pricewaterhouse Coopers, 2015). Bu nedenle bu tip risklerin ortadan kaldırılabilmesi için sisteme dâhil olan bireylerden kaynaklanabilecek hataların giderilmesi ve bu konuda çözüm üretilmesi gerekmektedir (Al-Shehri, 2012; Bogart, 2012). Bu noktada bilgi güvenliği farkındalığı kavramı önem kazanmaktadır.

Bilgi güvenliği farkındalığı terimi, bir kuruluştaki kullanıcıların güvenlik misyonlarının farkında olduğu bir durumu belirtmek için kullanılmaktadır (Siponen, 2000). Başka bir ifadeyle kullanıcıların bilgi güvenliğine yönelik tehditleri önlemeleri ve ilgili kişisel ve kurumsal bilgi güvenliği politikaları konusunda bilgi sahibi olmaları, bu tehditlere karşı bilinçli davranışlarda bulunmaları şeklinde ifade edilebilir (Öztemiz & Yılmaz, 2013; Siponen, 2000). Kazanım (hedef) ise bireyde gözlenmesi planlanan istendik özellikler olarak tanımlanmaktadır. Bunların bilgi, ilgi, beceri, tutum gibi özellikler olduğu belirtilmektedir (Sönmez, 2015). Bu bağlamda bilgi güvenliği kazanımları, öğrencilerin bilgi güvenliği konusunda hedeflenen istendik bilgi, beceri ve davranış kazanmaları olarak tanımlanabilir.

Gizlilik ve güvenlikle ilgili durumlarda, bilgi kaynaklarının korunmasının niyetten çok eyleme dayandığı belirtilmektedir (Crossler ve diğerleri, 2013). Son kullanıcıların söz konusu tehditler ve bu tehditlerin neden olacakları zararların farkında olmaları bilgi güvenliğinin sağlanmasında çok önemlidir. Bilgi güvenliğinin temel amacı, son kullanıcının davranışında olumlu değişiklikler yapmak veya mevcut davranışı istenen davranışla uyumlu hale getirmek için düzeltmektir (Alotaibi & Alfehaid, 2018). Yani bilgi güvenliğini sağlamaya yön verecek olan oluşacak tehditler karşısında bireylerin göstereceği davranışlardır. Bu durumu Rogers'ın Korunma Motivasyonu Teorisi (KMT) ile açıklamak mümkündür (Hassandoust & Techatassanasoontorn, 2020). Korunma Motivasyonu Teorisi (PMT, Protection Motivation Theory) bir tehdit karşısında davranışa aracılık eden bilişsel

süreçleri açıklamaya çalışır (Rogers, 1975). Bu teori, bireylerin tehdit oluşturan herhangi bir vaka ile karşı karşıya kaldıklarında iki değerlendirme süreci yürüttüklerini ileri sürer: biri tehdidin kendisine (tehdit değerlendirmesi), diğeri de bu tehdide karşı koyma becerilerine (başa çıkma değerlendirmesi) odaklanır. Başka bir ifadeyle, insanların bilgi birikimlerinin arttırılarak tehdide karşı farkındalıklarının artması (tehdit değerlendirmesi) ve alınacak uygun koruyucu tepkilerin farkına varmaları (başa çıkma değerlendirmesi) daha güvenli adımlar atmalarını sağlayacaktır (Van Bavel ve diğerleri, 2018; Canbek & Sağıroğlu, 2006). KMT'ya göre bireylerin istenen davranışları yapma olasılığını arttıran dört faktör vardır. Bunlardan birincisi kişiyi hata yapmaya iten mesajda yer alan tehdidin ciddiyeti yani bireylerin bilişsel olarak tehdidi değerlendirmesidir. İkincisi tehlikenin ortaya çıkma ihtimalinin değerlendirilmesidir. Üçüncüsü mesajda önerilen çözümün etkinliği, yani bu konuda yapılacak mücadelenin tehlikeyi ortadan kaldırıp kaldıramayacağına karar verilmesidir. Dördüncüsü ise bireylerin çözümü uygulama özyeterliliğini değerlendirmesidir (Roser & Thompson, 1995; Witte & Allen, 2000). Bu bağlamda öğrencilerin bilgi güvenliği konusunda farkındalıkları ve tehditlere yönelik alınması gereken önlemler hakkındaki yeterlilikleri önem taşımaktadır. Farkındalık tehditlerin ve olası saldırıların varlığından haberdar olmaları olarak ifade edilirken kazanım ise bu tehditler karşısında alınması gereken önlemler ve davranışlar olarak ifade edilebilir.

Elektronik güvenlik geniş bir yelpazeye sahiptir. Bir yönüyle kişiler arasında maruz kalınan siber zorbalık, sanal takip gibi güvenlik problemleri; diğer yönüyle güvenli şifre oluşturma, kişisel bilgilerin paylaşımıyla ilgili teknik bilgileri içermektedir (Šimandl & Vaníček, 2017). Bilgi Güvenliği ise gizlilik, bütünlük ve erişilebilirlik ilkelerini içermektedir. Gizlilik, bilgilerin yetkisi olmayan kişilerce erişiminin engellenmesini ifade eder. Bütünlük, bilginin iletimi esnasında herhangi bir değişim ya da kaybın olmadığının doğrulanmasını ifade eder. Erişilebilirlik ilkesi ise bilginin kurum içi ya da dışından bireylerce zarar verilmeden erişilebilirliğinin sağlamasını ifade eder (Von Solms & Von Solms, 2018). McIlwraith'e (2006) göre, bilgi güvenliği altyapısı sunucular, ağ bağlantıları gibi bileşenlerin ötesinde binaları, belgeleri ve en önemlisi insanları içermektedir.

Bilgi güvenliğinin sağlanmasında güçlü bir altyapı oluşturulabilmesi için yönetsel önlemler, teknoloji uygulamaları ile eğitim ve farkındalık yaratma süreçleri birlikte bir bütün olarak ele alınmalıdır (Pro-G & Oracle, 2003). Yapılan araştırmalara göre insan kaynaklı hataların giderilmesi için farkındalığı artırmak, bilgi güvenliği uygulayıcılarının kuruluşlarında olumlu bir fark yaratmak için yapabilecekleri en etkili şeydir (Al-Shehri, 2012; Bogart, 2012; McIlwraith, 2006). Tüm kullanıcıların risklerin ne olduğunu bilmeleri bilgi güvenliğine katkı sağlayacaktır. Bununla birlikte kullanıcıların etkileşim kurdukları, geliştirdikleri, destekledikleri bilgi işlem ve bilgi kaynaklarını tehditlere karşı nasıl korumaları gerektiğini anlamaları da önem taşımaktadır (Bogart, 2012). Bu bağlamda bu çalışmada bilgi güvenliği konusunda hedef (kazanım) ve farkındalık oluşturma süreci ele alınacaktır.

Günümüzde bilgisayar ağı ve teknoloji alt yapısına sahip olan, pek çok stratejik bilimsel bilginin üretilip dağıtıldığı kurumlardan biri de üniversitelerdir. Üniversitelerdeki sistem kullanıcı kitlelerinden birini de öğrenciler oluşturmaktadır. Bu bağlamda birer internet kullanıcısı olarak öğrencilerin de karşılaşabilecekleri tehditlerin farkında olmaları ve bu tehditler karşısında gösterecekleri davranışlar konusunda donanımlı olmaları önemlidir (Akgün & Topal, 2015; Akyol & Uzun, 2021; Demir, 2021).

Alanyazın incelendiğinde, çalışanların bilgi güvenliği farkındalığına yönelik birçok çalışmanın yapıldığı görülmektedir (Haeussinger, 2015; Hwang, Wakefield, Kim, & Kim, 2019; McCormac ve diğerleri, 2017; Öztemiz & Yılmaz, 2013; Tekerek & Tekerek, 2013; Yılmaz, Şahin, & Akbulut, 2016). Lisans öğrencilerinin bilgi

güvenliği farkındalıklarının ve akıllı telefonun bilgisayar ile karşılaştırıldığı çalışmalar (Filippidis, Hilas, Filippidis, & Politis, 2018; Taha & Dahabiyeh, 2020; Demir, 2021) mevcuttur.

Meslek yüksekokullarına yönelik yapılan çalışmalarda bilgi güvenliğine yönelik derslerin incelendiği (Kale, 2016), yüksekokul öğrencilerinin bilgi güvenliği farkındalığı davranışları ve bu davranışları etkileyen faktörler ve etki düzeylerinin belirlendiği (Akyol & Uzun, 2021; Rençber & Mete, 2016), üniversite öğrencilerinin dijital veri güvenliği bilinç düzeylerinin, siber güvenlik davranışları ile bilgi güvenliği farkındalıklarının belirlendiği (Avcı & Oruç, 2020; Erdoğmuş, 2017; Göldağ, 2021; Korkmaz, 2018; Korovessis, 2013), ve öğretmen adaylarının bilişim güvenliği bilgilerinin ve farkındalıklarının incelendiği (Efe, 2019; Gökmen & Akgün, 2015) görülmüştür. Bu çalışma alanyazına önlisans öğrencilerine yönelik yapılan bilgi güvenliği farkındalık ve kazanımları çalışmalarına katkı sunması ile bilgi güvenliğinin sağlanmasında farkındalık ve önlemlerin birlikte ele alınması gereksinimini sağlaması açısından önemlidir.

Bu bağlamda bu çalışmada öğrencilerin bilgi güvenliğine dair yeterlilik ve farkındalık düzeylerinin belirlenmesi amacıyla aşağıdaki araştırma problemlerine cevap aranacaktır.

1. Önlisans öğrencilerinin bilgi güvenliği yeterlilik düzeyleri nedir?
2. Önlisans öğrencilerinin bilgi güvenliği farkındalık düzeyleri nedir?
3. Önlisans öğrencilerinin BGK, BGF ve alt boyutlarına dair ortalama puanları öğrenim gördükleri programlara göre istatistiksel olarak anlamlı mıdır?
4. Önlisans öğrencilerinin BGK, BGF ve alt boyutlarına dair ortalama puanları yaşlarına göre istatistiksel olarak anlamlı mıdır?
5. Önlisans öğrencilerinin BGF, BGK ve alt boyutları puanlarının sınıf düzeylerine göre istatistiksel olarak anlamlı mıdır?
6. Önlisans öğrencilerinin BGF, BGK ve alt boyutları puanlarının bilgi güvenliğine ilişkin bilişim suçları hakkında bilgi sahibi olma durumlarına göre istatistiksel olarak anlamlı mıdır?

Yöntem

Çalışmanın bu kısmında araştırma modeli, çalışma grubu, veri toplamada kullanılan araçlar ve elde edilen verilerin analizlerine yer verilmiştir.

Araştırmanın Deseni

2019-2020 eğitim-öğretim yılında gerçekleştirilen bu çalışmada nicel araştırma desenlerinden biri olan tarama modeli kullanılmıştır. Tarama modeli geçmişte ya da var olan bir durumu olduğu şekilde betimlemeyi amaçlayan bir yaklaşımdır (Karasar, 1984).

Evren ve Örneklem / Çalışma Grubu / Katılımcılar

Bu çalışmanın örneklemini Hatay Mustafa Kemal Üniversitesi Kırıkhan Meslek Yüksekokulu'nda öğrenim gören ve çalışmaya gönüllü olarak katılan 161 önlisans öğrencisi oluşturmaktadır. Araştırmaya ölçek madde sayısının 5 katı olan en az toplam 90 katılımcı alınması düşünülmüştür (Tavşancıl, 2002). Örnekleme yöntemi olarak kolayda

örnekleme kullanılmıştır. Kolayda örnekleme, verilerin evrenden kolay, hızlı ve daha ekonomik şekilde toplandığı yöntemdir (Zikmund, 1997).

Çalışmaya katılan öğrencilerin bazı demografik özellikleri ve sosyal medya kullanım durumları ile bilgi güvenliğine ilişkin bilişim suçlarına dair bilgiye sahip olma durumlarına yönelik bulgular Tablo 1'de verilmiştir. Sosyal medya kullanım durumları ile bilgi güvenliğine ilişkin bilişim suçlarına dair bilgiye sahip olma durumları ayrıca sorulmuştur.

Tablo 1. Betimsel istatistikler

	Değerler	f	%
Bölümler	Bilişim Güvenliği Tek.	8	5.0
	Bilgisayar Tek.	21	13.0
	Büro Yönetimi ve Y.A.	51	31.7
	Dış Ticaret	15	9.3
	İş Sağlığı ve Güv.	24	14.9
	Muhasebe ve Vergi Uyg.	23	14.3
Yaş	18-19	39	24.2
	20-21	81	50.3
	22-23	25	15.5
	24+	16	9.9
Sınıf	1.sınıf	121	75.2
	2.sınıf	40	24.8
Sosyal medya kullanıyor musunuz?	Evet	141	87.6
	Hayır	20	12.4
Bilgi güvenliğine ilişkin bilişim suçlarını biliyor musunuz?	Evet	108	67.1
	Hayır	53	32.9

Çalışma grubu 18-48 yaş aralığında olup yaş ortalaması 21.6'dır. Çalışmaya katılanların %31.7'si Büro Yönetimi ve Yönetici Asistanlığı, %14.9'u İş Sağlığı ve Güvenliği, %14.3'ü Muhasebe ve Vergi Uygulamaları, %13'ü Bilgisayar Teknolojisi, %9.3'ü Dış Ticaret ve %5'i Bilişim Güvenliği Teknolojisi programları öğrencisidir. Öğrencilerin %75.2'si birinci sınıf, %24.8'i ikinci sınıf öğrencisidir. Katılımcıların %87.6'sı sosyal medya kullanırken %12.4'ü kullanmamaktadır. Yine öğrencilerin %67.1'i bilgi güvenliğine ilişkin bilişim suçlarından haberdar olduklarını bildirirken, %32.9'u konu hakkında bilgisinin olmadığını belirtmiştir.

Veri Toplama Araçları

Bu çalışma için araştırmacı tarafından öğrencilerin demografik özelliklerine dair bilgilerin toplandığı Demografik Bilgiler bölümü oluşturulmuştur. Verileri toplamak için de Bilgi Güvenliği Farkındalığı ve Bilgi Güvenliği Kazanımları Ölçekleri kullanılmıştır.

Bilgi Güvenliği Farkındalığı Ölçeği

Çalışmada analize dâhil edilen öğrencilerin bilgi güvenliği ölçmek için Erdoğmuş (2017)'un yüksek lisans tez çalışmasında oluşturduğu ölçek kullanılmıştır. Ölçek, 5'li likert tipinde olup İnternet Güvenliği (IG), Şifre Oluşturma (SO), Sosyal Medya Kullanımı (SMK), Sosyal Medya Tuzakları (SMT), İnternet tarayıcısı ve Ağ Güvenliği (ITA) olmak üzere beş boyuttan oluşan Bilgi Güvenliği Farkındalığı (BGF) ölçeğinden oluşmaktadır.

BGF maddeleri geneli için ise Cronbach's Alpha değeri 0.839 olarak hesaplanmıştır. Elde edilen verilerin BGF maddelerin geneli için Cronbach's Alpha güvenirlilik katsayısı .961 ve alt boyutlara ilişkin iç tutarlılık katsayısı sırasıyla; IG .896, SMK .939, ITS .872, SO .858, SMT .913 olarak hesaplanmıştır.

Bilgi Güvenliği Kazanımları Ölçeği

Çalışmada analize dâhil edilen öğrencilerin bilgi güvenliği kazanımlarını ölçmek için Erdoğmuş (2017)'un yüksek lisans tez çalışmasında oluşturduğu ölçek kullanılmıştır. Ölçek, 5'li likert tipinde olup Önlemler ve Tehditler alt boyutlarından oluşan Bilgi Güvenliği Kazanımları (BGK) ölçeğidir.

BGK maddelerin geneli için Cronbach's Alpha güvenirlilik katsayısı 0.912, Elde edilen verilerin güvenirliğini belirlemek için Cronbach's Alpha değeri hesaplanmış ve sırasıyla; BGK' ilişkin iç tutarlık katsayısı .939, Tehditlere ilişkin .908, Önlemlere ilişkin ise .906 olarak hesaplanmıştır. Bu sonuçlara göre Cronbach alfa katsayısına bağlı olarak bir ölçeğin güvenilirliğinin 0.80 ile 1.00 arasında olması ölçeğin güvenirliliğinin yüksek derecede olduğunu göstermektedir (Kalaycı, 2008). Bu bilgiler ışığında ölçeklerin yüksek derecede güvenilir olduğu söylenebilir.

Veri Toplama Süreci

Veriler çevrimiçi Google Formlar aracılığıyla oluşturulmuş olan formla toplanmıştır. Bağlantı (linki) katılımcılara sınıf temsilcileri aracılığı ile sosyal medya (Whatsapp) üzerinden iletilmiştir.

Veri Analizi

Bu araştırmada, toplanan verileri değerlendirmek için; demografik bilgiler bölümünde yer alan bağımsız değişkenler için frekans ve yüzde dağılımları hesaplanmıştır. Önlisans öğrencilerinin bilgi güvenliği farkındalık düzeylerini belirlemek amacıyla iki adımlı kümeleme analizi yapılmıştır. Kümeleme analizi p adet değişkene sahip olan N sayıdaki bireylerin benzerliklerine göre ayrık kümelerde toplanması amacıyla yapılmaktadır (Duran & Odel, 1974).

BGK ve BGF puanlarının bağımsız değişkenlere göre (bölüm, yaş,) farklılık gösterip göstermediğini belirlemek, buna bağlı olarak kullanılması gereken testlerin parametrik mi non-parametrik mi olduğuna karar vermek için öncelikle verilerin normallik dağılımlarına bakmak gerekmektedir. Bu amaçla verilerden elde edilen puanların ortalamalarına dair basıklık ve çarpıklık değerlerine bakılmıştır (Tablo 2, Tablo 3).

Tablo 2. Bilgi Güvenliği Kazanımları Ölçeğine Dair Betimsel İstatistikler

BGK	N	Ortalama	Standart Sapma	Çarpıklık	Basıklık
Tehditler	161	19.72	8.08	.277	-.937
Önlemler	161	18.70	7.06	-.123	-.907

Tablo 3. Bilgi Güvenliği Farkındalığı Ölçeğine Dair Betimsel İstatistikler

BGF	N	Ortalama	Standart Sapma	Çarpıklık	Basıklık
IG	161	20.69	5.26	-1.537	1.719
SMK	161	17.06	4.61	-1.688	1.887
ITA	161	11.70	3.70	-1.035	.023
SO	161	12.73	3.02	-1.470	1.503
SMT	161	12.51	3.42	-1.489	1.393

Çarpıklık ve basıklık katsayılarının -2 ile +2 arasında değişmesi verilerin normal dağılım gösterdiğini belirtilmektedir (Tabachnick & Fidell, 2013). Buna göre ölçeklerin normal dağılım gösterdiğine karar verilmiştir. Bu bağlamda veriler normal dağılım gösterdiğinden parametrik testlerden olan t-testi ve ANOVA testi yapılması uygun görülmüştür. Bir değişkenin farklı iki grup arasında değişip değişmediğini analiz etmek için bağımsız gruplar t-testi kullanılmıştır. Bir değişkenin ikiden fazla grup arasında değişip değişmediğini analiz etmek için ise tek yönlü ANOVA testi kullanılmıştır.

Bulgular

Önlisans öğrencilerinin bilgi güvenliği farkındalık düzeylerini belirlemek amacıyla iki adımlı kümeleme analizi yapılmıştır. Bulgular Tablo 4'te sunulmuştur.

Tablo 4. Önlisans Öğrencilerinin BGF Düzeyleri

Düzey	% (N)	X
Düşük	5.6(9)	24.89
Orta	26.1(42)	59.38
Yüksek	63.3(110)	84.65

Tablo 4'e göre önlisans öğrencilerinin %63.3'ü 84.65 ortalama değeriyle yüksek düzeyde farkındalığa sahip, %26.1'i ise 59.38 ortalamayla orta düzeyde ve %5.6'sı 24.89 ortalama ile düşük farkındalık düzeyine sahiptir. BGF ölçeğinden alınabilecek en düşük puan 18dir. En yüksek puan ise 90'dır. Buna göre öğrencilerin bilgi güvenliği farkındalık düzeylerinin yüksek olduğu söylenebilir.

Tablo 5. Önlisans Öğrencilerinin BGK Düzeyleri

Düzey	*% (N)*	*X*
Düşük	26.1(42)	20.14
Orta	45.3(73)	37.85
Yüksek	28.6 (46)	56.04

Tablo 5'e göre önlisans öğrencilerinin %28.6'sı 56.04 ortalama değeriyle yüksek, %45.3'ü ise 37.85ortalamayla orta düzeyde ve %26.1'i 20.14 ortalama ile düşük bilgi güvenliği kazanım düzeyine sahiptir. BGK ölçeğinden alınacak en düşük puan 13 iken en yüksek puan 65'tir. Bu bağlamda öğrencilerin bilgi güvenliği kazanımı genel olarak orta düzeyde olduğu söylenebilir.

Yapılan analizlerin kalitesini belirlemek amacıyla BGK ve BGF için yapılan Two Step Cluster testi sonucunda bulguların iyi düzeyde olduğu görülmüştür (Silhouette measure=good).

Tablo 6. Katılımcıların BGK Cevap Ortalamaları ve Standart Sapmaları

	Tehditler	*X*	*SS*
1.	Sahte virüs koruma yazılımının ne olduğunu biliyorum.	2.88	1.45
2.	Kimlik hırsızlığına karşı alınması gereken güvenlik tedbirlerini biliyorum	3.50	1.32
3.	Bilgisayarıma casus yazılım yüklenmesini engelleme yöntemlerini biliyorum	2.51	1.45
4.	Kötü niyetli yazılımlara (malware) karşı alınması gereken güvenlik tedbirlerini biliyorum.	2.81	1.45

5. Sosyal mühendislik saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum	2.82	1.45
6. Bilgisayarımda casus yazılım (spyware) olup olmadığını anlayabilirim.	2.49	1.40
7. Bilgisayarıma zararlı kod (maliciouscode) bulaşıp bulaşmadığını anlayabilirim	2.67	1.46
Önlemler		
1. Bilgi sistemlerinde kullanılan virüs koruma yazılımını nasıl kullanacağımı biliyorum.	2.74	1.45
2. Taşınabilir cihazlara (portable devices) yönelik fiziksel güvenliği sağlamak ile ilgili dikkat edilmesi gereken konuları biliyorum.	2.84	1.33
3. Bilgisayarımdaki virüs koruma yazılımının gerçek zamanlı koruma (realtimeprotection) özelliğini kullanmaktayım.	2.90	1.46
4. USB sürücülerini kullanırken dikkat edilmesi gereken hususları biliyorum.	3.62	1.38
5. Taşınabilir cihazlara yönelik veri güvenliği ile ilgili dikkat edilmesi gereken konuları biliyorum.	3.25	1.41
6. Bilgisayarımdaki virüs koruma yazılımının otomatik güncelleştirme yapmasını sağlayabilirim	3.33	1.50

Tablo 6'ya göre, öğrencilerin bilgi güvenliği kazanımlarından; kimlik hırsızlığına karşı alınması gereken önlemler, USB sürücülerini kullanırken dikkat edilmesi gereken hususlar, taşınabilir cihazlara yönelik veri güvenliği ile ilgili dikkat edilmesi gereken konular ve bilgisayarlarındaki virüs koruma yazılımını kullanmalarında en yüksek ortalamaya sahip oldukları belirlenmiştir.

Tablo 7. Katılımcıların BGF Alt Boyutları Ortalamaları ve Standart Sapmaları

	X	*SS*
İnternet Güvenliği	20.69	5.26
Sosyal Medya Kullanımı	17.06	4.61
İnternet Tarayıcısı ve Ağ Güvenliği	11.70	3.70
Şifre Oluşturma	12.73	3.02
Sosyal Medya Tuzakları	12.51	3.42

Tablo 7'ye göre bilgi güvenliği farkındalığı puanlarında en yüksek ortalamanın İnternet Güvenliği ve Sosyal Medya Kullanımı alt gruplarında olduğu belirlenmiştir. Bunları takiben sırasıyla Şifre Oluşturma, Sosyal Medya Tuzakları, İnternet Tarayıcısı ve Ağ Güvenliği gelmektedir.

Önlisans öğrencilerinin bilgi güvenliği kazanımları ve bilgi güvenliği farkındalık puan ortalamalarının öğrenim görmekte oldukları programlara göre istatistiksel olarak anlamlı olup olmadığını tespit etmek amacıyla varyans (ANOVA) analizi yapılmıştır. Programlar arasındaki farkın hangi programlar arasında olduğunu bulmak için gruplar arası varyansları eşit ve örneklem sayısı farklı olduğundan Gabriel testi uygulanmıştır (Gayri, 2009). Test sonuçları Tablo 8'de verilmiştir.

Tablo 8. Öğrencilerin Öğrenim Gördükleri Programlara Göre BGK ve BGF Ortalamaları İçin Varyans Analizi Sonuçları

Değişken	*Değişim Kaynağı*	*Kareler Toplamı*	*SD*	*Kareler ortalaması*	*F*	*p.*	*Fark*
BGK	Guruplar arası	2561.53	6	426.923	2.210	.045*	Bilişim Güv.>Büro Yönt.
	Gruplar içi	29749.89	154	193.181			
	Toplam	32311.42	160				
BGF	Guruplar arası	3148.42	6	524.738	1.759	.111	
	Gruplar içi	45945.99	154	298.351			
	Toplam	49094.42	160				
Tehditler	Guruplar arası	803.59	6	133.933	2.135	.052	
	Gruplar içi	9658.82	154	62.720			
	Toplam	10462.42	160				
Önlemler	Guruplar arası	576.89	6	96.149	1.998	.069	
	Gruplar içi	7410.38	154	48.119			
	Toplam	7987.28	160				
İnternet Güvenliği	Guruplar arası	322.96	6	53.827	2.013	.067	
	Gruplar içi	4117.12	154	26.735			
	Toplam	4440.08	160				
Sosyal Medya Kullanımı	Guruplar arası	222.60	6	37.100	1.797	.103	
	Gruplar içi	3179.64	154	20.647			
	Toplam	3402.24	160				
İnternet Tarayıcısı ve Ağ Güvenliği	Guruplar arası	90.22	6	15.038	1.097	.367	
	Gruplar içi	2111.46	154	13.711			
	Toplam	2201.68	160				
Şifre Oluşturma	Guruplar arası	87.72	6	14.621	1.635	.141	
	Gruplar içi	1377.31	154	8.944			
	Toplam	1465.04	160				
Sosyal M. Tuzakları	Guruplar arası	95.99	6	15.999	1.387	.223	
	Gruplar içi	1776.21	154	11.534			
	Toplam	1872.21	160				

Tablo 8'e göre öğrencilerin BGK ortalamaları öğrenim gördükleri programlara göre farklılık göstermektedir (p=.45). Söz konusu farkın Bilişim güvenliği programı ile Büro yönetimi ve yönetici asistanlığı arasında Bilişim güvenliği program öğrencileri lehine olduğu bulunmuştur. Bilgi güvenliği farkındalığı, BGF ile BGK alt boyutları ortalama puanlarının programlara göre istatistiksel olarak farklılık göstermediği tespit edilmiştir (p>.05).

Önlisans öğrencilerinin BGF, BGK ile alt boyutları puanlarının öğrencilerin yaş gruplarına göre istatistiksel olarak farklılık gösterip göstermediğini belirlemek amacıyla Anova testi yapılmıştır. Post-Hoc analizi için Scheffe testi kullanılmıştır. Scheffe testi, gruplardaki gözlem sayılarının eşit olması varsayımını ihmal eden ve alfa hata payını kontrol altında tutabilen bir test türüdür (Scheffe, 1959). Bulgular Tablo 9'da verilmiştir.

Tablo 9. BGK, BGF ve Alt Boyutları Puanlarının Öğrencilerin Yaşına Göre ANOVA Sonuçları

Değişken	*Değişim Kaynağı*	*Kareler Toplamı*	*SD*	*Kareler ortalaması*	*F*	*p.*	*Fark*
BGK	Guruplar arası	1914.49	3	638.164	2.124	.099	
	Gruplar içi	47179.93	157	300.509			
	Toplam	49094.42	160				
BGF	Guruplar arası	607.40	3	202.468	1.003	.393	
	Gruplar içi	31704.02	157	201.936			
	Toplam	32311.42	160				
Tehditler	Guruplar arası	106.58	3	35.527	.539	.657	
	Gruplar içi	10355.84	157	65.961			
	Toplam	10462.42	160				
Önlemler	Guruplar arası	244.68	3	81.562	1.654	.179	
	Gruplar içi	7742.59	157	49.316			
	Toplam	7987.28	160				
İnternet Güvenliği	Guruplar arası	191.87	3	63.960	2.364	.073	
	Gruplar içi	4248.20	157	27.059			
	Toplam	4440.08	160				
Sosyal Medya Kullanımı	Guruplar arası	78.15	3	26.053	1.231	.301	
	Gruplar içi	3324.08	157	21.173			
	Toplam	3402.24	160				
İnternet Tarayıcısı ve Ağ Güvenliği	Guruplar arası	128.80	3	42.934	3.252	.023	20-21>24+
	Gruplar içi	2072.88	157	13.203			
	Toplam	2201.68	160				
Şifre Oluşturma	Guruplar arası	49.53	3	16.512	1.831	.144	
	Gruplar içi	1415.50	157	9.016			
	Toplam	1465.04	160				
Sosyal Medya Tuzakları	Guruplar arası	36.65	3	12.218	1.045	.374	
	Gruplar içi	1835.55	157	11.691			
	Toplam	1872.21	160				

Tablo 9'da görüldüğü gibi önlisans öğrencilerinin BGF İnternet Tarayıcısı ve Ağ Güvenliği alt boyut puanlarının öğrencilerin yaşlarına göre istatistiksel olarak önemli ölçüde farklılık gösterdiği belirlenmiştir. Söz konusu farkın 20-21 yaş grubu ile 24+ grubu arasında ve 20-21 yaş grubundaki öğrencilerin lehine olduğu belirlenmiştir. BGF ve diğer alt boyutları ile BGK ve alt boyutları ortalama puanlarının istatistiksel olarak yaşa göre önemli ölçüde farklılaşmadığı tespit edilmiştir.

Önlisans öğrencilerinin BGF, BGK ve alt boyutları ortalama puanlarının sınıf düzeylerine göre istatistiksel olarak farklılık gösterip göstermediğini tespit etmek amacıyla bağımsız gruplar t testi yapılmış, sonuçlar Tablo 10'da verilmiştir.

Tablo 10. *Önlisans öğrencilerinin BGF ve BGK ile alt boyut puanlarının sınıf düzeylerine göre T-testi sonuçları*

Ölçekler	*Sınıf*	*N*	*X*	*SS*	*t*	*p*
BGF	1.sınıf	121	74.91	18.06	.247	.805
	2.sınıf	40	74.12	15.96		
BGK	1.sınıf	121	39.53	14.07	1.732	.085
	2.sınıf	40	35.07	14.26		
Tehditler	1.sınıf	121	20.42	8.23	1.929	.055
	2.sınıf	40	17.60	7.31		
Önlemler	1.sınıf	121	19.11	6.83	1.276	.204
	2.sınıf	40	17.47	7.68		
İnternet Güvenliği	1.sınıf	121	21.01	5.05	1.348	.180
	2.sınıf	40	19.72	5.83		
Sosyal Medya Kullanımı	1.sınıf	121	16.96	4.63	-.484	.629
	2.sınıf	40	17.37	4.58		
İnternet Tarayıcısı ve Ağ Güvenliği	1.sınıf	121	11.81	3.58	.691	.491
	2.sınıf	40	11.35	4.09		
Şifre Oluşturma	1.sınıf	121	12.61	3.15	-.930	.354
	2.sınıf	40	13.12	2.58		
Sosyal Medya Tuzakları	1.sınıf	121	12.50	3.45	-.073	.942
	2.sınıf	40	12.55	3.34		

Tablo 10'a göre, önlisans öğrencilerinin BGF, BGK ve alt boyutları puanlarının sınıf düzeylerine göre istatistiksel olarak önemli ölçüde farklılık göstermediği tespit edilmiştir.

Tablo 11. Önlisans Öğrencilerinin BGF ve BGK İle Alt Boyut Puanlarının Bilgi Güvenliğine İlişkin Bilişim Suçlarını Bilme Durumuna Göre T-Testi Sonuçları

Ölçekler	*Sınıf*	*N*	*X*	*SS*	*t*	*P*
BGF	Evet	108	76.93	15.06	2.074	.041*
	Hayır	53	70.20	21.11		
BGK	Evet	108	41.86	14.53	4.648	.000*
	Hayır	53	31.43	10.60		
Tehditler	Evet	108	21.82	8.03	5.061	.000*
	Hayır	53	15.43	6.35		
Önlemler	Evet	108	20.03	7.24	3.527	.001*
	Hayır	53	16.00	5.86		
İnternet Güvenliği	Evet	108	21.37	4.55	2.353	.020*
	Hayır	53	19.32	6.30		
Sosyal Medya Kullanımı	Evet	108	17.41	4.00	1.372	.172
	Hayır	53	16.35	5.61		
	Evet	108	12.29	3.19	2.973	.003*

İnternet Tarayıcısı ve Ağ Güvenliği	Hayır	53	10.49	4.37		
Şifre Oluşturma	Evet	108	13.00	2.66	1.569	.119
	Hayır	53	12.20	3.62		
Sosyal M. Tuzakları	Evet	108	12.85	3.06	1.793	.075
	Hayır	53	11.83	3.99		

Tablo 11'e göre, önlisans öğrencilerinin bilgi güvenliği kazanımları ve alt boyutları ile bilgi güvenliği farkındalığı, internet güvenliği, internet tarayıcısı ve ağ güvenliği alt boyutlarına göre bilgi güvenliğine ilişkin bilişim suçları hakkında bilgi sahibi olanların lehine istatistiksel olarak farklılık gösterdiği tespit edilmiştir ($p<.05$) . Sosyal medya kullanımı, şifre oluşturma ve sosyal medya tuzakları alt boyutlarında istatistiksel olarak önemli ölçüde bir farklılık olmadığı belirlenmiştir ($p>.05$).

Tartışma ve Sonuç

Bu araştırmanın sonucunda önlisans öğrencilerinin bilgi güvenliği farkındalık düzeylerinin yüksek olduğu, bilgi güvenliği kazanım düzeylerinin ise orta olduğu görülmektedir. Öğrencilerin bilgi güvenliği kazanımlarından kimlik hırsızlığına karşı alınması gereken önlemler, USB sürücülerini kullanırken dikkat edilmesi gerekenler, taşınabilir aygıtlara yönelik veri güvenliğini sağlamak için dikkat edilmesi gerekenler ve bilgisayarlarındaki virüs koruma yazılımını kullanma konusunda bilgi sahibi oldukları belirlenmiştir. Bilgi güvenliği farkındalığı puanlarında en yüksek ortalamanın İnternet Güvenliği ve Sosyal Medya Kullanımı alt gruplarında olduğu belirlenmiştir. Bu faktörleri takiben sırasıyla Şifre Oluşturma, Sosyal Medya Tuzakları, İnternet Tarayıcısı ve Ağ Güvenliği'nin geldiği görülmektedir. Bu bağlamda önlisans öğrencilerinin bilgi güvenliği farkındalıkları yüksek olmasına rağmen bu konudaki tedbirler açısından yeterli bilgiye sahip olmadıkları söylenebilir. Avcı ve Oruç (2020) ile Göldağ (2021) çalışmalarında lisans öğrencilerinin bilgi güvenliği farkındalıklarının yüksek olduğunu bulmuşlardır. Buna paralel olarak, Erdoğmuş (2017) çalışmasında, lisans öğrencilerinin bilgi güvenliği farkındalıklarının "İnternet Güvenliği Farkındalığı" alt boyutunda en yüksek olduğunu tespit etmiştir. Bu bulguları destekler nitelikte olan, Rençber ve Mete'nin (2016) yapmış oldukları araştırmaya bakıldığında, bilgi güvenliğine yönelik tehditlere karşı oluşturulacak farkındalığı etkileyen faktörlerin sırasıyla şifre yönetimi, mobil internet kullanımı, e-posta, internet kullanımı ve sosyal ağ sitelerinin kullanımı bağlamındaki davranışlar olduğu belirtilmiştir. Karlov (2016)'nın insanların bilgi güvenliği farkındalığının olmadığını belirttiği çalışmasından bugüne gelindiğinde bilinç düzeyinde artış sağlandığını gösteren çalışmalar gelinen noktayı göstermektedir (Avcı & Oruç, 2020; Göldağ, 2021). Filippidis ve diğerleri (2018) çalışmalarında, öğrencilerin bilgi güvenliği farkındalığına sahip olsalar da bilgi güvenliğine dair teknik ve araçlar konusunda yeterli bilgiye sahip olmadıkları belirtmişlerdir. Bu bulgulardan yola çıkarak bilgi güvenliği konusundaki farkındalığın kendi başına yeterli olmadığı bununla birlikte teknik olarak korunma, savunma konularında da bilgi sahibi olunması gerektiği söylenebilir.

Önlisans öğrencilerinin BGK ortalamalarının öğrenim gördükleri programlara göre farklılık gösterdiği bulunmuştur. Buna göre Bilişim Güvenliği Programı öğrencilerinin genel olarak bilgi güvenliği bilgi düzeylerinin Büro Yönetimi ve Yönetici Asistanlığı Programı öğrencilerinden yüksek olduğu söylenebilir. Bilgi güvenliği farkındalığı ortalama puanları ile BGF ve BGK alt boyutları ortalama puanlarının da programlara göre istatistiksel olarak farklılık göstermediği bulgular arasında yer almaktadır. Buna göre hangi programda olursa olsun önlisans

öğrencilerinin bilgi güvenliği konusunda farkındalık sahibi oldukları ve tehlikelerin farkında olup bu tehlikelere karşı almaları gereken önlemler konusunda bilgi sahibi oldukları söylenebilir. Benzer çalışma yürütmüş olan Erdoğmuş (2017) İktisat ve İstatistik Bölümü öğrencilerinin BGF ortalama puanlarının diğer bölümlerde okuyan öğrencilere göre daha düşük olduğu, buna karşın en yüksek puan ortalamasının Uluslararası Ticaret ve Finans Bölümü öğrencilerine ait olduğunu belirtmiştir. Avcı ve Oruç'un (2020) yapmış oldukları çalışmada Mühendislik Fakültesi öğrencilerinin internet güvenliği ve bilgi güvenliği farkındalığı toplam puan ortalamalarının Eğitim Fakültesi öğrencilerine göre daha yüksek olduğu belirlenmiştir. Bu bulgular ışığında Bilişim Güvenliği Programı öğrencilerinin bilgi güvenliği kazanım düzeylerinin Büro Yönetimi ve Yön. Asis. Programında öğrenim gören öğrencilere nazaran yüksek olmasının bölümün bilgi ve iletişim teknolojileri ve güvenliğine yönelik dersleri alıyor olmalarından kaynaklandığı söylenebilir.

Yine çalışmanın sonucunda önlisans öğrencilerinin BGF İnternet Tarayıcısı ve Ağ Güvenliği alt boyut ortalama puanlarının öğrencilerin yaşlarına göre istatistiksel olarak anlamlı farklılık ortaya koyduğu belirlenmiştir. Buna göre 20-21 yaş grubundaki öğrencilerin 24 yaş ve üstündeki öğrencilere göre girdikleri web sitelerine ait bilgilerin çerezlerde tutulduğu, bu sırada herhangi bir ağdan paket dinleyicileri tarafından izlenebilecekleri ve sahte web sayfalarına yönlendirilme risklerinin farkında oldukları söylenebilir. Erdoğmuş'un (2017) çalışmasına göre ise 18-20 yaş grubunda bulunan öğrencilerin diğer yaş gruplarındaki öğrencilere göre BGF ve BGK ortalama puanlarının daha düşük olduğu, buna karşın 24 yaş ve üzeri olanların aynı ortalama puanlarından daha yüksek olduğu bulunmuştur. Canoğulları'nın (2021) öğretmenlere yönelik yaptığı çalışmasında 24-30 yaş aralığındakilerin lehine, 46 ve üzeri yaş üzerinin ise aleyhine farklılık olduğu tespit edilmiştir. Buna göre yaş ilerledikçe bilgi güvenliği farkındalığının azaldığı belirtilmiştir. Tüm bu bulgular ışığında bilgi güvenliği farkındalığının 24-30 yaş gruplarında daha yüksek düzeyde olduğu söylenebilir. Bir başka bulguya göre önlisans öğrencilerinin BGF, BGK ve alt boyutları ortalama puanlarının öğrencilerin sınıf düzeylerine göre farklılık göstermediği tespit edilmiştir. Erdoğmuş'a (2017) göre ise öğrencilerin sınıf düzeylerine bakıldığında, BGF'nin 3. ve 4. sınıflarda benzer fakat diğer gruplara göre daha yüksek olduğu, buna karşılık 1. sınıf öğrencilerinde BGF'nin diğer gruplarla kıyaslandığında en düşük seviyede olduğu tespit edilmiştir. Önlisans öğrencilerinde bilgi güvenliği kazanım ve farkındalıklarında sınıf düzeyinin etkisi olmamasına rağmen lisans öğrencilerinde üst düzey sınıflara doğru gidildikçe bilgi güvenliği farkındalıklarının arttığı ve daha etik oldukları söylenebilir (Filippidis ve diğerleri, 2018). 2021 yılında yapılan bir çalışmada önlisans ve lisans öğrencilerinin bilgi güvenliği hakkındaki bilgi düzeyleri ve farkındalıkları arasında bir fark olmadığı tespit edilmiştir (Göldağ, 2021). Bu veri de söz konusu bulguyu destekler niteliktedir. Bu bağlamda artık önlisans ve lisans düzeyindeki öğrencilerin farkındalık düzeyinin arttığı, kazanımlar noktasındaki eksikliklerin giderilmesi konusunda ise çalışmaların arttırılması gerektiği söylenebilir.

Önlisans öğrencilerinin bilgi güvenliği kazanımları ve alt boyutlarındaki ortalama puanları ile bilgi güvenliği farkındalığı, internet güvenliği, internet tarayıcısı ve ağ güvenliği alt boyutlarının ortalama puanlarına göre bilgi güvenliği kapsamındaki bilişim suçları hakkında bilgi sahibi olanların lehine istatistiksel olarak farklılık gösterdiği tespit edilmiştir ($p<.05$). Sosyal medya kullanımı, şifre oluşturma ve sosyal medya tuzakları alt boyutlarında istatistiksel olarak anlamlı bir farklılık olmadığı belirlenmiştir. Fakat bilgi güvenliğine ilişkin bilişim suçlarının bilincinde olan öğrencilerin bilgi sahibi olmayanlara göre sosyal medya ve şifre oluşturma dışındaki internet ağları ve güvenliği konusunda farkındalık ve kazanımlarının daha yüksek olduğu söylenebilir. Bu gibi suç unsurlarının bilincinde olmaları farkındalıklarının yüksek düzeyde olması bulgusunu da desteklemektedir. Aynı zamanda

Göldağ (2021) çalışmasında, öğrencilerin dijital araç kullanma düzeylerinin artmasıyla dijital okuryazarlık ve dijital veri güvenliği farkındalık düzeylerinin de arttığını tespit etmiştir. Bu da çalışmanın bulgusu ile örtüşmektedir.

Değişen ve gelişen teknolojik cihazların kullanımının ve bunlara duyulan ihtiyacın her geçen gün arttığı, neredeyse her ortamda ve kurumda kullanımının zorunlu hale gelmiş olduğu bilinmektedir. Buna paralel olarak öğrencilerin de her geçen gün değişen ve artan siber saldırılara maruz kalmaları olasılığı artmaktadır. Bu nedenle okudukları bölüm ve düzey fark etmeksizin öğrencilerin sanal ortamda bilgi paylaşımı, şifre oluşturma, olası oltalama ve sosyal mühendislik başta olmak üzere siber saldırılara yönelik alınması gereken tedbirler konusunda bilgilendirilmesi gerekmektedir. Bunu sağlamak üzere siber saldırı çeşitleri ve bunlardan korunma yollarını içeren seminer ve çevrimiçi içerik üretiminin arttırılması önerilmektedir. Öğrencilerin düzenlenen etkinliklere katılımını ve üretilen içerikleri takip etmesini teşvik etmek için afişlerden, kısa mesaj ve elektronik posta bildirimlerinden faydalanılabilir.

Aynı zamanda okullarda ilgili konuları içeren derslere yer verilmesi (Tekerek & Tekerek, 2013) ya da ilgili derslerin içeriklerinin güncellenmesi önerilmektedir. Bu çalışmaların öğrencilerde ya da bireylerdeki etkisini ortaya koyacak yeni çalışmalar ve bunun sonucunda söz konusu zafiyetlerindeki değişim oranlarını gösteren çalışmalar yapılabilir. İnternetin kullanım yaşının düştüğü göz önüne alındığında okul öncesi dönemden başlanarak bilgi güvenliği farkındalığı oluşturma çalışmalarına ihtiyacın arttığı söylenebilir. Bununla birlikte konunun hukuki boyutu hakkında bilgi verilmesi ve karşılaşılan tehditlerin bildirilmesi gereken kurum ve kuruluşların öğretilmesi de önem arz etmektedir.

Bu çalışma sadece Kırıkhan MYO bağlamında ele alınmasıyla sınırlandırılmıştır. Bu nedenle aynı düzeydeki öğrencilerin bulunduğu farklı üniversitelerde de benzer çalışmalar gerçekleştirilerek ülke bazında genel bir yargıya varılması sağlanabilir. Güncelliğini koruyan ve her geçen gün gelişen bir alan olması sebebiyle farklı gruplar üzerinde farklı yöntemler kullanılarak çeşitli çalışmalar gerçekleştirilebilir.

Yayın Etiği Bildirimi / Research Ethics

Bu çalışmada örneklem grubuna uygulanan veri toplama araçları hakkında bilgilendirme yapılmış, verilerin kullanım amacı açıklanmıştır. Katılımcılara dair kişisel bilgiler (ad, soyad gibi) istenmemiştir. Araştırmacıların bilgileri ve ulaşabilecekleri e-posta bilgisine yer verilmiştir. / In this study, information was given about the data collection tools applied to the sample group, and the purpose of using the data was explained. Personal information about the participants (such as name and surname) was not requested. The information of the researchers and the e-mail information they can reach are included.

Araştırmacıların Katkı Oranı / Contribution Rate of Researchers

Yazar her aşamayı tek başına gerçekleştirmiş ve yazmıştır. / The author performed and wrote each step alone.

Çıkar Çatışması / Conflict of Interest

Bu çalışmanın herhangi bir çıkar çatışması yoktur. / This study has no conflict of interest.

Fon Bilgileri / Funding

Bu çalışma için herhangi bir fon ya da destekleyen kurum bulunmamaktadır. / There is no funding or supporting institution for this study.

Etik Kurul Onayı / The Ethical Commitee Approval

Bu çalışma 2019-2020 güz döneminde, etik kurul izin belgesi zorunluluğu getirilmeden önce gerçekleştirildiğinden etik izin raporu bulunmamaktadır. / Since this study was carried out in the fall semester of 2019-2020, before the ethics committee permission document was required, there is no ethical permission report.

Kaynakça / References

Akgün, Ö.E., & Topal, M. (2015). Eğitim fakültesi son sınıf öğrencilerinin bilişim güvenliği farkındalıkları: Sakarya Üniversitesi eğitim fakültesi örneği. *SAÜ Eğitim Bilimleri Enstitüsü*. *5*(2), 98-121.

Akyol, E., & Uzun, Y., (2021). Bilgi ve iletişim teknolojisi dersi alan sağlık meslek yüksekokul öğrencilerinin bilişim güvenliği farkındalığı. *Ufuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *10*(19), 69-83.

Alotaibi, M., & Alfehaid, W. (2018). Information security awareness: A review of methods, challenges and solutions. *Proceedings of the ICITST-WorldCIS-WCST-WCICSS-2018*, Cambridge, UK, 10-13.

Al-Shehri, Y. (2012). Information security awareness and culture. *British Journal of Arts and Social Sciences*, *6*(1), 61-69.

Avcı, Ü., & Oruç, O. (2020). Üniversite öğrencilerinin kişisel siber güvenlik davranışları ve bilgi güvenliği farkındalıklarının incelenmesi. *Inonu University Journal of the Faculty of* Education *(INUJFE), 21*(1), 284-303. https://doi.org/10.17679/inuefd.526390

Bogart, K.J. (2012). Information security awareness: How to get users asking for more. Retrieved December 19, 2020, from https://silo.tips/download/information-security-awareness-how-to-get-users-asking-for-more

Canbek, G., & Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Journal of Polytechnic, 3*(9), 165-174.

Canoğulları, E. (2021). Öğretmenlerin bilgi güvenliği konusundaki farkındalıklarının incelenmesi. *Kalem Uluslararası Eğitim ve İnsan Bilimleri Dergisi, 11*(2), 651-679.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioural information society research. *Computer Security*, 32, 90-101. https://doi.org/10.1016/j.cose.2012.09.010

Demir, Ü. (2021). *Uluslararası güvenlik açısından ülkemizdeki bilgi güvenliği ve siber güvenlik eğitimlerinin mevcut durumunun incelenmesi.* İstanbul Rumeli Üniversitesi Uluslararası Güvenlik Sempozyumu, 25-26 Mart, İstanbul.

Efe, N. K. (2019). *Ondokuz Mayıs Üniversitesi öğretmen adaylarının bilgi güvenliği farkındalıklarının bazı değişkenler açısından incelenmesi*. [Yüksek lisans tezi]. Ondokuz Mayıs Üniversitesi.

Erdoğmuş, A. (2017). *Üniversite öğrencilerinin bilgi güvenliği kazanımları, farklılıkları üzerindeki etkilerinin analizi: Afyon Kocatepe Üniversitesi örneği* [Yüksek lisans tezi]. Afyon Kocatepe Üniversitesi.

Ersoy, A. F., & Ersoy, A. (2008). *İnternet ve çocuk hakları eğitimi*, VIII. Uluslararası Eğitim Teknolojileri Konferansı, Eskişehir, Türkiye.

Filippidis, A. P., Hilas, C. S., Filippidis, G., & Politis, A. (2018). *Information security awareness of greek higher education students-Preliminary findings.* 7th International Conference on Modern Circuits and Systems Technologies (MOCAST), IEEE, 1-4.

Gökmen, Ö. F., & Akgün, Ö. E. (2015). Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği bilgilerinin çeşitli değişkenlere göre incelenmesi. *Çukurova Üniversitesi Eğitim Fakültesi Dergisi,44*(1), 61-84.

Göldağ, B. (2021). Üniversite öğrencilerinin dijital okuryazarlık düzeyleri ile dijital veri güvenliği farkındalık düzeyleri arasındaki ilişkinin incelenmesi. *e-Uluslararası Eğitim Araştırmaları Dergisi, 12*(3), 82-100.44(1), 61-84.

Haeussinger, F. (2015). Studies on employees' information security awareness. Retrieved November 23, 2020, from https://ediss.uni-goettingen.de/bitstream/handle/11858/00-1735-0000-0022-6021-8/Dissertation_Haeussinger_FINAL.pdf?sequence=1

Hassandoust, F., & Techatassanasoontorn, A. A. (2020*). Understanding users' information security awareness and intentions: A full nomology of protection motivation theory.* In Cyber Influence and Cognitive Threats, (129-143). Academic Press.

Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2019). Security awareness: The first step in information security compliance behavior. *Journal of Computer Information Systems*, *61*(4), 345-356.

Kahraman, M. E. (2020). COVID-19 salgınının uygulamalı derslere etkisi ve bu derslerin uzaktan eğitimle yürütülmesi: Temel tasarım dersi örneği. *Medeniyet Sanat Dergisi*, *6*(1), 44-56. https://doi.org/10.1080/08874417.2019.1650676

Kalaycı, Ş. (2008). *SPSS Uygulamalı çok değişkenli istatistik teknikleri*. Asil Yayın Dağıtım, Ankara.

Kale, G. (2016). *Meslek yüksekokullarında bilgi güvenliği eğitimi ve önemi.* International Conference on Quality in Higher Education, Sakarya, Türkiye.

Korkmaz, E. V. (2018). Üniversite öğrencilerinin internet ve veri güvenliği farkındalıkları. *Journal of Social And Humanities Sciences Research (JSHSR*), *5*(25), 2222-2229.

Karlov, A. A. (2016). Virtualization in education: Information Security lab in your hands. *Physics of Particles and Nuclei Letters*, *13*(5), 640-643.

Korovessis, P. (2013). *Information security awareness in academia*: Governance, Communication, and Innovation in a Knowledge Intensive Society. 88-104, IGI Global.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers & Security, 28(7), 509- 520. https://doi.org/10.1016/j.cose.2009.04.006

Markelj, B., & Bernik, I. (2015). Safe use of mobile devices arises from knowing the threats, *Journal of Information Security and Applications, 20,* 84–89. https://doi.org/10.1016/j.jisa.2014.11.001

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior, 69*, 151-156. https://doi.org/10.1016/j.chb.2016.11.065

McIlwraith, A. (2006). *Information security and employee behaviour: How to reduce risk through employee education, training and awareness.* Gower Publishing, Ltd.:England.

Öztemiz, S., & Yılmaz, B. (2013). Bilgi merkezlerinde bilgi güvenliği farkındalığı: Ankara'daki üniversite kütüphaneleri örneği. *Bilgi Dünyası, 1*(14), 87-100. https://doi.org/10.15612/BD.2013.136

Pricewaterhouse Coopers. (2015). Key findings from the global state of information security survey 2016. Turnaround and transformation in cyber security, Retrieved December 20, 2020, from https://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf

Pro-G & Oracle. (2003). Bilişim güvenliği. Retrieved December 20, 2020, from https://docplayer.biz.tr/6090046-Bu-kitapcigin-hazirlanmasina-katkida-bulunan-oracle-turkiye-ye-tesekkur-ederiz.html

Rençber, Ö. F., & Mete, S. (2016). Bilgi güvenlik farkındalığını etkileyen faktörlerin belirlenmesi: Yüksekokul öğrencileri üzerine bir inceleme. *Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 18*(3), 800-823.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Scheffe, H. (1959). *The analysis of variance.* Wiley.

Šimandl, V., & Vaníek, J. (2017). Influences on ICT teachers' knowledge and routines in a technical e-safety context. *Telematics and Informatics, 34*(8), 1488-1502. https://doi.org/10.1016/j.tele.2017.06.012

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1): 31-41.

Sönmez,V. (2015). *Öğretim ilke ve yöntemleri*.(8. Baskı). Anı Yayıncılık.

Tabachnick, B. G., & Fidell, L. S. (2013). *Using multivariate statistics* (6th ed.). United States: Pearson Education.

Taha, N., & Dahabiyeh, L. (2020). College students information security awareness: a comparison between smartphones and computers. *Educ Inf Technol, 26,* 1721–1736. https://doi.org/10.1007/s10639-020-10330-0

Taylan, G. (2020). Okuryazarlık: Araçlar, metodolojiler, uygulamalar ve öneriler içinde *Dıjıtal eğitim amaçlı internet kullanımı*. Nobel Akademi Yayıncılık. Ankara. ISBN : 978-625-406-591-0

Tekerek, M., & Tekerek, A. (2013). Öğrencilerin bilgi güvenliği farkındalığı üzerine bir araştırma. *Turkish Journal of Education, 2*(3), 61-70.

TÜİK, (2020). Hanehalkı bilişim teknolojileri (BT) kullanım araştırması. https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2020-33679

Van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies, 123*, 29-39.

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security–what goes where?. *Information & Computer Security, 26*(1), 2-9.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102.

Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior, 27* (5), 591- 615. ttps://doi.org/10.1177/109019810002700506

Yılmaz, E., Şahin, Y., & Akbulut, Y. (2016). Öğretmenlerin dijital veri güvenliği farkındalığı. *Sakarya University Journal of Education, 6*,(2), 26-45. https://doi.org/10.19126/suje.29650