Mersin Üniversitesi Eğitim Fakültesi Dergisi - Mersin University Journal of the Faculty of Education

"Mersin Üniversitesi Eğitim Fakültesi Dergisi, 2019; 15(1): 186-215"
Araştırma Makalesi / DOI: 10.17860/mersinefd.437610

Öğrencilerin Siber Güvenlik Davranışlarının Beş Faktör Kişilik Özellikleri ve Çeşitli Diğer Değişkenlere Göre İncelenmesi*

Investigating Students' Cyber Security Behaviors in Relation to Big Five Personality Traits and Other Various Variables

Mehmet Fatih YİĞİT**, Süleyman Sadi SEFEROĞLU***

Öz: Bu çalışmanın amacı üniversite öğrencilerinin siber güvenlik davranışlarının beş faktör kişilik özellikleri ve cinsiyet, sınıf düzeyi, bölüm, bilişim güvenliği eğitimi alma durumu ve haftalık internet kullanım süresi değişkenlerine göre incelenmesidir. Çalışmaya farklı üniversite, bölüm ve sınıflardan 420 öğrenci katılmıştır. Verilerin toplanmasında Siber Güvenliği Sağlama Ölçeği, Beş Faktör Kişilik Özellikleri Ölçeği ve araştırmacılar tarafından geliştirilen Kişisel Bilgi Formu kullanılmıştır. Çalışma betimsel tarama modeline göre gerçekleştirilmiştir. Verilerin analizi Pearson korelasyon katsayısı, bağımsız örneklemler t-testi ve tek yönlü varyans analizi (ANOVA) gibi istatistiksel teknikler kullanılarak yapılmıştır. Çalışmadan elde edilen bulgular, öğrencilerin siber güvenlik davranış düzeylerinin kabul edilebilir bir seviyede olduğunu göstermiştir. Ayrıca öğrenciler kendilerini uyumlu, sorumlu ve deneyime açık kişiler olarak değerlendirirken, dışadönük ve nevrotik oldukları konusunda kararsız bir görüş bildirmişlerdir. Öğrencilerin siber güvenlik davranışları deneyime açıklık, sorumluluk, uyumluluk, nevrotiklik ve dışadönüklük olmak üzere tüm beş faktör kişilik boyutlarıyla anlamlı bir ilişki sergilediğini göstermiştir. Siber güvenlik davranışlarıyla en güçlü ilişkiye deneyime açıklık, en zayıf ilişkiye ise dışadönüklük kişilik özelliklerinin sahip olduğu tespit edilmiştir. Bunlara ek olarak, BÖTE ve bilgisayar programcılığı öğrencilerinin, sınıf düzeyi açısından 3. ve 4. sınıf öğrencilerinin, bilişim güvenliği eğitimi almış olan öğrencilerin ve haftalık 6-10 saat arası internet kullanan öğrencilerin siber güvenlik davranış düzeyleri bakımından daha yeterli oldukları bulunmuştur. Çalışma sonunda, ulaşılan bulgular ışığında siber güvenlik eğitimlerine ağırlık verilmesi ve öğrencilerin kişilik özelliklerinin bu eğitimlerde dikkate alınması önerilmiştir.
***Anahtar Kelimeler*:** Siber güvenlik, beş faktör kişilik özellikleri, üniversite öğrencileri, farkındalık

Abstract: The aim of this study is to examine the cyber security behaviors of university students according to the five factor personality traits and the variables such as gender, grade level, department, status of receiving information security training and weekly Internet usage. 420 students from different universities, departments and grade levels participated in the study. This study was conducted according to descriptive research model. The data were collected using Personal Information Form developed by the researchers, Personal Cyber Security Provision Scale and Big Five Personality Traits Scale. Pearson correlation coefficient, independent samples t-test and one-way analysis of variance (ANOVA) were used to analyze the data. Findings indicated that students' levels of cyber security behavior were at an acceptable level. Moreover, while students considered themselves as agreeable, conscientious, and open to experience, they remained neutral in deciding whether they were extroverted and neurotic. Furthermore, the students' cyber safety behaviors showed a significant relationship with all five-factor personality dimensions, namely, openness to experience, conscientiousness, agreeableness, neuroticism and extroversion. Openness to experience has been identified as the personality trait with strongest relationship with cyber security behaviors, whereas extroversion has the weakest. In addition, the students from CEIT and computer programming departments, those in the 3rd and 4th grades, those who received information security training and those using the internet 6-10 hours weekly were found to be more adequate in terms of cyber security behavior levels. At the end of the study, in the light of these findings, it was suggested to emphasize the cyber security trainings and to consider the personality traits of the students in these trainings.
***Keywords*:** Cyber security, big five personality traits, university students, awareness

*Bu çalışma 12. Uluslararası Bilgisayar ve Öğretim Teknolojileri Sempozyumu'nda sözlü bildiri olarak sunulan çalışmanın genişletilmiş halidir.

**Arş. Gör., Hakkari Üniversitesi, Eğitim Fakültesi, Hakkari-Türkiye, ORCID: 0000-0002-3476-7619, e-posta: mehmetfatihyigit57@gmail.com

***Prof. Dr., Hacettepe Üniversitesi, Eğitim Fakültesi, Ankara-Türkiye, ORCID: 0000-0002-5010-484X, e-posta: sadi@hacettepe.edu.tr

Gönderi Tarihi: 27.06.2018 - Kabul Tarihi: 28.03.2019

Giriş

Bilgi ve iletişim teknolojilerinin (BİT) çeşitli yönleriyle özellikle son yıllarda çok gelişmesi ve bireyler için ekonomik olarak daha kolay erişilebilir hale gelmesi, internetin tüm dünyada daha yaygın bir biçimde kullanımını beraberinde getirmektedir. Bilgiye erişim, bilgi paylaşımı, iletişim ve alışveriş gibi gündelik işleri kolay ve hızlı hale getirmesi ile internet, toplum için önemli bir ihtiyaç haline gelmiştir (Rahim, Hamid, Mat Kiah, Shamshirband ve Furnell, 2015). Bu konuda yapılan çeşitli araştırmalardan elde edilen veriler de internet kullanımının giderek hızlı bir şekilde büyüme gösterdiğini istatistiksel olarak ortaya koymaktadır. Örneğin 2018 yılı itibariyle tüm dünyada 4 milyardan fazla internet kullanıcısı olduğu belirtilmektedir (Internet World Stats, 2018). Öte yandan bazı uluslararası birimlere göre, 2017 yılında 1.5 milyardan fazla insan tarafından yaklaşık olarak 2.3 trilyon Amerikan doları çevrimiçi alışveriş gerçekleştirilmiştir (STATISTA, 2018). Türkiye'de ise TÜİK tarafından 2016 yılında gerçekleştirilen bilişim teknolojileri kullanımı araştırmasında, internet kullanan birey oranının artarak %61.2'ye yükseldiği, yaklaşık on hanenin sekizinde internet erişim imkânına sahip olunduğu, internet üzerinden alışverişin arttığı ve e-devleti kullanan bireylerin oranının önceki yıllara oranla artarak %61.8'e ulaştığı tespit edilmiştir (TÜİK, 2018).

İnternet her ne kadar toplum yaşamına çeşitli açılardan yararlar sağlasa da, insanların interneti kullanma sürecinde çeşitli risk ve tehditlerle karşılaşması da bir gerçeklik olarak kendisini hissettirmektedir. Özellikle internetin yapısı itibariyle, bireyler suç işleme konusunda kimliklerini daha rahat bir şekilde gizleyebilmekte ve bu sebeple internet üzerinden işlenen siber suçlar daha kolay ve yaygın bir hale gelebilmektedir (Moore, 2014). Dolayısıyla internet kullanan her bireyin çevrimiçi olarak işlenen bir takım suçların olumsuz etkilerine maruz kalabileceği söylenebilir (Chen, Beaudoin ve Hong, 2017).

İnternet kullanıcıları çevrim-içi ortamda çeşitli suç unsuru taşıyan çeşitli durumlarla ve tehditlerle karşılaşabilmektedirler. İnternet üzerinden maruz kalınan bu siber suç ve tehditlerin en yaygın bilinenleri; kötücül yazılım (malware) olarak adlandırılan virüs, solucan (worm), truva atları (trojans), casus yazılımlar (spyware) ve oltalama (phishing) ile yetkisiz erişim, kişisel bilgilerin ele geçirilmesi ve siber zorbalık gibi saldırılardır (Çakır ve Kesler, 2012; Çelen ve Seferoğlu, 2016; Mishna, Khoury-Kassabri, Gadalla ve Daciuk, 2012). Alanyazında bu tür siber saldırılara maruz kalınmasının ve bu saldırıların amacına ulaşarak olumsuz sonuçlara yol açmasının ardında insandan kaynaklı hataların önemli pay sahibi olduğu belirtilmektedir (Anwar, He, Ash, Yuan, Li ve Xu, 2017; Wagner ve Brooke, 2007; Yan ve diğerleri, 2018). Diğer bir ifadeyle e-ortam kullanıcılarının siber güvenlik konusundaki farkındalık düzeylerinin düşük olması, internet üzerinde gezinirken dikkatsiz ve ihmalkâr davranmaları, işlenen siber suçların gerçek hedefine ulaşarak insanlara zarar vermesine yol açabilmektedir. Bu sebeple, günümüzde yaygınlaşarak artan siber suçları engellemek ve bu suçların olası sonuçlarına maruz kalmamak için siber güvenlik konusuna dikkat çekilmesi büyük önem taşımaktadır (Furnell, 2008; Rahim ve diğerleri, 2015).

Siber güvenliği sağlamada teknolojinin gücünden yararlanarak teknoloji tabanlı önlemler alınabileceği gibi, siber güvenlik için öncelikli olarak insanlara siber güvenlik farkındalığının kazandırılması gerektiği de ifade edilmektedir (Keser ve Güldüren, 2015; Shaw Chen, Harris ve Huang, 2009). Bununla ilgili olarak alanyazında siber güvenlik konusunda "en zayıf halkanın" insan olduğu ve çok sayıda siber güvenlik saldırısı ve siber güvenlik açığının insan hatalarından kaynaklandığı belirtilmektedir (Öğütçü, Testik ve Chouseinoglou, 2016; Sasse, Brostoff ve Weirich, 2001). Diğer bir ifadeyle siber güvenlik için kullanılan teknoloji ne kadar gelişmiş olursa olsun, o teknolojiyi kullananın da insan olması ve siber saldırganların kullanılan güvenlik teknolojilerini aşma konusunda insan hatalarından da yararlanmak istemeleri, siber güvenliğin sadece teknolojik önlemlerle sağlanamayacağının bir göstergesi olarak değerlendirilebilir (Abawajy, 2014; Rezgui ve Marks, 2008). Dolayısıyla, kişisel ve kurumsal olarak siber güvenliği sağlamak ve siber tehdit risklerinin etkilerini en aza indirmek için insan faktörünün de göz önünde bulundurulması ve insanlara siber güvenlik farkındalığının kazandırılması için eğitimlerin düzenlenmesi önerilmektedir (Keser ve Güldüren, 2015; Standage, 2002).

Siber güvenlik konusunda insanın ön planda olması, siber güvenlik ile ilgili yapılan araştırmalarda insan özelliklerinin ele alınmaya başlanması sonucunu doğurmuştur (Hadlington, 2017). Bununla ilgili olarak siber güvenlik ile beraber cinsiyet (Gökmen ve Akgün, 2015), öz-

yeterlik (Thompson, McGill ve Wang, 2017), internet kullanım süresi (Akgün ve Topal, 2015) ve motivasyonel faktörler (Tsai, Jiang, Alhabash, LaRose, Rifon ve Cotten, 2016) gibi değişkenler incelenmiştir. Bu çalışmada ise siber güvenlik alanyazınında sınırlı sayıda çalışma içeren kişilik değişkeni (Egelman ve Peer, 2015) ele alınmıştır. Çalışma kapsamında kişilik değişkeninin incelenmek istenmesinin ardında sınırlı sayıda çalışma bulunmasının yanı sıra çeşitli diğer nedenler de bulunmaktadır. Öncelikle kişilik insan davranışlarını etkileyen temel özelliklerden birisidir (Kayış, Satıcı, Yılmaz, Şimşek, Ceyhan ve Bakioğlu, 2016). Bunun yanında alanyazında internet kullanım davranışlarının da kişilik özelliklerinden etkilendiği ileri sürülmektedir (Landers ve Lounsbury, 2006; Servidio, 2014; Uffen, Guhr ve Breitner, 2012). Bu nedenle, siber güvenlik ile internet kullanım davranışlarının ilişkili olduğu düşünüldüğünden, bu çalışmada kişilik değişkeninin siber güvenlik davranışları ile birlikte değerlendirilmesinin uygun olduğuna karar verilmiştir.

Alanyazında kişilik özelliklerinin değerlendirilmesinde Beş Faktör Kişilik Modeli (Five Factor Model) en çok kabul gören model olarak ele alınmaktadır (Landers ve Lounsbury, 2006; Lynam ve Miller, 2015; Pervin ve John, 2013). John ve Naumann (2010) yaptıkları incelemede 2010 yılı itibariyle Beş Faktör Kişilik Modeli'ni (BFKM) çalışmalarında dayanak olarak kullanan 3000'den fazla çalışmanın olduğunu ifade etmektedir. Bu sebeple, bu çalışma kapsamında da, kişilik özelliklerinin değerlendirilmesinde BFKM tercih edilmiştir. BFKM'ye göre kişilik özellikleri "Dışadönüklük (Extraversion), Uyumluluk (Agreeableness), Sorumluluk (Conscientiousness), Nevrotiklik (Neuroticism) ve Deneyime Açıklık (Openness to Experience)" şeklinde beş boyut altında toplanmaktadır (Goldberg, 1990).

Bu çalışmada öğrencilerin siber güvenlik davranışlarıyla kişilik özellikleri arasındaki ilişki incelenmiştir. Bunun yanı sıra, siber güvenlik davranışlarının cinsiyet, sınıf düzeyi, bölüm, bilişim güvenliği eğitimi alma durumu ve haftalık internet kullanım süresine göre farklılaşma durumu da araştırılmıştır. İnterneti en fazla kullanan ve internet risklerine en fazla maruz kalan bireylerin 18-30 yaş grubundaki bireyler olduğundan (Öğütçü, Testik ve Chouseinoglou, 2016) hareketle, çalışma ön lisans ve lisans öğrencileriyle gerçekleştirilmiştir.

Siber tehditler

İnternetin gelişmesi ve yaygınlaşmasıyla birlikte, bu aracı öğrenme ve iletişim gibi yararlı eylemler için kullananların yanı sıra, uygunsuz bir biçimde çıkar elde etme amacını taşıyarak etik dışı kullananların sayısı da her geçen gün artmaktadır. Bu tür yanlış kullanımlar bilişim suçları ya da siber suçlar olarak adlandırılmaktadır. Türk Ceza Kanunu'nda bilişim veya siber suçlar bir bilişim sistemine girme, sistemi engelleme, bozma, sistemdeki verileri yok etme veya değiştirme, banka veya kredi kartlarının kötüye kullanılması olarak sınıflandırılmıştır (TCK, 2018). İnternetin bu şekilde kötü niyetli olarak kullanılması sonucunda insanlar çeşitli siber tehditlere maruz kalabilmekte ve bu tehditlerin olumsuz sonuçlarından etkilenebilmektedirler. Siber tehditler geniş bir çerçevede, bireyleri veya kurumları hedef alarak onların savunmasızlıklarından faydalanmak suretiyle birey veya kurumlara ait varlıkları ele geçirme ve kötüye kullanma durumu şeklinde tanımlanmaktadır (NICCS, 2018).

Siber tehditler genel olarak insan ve teknoloji kaynaklı olarak iki şekilde gerçekleştirilmektedir (Pagani, 2005). Diğer bir ifadeyle, siber tehditler çeşitli teknolojik araçların kullanılmasıyla gerçekleştirilebildiği gibi, herhangi bir teknolojiden yararlanmaksızın doğrudan insanların zayıf noktalarını kullanarak da gerçekleştirilebilmektedir. İnsan odaklı siber tehditlerin en bilineni "Nijerya Dolandırıcılığı" olarak adlandırılmaktadır. Bu dolandırıcılık türünü kullanan kişiler birçok kişiye e-posta göndererek, Nijerya'da zengin bir tanıdığının vefat ettiği, arkasında büyük meblağda para bıraktığı ancak bu parayı güvenlik gerekçesiyle ülke dışına çıkaramadığı ve kullanamadığı senaryosu üzerinden hareket etmektedir. Paranın ülke dışına çıkarılıp kullanılabilmesi için paranın ulaşılan kişilerin banka hesabına transfer edilmek istendiği ve eğer kabul edilirse bu paradan o kişiye de pay verileceği belirtilmektedir. Daha sonra para transferi işleminde yardımcı olabileceğini söyleyen kişiden yapılacak para transferi için havale masrafı adı altında bir miktar para talep edilmektedir. Büyük miktarlarla ifade edilen bu paralardan pay alabileceği şeklindeki vaade inanan insanlar kendilerinden havale ücreti adı altında alınan bu paralarla dolandırılmaktadırlar (Hekim ve Başıbüyük, 2013). Buna benzer dolandırma türleri alanyazında sosyal mühendislik (social engineering) olarak da ifade edilmektedir. Sosyal

mühendislik temel olarak insanları psikolojik hilelerle kandırarak kendilerine ait bilgi ve kaynakları ele geçirme şeklinde tanımlanmaktadır (Peltier, 2006).

Bir diğer siber tehdit türünde ise çeşitli teknolojik araçlar aracılık etmektedir. Bu teknolojik araçlar kötü amaçlar için kullanıldığından kötücül yazılımlar olarak da isimlendirilmektedir. Bu şekildeki teknolojik yazılımlar genellikle virüs, solucan, truva atı, casus yazılım gibi türlerde kendilerini göstermektedir (Kaspersky, 2018). Kaspersky Lab (2017) raporuna göre, 2017 yılı içinde 1 milyardan fazla kötücül yazılım ile karşılaşıldığı belirtilmektedir. Kötücül yazılımlar genel olarak gönderilen bir e-posta bağlantısının açılmasıyla ya da "Tebrikler para kazandınız" veya "Sisteminizde virüs var, temizlemek için anti virüs programını indirin" gibi ifadelerle kullanıcıların kandırılması yoluyla sisteme bulaşmaktadır. Bunun sonucunda insanların bilgi ve para gibi kaynakları ele geçirilmekte veya tahrif edilmektedir (Sithira ve Niguwi, 2014). Teknoloji kullanılarak gerçekleştirilen diğer bir tehdit ise oltalama olarak bilinen tehdittir (Bkz. Şekil 1). Sık olarak rastlanan oltalama saldırılarında, sahte ancak inandırıcı ve insanların şüphe etmeyecekleri şekilde bir arayüzün tasarlanması ve insanların bu arayüze kimlik ya da banka bilgilerini girmesi söz konusudur (Abbasi ve diğerleri, 2010). Bu şekilde ele geçirilen bilgiler sonucunda insanlar maddi ve manevi kayıplarla karşı karşıya kalabilmektedirler. Bununla birlikte yaşanan kayıplar sadece kişileri değil, kurumları da etkilemektedir (Parrish, Bailey ve Courtney, 2009). Çeşitli kurumlarda çalışan insanların maruz kaldıkları siber saldırılar sonucunda, kurumsal kaynakların da tehlikeye girmesi ve özellikle ekonomik anlamda sıkıntılarla karşılaşılması söz konusu olabilmektedir (Shropshire ve diğerleri, 2006). Yapılan araştırmalarda kurumların siber saldırılar sonucunda milyonlarca dolar zarara uğradığı tespit edilmiştir (Coopers, 2013; Leszczyna, 2013).

Şekil 1. Siber tehditlere örnekler

Siber güvenlik

Alanyazında bahsedilen siber tehditler incelendiğinde teknolojik yetersizlikten çok insan hatalarının ön planda olduğu görülmektedir (Mamanov ve Benbunan-Fich, 2018). Örneğin, Nijerya Dolandırıcılığında bazı insanların psikolojik olarak karşıdakine kolayca inanma durumu bulunmaktadır. Kötücül yazılım ya da oltalama ile gerçekleştirilen saldırılarda da insanların siber güvenlik ile ilgili bilgilerinin yetersiz olması sonucunda yaptıkları hata ve ihmaller söz konusudur. Dolayısıyla, siber tehditlerin engellenmesi açısından birey merkezli siber güvenlik önlemlerinin alınması gerekmektedir.

Siber güvenlik, kişi ve kurumların ve bunlara ait bilgi ve kaynakların siber ortamdan gelen tehditlere karşı korunmasını içeren teknolojik uygulamalar ve sahip olunan yetenekler olarak tanımlanmaktadır (NICCS, 2018). Tanımdan da anlaşılacağı üzere, siber güvenliğin tanımında son yıllarda insan faktörü de göz önüne alınmakta ve sadece teknolojik uygulamaların değil, insana özgü yeteneklerin de siber güvenlik için gerekli olduğu vurgulanmaktadır (Yan ve

diğerleri, 2018). Goodrich ve Tamassio (2011) siber güvenliğin sağlanabilmesini "gizlilik (confidentiality), bütünlük (integrity) ve erişilebilirlik (availability)" şeklinde 3 boyutta ele almıştır. *Gizlilik*, bilgilerin sadece bilginin sahibi veya ilgili kişilerce erişilebilmesi anlamına gelmektedir. *Bütünlük*, bilginin hâlihazırda var olan yapısının değiştirilmeden, bozulmadan ve yok edilmeden saklanması şeklinde ifade edilmektedir. *Erişilebilirlik* ise bilginin ilgili kişiler tarafından gerektiğinde ulaşılabilir bir durumda olması anlamını taşımaktadır. Sözü edilen üç özellik siber güvenlikten bahsedilebilmesi için birer öncül olarak değerlendirilebilir.

Alanyazında bireylerin siber güvenlik davranışlarını ve düzeylerini ele alan çeşitli çalışmalar bulunmaktadır. Bu çalışmaların bulguları incelendiğinde, bireylerin genellikle siber güvenlik konusunda istenilen düzeyde olmadıkları tespit edilmiştir. Örneğin, Gökmen ve Akgün (2015) Bilgisayar ve Öğretim Teknolojileri Eğitimi bölümündeki öğretmen adaylarının bilişim güvenliği ile ilgili bilgi düzeylerini belirlemeye yönelik bir çalışma gerçekleştirmiştir. 375 katılımcının bulunduğu çalışmada, öğretmen adaylarının bilişim güvenliği bilgi düzeylerinin düşük olduğu tespit edilmiştir. Ayrıca bilişim güvenliği bilgilerinin cinsiyete göre farklılaştığı, yaş, sınıf, bilgisayara sahip olma yılı, günlük bilgisayar ve internet kullanım süresi ve bilişim güvenliğine dayalı bir eğitim alma durumlarına göre farklılaşmadığı belirlenmiştir. Tekerek ve Tekerek (2013) ilköğretim ve lise öğrencilerinin bilgi ve bilgisayar güvenliği farkındalık düzeylerini incelemiştir. 2449 öğrenciye uygulanan bir ölçek aracılığıyla toplanan veriler, öğrencilerin etik konulardaki bilgi güvenlik düzeylerinin yeterli olduğunu, buna karşın kural ve bilgi gerektiren konulardaki bilgi güvenlik düzeylerinin düşük olduğunu göstermektedir. Buna ek olarak, elde edilen sonuçlar genel olarak kız öğrencilerin bilgi güvenliği açısından farkındalıklarının daha yüksek olduğunu ve sınıf düzeyi arttıkça bilgi güvenliği farkındalığının da arttığını göstermektedir.

Karaoğlan Yılmaz, Yılmaz ve Sezer (2014) çalışmalarında üniversite 1. sınıf öğrencilerinin bilgi güvenliğine ilişkin davranışlarını incelemişlerdir. 124 öğrenciden nicel ve nitel olarak toplanan verilerin öğrencilerin bilgisayara erişim güvenliği, kötücül yazılımlar ve bu yazılımlardan korunma yolları, yedekleme yapma, parola güvenliği, ağ güvenliği, dosya erişim ve paylaşım güvenliği ve e-posta güvenliği konularında yeterli düzeyde önlem almadıklarını göstermiştir. Bir başka araştırmada ise üniversite öğrencilerinin siber güvenlik davranışları incelenmiştir (Karacı, Akyüz ve Bilgici, 2017). 170 öğrencinin katıldığı çalışmanın sonuçlarına göre, öğrencilerin siber güvenlik davranışlarının yeterli düzeyde olduğu tespit edilmiştir. Siber güvenlik alt boyutlarına göre incelendiğinde ise öğrencilerin kişisel ve ödeme bilgilerini koruma, güvenilmeyen uygulamalardan kaçınma ve iz bırakmama konularında yeterli düzeyde siber güvenlik bilgisine sahip oldukları belirlenmiştir. Buna ek olarak, siber güvenlik davranışları bağlamında cinsiyet ve sınıf düzeyi açısından herhangi bir fark gözlenmezken, bilişim güvenliği eğitimi alma konusunda eğitim alanların lehine bulgulara erişilmiştir.

Pusey ve Sadera (2011) öğretmen adaylarının bilişim güvenliği ve bilişim etiği konularını bilme ve bu konuları öğretebilme algılarını inceleyen bir çalışma gerçekleştirmişlerdir. 318 katılımcıdan toplanan veriler sonucunda, öğretmen adaylarının bilişim güvenliği bilişim etiği konularını bildikleri ancak bunları öğretme noktasında yeterince hazır olmadıkları tespit edilmiştir. Akgün ve Topal (2015) eğitim fakültesi son sınıfa kayıtlı öğrencilerin bilişim güvenliği farkındalıklarını inceleyen bir çalışma gerçekleştirmiştir. 217 öğrenciden araştırmacılar tarafından geliştirilen bir anket ile toplanan veriler öğrencilerin önemli bir kısmının yeterli düzeyde bilişim güvenliği farkındalığına sahip olmadıklarını göstermiştir. Buna ek olarak, cinsiyet ve ortalama bilgisayar ve internet kullanım sürelerinin siber güvenlik farkındalığı üzerinde anlamlı bir etkisi gözlenirken, bilişim güvenliği eğitimi alma durumunun herhangi bir etkiye sahip olmadığı saptanmıştır. Bir diğer çalışmada üniversite öğrencilerinin siber güvenlik farkındalık düzeyleri incelenmiştir (Subramaniam, 2017). 318 öğrencinin katıldığı çalışma sonunda öğrencilerin siber güvenlik farkındalıklarının orta düzeyde olduğu saptanmıştır. Ayrıca siber güvenlik farkındalık düzeyleri üzerinde cinsiyet ve bilgisayar kullanım süresinin anlamlı bir etkisinin olmadığı ortaya çıkmıştır. Bir başka çalışmada ise lisans öğrencilerinin siber güvenlik ile ilgili doğru karar alma davranışları incelenmiştir (Yan ve diğerleri, 2018). 462 öğrenci ile gerçekleştirilen çalışma sonunda öğrencilerin siber güvenlik ile ilgili doğru karar verme ortalamalarının %65 olduğu tespit edilmiştir. Buna ek olarak, 104 öğrencinin %50 gibi bir düzeyde doğru karar verebildikleri bulgusu edinilmiştir.

Siber güvenlikle ilgili alanyazın incelendiğinde, birçok çalışmada siber güvenlik düzeyine ilişkin olumsuz nitelikli bulgulara erişilmiş olduğu ancak az sayıda da olsa olumlu bulgulara ulaşılan çalışmaların bulunduğu anlaşılmaktadır. Buna ek olarak, siber güvenlik düzeyi üzerinde etkisi araştırılan cinsiyet, sınıf düzeyi, internet kullanım süresi ve siber güvenlik eğitimi alma durumu gibi değişkenlerle ilgili olarak da tutarsız bulgulara rastlamak mümkündür. Bu sebeple, bu değişkenlerin siber güvenlik bağlamındaki etkisinin açığa kavuşturulması amacıyla tekrar incelenmesinin gerekli olduğu düşünülerek, bu çalışmada söz konusu değişkenlere yer verilmiştir.

Yapılan çalışmalarda siber güvenlikle ilişkili olduğu düşünülen birey merkezli değişkenler olarak cinsiyet (Anwar ve diğerleri, 2017), öz-yeterlik, algılanan savunmasızlık, öznel norm (Thompson, McGill ve Wang, 2017), kontrol algısı (Anderson ve Agarwal, 2010), kişisel sorumluluk, önceki bilgiler ve müdahale stratejileri (Shillair, Cotten, Tsai, Alhabash, LaRose ve Rifon, 2015), bilgisayar ve internet kullanım süresi (Gökmen ve Akgün, 2015) ve bilişim eğitimi alma durumları (Karacı, Akyüz ve Bilgici, 2017) gibi değişkenlerin ele alındığı göze çarpmaktadır. Bunlara ek olarak, siber güvenlik konusunun insanların davranışlarında pay sahibi olduğu ileri sürülen kişilik değişkeni bağlamında da incelenmesinin araştırmacılar tarafından önerildiği ve özellikle son yıllarda bu konunun çalışılmaya başlandığı görülmektedir (Gratian ve diğerleri, 2018; McCormac ve diğerleri, 2017).

Kişilik özellikleri

Bireylerin belli bir durum karşısındaki davranış biçimleri, tepkileri ve algıları farklılık gösterebilmektedir. Bireylerdeki bu tür farklılıkların altında yatan sebeplerden biri olarak kişilik özellikleri gösterilebilir (Gustavsson, Jönsson, Linder ve Weinryb, 2003). Kişilik kavramı insanların düşünme, hissetme ve davranma konularında birbirlerinden farklılaşmasına katkı sağlayan göreceli olarak kalıcı psikolojik nitelikler olarak tanımlanabilir (Pervin ve John, 2013). Tanımdan da anlaşılacağı üzere bir kişilik özelliğinden bahsedilebilmesi için insanları birbirinden ayırt etmesi ve farklı zaman ve durumlarda tutarlılık gösteren nispeten kalıcı psikolojik özellikler olması gerekmektedir. Bununla birlikte kişilik özellikleri bireyin yaşamında tamamen kalıcı bir özellik olmayıp, çeşitli müdahaleleri içeren uzun süreçler sonunda değişiklik gösterebilen bir psikolojik yapıdır (Roberts, Luo, Briley, Chow, Su ve Hill, 2017). Örneğin, içine kapanık bir birey zaman içinde gelişen süreçler sonucunda dışadönük bir karaktere sahip olabilmektedir.

Kişilik ile ilgili alanyazında, kişilik özelliklerinin ölçülmesi ve ortaya konmasında kullanılan çeşitli modeller bulunmaktadır. Yapılan çalışmalarda en yaygın olarak kullanılan modellerden birisi Beş Faktör Kişilik Modeli (BFKM) olarak bilinen modeldir (Pervin ve John, 2013). BFKM'ye göre kişilik özellikleri birbirinden bağımsız beş boyut altında toplanmaktadır. Bu boyutlar dışadönüklük, uyumluluk, sorumluluk, nevrotiklik ve deneyime açıklık olarak adlandırılmaktadır (Bkz. Şekil 2). Sözü edilen kişilik boyutları bireylere ait çeşitli kişilik özelliklerinin faktör analizi ile gruplandırılması yoluyla daha "geniş" bir kategori altında toplanması sonucunda ortaya çıkmıştır (McCrae ve John, 1992). Her boyutta alınan puanın düzeyi, bireyin o boyuttaki kişilik ile ilgili durumunu belirtmektedir. Örneğin, dışadönüklük boyutunda yüksek puana sahip bir birey "dışadönük" olarak nitelendirilirken, düşük puan alan bir birey "dışadönük olmayan" veya "içedönük" kimse olarak tanımlanmaktadır.

Dışadönüklük bireylerin yoğun bir biçimde sosyal etkileşim içinde olmaları ve kendine güven ve rekabet içinde hareket edebilmeleri olarak tanımlanmaktadır (McCrae ve Costa, 1987). Dışadönük kimseler enerjik, aktif, heyecan arayan, sıcakkanlı kişilik özelliklerini taşımaktadır (Buckley ve Doyle, 2017; Smidt, 2015). Bunun tam tersi olarak içedönük bireyler ise genellikle utangaç, pasif, yalnızlığı seven, risk ve heyecan aramayan kimselerdir (Ayduk, Mendoza-Denton, Mischel, Downey, Peake ve Rodriguez, 2000; Floros ve Siomos, 2014). Dışadönük bireyler insanlarla etkileşim kurmayı ve sosyal etkinlikleri severken, içedönük bireyler yalnız vakit geçirmeyi tercih etmektedirler (Karim, Zamzuri ve Nor, 2009).

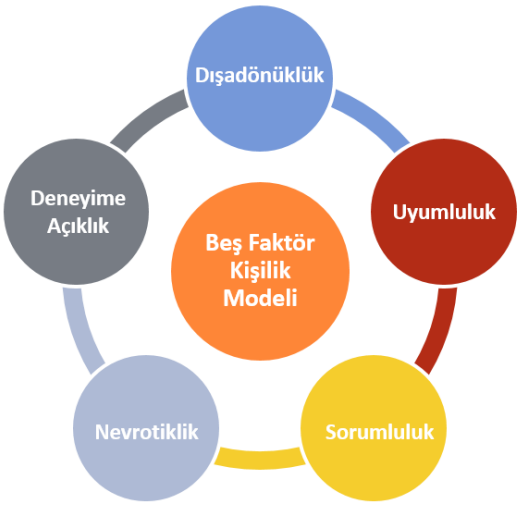
Öte yandan uyumluluk boyutu kişiler arası ilişkilerde ön plana çıkan bir boyuttur (McCrae ve Costa, 1987). Uyumlu olarak nitelendirilebilecek kimselerin kişilik özellikleri incelendiğinde, bu kimselerin makul, anlaşılması kolay, işbirliğine yatkın, hoşgörülü ve karşıdakini düşünen kimseler olduğu belirtilmektedir (Buckley ve Doyle, 2017; Smidt, 2015).

Uyumlu olmayan kişiler ise daha çok kendini düşünen, karşıdakine güvenmeyen, işbirlikçi olmayan ve tartışma çıkaran kişilerdir (Buckley ve Doyle, 2017).

BFKM'deki bir başka boyut olan sorumluluk boyutu ise bireylerin planlı, düzenli ve disiplinli olma, kurallara uyma ve sıkı çalışma durumlarını yansıtan bir boyuttur (Costa ve McCrae, 1992). Sorumluluk kişiliğine sahip kimseler disiplinli, kurallara uyan, düzenli, başarı odaklı, düzeni ve plan yapmayı seven kimselerdir (Buckley ve Doyle, 2017; Lounsbury ve Gibson, 2009). Bununla birlikte sorumluluk düzeyi düşük olan bireyler ise başarı aramayan, dağınık ve görevleri erteleme eğiliminde olan bireylerdir (Karim, Zamzuri ve Nor, 2009).

Nevrotiklik bireyin duygusal anlamda bir dengesizlik yaşaması durumu ile ilişkili bir kişilik boyutudur (McCrae ve Costa, 1997). Nevrotik bireyler öfkeli, stresli, tedirgin, düşük öz-güvene sahip, üzgün ve olumsuz durumlarla baş etmekte güçlük yaşayan bireylerdir (Buckley ve Doyle, 2017; Floros ve Siomos, 2014). Nevrotikliğin zıttı olan duygusal dengelilik özelliğine sahip kimseler ise rahat, sakin, stresle başa çıkabilen ve öz-güven sahibi kimselerdir (John ve Gross, 2004; Lounsbury ve Gibson, 2009).

Son olarak deneyime açıklık ise yeni duygu ve düşüncelere açık olma ve geleneksellikten kaçınma ile ilgili bir kişilik boyutudur (Smidt, 2015). Deneyime açık bireyler yeniliği arayan, açık fikirli, meraklı, entelektüel, esnek ve hayal gücüne sahip bireylerdir (Buckley ve Doyle, 2017; Chong, Teh ve Tan, 2014). Diğer taraftan, deneyime açık olmayan kimseler ise geleneksel, yeniliğe kapalı, tekdüzeliği seven ve entelektüel girişimleri düşük kimseler olarak tanımlanmaktadır (Costa ve McCrae, 1992; Glass, Prichard, Lafortune ve Schwab, 2013).



Şekil 2. Beş faktör kişilik modeli

Kişilik özelliklerinin bireylerin davranışlarına yansımaları

Kişilik özelliklerinin bireyin davranışlarında önemli bir etkisinin olduğu belirtilmektedir (Costa ve McCrae, 1992). Bununla ilgili olarak alanyazında kişilik özelliklerinin okula devam etme (Lounsbury, Steel, Loveland ve Gibson, 2004), oyun bağımlılığı, şiddet (Kim, Namkoong, Ku ve Kim, 2008), internet bağımlılığı (Kayış ve diğerleri, 2016), siber zorbalık (Pabian, De Backer ve Vandebosch, 2015) ve madde bağımlılığı (Sussman, McCuller ve Dent, 2003) gibi davranışsal değişkenler üzerinde etkili olduğu ifade edilmektedir.

Alanyazında kişilik özelliklerinin siber güvenlik, siber güvenlik davranışları ve bilgi güvenliği bağlamlarında ele alındığı çalışmalar da bulunmaktadır. Dört ülkeden katılımcılar ile gerçekleştirilen bir çalışmada kişilik özelliklerinin siber güvenlik üzerindeki etkisi incelenmiştir (Halevi, Memon, Lewis, Kumaraguru, Arora, Dagar ve Chen, 2016). Çalışma sonunda beş faktör kişilik özelliklerinden sadece sorumluluk boyutunun siber güvenlik üzerinde anlamlı bir etkisinin olduğu bulgusuna ulaşılmıştır. Warrington (2017) ise bir işte çalışmakta olan 18 yaşından büyük katılımcılar ile siber güvenlik konusunda bir çalışma gerçekleştirmiştir. Bulgular beş faktör kişilik özelliklerinin dosya koruma davranışlarını anlamlı bir biçimde etkilediğini göstermiştir. Halevi, Lewis ve Memon (2013) beş faktör kişilik özellikleri ile oltalama saldırılarına maruz kalma arasındaki ilişkiyi inceleyen bir çalışma yürütmüştür. Çalışma sonuçlarına göre nevrotiklik kişilik

özelliği baskın olan bireylerin oltalama saldırılarına maruz kalma olasılığının anlamlı bir biçimde daha yüksek olduğu tespit edilmiştir. Bir diğer çalışmada siber güvenlik davranış niyeti ile beş faktör kişilik özellikleri arasındaki ilişki incelenmiştir (Gratian, Bandi, Cukier, Dykstra ve Ginther, 2018). Çalışma sonunda dışadönüklük özelliğinin cihaz koruma davranışı ile sorumluluk özelliğinin ise parola kullanımı ve sistem güncelleştirilmesi davranışları ile anlamlı bir ilişkisinin olduğu saptanmıştır.

Araştırmanın önemi

İnternet, sunduğu hizmetler ve çeşitli diğer imkânlar nedeniyle toplumsal yaşam için vazgeçilmez bir teknoloji konumundadır. Öte yandan, İnternet yapısı itibariyle kötü amaçlı kullanımlar konusunda da sıkça tercih edilen ve türlü riskleri barındıran bir teknolojidir. İnternet üzerinden işlenen siber suçlar ve karşılaşılan siber tehditler sonucunda birçok kurum ve kişi başta ekonomik olmak üzere çeşitli zararlara maruz kalabilmektedir. İnternet üzerinden karşılaşılan riskler ve bu riskli durumların doğurduğu sonuçlar incelendiğinde, bu risklere maruz kalma konusunda insandan kaynaklı hata ve ihmallerin önemli bir payı olduğu anlaşılmaktadır (Öğütçü, Testik ve Chouseinoglou, 2016). Bunun en başta gelen sebebi olarak insanların siber güvenlik konusundaki farkındalık ve bilgi düzeylerinin düşük olması gösterilmektedir. Dolayısıyla siber güvenlik konusunda teknolojik yatırımlar ile alınabilecek önlemlerin yanı sıra bireylere siber güvenlik farkındalığının kazandırılmasının ve bu farkındalığı etkileyebilecek bireye dayalı özelliklerin ortaya konmasının önemli olduğu söylenebilir (Hadlington, 2017; Keser ve Güldüren, 2015).

Alanyazında siber güvenlik ve kişilik özelliklerini ele alan az sayıda çalışma bulunmaktadır. Bu bağlamda yapılan çalışmalarda, siber güvenlik olarak ele alınan yapının çalışmalar arasında farklılık gösterdiği de görülmektedir. Bazı çalışmalarda siber güvenlik olarak sadece dosya koruma veya cihaz koruma davranışları incelenirken, bazılarında ise oltalama saldırılarından kaçış davranışları ele alınmıştır. Bu çalışmada ise farklı olarak, siber güvenlik davranışları daha kapsamlı ve farklı yapılar altında incelenmektedir. Ayrıca kişilik özelliklerinin siber güvenlik davranışlarıyla olan ilişkilerinde de tutarlı bulgulara erişilmediği ve bundan dolayı bu konuda ek çalışmalara gereksinim olduğu düşünülmektedir. Bunun yanında Türkiye bağlamında kişilik özellikleri ve siber güvenlik davranışlarını birlikte ele alan bir çalışmaya da rastlanamamıştır. Bu sebeplerden dolayı, bu çalışmada özellikle ulusal alanyazına katkı sağlayacağı düşünülerek siber güvenlik davranışlarının beş faktör kişilik özellikleri bağlamında incelenmesine karar verilmiştir. Bu çalışma ile bireylerin siber güvenlik davranışlarında hangi kişilik özelliklerinin etkisinin olabileceğini ortaya koymak amaçlanmıştır. Bu sayede, kişilik özelliklerinin dikkate alındığı siber güvenlik eğitimlerinin gerçekleştirilmesine ışık tutması açısından, bu çalışma ile sadece alanyazına değil uygulamaya da katkı sağlanacağına inanılmaktadır (McBride, Carter ve Warkentin, 2012). Diğer bir ifadeyle, siber güvenlik konusunda yetersiz olan bireylere özgü kişilik özelliklerinin belirlenmesiyle, özellikle bu kişilik grubundaki bireylere odaklanan daha kapsamlı ve ayrıntılı siber güvenlik eğitimlerinin verilebileceği düşünülmektedir.

Araştırmanın amacı

Bu çalışmada üniversite öğrencilerinin siber güvenlik davranışlarının beş faktör kişilik özellikleri ve çeşitli diğer değişkenlere göre incelenmesi amaçlanmıştır. Bu amaca ulaşmada aşağıdaki sorulara yanıt aranmıştır:

1. Üniversite öğrencilerinin siber güvenlik davranış düzeyleri nasıldır?
2. Üniversite öğrencilerinin beş faktör kişilik özellikleri nasıldır?
3. Üniversite öğrencilerinin siber güvenlik davranış düzeyleri ile beş faktör kişilik özellikleri arasındaki ilişki nasıldır?
4. Üniversite öğrencilerinin siber güvenlik davranış düzeylerinin;
    a) Cinsiyet
    b) Sınıf düzeyi
    c) Bölüm
    d) Bilişim güvenliği eğitimi alma durumu
    e) Haftalık internet kullanım süresi

gibi değişkenlere göre farklılaşma durumu nedir?

Yöntem

Bu çalışmada üniversite öğrencilerinin siber güvenlik davranışları ve beş faktör kişilik özellikleri ile ilgili var olan durumun betimlenmesi ve bu değişkenler arasındaki ilişkinin incelenmesi amaçlanmıştır. Buna ek olarak siber güvenlik davranışlarının çeşitli değişkenlere göre farklılık gösterme durumu da incelenmiştir. Bu sebeple, çalışmada betimsel tarama modeli kullanılmıştır (Fraenkel, Wallen ve Hyun, 2012).

Çalışma grubu

Bu araştırmanın çalışma grubunu 2017-2018 eğitim-öğretim yılı bahar döneminde Türkiye'nin farklı üniversitelerinde ön lisans ve lisans düzeylerinde öğrenim gören 420 öğrenci oluşturmaktadır. Çalışmaya katılımda gönüllülük esas alınmıştır. Çalışma grubuna ait demografik özellikler Tablo 1'de yer almaktadır.

Tablo 1.
Çalışma Grubunun Demografik Özellikleriyle İlgili Dağılımlar

Değişken	Kategori	Sıklık (f)	Yüzde (%)
Cinsiyet	Erkek	177	42.1
	Kadın	243	57.9
	Toplam	420	100
Üniversite	Amasya Üniversitesi	25	6.0
	Atatürk Üniversitesi	9	2.1
	Bingöl Üniversitesi	5	1.2
	Celal Bayar Üniversitesi	42	10.0
	Erzincan Üniversitesi	101	24.0
	Hacettepe Üniversitesi	135	32.1
	İnönü Üniversitesi	6	1.4
	Kahramanmaraş Sütçü İmam Üniversitesi	37	8.8
	Mustafa Kemal Üniversitesi	12	2.9
	Ondokuz Mayıs Üniversitesi	10	2.4
	Sinop Üniversitesi	22	5.2
	Süleyman Demirel Üniversitesi	4	1.0
	Yüzüncü Yıl Üniversitesi	12	2.9
	Toplam	420	100
Bölüm	Bilgisayar ve Öğretim Teknolojileri Eğitimi (BÖTE)	282	67.1
	Bilgisayar Programcılığı	37	8.8
	Lojistik	14	3.3
	Tapu ve Kadastro	13	3.1
	Psikolojik Danışmanlık ve Rehberlik (PDR)	42	10.0
	Okul Öncesi Eğitimi	32	7.6
	Toplam	420	100
Sınıf Düzeyi	Ön lisans	64	15.2
	1. sınıf	63	15.0
	2. sınıf	124	29.5
	3. sınıf	103	24.5
	4. sınıf	66	15.7
	Toplam	420	100
Bilişim Güvenliği Eğitimi Alma Durumu	Evet	173	41.2
	Hayır	247	58.8
	Toplam	420	100
Haftalık İnternet Kullanım Süresi	5 saat ve altı	47	11.2
	6-10 saat	69	16.4
	11-15 saat	49	11.7
	16-20 saat	56	13.3
	20 saat ve üzeri	199	47.4
	Toplam	420	100

Tablo 1 incelendiğinde katılımcı olarak kadın öğrencilerin (%57.9) az bir farkla da olsa erkek öğrencilere göre (%42.1) daha fazla olduğu görülmektedir. Ayrıca, çalışma grubunun çoğunluğu Hacettepe Üniversitesi (%32.1) ve Erzincan Üniversitesi öğrencilerinden (%24.0) oluşmaktadır. Katılımcıların büyük bir kısmı 2. sınıf (%29.5) ve 3. sınıf (%24.5) düzeyinde ve bölüm olarak BÖTE bölümünde (%67.1) öğrenim gören öğrencilerdir. Verilere göre katılımcıların önemli sayılabilecek bir bölümü (%58.8) bilişim güvenliği eğitimi almamıştır. Bunlara ek olarak, öğrencilerin büyük bir kısmı haftada 20 saat ve üzeri sürelerde internette vakit geçirdiğini belirtmiştir (%47.4).

Veri toplama araçları

Bu araştırma kapsamında verilerin toplanması için üç adet veri toplama aracı kullanılmıştır. Bu araçlar sırasıyla Kişisel Bilgi Formu, Kişisel Siber Güvenliği Sağlama Ölçeği ve Beş Faktör Kişilik Özellikleri Ölçeği'dir.

Kişisel bilgi formu: Çalışmadaki veri toplama araçlarından ilki, çalışma grubuyla ilgili olarak cinsiyet, sınıf düzeyi, bölüm, bilişim güvenliği eğitimi alma durumu ve haftalık bilgisayar ve internet kullanım sürelerinin belirlendiği Kişisel Bilgi Formu'dur. Bu form araştırmacılar tarafından geliştirilmiştir.

Kişisel Siber Güvenliği Sağlama Ölçeği: Çalışmada öğrencilerin siber güvenlik düzeylerinin belirlenmesi amacıyla Erol, Şahin, Yılmaz ve Haseski (2015) tarafından geliştirilen "Kişisel Siber Güvenliği Sağlama Ölçeği" kullanılmıştır. Ölçek 5 faktör ve 25 maddeden oluşmaktadır. Bu faktörler "kişisel gizliliği koruma" (10 madde), "güvenilmeyenden kaçınma" (4 madde), "önlem alma" (5 madde), "ödeme bilgilerini koruma" (2 madde) ve "iz bırakmama" (4 madde) şeklinde isimlendirilmiştir. 5'li likert tipindeki ölçeğin Cronbach Alfa güvenirlik katsayısı 0.735 olarak hesaplanmıştır. Alt boyutlara ilişkin güvenirlik katsayıları ise "kişisel gizliliği koruma" 0.763, "güvenilmeyenden kaçınma" 0.771, "önlem alma" 0.704, "ödeme bilgilerini koruma" 0.829 ve "iz bırakmama" 0.557 şeklindedir. Ölçek 18 yaş ve üzeri bireyler için uygun bir ölçektir.

Beş Faktör Kişilik Özellikleri Ölçeği: Çalışmada kullanılan bir diğer ölçek ise öğrencilerin kişilik özelliklerinin belirlendiği "Beş Faktör Kişilik Özellikleri Ölçeği" başlıklı ölçektir. Ölçek John ve Srivastava (1999) tarafından geliştirilmiş olup, Türkçeye uyarlanması Sümer, Lajunen ve Özkan (2005) tarafından yapılmıştır. Ölçek 5'li likert tipinde olup, 5 faktör ve 44 maddeden oluşmaktadır. Her bir faktörün bir kişilik boyutunu yansıttığı ölçekte "dışadönüklük" (8 madde), "nevrotiklik" (8 madde), "uyumluluk" (9 madde), "sorumluluk" (9 madde) ve "deneyime açıklık" (10 madde) olarak isimlendirilen kişilik boyutları bulunmaktadır. Ölçeğin Cronbach Alfa güvenirlik katsayısı alt boyutlar düzeyinde Türkiye örneklemi için 0.64 ile 0.77 arasında değişiklik göstermektedir.

Verilerin analizi

Verilerin analizinde hangi istatistiksel tekniklerin kullanılacağına karar verebilmek amacıyla öncelikle çalışmadaki bağımlı değişkenler için her bir kategoriye ait normallik testi yapılmıştır. Normallik testi için değişkenlere ilişkin çarpıklık ve basıklık değerleri incelenmiştir. Gravetter ve Walnau (2014) bir değişkene ait verilerin normal dağılım gösterebilmesi için, çarpıklık ve basıklık değerlerinin -2.0 ve +2.0 aralığında olması gerektiğini belirtmiştir. Buna ek olarak, kullanılması planlanan istatistiksel analizlerin gerektirdiği normallik dışındaki diğer varsayımlar da kontrol edilmiştir. Her bir bulguyu sunmadan önce ilgili başlık altında istatistiksel analiz varsayımları raporlanmıştır. Varsayım testlerinin sonuçlarına göre parametrik veya parametrik olmayan testlerin kullanılmasına karar verilmiştir.

Çalışma kapsamında betimsel istatistiklerle ilgili olarak yüzde ve frekanslar hesaplanmıştır. Ölçeklerden alınan puanların anlamlı bir şekilde yorumlanabilmesi için puan aralıklarının karşılıklarının bilinmesi gerekmektedir. Bu bağlamda 5'li likert ölçeklerinde puan aralıklarıyla ilgili olarak Yenilmez (2008) tarafından yapılan sınıflama dikkate alınarak "kesinlikle katılmıyorum" için 1.00-1.80, "katılmıyorum" için 1.81-2.60, "kararsızım" için 2.61-3.40, "katılıyorum" için 3.41-4.20 ve "kesinlikle katılıyorum" için 4.21-5.00 şeklindeki bir puanlamanın uygun olduğuna karar verilmiştir. Sözü edilen kategorilendirme şekli göz önünde

bulundurularak, bu çalışma kapsamında kullanılan 5'li likert ölçeklerinden alınan puanlar Tablo 2'de sunulan biçimde yorumlanmıştır.

Tablo 2.
Ölçek Verilerinin Yorumlanması

Puan Aralığı	Kişisel Siber Güvenliği Sağlama Ölçeği	Beş Faktör Kişilik Özellikleri Ölçeği
1.00-1.80	Hiçbir zaman	Hiç katılmıyorum
1.81-2.60	Nadiren	Biraz katılmıyorum
2.61-3.40	Ara sıra	Kararsızım
3.41-4.20	Sık Sık	Biraz katılıyorum
4.21-5.00	Her zaman	Tamamen katılıyorum

Bulgular

Bulgular, bu araştırmanın amacı doğrultusunda belirlenen araştırma soruları ayrı ayrı cevaplandırılacak şekilde sunulmuştur. Bu bağlamda üniversite öğrencilerinin siber güvenlik davranış düzeyleri, beş faktör modeli bağlamındaki kişilik özellikleri, bu iki değişken arasındaki ilişki ve öğrencilerin siber güvenlik davranış düzeylerinin cinsiyet, sınıf, bölüm, bilişim güvenliği eğitimi alma durumu ve haftalık internet ve bilgisayar kullanım sürelerine göre değişimi ayrıntılı olarak açıklanmıştır.

Üniversite öğrencilerin siber güvenlik davranış düzeyleri (SGDD)

Çalışmadaki ilk araştırma sorusu *"Üniversite öğrencilerinin siber güvenlik davranış düzeyleri nasıldır?"* şeklinde belirlenmiştir. Bu sorunun yanıtlanması için betimsel istatistik tekniklerine başvurulmuştur. Bu bağlamda, siber güvenlik davranış düzeyleri ile ilgili her bir boyuta ilişkin minimum, maksimum ve ortalama değerler hesaplanmış ve sonuçlar Tablo 3'te verilmiştir.

Tablo 3.
Üniversite Öğrencilerin Siber Güvenlik Davranış Düzeyleriyle İlgili Değerlerin Dağılımı

Değişken	N	Minimum	Maksimum	Ortalama
F1- Kişisel Gizliliği Koruma	420	1.00	5.00	3.59
F2- Güvenilmeyenden Kaçınma	420	1.00	5.00	4.05
F3- Önlem Alma	420	1.00	5.00	3.55
F4- Ödeme Bilgilerini Koruma	420	1.00	5.00	4.06
F5- İz Bırakmama	420	1.25	5.00	3.85
Siber Güvenlik Ölçeği	420	2.48	4.84	3.73

Tablo 3'te yer alan siber güvenlik davranışlarına ve alt boyutlarına ait ortalama puanlar Yenilmez (2008) tarafından belirlenen kategorilendirme şekline göre değerlendirildiğinde, tüm değişkenlerin "Sık sık" aralığına denk geldiği görülmektedir. Buna göre üniversite öğrencilerinin kişisel gizliliği koruma, güvenilmeyenden kaçınma, önlem alma, ödeme bilgilerini koruma ve iz bırakmama siber güvenlik davranışlarını gündelik yaşamlarında sık sık sergiledikleri tespit edilmiştir. Buna ek olarak, üniversite öğrencileri en fazla ödeme bilgileri ile ilgili davranışlara dikkat ederken, en az ise siber tehditlere karşı önlem alma ile ilgili davranışlara dikkat etmektedirler.

Üniversite öğrencilerinin beş faktör kişilik özellikleri

Çalışmadaki ikinci araştırma sorusu *"Üniversite öğrencilerinin beş faktör kişilik özellikleri nasıldır?"* şeklinde belirlenmiştir. Bu sorunun yanıtlanması için ilk araştırma sorusunun yanıtlanmasında olduğu gibi betimsel istatistik tekniklerine başvurulmuş ve minimum, maksimum ve ortalama değerler hesaplanmıştır. Öğrencilerin beş faktör kişilik özelliklerine ilişkin veriler Tablo 4'te verilmiştir.

Tablo 4'te verilen beş faktör kişilik özelliklerine ait ortalama puanlara bakıldığında, üniversite öğrencilerinin kendilerini dışadönük ve nevrotik bireyler olarak değerlendirme konusunda kararsız oldukları, çevresiyle uyumlu, sorumluluk bilincine sahip ve deneyime açık bireyler oldukları konusuna biraz katıldıkları anlaşılmaktadır.

Tablo 4.
Üniversite Öğrencilerinin Beş Faktör Kişilik Özellikleriyle İlgili Değerlerin Dağılımı

Değişken	N	Minimum	Maksimum	Ortalama
Dışadönüklük	420	1.25	5.00	3.34
Nevrotiklik	420	1.00	4.75	2.88
Uyumluluk	420	1.89	5.00	3.74
Sorumluluk	420	1.89	5.00	3.56
Deneyime Açıklık	420	1.90	4.80	3.59

Siber güvenlik davranış düzeyleri ile beş faktör kişilik özellikleri arasındaki ilişki

Çalışmanın üçüncü araştırma sorusu *"Üniversite öğrencilerinin siber güvenlik davranış düzeyleri ile beş faktör kişilik özellikleri arasındaki ilişki nasıldır?"* şeklinde belirlenmiştir. Bu sorunun yanıtlanmasına geçilmeden önce bağımlı değişkenlere ait çarpıklık ve basıklık değerleri incelenerek normallik testi yapılmıştır (Tablo 5).

Tablo 5.
Siber Güvenlik Davranışları ve Kişilik Özelliklerine İlişkin Normallik Testi

Değişken	Kategori	Çarpıklık	Basıklık
Siber Güvenlik Davranışları	F1- Kişisel Gizliliği Koruma	-.611	.893
	F2- Güvenilmeyenden Kaçınma	-1.13	.846
	F3- Önlem Alma	-.427	-.166
	F4- Ödeme Bilgilerini Koruma	-1.26	.722
	F5- İz Bırakmama	-.597	.148
	Siber Güvenlik Ölçeği	-.176	-.430
Beş Faktör Kişilik Özellikleri	Dışadönüklük	.037	-.336
	Nevrotiklik	.092	.053
	Uyumluluk	-.324	.183
	Sorumluluk	-.166	-.293
	Deneyime Açıklık	-.331	-.226

Tablo 5'teki değişkenlere ait çarpıklık ve basıklık değerleri -2.0 ve +2.0 aralığında olduğundan verilerin normal dağıldığı kabul edilmiştir (Gravetter ve Walnau, 2014). Bu sebeple, siber güvenlik davranışları ile beş faktör kişilik özellikleri arasındaki ilişkinin incelenmesinde parametrik testlerden Pearson korelasyon katsayılarına bakılmıştır. Değişkenler arasındaki ilişki Tablo 6'da yer alan korelasyon matrisinde belirtilmiştir.

Tablo 6.
SGDD ile Beş Faktör Kişilik Özellikleri Arasındaki İlişkiye Ait Korelasyon Matrisi

	DD	N	U	S	DA	K	G	ÖA	ÖB	İ	SG
DD	-										
N	-0.17**	-									
U	0.14**	-0.28**	-								
S	0.21**	-0.25**	0.21**	-							
DA	0.41**	-0.22**	0.20**	0.24**	-						
K	-0.06	-0.10*	0.06	0.09	0.09	-					
G	0.03	-0.01	0.11*	0.10*	0.12*	-0.03	-				
ÖA	0.17**	-0.17**	0.05	0.23**	0.28**	-0.06	0.31**	-			
ÖB	0.14**	-0.10	0.06	0.08	0.27**	-0.04	0.28**	0.42**	-		
İ	0.17**	-0.12*	0.12*	0.18**	0.28**	-0.07	0.42**	0.54**	0.31**	-	
SG	0.11*	-0.17**	0.13**	0.23**	0.32**	0.53**	0.59**	0.66**	0.50**	0.62**	-

Not. *DD: Dışadönüklük, N: Nevrotiklik, U:Uyumluluk, S: Sorumluluk, DA: Deneyime Açıklık, K: Kişisel Gizliliği Koruma,*
G: Güvenilmeyenden Kaçınma, ÖA: Önlem Alma, ÖB: Ödeme Bilgilerini Koruma, İ: İz Bırakmama, SG: Genel Siber Güvenlik Davranış Düzeyi. (**): p<0.01; (*): p<0.05

Tablo 6'da yer alan Pearson korelasyon katsayıları incelendiğinde, bütün kişilik özelliklerinin genel siber güvenlik davranış düzeyi ile istatistiksel olarak anlamlı bir ilişki içinde olduğu görülmektedir. Nevrotiklik dışındaki tüm kişilik özellikleri genel siber güvenlik davranış düzeyi ile pozitif bir ilişki içindedir. Kişilik özelliklerinin genel siber güvenlik davranışları ile ilişki düzeyleri incelendiğinde ise, en güçlü ilişkiye deneyime açıklık (r=0.32, p<0.01) kişilik özelliğinin sahip olduğu, bunu ise sırasıyla sorumluluk (r=0.23, p<0.01), nevrotiklik (r=-0.17, p<0.01), uyumluluk (r=0.13, p<0.01) ve dışadönüklük (r=0.11, p<0.05) kişilik özelliklerinin izlediği görülmektedir.

Siber güvenlik davranış düzeylerinin cinsiyete göre incelenmesi

Çalışmanın dördüncü araştırma sorusunun ilk bölümü *"Üniversite öğrencilerinin siber güvenlik davranış düzeylerinin cinsiyete göre farklılaşma durumu nedir?"* şeklinde belirlenmiştir. Bu sorunun yanıtlanmasında öncelikle değişkenlerin cinsiyet kategorilerine göre normal dağılımları çarpıklık ve basıklık değerlerine bakılarak incelenmiş ve inceleme sonuçları Tablo 7'de raporlanmıştır.

Tablo 7.
SGDD'nin Cinsiyete Göre İncelenmesine İlişkin Normallik Testi

Değişkenler	Cinsiyet	Çarpıklık	Basıklık
F1- Kişisel Gizliliği Koruma	Erkek	-.500	.543
	Kadın	-.648	1.194
F2- Güvenilmeyenden Kaçınma	Erkek	-.744	.224
	Kadın	-1.407	1.405
F3- Önlem Alma	Erkek	-.429	-.207
	Kadın	-.357	-.245
F4- Ödeme Bilgilerini Koruma	Erkek	-1.308	.950
	Kadın	-1.228	.604
F5- İz Bırakmama	Erkek	-.714	.307
	Kadın	-.519	.079
Siber Güvenlik Ölçeği	Erkek	-.229	-.437
	Kadın	-.114	-.464

Tablo 7'deki çarpıklık ve basıklık değerleri normallik varsayımını karşıladığı için (Gravetter ve Walnau, 2014) bağımsız örneklemler *t*-testi kullanılmıştır. Siber güvenlik davranışlarının cinsiyete göre incelenmesinden elde edilen bulgular Tablo 8'de verilmiştir.

Tablo 8.
SGDD'nin Cinsiyete Göre İncelenmesine İlişkin *t*-Testi Sonuçlarının Dağılımı

Değişkenler	Cinsiyet	N	Ortalama	Ss	*t*	sd	*p*
F1 -Kişisel Gizliliği Koruma	Erkek	177	3.51	0.72	-2.23	418	0.026*
	Kadın	243	3.65	0.62			
F2- Güvenilmeyenden Kaçınma	Erkek	177	3.94	0.86	-2.13	418	0.034*
	Kadın	243	4.13	0.98			
F3- Önlem Alma	Erkek	177	3.70	0.75	3.23	418	0.001**
	Kadın	243	3.44	0.86			
F4- Ödeme Bilgilerini Koruma	Erkek	177	4.10	1.11	0.58	418	0.562
	Kadın	243	4.03	1.16			
F5- İz Bırakmama	Erkek	177	3.88	0.74	0.81	418	0.417
	Kadın	243	3.82	0.78			
Siber Güvenlik Ölçeği	Erkek	177	3.72	0.48	-0.50	418	0.618
	Kadın	243	3.74	0.44			

Not. *(**): p<0.01; (*): p<0.05*

Üniversite öğrencilerinin siber güvenlik davranış düzeyleri cinsiyete göre incelendiğinde, tüm ölçekten alınan siber güvenlik davranış puanlarının cinsiyete göre farklılaşmadığı tespit

edilmiştir (t=-0.50, p>0.05). Buna göre erkek ve kadın öğrenciler eşit düzeyde siber güvenlik davranışları sergilemektedirler. Bununla birlikte, ölçeğin alt boyutları düzeyinde cinsiyetler arasında bazı farklılıklar gözlenmektedir. Örneğin kişisel gizliliği koruma (t=-2.23, p<0.05) ve güvenilmeyenden kaçınma (t=-2.13, p<0.05) konularında kadın öğrencilerin lehine anlamlı bir fark bulunurken, önlem alma (t=3.23, p<0.01) konusunda ise erkek öğrencilerin lehine anlamlı bir farklılık saptanmıştır. Bunlara ek olarak, ödeme bilgilerini koruma (t=0.58, p>0.05) ve iz bırakmama (t=0.81, p>0.05) ile ilgili davranışlar için kadın ve erkek öğrenciler arasında anlamlı bir fark bulunamamıştır.

Siber güvenlik davranış düzeylerinin sınıf düzeyine göre incelenmesi

Çalışmanın dördüncü araştırma sorusunun ikinci bölümü *"Üniversite öğrencilerinin siber güvenlik davranış düzeylerinin sınıf düzeyine göre farklılaşma durumu nedir?"* şeklinde belirlenmiştir. Bu sorunun yanıtlanmasında öncelikle ANOVA varsayımları kontrol edilmiştir. ANOVA'nın uygulanması için gözlemlerin bağımsız olması, verilerin normal dağılması ve varyansların homojen olması varsayımları bulunmaktadır (Gravetter ve Walnau, 2014). Varsayımlara ilişkin olarak, bu çalışmadaki tüm gözlemler bağımsızdır. Normal dağılım için her bir bağımlı değişkenin tüm kategorilere ilişkin çarpıklık ve basıklık değerleri incelenmiştir. Varyansların homojenliği için ise Levene Testi yapılmıştır. ANOVA varsayımlarına ilişkin sonuçlar Tablo 9'da raporlanmıştır.

Tablo 9.
SGDD'nin Sınıf Düzeyine Göre İncelenmesine İlişkin ANOVA Varsayımları

Değişken	Sınıf	Çarp.	Basık.	Levene	Değişken	Sınıf	Çarp.	Basık.	Levene
F1- Kişisel Gizliliği Koruma	Ön lis.	-.050	.419	.905	F4- Ödeme Bilgilerini Koruma	Ön lis.	-.770	-.649	.000
	1. snf.	-.537	.440			1. snf.	-1.013	-.256	
	2. snf.	-.866	1.599			2. snf.	-1.222	.792	
	3. snf.	-.726	1.092			3. snf.	-1.569	2.460	
	4. snf.	-.389	-.138			4. snf.	-1.702	2.606	
F2- Güvenil-meyenden Kaçınma	Ön lis.	-.725	-.016	.182	F5- İz Bırakmama	Ön lis.	-.503	-.171	.048
	1. snf.	-.912	-.024			1. snf.	-.762	.261	
	2. snf.	-1.311	1.771			2. snf.	-.629	.164	
	3. snf.	-1.150	1.310			3. snf.	-.240	-.581	
	4. snf.	-1.467	1.556			4. snf.	-.252	-.799	
F3- Önlem Alma	Ön lis.	-.206	-.051	.012	Siber Güvenlik Ölçeği	Ön lis.	.145	-.879	.307
	1. snf.	-.535	-.627			1. snf.	-.069	-.451	
	2. snf.	-.234	-.659			2. snf.	-.085	-.498	
	3. snf.	.033	-.321			3. snf.	-.323	.636	
	4. snf.	-.606	-.165			4. snf.	-.509	-.321	

Tablo 9'a göre, kişisel gizliliği koruma, güvenilmeyenden kaçınma ve tüm siber güvenlik ölçeğine ait verilerin çarpıklık, basıklık ve Levene testi sonuçlarına bakıldığında, bu değişkenlerin ANOVA varsayımlarını karşıladığı görülmüştür. Bununla birlikte, önlem alma, ödeme bilgilerini koruma ve iz bırakmama değişkenlerine ait verilerin varyansların homojenliği varsayımını karşılamadığı görülmüştür. Bu sebeple, bu üç değişkenin sınıf düzeyine göre farklılaşma durumu parametrik olmayan testlerden Kruskal-Wallis testi ile incelenmiş ve sonrasında her bir sınıf arasındaki farklılık Mann-Whitney testi ile ortaya konulmuştur.

Siber güvenlik davranışlarının ANOVA kullanılarak sınıf düzeyine göre incelenmesinden elde edilen bulgulara Tablo 10'da yer verilmiştir.

Tablo 10.
SGDD'nin Sınıf Düzeyine Göre İncelenmesine İlişkin ANOVA Sonuçları

Değişken	Sınıf	N	$\bar{X}$	Ss	F	p	Fark
F1- Kişisel Gizliliği Koruma	Ön lisans [a]	64	3.52	0.65	0.913	0.456	-
	1. sınıf [b]	63	3.67	0.62			
	2. sınıf [c]	124	3.56	0.68			
	3. sınıf [d]	103	3.54	0.69			
	4. sınıf [e]	66	3.68	0.63			

F2- Güvenil-meyenden Kaçınma	Ön lisans [a]	64	3.69	1.03	3.395	0.010**	a < c, d, e
	1. sınıf [b]	63	3.95	1.02			
	2. sınıf [c]	124	4.12	0.89			
	3. sınıf [d]	103	4.16	0.81			
	4. sınıf [e]	66	4.17	0.95			
Tüm Siber Güvenlik Ölçeği	Ön lisans [a]	64	3.56	0.48	5.094	0.001**	a < d, e b < e
	1. sınıf [b]	63	3.67	0.47			
	2. sınıf [c]	124	3.71	0.41			
	3. sınıf [d]	103	3.78	0.42			
	4. sınıf [e]	66	3.89	0.47			

Not. *(**): p<0.01; (*): p<0.05*

Siber güvenlik davranışlarının Kruskal-Wallis kullanılarak sınıf düzeyine göre incelenmesinden elde edilen bulgulara ise Tablo 11'de yer verilmiştir.

Tablo 11.
SGDD'nin Sınıf Düzeyine Göre İncelenmesine İlişkin Kruskal-Wallis Sonuçları

Değişken	Sınıf	N	$\bar{X}$	Ss	Ort.Sıra	χ^2	*p*	Fark
F3- Önlem Alma	Ön lisans [a]	64	3.40	0.88	188.34	22.002	0.000**	a < d, e b < d, e c < d, e
	1. sınıf [b]	63	3.22	0.91	172.03			
	2. sınıf [c]	124	3.47	0.85	199.83			
	3. sınıf [d]	103	3.72	0.66	231.23			
	4. sınıf [e]	66	3.85	0.70	256.41			
F4- Ödeme Bilgilerini Koruma	Ön lisans [a]	64	3.75	1.32	185.57	6.321	0.176	-
	1. sınıf [b]	63	3.91	1.35	208.04			
	2. sınıf [c]	124	4.02	1.11	204.33			
	3. sınıf [d]	103	4.23	0.93	222.26			
	4. sınıf [e]	66	4.27	0.97	230.25			
F5- İz Bırakmama	Ön lisans [a]	64	3.63	0.86	181.61	5.723	0.221	-
	1. sınıf [b]	63	3.84	0.88	216.26			
	2. sınıf [c]	124	3.83	0.77	209.93			
	3. sınıf [d]	103	3.88	0.66	212.57			
	4. sınıf [e]	66	4.00	0.64	230.86			

Not. *(**): p<0.01; (*): p<0.05*

Tablo 10 ve Tablo 11'deki veriler incelendiğinde genel siber güvenlik davranışlarında sınıf düzeyleri arasında birtakım farklılıkların olduğu görülmektedir ($F_{(4, 415)}$=5.094, p<0.01). Hangi sınıflar arasında anlamlı farklılığın olduğunu bulmak için Tukey testi uygulanmıştır. Bulgulara göre ön lisans öğrencileri 3. sınıf ve 4. sınıf öğrencilerine göre daha düşük seviyede siber güvenlik davranışlarına sahiptir. Benzer bir şekilde 1. sınıf öğrencileri de 4. sınıf öğrencilerinden siber güvenlik konusunda daha yetersiz durumdadır. Siber güvenliğin alt boyutlarına göre bakıldığında ise ön lisans öğrencilerinin güvenilmeyenden kaçınma konusunda 2. sınıf, 3. sınıf ve 4. sınıf öğrencilerine göre daha düşük düzeyde olduğu tespit edilmiştir ($F_{(4, 415)}$=3.395, p<0.05). Önlem alma ile ilgili davranışlarda ön lisans, 1.sınıf ve 2. sınıf öğrencileri, 3.sınıf ve 4. sınıf öğrencilerinden düşük puanlar almışlardır (χ^2=6.897, p<0.01). Kişisel gizliliği koruma ($F_{(4, 415)}$=0.913, p>0.05), ödeme bilgilerini koruma (χ^2=6.321, p>0.05) ve iz bırakmama (χ^2=5.723, p>0.05) davranışlarında sınıflar arası bir farklılık bulunmamaktadır. Bulgular genel olarak değerlendirildiğinde, siber güvenlik ve alt boyutları konusunda en düşük düzeyde olan grubun ön lisans öğrencileri olduğu, en yüksek düzeyde olan grubun ise 4. sınıf öğrencileri olduğu görülmektedir.

Siber güvenlik davranış düzeylerinin bölümlere göre incelenmesi

Çalışmanın dördüncü araştırma sorusunun üçüncü bölümü *"Üniversite öğrencilerinin siber güvenlik davranış düzeylerinin bölümlere göre farklılaşma durumu nedir?"* şeklinde belirlenmiştir. Bu sorunun yanıtlanmasına geçilmeden önce ANOVA varsayımları kontrol edilmiş ve sonuçlar Tablo 12'de raporlanmıştır.

Tablo 12.
SGDD'nin Bölümlere Göre İncelenmesine İlişkin ANOVA Varsayımları

Değişken	Bölüm	Çarp.	Basık.	Levene	Değişken	Bölüm	Çarp.	Basık.	Levene
F1- Kişisel Gizliliği Koruma	BÖTE	-.597	.749	.978	F4- Ödeme Bilgilerini Koruma	BÖTE	-1.430	1.574	.000
	Bil.Prg.	.000	.075			Bil.Prg.	-1.296	.785	
	Lojistik	.901	.719			Lojistik	.291	-.011	
	Tapu K.	-1.099	3.104			Tapu K.	-1.013	-.575	
	PDR	-1.233	2.968			PDR	-1.312	.980	
	Okul Ö.	-.950	.420			Okul Ö.	-.567	-1.192	
F2- Güvenil-meyenden Kaçınma	BÖTE	-1.279	1.508	.003	F5- İz Bırakmama	BÖTE	-.439	-.103	.000
	Bil.Prg.	-.275	-1.050			Bil.Prg.	-.115	-.683	
	Lojistik	-.766	.658			Lojistik	-.048	-1.136	
	Tapu K.	-1.194	.286			Tapu K.	-.409	-.197	
	PDR	-1.331	1.979			PDR	-.539	-.324	
	Okul Ö.	-.574	-.983			Okul Ö.	-.895	.124	
F3- Önlem Alma	BÖTE	.-299	.-290	.000	Siber Güvenlik Ölçeği	BÖTE	-.246	-.031	.678
	Bil.Prg.	-.453	.983			Bil.Prg.	.027	-.997	
	Lojistik	-.377	-1.001			Lojistik	.438	-1.290	
	Tapu K.	-.455	-.638			Tapu K.	.660	-.212	
	PDR	.130	-1.087			PDR	.178	-.530	
	Okul Ö.	-.281	-.981			Okul Ö.	.050	-.840	

Tablo 12'ye göre, sadece tüm siber güvenlik ölçeğine ait verilerin ANOVA varsayımlarını karşıladığı görülmüştür. Kişisel gizliliği koruma değişkenine ait veriler normal dağılım varsayımını; güvenilmeyenden kaçınma, önlem alma, ödeme bilgilerini koruma ve iz bırakmama değişkenleri ise varyansların homojenliği varsayımını ihlal etmiştir. Bu sebeple, siber güvenliğe ilişkin tüm alt boyutlara ait verilerin bölümlere göre farklılaşma durumu Kruskal-Wallis testi ile incelenmiştir.

Siber güvenlik davranışlarının ANOVA kullanılarak bölümlere göre incelenmesinden elde edilen veriler Tablo 13'te yer almaktadır.

Tablo 13.
SGDD'nin Bölümlere Göre İncelenmesine İlişkin ANOVA Sonuçları

Değişken	Bölüm	N	X̄	Ss	F	*p*	Fark
Siber Güvenlik Ölçeği	BÖTE [a]	282	3.81	0.42	7.857	0.000**	c < a, b e < a f < a
	Bilg. Prog. [b]	37	3.67	0.46			
	Lojistik [c]	14	3.24	0.45			
	Tapu Kad. [d]	13	3.60	0.46			
	PDR [e]	42	3.59	0.44			
	Okul Ön. [f]	36	3.54	0.49			

Not. *(**): p<0.01; (*): p<0.05*

Siber güvenlik davranışlarının Kruskal-Wallis yöntemi kullanılarak bölümlere göre incelenmesinden elde edilen veriler ise Tablo 14'te yer almaktadır.

Tablo 14.
SGDD'nin Bölümlere Göre İncelenmesine İlişkin Kruskal-Wallis Sonuçları

Değişken	Bölüm/ Program	N	$\bar{X}$	Ss	Ort.Sıra	χ^2	*p*	Fark
F1- Kişisel Gizliliği Koruma	BÖTE [a]	282	3.62	0.66	217.61	8.317	0.140	-
	Bilg. Prog. [b]	37	3.50	0.58	185.43			
	Lojistik [c]	14	3.40	0.68	163.86			
	Tapu Kad. [d]	13	3.72	0.79	239.54			
	PDR [e]	42	3.42	0.70	180.79			
	Okul Ön. [f]	36	3.62	0.67	224.44			
F2- Güvenilme yenden Kaçınma	BÖTE [a]	282	4.15	0.85	221.72	14.579	0.012*	b, c < e b, c < a
	Bilg. Prog. [b]	37	3.78	0.91	169.46			
	Lojistik [c]	14	3.46	1.10	136.46			
	Tapu Kad. [d]	13	3.71	1.31	183.46			
	PDR [e]	42	4.13	0.92	223.08			
	Okul Ön. [f]	36	3.72	1.21	185.91			
F3- Önlem Alma	BÖTE [a]	282	3.70	0.71	231.03	38.036	0.000**	c < a, b e < a, b f < a, b
	Bilg. Prog. [b]	37	3.61	0.82	216.45			
	Lojistik [c]	14	2.85	0.54	99.50			
	Tapu Kad. [d]	13	3.43	1.13	204.00			
	PDR [e]	42	3.15	0.96	158.94			
	Okul Ön. [f]	36	2.96	0.97	141.56			
F4- Ödeme Bilgilerini Koruma	BÖTE [a]	282	4.19	0.99	220.93	18.815	0.002*	c < a, b, e f < a
	Bilg. Prog. [b]	37	4.08	1.18	216.77			
	Lojistik [c]	14	2.89	1.21	100.50			
	Tapu Kad. [d]	13	3.73	1.48	188.38			
	PDR [e]	42	4.02	1.16	206.76			
	Okul Ön. [f]	36	3.50	1.54	173.36			
F5- İz Bırakmama	BÖTE [a]	282	3.89	0.68	215.39	8.685	0.122	-
	Bilg. Prog. [b]	37	3.86	0.67	206.78			
	Lojistik [c]	14	3.26	1.14	149.07			
	Tapu Kad. [d]	13	3.38	0.88	145.00			
	PDR [e]	42	3.81	0.83	207.98			
	Okul Ön. [f]	36	3.87	1.03	228.52			

Not. *(**): p<0.01; (*): p<0.05*

Tablo 13 ve Tablo 14'e göre bölümlerin genel siber güvenlik davranışlarında bazı farklılıklar bulunmaktadır ($F_{(5,\ 414)}$=7.857, *p*<0.01). BÖTE bölümü öğrencilerinin genel siber güvenlik davranışlarının lojistik, PDR ve okul öncesi programı öğrencilerininkine göre daha yeterli olduğu; bilgisayar programcılığı bölümü öğrencilerinin de siber güvenlik konusunda lojistik bölümü öğrencilerinden daha donanımlı olduğu tespit edilmiştir. Siber güvenliğin alt boyutlarında da bölümler arası istatistiksel farklar bulunmaktadır. Örneğin, güvenilmeyenden kaçınma davranışlarında BÖTE ve PDR öğrencilerinin, lojistik ve bilgisayar programcılığı bölümü öğrencilerine göre daha önde olduğu görülmektedir (χ^2=14.579, *p*<0.05). Önlem alma davranışları ile ilgili olarak ise BÖTE ve bilgisayar programcılığı bölümü öğrencileri, lojistik, PDR ve okul öncesi programı öğrencilerine göre daha başarılıdırlar (χ^2=38.036, *p*<0.01). Lojistik bölümü öğrencileri BÖTE, bilgisayar programcılığı ve PDR öğrencilerine göre; okul öncesi programı öğrencileri de BÖTE öğrencilerine göre ödeme bilgilerini koruma konusunda daha düşük düzeydedir (χ^2=18.815, *p*<0.01). Kişisel gizliliği koruma davranışlarında (χ^2=8.317, *p*>0.05) ve iz bırakmama davranışlarında (χ^2=8.685, *p*>0.05) bölümler arasında anlamlı bir farklılık saptanamamıştır. Genel bir çerçeveden bakıldığında siber güvenlik ve alt faktörleri bağlamında BÖTE ve bilgisayar programcılığı bölümünde öğrenim gören öğrencilerin diğer bölümdeki öğrencilere göre daha önde olduğu görülmektedir.

Siber güvenlik davranış düzeylerinin bilişim güvenliği eğitimi alma durumuna göre incelenmesi

Çalışmadaki dördüncü araştırma sorusunun dördüncü bölümü "*Üniversite öğrencilerinin siber güvenlik davranış düzeylerinin bilişim güvenliği eğitimi alma durumuna göre farklılaşma durumu nedir*?" şeklinde belirlenmiştir. Bunun için ilk olarak bağımlı değişkenlerin çarpıklık ve basıklık değerleri incelenerek normallik testi yapılmıştır (Tablo 15).

Tablo 15.
SGDD'nin Bilişim Güvenliği Eğitimi Alma Durumuna Göre İncelenmesine İlişkin Normallik Testi

Değişkenler	Bil. Güv. Eğt.	Çarpıklık	Basıklık
F1- Kişisel Gizliliği Koruma	Evet	-.305	.338
	Hayır	-.769	1.092
F2- Güvenilmeyenden Kaçınma	Evet	-1.272	1.022
	Hayır	-1.064	.850
F3- Önlem Alma	Evet	-.520	.248
	Hayır	-.300	-.349
F4- Ödeme Bilgilerini Koruma	Evet	-1.488	1.594
	Hayır	-1.115	.290
F5- İz Bırakmama	Evet	-.543	.154
	Hayır	-.537	-.031
Siber Güvenlik Ölçeği	Evet	-.320	-.226
	Hayır	-.082	-.448

Tablo 15'teki çarpıklık ve basıklık değerleri normallik varsayımını karşıladığı için bu sorunun yanıtlanmasında bağımsız örneklemler *t*-testi kullanılmıştır. Buna ilişkin bulgulara Tablo 16'da yer verilmiştir.

Tablo 16.
SGDD'nin Bilişim Güvenliği Eğitimi Alma Durumuna Göre İncelenmesine İlişkin *t*-Test Sonuçları

Değişken	Bil. Güv. Eğt.	N	X̄	Ss	*t*	sd	*p*
F1- Kişisel Gizliliği Koruma	Evet	173	3.63	0.63	1.178	418	0.240
	Hayır	247	3.55	0.68			
F2- Güvenilmeyenden Kaçınma	Evet	173	4.14	0.94	1.598	418	0.111
	Hayır	247	3.99	0.92			
F3- Önlem Alma	Evet	173	3.80	0.73	5.503	418	0.000**
	Hayır	247	3.37	0.84			
F4- Ödeme Bilgilerini Koruma	Evet	173	4.23	1.03	2.629	418	0.009**
	Hayır	247	3.93	1.19			
F5- İz Bırakmama	Evet	173	4.01	0.67	3.844	418	0.000**
	Hayır	247	3.72	0.79			
Siber Güvenlik Ölçeği	Evet	173	3.85	0.43	4.778	418	0.000**
	Hayır	247	3.64	0.45			

Not. *(**): p<0.01; (*): p<0.05*

Üniversite öğrencilerinin siber güvenlik davranış düzeyleri bilişim güvenliği ile ilgili bir eğitim alıp almamalarına göre incelendiğinde, tüm ölçekten alınan genel siber güvenlik davranış puanlarının eğitim alanların lehine bir farklılık gösterdiği tespit edilmiştir (t=4.778, p<0.01). Buna ek olarak, siber güvenlik alt boyutları açısından incelendiğinde, bilişim güvenliği eğitimi alan öğrencilerin önlem alma (t=5.503, p<0.01), ödeme bilgilerini koruma (t=2.629, p<0.01) ve iz bırakmama (t=3.844, p<0.01) davranışlarını eğitim almayan öğrencilere göre daha sık olarak sergiledikleri saptanmıştır. Bunun yanında, bilişim güvenliği eğitimi alma durumunun kişisel gizliliği koruma (t=1.178, p>0.05) ve güvenilmeyenden kaçınma (t=1.598, p>0.05) konularında

anlamlı bir fark oluşturmadığı görülmüştür. Genel olarak incelendiğinde bilişim güvenliği eğitimi almanın siber güvenlik davranışları üzerinde anlamlı bir etkisinin olduğu ifade edilebilmektedir.

Siber güvenlik davranış düzeylerinin haftalık internet kullanım süresine göre incelenmesi
Çalışmadaki dördüncü araştırma sorusunun beşinci ve son bölümü "*Üniversite öğrencilerinin siber güvenlik davranış düzeylerinin haftalık internet kullanım süresine göre farklılaşma durumu nedir*?" şeklinde belirlenmiştir. Sorunun yanıtlanması için istatistiksel analize geçmeden önce ANOVA varsayımları kontrol edilmiş ve sonuçlar Tablo 17'de raporlanmıştır.

Tablo 17.
SGDD'nin Haftalık İnternet Kullanım Süresine Göre İncelenmesine İlişkin ANOVA Varsayımları

Değişken	Haft. İnt. (saat)	Çarp.	Basık.	Levene	Değişken	Haft. İnt. (saat)	Çarp.	Basık.	Levene
F1- Kişisel Gizliliği Koruma	< 5	-.306	.190	.051	F4- Ödeme Bilgilerini Koruma	< 5	-.819	-.820	.002
	6-10	-.682	.518			6-10	-1.004	.176	
	11-15	-.409	.718			11-15	-1.174	.679	
	16-20	-.122	.680			16-20	-1.093	.541	
	> 20	-.659	.905			> 20	-1.528	1.742	
F2- Güvenil-meyenden Kaçınma	< 5	-.866	-.131	.001	F5- İz Bırakma-ma	< 5	-.456	-.226	.020
	6-10	-1.049	.114			6-10	-.442	-.334	
	11-15	-1.073	.604			11-15	-.300	-.704	
	16-20	-.641	-.080			16-20	-.433	-.730	
	> 20	-1.133	1.047			> 20	-.791	1.078	
F3- Önlem Alma	< 5	-.258	-.620	.062	Siber Güvenlik Ölçeği	< 5	-.067	-.951	.234
	6-10	-.045	-.698			6-10	.213	-.208	
	11-15	-.633	.819			11-15	-.059	-.558	
	16-20	-.616	.027			16-20	-.649	.517	
	> 20	-.430	-.135			> 20	-.220	-.296	

Tablo 17'deki değerlere göre, kişisel gizliliği koruma, önlem alma ve tüm siber güvenlik ölçeğine ilişkin veriler ANOVA varsayımlarını karşılamaktadır. Bununla birlikte, güvenilmeyenden kaçınma, ödeme bilgilerini koruma ve iz bırakmama alt boyutlarına ait veriler ANOVA varsayımlarını ihlal ettiğinden dolayı, haftalık internet kullanım süresinin bu değişkenlere göre farklılaşma durumu parametrik olmayan testlerden Kruskal-Wallis testi ile analiz edilmiştir.

Siber güvenlik davranışlarının ANOVA kullanılarak haftalık internet kullanım süresine göre incelenmesinden elde edilen bulgulara Tablo 18'de yer verilmiştir.

Tablo 18.
SGDD'nin Sınıf Düzeyine Göre İncelenmesine İlişkin ANOVA Sonuçları

Değişken	Haft. İnt.Kul.	N	X̄	Ss	F	*p*	Fark
F1- Kişisel Gizliliği Koruma	< 5 saat [a]	47	3.74	0.63	1.182	0.318	-
	6-10 saat [b]	69	3.47	0.79			
	11-15 saat [c]	49	3.58	0.63			
	16-20 saat [d]	56	3.52	0.52			
	> 20 saat [e]	199	3.59	0.66			
F3- Önlem Alma	< 5 saat [a]	47	3.36	1.03	2.371	0.052	-
	6-10 saat [b]	69	3.39	0.85			
	11-15 saat [c]	49	3.46	0.81			
	16-20 saat [d]	56	3.55	0.76			
	> 20 saat [e]	199	3.66	0.76			
Tüm Siber Güvenlik Ölçeği	< 5 saat [a]	47	3.69	0.50	2.424	0.048*	b < e
	6-10 saat [b]	69	3.60	0.46			
	11-15 saat [c]	49	3.68	0.49			
	16-20 saat [d]	56	3.76	0.42			
	> 20 saat [e]	199	3.79	0.43			

Not. *(**): p<0.01; (*): p<0.05*

Siber güvenlik davranışlarının Kruskal-Wallis kullanılarak haftalık internet kullanım süresine göre incelenmesinden elde edilen verilere Tablo 19'da yer verilmiştir.

Tablo 19.
SGDD'nin Sınıf Düzeyine Göre İncelenmesine İlişkin Kruskal-Wallis Sonuçları

Değişken	Haft. İnt.Kul.	N	$\bar{X}$	Ss	Ort.Sıra	χ^2	*p*	Fark
F2- Güvenil-meyenden Kaçınma	< 5 saat [a]	47	3.96	1.06	206.35	2.176	.703	-
	6-10 saat [b]	69	3.92	1.12	205.88			
	11-15 saat [c]	49	3.91	1.01	193.10			
	16-20 saat [d]	56	4.25	0.64	225.69			
	> 20 saat [e]	199	4.09	0.87	213.09			
F4- Ödeme Bilgilerini Koruma	< 5 saat [a]	47	3.63	1.46	179.52	11.912	.018*	a, b < e
	6-10 saat [b]	69	3.84	1.18	185.46			
	11-15 saat [c]	49	4.05	1.05	203.97			
	16-20 saat [d]	56	4.05	1.08	207.01			
	> 20 saat [e]	199	4.23	1.03	229.09			
F5- İz Bırakmama	< 5 saat [a]	47	3.73	0.94	197.72	2.111	.715	-
	6-10 saat [b]	69	3.78	0.80	201.81			
	11-15 saat [c]	49	3.78	0.83	200.27			
	16-20 saat [d]	56	3.87	0.72	212.78			
	> 20 saat [e]	199	3.90	0.69	218.41			

Not. *(**): p<0.01; (*): p<0.05*

Tablo 18 ve Tablo 19'daki veriler incelendiğinde haftalık internet kullanım süresinin genel siber güvenlik davranışları üzerinde az da olsa bir etkisinin olduğu görülmektedir ($F_{(4, 415)}$=2.424, p<0.05). Buna göre haftada 20 saatten fazla internet kullanan öğrencilerin siber güvenlik davranış düzeyleri haftada 6-10 saat arası internet kullanan öğrencilerinkinden daha yüksektir. Siber güvenliğin alt boyutlarına bakıldığında ise tek anlamlı farklılığın ödeme bilgilerini koruma davranışlarında olduğu tespit edilmiştir (χ^2=11.912, p<0.05). Haftalık internet kullanım süreleri 20 saatten fazla olan öğrenciler, internette 10 saatten az vakit geçiren öğrencilere göre ödeme bilgilerini koruma konusunda daha iyi durumdadır. Bununla birlikte haftalık internet kullanım süresinin kişisel gizliliği koruma ($F_{(4, 415)}$=1.182, p>0.05), güvenilmeyenden kaçınma (χ^2=2.176, p>0.05), önlem alma ($F_{(4, 415)}$=2.371, p>0.05) ve iz bırakmama (χ^2=2.111, p>0.05) davranışlarında herhangi bir etkisinin olmadığı saptanmıştır. Özet olarak, öğrencilerin siber güvenlik davranışları genel itibariyle haftalık internette geçirilen süreye göre anlamlı olarak farklılaşmamaktadır.

Tartışma

Bu çalışmada üniversite öğrencilerinin siber güvenlik davranış düzeyleri beş faktör kişilik özellikleri ve cinsiyet, bölüm, sınıf düzeyi, bilişim güvenliği eğitimi alma durumu ve haftalık internet kullanım sürelerine göre incelenmiştir.

Ulaşılan bulgulardan ilki öğrencilerin siber güvenlik davranışları ile ilgili düzeylerinin yeterli denebilecek düzeyde olduğu yönündedir. Gerek ölçeğin tamamından alınan genel siber güvenlik puanları, gerekse de siber güvenlik alt boyutlarından alınan puanlar, öğrencilerin siber güvenlik ile ilgili davranışları Yenilmez'in (2008) ölçek puanlarını kategorilendirme biçimine göre günlük yaşamlarında "sık sık" sergilediklerine işaret etmektedir. Buna göre üniversite öğrencilerinin kişilik gizliliklerini koruma, güvenilmeyenden kaçınma, siber tehditlere karşı önlem alma, ödeme bilgilerini koruma ve iz bırakmama konularına gereken önemi verdikleri görülmektedir. Bu bulgu, alanyazındaki bazı çalışma bulgularıyla paralellik göstermektedir (Karacı, Akyüz ve Bilgici, 2017; Pusey ve Seadra; Yan, Robertson, Yan, Park, Bordoff, Chen ve Sprissler, 2018). Bununla birlikte, bu çalışmadaki bulgunun aksine, öğrencilerin siber güvenlik davranış düzeylerinin yeterli olmadığı sonucuna ulaşan çalışmalar da bulunmaktadır (Akgün ve Topal, 2015; Gökmen ve Akgün, 2015; Karaoğlan Yılmaz, Yılmaz ve Sezer, 2014; Tekerek ve Tekerek, 2013).

Çalışmada öğrencilerin beş faktör kişilik özellikleri de incelenmiştir. Beş farklı kişilik boyutunu yansıtan ölçeğin her bir boyutundan alınan puanlar Yenilmez'in (2008) ortaya koyduğu yorumlama biçimine göre değerlendirilmiştir. Buna göre öğrenciler kendilerini dışadönük ve nevrotik bireyler olarak tanımlama konusunda kararsız kalmışlardır. Bunun yanında, öğrenciler kendilerini uyumlu, sorumluluk bilincine sahip ve deneyime açık kişiler olarak nitelendirme konusuna katıldıklarını bildirmişlerdir.

Çalışmada ortaya konmaya çalışılan durumlardan birisi siber güvenlik davranışları ile beş faktör kişilik özellikleri arasındaki ilişkidir. Bu konuda elde edilen bulgular, tüm kişilik özelliklerinin siber güvenlik davranışları ile anlamlı bir ilişki içinde olduğunu göstermektedir. Nevrotiklik dışındaki tüm kişilik özellikleri siber güvenlik davranışlarıyla pozitif yönde bir ilişki sergilemektedir. Bu sonuca göre öğrencilerin deneyime açıklık, sorumluluk, uyumluluk, dışadönüklük özellikleri geliştikçe ve nevrotiklik özelliği kontrol altına alınarak bastırıldıkça, siber güvenlik davranış düzeyleri de bu ölçüde gelişim göstermektedir. Buna ek olarak, kişilik özellikleri siber güvenlik davranışlarıyla aralarındaki ilişkinin büyüklüğü bakımından büyükten küçüğe doğru, deneyime açıklık, sorumluluk, nevrotiklik, uyumluluk ve dışadönüklük şeklinde sıralanmaktadır.

Deneyime açıklık, siber güvenlik davranışları ile ilişkili bir kişilik özelliği olarak tespit edilmiştir. Buna göre deneyime açık bireyler siber güvenlik konusunda daha dikkatli davranışlar sergilemektedirler. Alanyazında deneyime açık kişilik özelliğine sahip bireylerin yeni olan fikir, teknik, ürün ve deneyim gibi konularda ilgili ve girişken olduğu belirtilmektedir (Lounsbury ve Gibson, 2009). Buna ek olarak deneyime açık kişilerin teknolojik yenilikleri takip etme ve bunları kullanma konusunda başarılı oldukları ifade edilmektedir (Svendse, Johnsen, Almas-Sorensen ve Vitterso, 2013; Woszczynski, Roth ve Segars, 2002). Bu bağlamda, siber tehditlerin her geçen gün yeni teknolojiler aracılığıyla yeni biçimlerde ortaya çıktığı düşünülürse, deneyime açık bireylerin bu teknolojileri takip etmedeki ilgililiği, bu kişilik özellikteki kişilerin siber güvenlik konusunda daha dikkatli olma durumlarını açıklamaktadır. Alanyazın incelendiğinde, McBride, Carter ve Warkentin (2012) ile McCormac ve diğerlerinin (2017) bulgularının deneyime açıklık ile ilgili olarak bu çalışmada ulaşılan bulguyu desteklediği, Gratian ve diğerleri (2018) ile Halevi ve diğerlerinin (2016) bulgularının ise ulaşılan bu bulguyu desteklemediği görülmektedir.

Siber güvenlik davranışlarıyla ilişkili olduğu tespit edilen kişilik özelliklerinden birisi de sorumluluktur. Çalışma bulgularına göre sorumluluk kişilik özelliği güçlendikçe, siber güvenlik davranışlarının da daha yeterli hale geldiği tespit edilmiştir. Sorumluluk kişilik özelliğine sahip kişiler planlı, dikkatli, disiplinli ve kurallara uyan kişiler olarak nitelendirilmektedir (Costa ve McCrae, 1992). Çalışmada sorumluluk ile siber güvenlik davranışları arasında anlamlı bir ilişkinin bulunmasının altında yatan sebeplerden birisi, siber güvenlik konusunun dikkat ve sorumluluk bilinci gerektirmesi ve uyulması ile bununla ilgili olarak gereken belli kuralları içermesi şeklinde ifade edilebilir. Bu çalışma kapsamında sorumluluk kişilik özelliği ile elde edilen bulguyu destekleyen çeşitli çalışmalara da alanyazında rastlanmaktadır (Gratian ve diğerleri, 2018; Halevi ve diğerleri, 2016; McCormac, Zwaans, Parsons, Calic, Butavicius ve Pattinson 2017).

Çalışmada nevrotikliğin siber güvenlik davranışlarıyla negatif bir ilişki içinde olduğu saptanmıştır. Bu bağlamda, nevrotiklik kişiliği baskın olan bireyler siber güvenlik konusunda daha az yeterli olmaktadır. Alanyazında nevrotik bireyler gergin, sinirli ve özellikle olumsuz durumlarla başa çıkmada zorluk yaşayan ve bu gibi durumların üstesinden gelirken uygun olmayan birtakım stratejilere başvuran kişiler olarak betimlenmektedir (Carver ve Connor-Smith, 2010). Dolayısıyla, bu çalışmada da bulunduğu üzere, nevrotik bireylerin siber tehditler gibi olumsuz durumlar karşısında yeterli güvenlik davranışları sergileyememesi söz konusu olabilmektedir. McCormac ve diğerleri (2017) yaptıkları araştırmada bu çalışmadakine benzer bir bulguya ulaşmışlar ve nevrotiklik ile siber güvenlik arasında anlamlı bir ilişki tespit etmişlerdir. Bununla birlikte alanyazında, nevrotiklik ile ilgili bu çalışmadaki bulguyu desteklemeyen çalışmalar da yer almaktadır (Gratian ve diğerleri, 2018; Halevi ve diğerleri, 2017).

Beş faktör kişilik özelliklerinden uyumluluk boyutu da üniversite öğrencilerinin siber güvenlik davranışlarıyla ilişkili bulunmuştur. Buna göre uyumluluk kişilik özelliği geliştikçe, bireylerin siber güvenlik davranışları da daha etkili hale gelmektedir. Zhao ve Seibert (2006) uyumlu kişilik özelliğindeki bireylerin kanun ve kurallara uymama ve bu sebepten dolayı zarar

görme konusunda çekince sahibi bireyler olduğunu belirtmektedir. Bu bağlamda, siber güvenliğin de belirli kurallar gerektirdiği ve uyulmadığı takdirde bireyin zarar görme durumunun oluşabileceği göz önüne alındığında, uyumluluk kişilik özelliğinin siber güvenlik davranışları ile anlamlı bir ilişkiye sahip olduğu durumu açıklanabilmektedir. McCormac ve diğerleri (2017) de çalışmalarında benzer bir bulguya erişirken, farklı bulgulara da ulaşan çalışmalar bulunmaktadır (Gratian ve diğerleri, 2018; Halevi ve diğerleri, 2017).

Kişilik özelliklerinden son olarak dışadönüklüğün de siber güvenlik davranışlarıyla anlamlı bir ilişkiye sahip olduğu, çalışma bulguları arasında yer almaktadır. Her ne kadar iki değişken arasındaki ilişki düzeyi düşük olsa da, dışadönüklük yönü güçlü olan bireylerin siber güvenlik konusunda sergiledikleri davranışlar daha etkili olmaktadır. Alanyazında dışadönük olmayan bireylerin yalnızlığı tercih ettiği, sosyal çevreleriyle ilişkisinin zayıf olduğu ve sosyalleşme gereksinimlerini çevrimiçi ortamlarda karşıladıkları belirtilmektedir (Karim, Zamzuri ve Nor, 2009). Bu doğrultuda, dışadönük olmayan bireylerin internet kullanım davranışlarının daha yoğun olabileceği ileri sürülebilir. Dolayısıyla, dışadönük olmayan bireylerin internette daha fazla vakit geçirecekleri varsayımından hareketle, siber güvenlik konusunda da daha başarılı olacakları ifade edilebilir. Ancak bu çalışmada bunun tam tersi bir bulguya ulaşılmış ve dışadönüklük ile siber güvenlik davranışları arasında pozitif yönlü bir ilişkiye rastlanmıştır. Bu konuyla ilgili olarak alanyazın incelendiğinde, Gratian ve diğerleri (2018) dışadönüklük ile siber güvenlik arasında anlamlı bir ilişki tespit ederken, farklı çalışmalarda herhangi bir ilişki bulunamamıştır (Halevi ve diğerleri, 2016; McCormac ve diğerleri, 2017).

Çalışmada üniversite öğrencilerinin siber güvenlik davranışlarının cinsiyete göre farklılaşma durumu incelenen bir diğer noktadır. Ulaşılan bulgular tüm ölçekten alınan genel siber güvenlik davranış puanlarının cinsiyete göre farklılaşmadığını göstermiştir. Siber güvenlik alt boyutlarına bakıldığında ise kişisel gizliliği koruma ve güvenilmeyenden kaçınma konularında kadın öğrencilerin lehine anlamlı bir farklılık gözlenirken, önlem alma konusunda erkek öğrenciler daha başarılı sonuçlar almışlardır. Bununla birlikte, ödeme bilgilerini koruma ve iz bırakmama ile ilgili davranışlarda kadın ve erkek öğrenciler arasında bir farklılık bulunmamıştır. Alanyazındaki çalışma bulguları değerlendirildiğinde ise, birçok çalışmada siber güvenlik davranışları açısından cinsiyetler arasında herhangi bir fark bulunmazken (Gökmen ve Akgün, 2015; Karacı, Akyüz ve Bilgici, 2017; Subramaniam, 2017; Yan ve diğerleri, 2018), cinsiyetler arası fark tespit edilip kadın öğrencilerin (Tekerek ve Tekerek, 2013) veya erkek öğrencilerin (Akgün ve Topal, 2015) siber güvenlik bağlamında daha önde olduğu çalışmalar da mevcuttur.

Çalışmada siber güvenlik davranışlarının sınıf düzeyine göre farklılaşma durumu da incelenmiştir. Çalışma bulgularına göre siber güvenlik puanlarının genel olarak 3. ve 4. sınıf öğrencilerinin lehine daha yüksek olduğu bulgulanmıştır. Siber güvenlik alt boyutları açısından değerlendirildiğinde ise, güvenilmeyenden kaçınma ve önlem alma davranışlarında genel itibariyle 3. ve 4. sınıf öğrencileri daha yeterli olarak tespit edilmiştir. Kişisel gizliliği koruma ödeme bilgilerini koruma ve iz bırakmama davranışları için sınıf düzeyleri arasında anlamlı bir fark saptanamamıştır. Bulgulara bakıldığında, yaşlarının büyük olması sebebiyle deneyimsel açıdan diğer öğrencilere göre daha avantajlı olan üst sınıflardaki öğrencilerin genel olarak siber güvenlik konusunda daha başarılı olduğu çıkarımı yapılabilmektedir. Alanyazındaki diğer çalışmalarda ise sınıf düzeyinin siber güvenlik açısından fark oluşturacak bir değişken olmadığına yönelik bulgulara ulaşılmıştır (Gökmen ve Akgün, 2015; Karacı, Akyüz ve Bilgici, 2017; Yan ve diğerleri, 2018).

Çalışmadaki katılımcıların farklı bölümlerden olması, siber güvenlik davranış düzeylerinin bölüme göre farklılaşma durumunun incelenmesini de beraberinde getirmiştir. Bulgular incelendiğinde, kişisel gizliliği koruma ve iz bırakmama boyutları dışındaki tüm siber güvenlik alt boyutları ve genel siber güvenlik puanlarının bölüme göre farklılaştığı tespit edilmiştir. Genel olarak, bilgisayar ile yakından ilişkili olarak sayılabilecek bölümler olan BÖTE ve bilgisayar programcılığı bölümü öğrencilerinin siber güvenlik davranışları diğer bölümlerdeki öğrencilerinkine göre daha kabul edilebilir bir düzeydedir.

Siber güvenlik davranışlarında gruplar arası farklılığın incelendiği bir diğer değişken ise üniversite öğrencilerinin bilişim güvenliği eğitimi alma durumudur. Çalışma bulguları bilişim güvenliği ile ilgili bir eğitim alan öğrencilerin genel siber güvenlik puanlarının eğitim almayan

öğrencilerinkine göre daha yüksek olduğunu göstermiştir. Buna ek olarak, önlem alma, ödeme bilgilerini koruma ve iz bırakmama puanlarında da bilişim güvenliği eğitimi alanların lehine bir farklılık gözlenmiştir. Kişisel gizliliği koruma ve güvenilmeyenden kaçınma alt boyutlarında ise bilişim güvenliği eğitimi alanların puanları eğitim almayanlarınkine göre istatistiksel olarak anlamlı olmasa da daha yüksek olarak bulunmuştur. Bahsedilen bulgular bilişim güvenliği eğitimi almanın bireylerin siber güvenlik davranışlarına önemli bir katkı yaptığını göstermektedir. Karacı, Akyüz ve Bilgici (2017) üniversite öğrencileriyle gerçekleştirdiği çalışmada bu çalışmadakine benzer bir bulguya ulaşmıştır. Bununla birlikte, bilişim güvenliği eğitimi almanın siber güvenlik düzeylerinde bir farklılık yaratmadığı sonucuna ulaşan çalışmalar da alanyazında yer almaktadır (Akgün ve Topal, 2015; Gökmen ve Akgün, 2015).

Son olarak çalışmada öğrencilerin siber güvenlik davranışlarının haftalık internet kullanım süresine göre farklılaşma durumu araştırılmıştır. Buna ilişkin bulgular haftalık 20 saat ve üzeri internet kullanan öğrencilerin siber güvenlik davranışlarının, haftalık 6-10 saat süreyle internet kullanan öğrencilerinkine göre daha iyi durumda olduğunu göstermiştir. Bununla birlikte, genel olarak değerlendirildiğinde, bu çalışmada haftalık internet kullanım süresinin siber güvenlik davranışları açısından yeterince etkili bir değişken olmadığı tespit edilmiştir. Bu çalışmadakine benzer bir bulguya da Gökmen ve Akgün (2015) ulaşmış ve öğrencilerin sahip olduğu bilişim güvenliği bilgi düzeylerinin günlük internet kullanım süresine göre farklılaşmadığı belirtilmiştir. Akgün ve Topal (2015) ise internet kullanım süresinin bilişim güvenliği farkındalığına anlamlı bir etkisinin olduğunu bulgulamıştır.

Görüldüğü üzere, bu çalışmada erişilen bulguları alanyazında destekleyen ve desteklemeyen çalışmalar bulunmaktadır. Bu durumun altında yatan belli nedenlerden bahsetmek mümkündür. Söz konusu nedenler bu çalışmada üç açıdan ele alınmıştır. İlk olarak, çalışmalarda erişilen bulguların çelişkili olarak görünmesinin, çalışmaların gerçekleştirildiği bağlamdan kaynaklandığı ileri sürülebilir. Bazı çalışmalar siber güvenliği çalışan insanların bir kurumda çalışmaları sırasında gösterdiği kurumsal bazda siber güvenlik davranışları olarak ele alırken, bazı çalışmalar ise bireysel yaşamdaki siber güvenlik kavramını ele almaktadır. Dolayısıyla siber güvenlik olarak farklı bağlamların ele alınması, çalışmalarda ulaşılan bulguların da farklılaşmasına sebep olmuş olabilir.

İkinci olarak, alanyazın incelendiği zaman siber güvenlik adı altında ele alınan yapıların da çalışmalar arasında farklılık gösterdiği görülmektedir. Bazı çalışmalarda sadece dosya koruma veya cihaz koruma gibi siber güvenlik davranışları değerlendirilirken, bazılarında ise oltalama saldırılarından kaçış davranışları ele alınmıştır. Bu çalışmada ise siber güvenlik olarak daha genel bir çerçeveden bakılmış ve kişisel gizliliği koruma, güvenilmeyenden kaçınma, önlem alma, ödeme bilgilerini koruma ve iz bırakmama boyutları incelenmiştir. Kısacası, çalışmalarda siber güvenliğin tek bir biçimde değil farklı boyutlardan inceleniyor olması, çalışma bulguları arasında farklılıklara yol açmış olabilir.

Üçüncü olarak, çalışmaların gerçekleştirildiği bağlam siber güvenlik davranışlarının gönüllü ya da görece zorunlu bir biçimde yapılmasını gerektirmiş olabilir. Bir diğer ifadeyle, kurum içinde çalışan insanların siber güvenlik davranışlarına uyması daha zorunlu gibi gözükürken, bireysel olarak gerçekleştirilen siber güvenlik davranışlarında kişi üzerinde herhangi bir zorunluluk hissetmemiş olabilir. Bu durum da siber güvenlik davranışlarının sıklığında farklılık oluşturmuş olabilir. Nitekim Venkatesh ve diğerleri (2003) de gönüllük düzeyinin herhangi bir davranışı gerçekleştirme niyetinde belirleyici olduğunu ifade etmektedir. Bu sebeple, çalışmalara katılan katılımcıların siber güvenlik davranışlarını gerçekleştirmelerindeki bağlamdan kaynaklı gönüllülük durumu, çalışma bulguları arasında tutarsızlığa yol açmış olabilir. Tartışılan bu 3 nedene ek olarak, kişilik ve siber güvenlik konusunu ele alan çalışmaların az sayıda olması ve çalışma yıllarına bakıldığında bu çalışmaların daha yeni denebilecek düzeyde olması, çalışma bulgularının kısmen de olsa tutarlı olmamasını beraberinde getirmiş olabilir.

Sonuçlar ve Öneriler

Bu çalışmada ulaşılan ilk sonuç üniversite öğrencilerinin siber güvenlik davranışlarının yeterli düzeyde olduğu şeklindedir. Öğrenciler kendilerini uyumlu, sorumlu ve deneyime açık kişiler olarak değerlendirirken, dışadönük ve nevrotik oldukları konusunda kararsız bir görüş bildirmişlerdir. Kişilik özelliklerinin tamamı siber güvenlik davranışlarıyla anlamlı bir ilişki

içindedir. Siber güvenlik davranışlarıyla en güçlü ilişkiye sahip kişilik özelliği "deneyime açıklık" iken, en zayıf ilişki ise "dışadönüklük"tür. Bunlara ek olarak, öğrencilerin siber güvenlik davranışları cinsiyete göre farklılaşmazken, bölüm, sınıf düzeyi, bilişim güvenliği eğitimi alma durumu ve haftalık internet kullanım süresine göre farklılaşmaktadır. Buna göre, bölüm bazında BÖTE ve bilgisayar programcılığı bölümü öğrencileri, sınıf düzeyi olarak 3. ve 4. sınıf öğrencileri, bilişim güvenliği eğitimi alan öğrenciler ve haftalık 6-10 saat arası internet kullanan öğrencilerin siber güvenlik davranış düzeyleri daha yüksektir.

Çalışmada ulaşılan sonuçlar ışığında uygulamaya ve araştırmaya yönelik birtakım öneriler getirmek mümkündür. Sonuçlara göre bilgisayar ile doğrudan ilişkili olmayan lojistik, PDR ve okul öncesi öğretmenliği programı öğrencilerinin siber güvenlik davranışları istenen düzeyde değildir. Günümüzde hangi alandan olursa olsun, bölümlerinden mezun olan öğrenciler iş hayatına atıldıklarında bilgi ve iletişim teknolojilerini kullanma durumunda olmaktadırlar. Dolayısıyla, özellikle bilgisayar ile yakından ilişkisi bulunmayan lisans bölümlerinin öğretim programlarında siber güvenlik konusuna ağırlık verilmesi önemli görülmektedir. Buna ek olarak, sınıf düzeyi temeline göre siber güvenlik konusunda en düşük düzeyde olan öğrenciler ön lisans öğrencileridir. Burada ön lisans öğrencilerinin gerek gördükleri eğitim kalitesi, gerekse de eğitim süreleri bakımından lisans öğrencilerine göre dezavantajlı olma durumu rol oynamış olabilir. Dolayısıyla, ön lisans düzeyindeki öğrencilere de siber güvenlik davranışlarının daha yeterli hale getirilmesi için eğitim ve etkinlikler düzenlenebilir.

Bu çalışmanın sonuçlarından birisi de bilişim güvenliği eğitimi alma durumunun siber güvenlik davranışlarına önemli derecede katkı sağladığı yönündedir. Hem bu sonuç hem de alanyazındaki diğer çalışmalarda ulaşılan sonuçlardan hareketle, üniversitelerin ilgili bölümlerinin öğretim programlarında siber güvenlik konusunun etkili bir biçimde işlenmesi önerilebilir (Gökmen ve Akgün, 2015; Karacı, Akyüz ve Bilgici, 2017). Öğretim programlarına dönük müdahalelerin yanı sıra, siber güvenliğin sağlanmasına yönelik çevrimiçi olarak yürütülen bilinçlendirme çalışmaları (Bilgimi Koruyorum, 2018; SGEP, 2018), yüz yüze eğitimler (BTK, 2018) ve konferanslar (ISCTurkey, 2018) gibi birtakım müfredat dışı etkinliklerin de bu doğrultuda uygulanabileceği ifade edilebilir.

Çalışma kapsamında ele alınan kişilik özellikleri değişkeni de siber güvenlik bağlamında uygulamaya dönük bazı önerilerin getirilmesini mümkün kılmıştır. Çalışma sonuçlarına göre siber güvenlik konusunda deneyime açıklık, sorumluluk, uyumluluk ve dışadönüklük katkı sağlayıcı, nevrotiklik ise engelleyici bir kişilik özelliği olarak karşımıza çıkmaktadır. Buna göre, öğrencilerin siber güvenlik konusunda kendilerine yarar sağlayan kişilik özelliklerine sahip olmalarına yönelik etkinlikler düzenlenebilir. Ayrıca, kişiliğin genel itibariyle çocukluk döneminde şekillendiği ve sonrasında değişiminin zaman aldığı düşünüldüğünde, ebeveynlerin çocuklarını deneyime açık, sorumluluk bilincine sahip, uyumlu ve dışadönük gibi özelliklere sahip bireyler olarak yetiştirmesi belirtilmesi gereken diğer bir husustur (Smrtnik, Vitulić ve Zupančič, 2011). Buna ek olarak, siber güvenlik ile ilgili verilen eğitimlerde her bireyi eşit kabul etmektense onları birbirinden ayıran kişilik özelliklerinin göz önüne alınması ve eğitimlerin buna göre verilmesi önerilebilir. Ayrıca, verilen eğitimlerin güçlüğü ve maliyeti gibi durumlar değerlendirildiğinde, siber güvenlik konusunda diğerlerine göre daha fazla sorun yaşayan belli kişilik özelliklerindeki öğrencilerin belirlenmesiyle, bu öğrencilere yönelik daha odaklı ve maliyet açısından daha ekonomik eğitimler verilebilir.

Uygulamaya yönelik önerilerin yanı sıra bu çalışma ile ilgili olarak gelecekte yapılacak araştırmalara da öneriler getirmek mümkündür. Öncelikle, bu çalışma bölüm çeşitliliğinin ve öğrenim gören öğrenci sayısının daha fazla olduğu bir bağlamda tekrarlanarak daha geçerli ve güvenilir bulgulara ulaşmak sağlanabilir. Buna ek olarak, bu çalışmanın katılımcıları üniversite öğrencileriyle sınırlıdır. Bu bakımdan, ulaşılan sonuçların farklı eğitim düzeylerine göre durumlarının karşılaştırmalı olarak değerlendirilebilmesi için, ilköğretim ve lise düzeyindeki öğrencilerinin katıldığı bir çalışma gerçekleştirilebilir.

Kaynaklar

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology, 33*(3), 237-248.

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H. ve Nunamaker Jr, J. F. (2010). Detecting fake websites: the contribution of statistical learning theory. *MIS Quarterly*, 435-461.

Akgün, Ö. E. ve Topal, M. (2015). Eğitim fakültesi son sınıf öğrencilerinin bilişim güvenliği farkındalıkları: Sakarya Üniversitesi Eğitim Fakültesi örneği. *Sakarya University Journal of Education, 5*(2), 98-121.

Anderson, C. L. ve Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS quarterly*, *34*(3), 613-643.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L. ve Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437-443.

Ayduk, O., Mendoza-Denton, R., Mischel, W., Downey, G., Peake, P. K. ve Rodriguez, M. (2000). Regulating the interpersonal self: strategic self-regulation for coping with rejection sensitivity. *Journal of Personality and Social Psychology*, *79*(5), 776.

Bilgimi Koruyorum (2018). *Bilgimi koruyorum*. Erişim adresi: http://www.bilgimikoruyorum.org.tr

BTK (2018). *İnternetin güvenli ve bilinçli kullanımı eğitim programı*. Erişim adresi: http://etkinlik.btk.gov.tr/etkinlik/detay/internetin_guvenli_ve_bilincli_kullanimi_egitim_programi

Buckley, P. ve Doyle, E. (2017). Individualising gamification: An investigation of the impact of learning styles and personality traits on the efficacy of gamification using a prediction market. *Computers & Education*, 106, 43-55.

Carver, C. S. ve Connor-Smith, J. (2010). Personality and coping. *Annual Review of Psychology*, *61*, 679-704.

Chen, H., Beaudoin, C. E. ve Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, *70*, 291-302.

Chong, C. W., Teh, P. L. ve Tan, B. C. (2014). Knowledge sharing among Malaysian universities' students: do personality traits, class room and technological factors matter? *Educational Studies*, *40*(1), 1-25.

Coopers, P. (2013). *Key findings from the Global State of Information Security Survey 2013 Changing the game.* Erişim adresi: https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2013-giss-report.pdf

Costa, P. T. ve McCrae, R. R. (1992). Four ways five factors are basic. *Personality and Individual Differences*, *13*(6), 653-665.

Çakır, S. ve Kesler, M. (2012). Bilgisayar güvenliğini tehdit eden virüsler ve antivirüs yazılımları. *XIV. Akademik Bilişim Konferansı Bildirileri* içinde (ss. 551-558).

Çelen, F. K. ve Seferoğlu, S. S. (2016). Bilgi ve iletişim teknolojilerinin kullanımı ve etik olmayan davranışlar: sorunlar, araştırmalar ve değerlendirmeler. *Journal of Computer and Education Research*, *4*(8), 124-153.

Egelman, S. ve Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (sebis). *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* içinde (ss. 2873-2882).

Erol, O., Şahin, Y. L., Yılmaz, E. ve Haseski, H. İ. (2015). Kişisel siber güvenliği sağlama ölçeği geliştirme çalışması. *Journal of Human Sciences*, *12*(2), 75-91.

Floros, G. ve Siomos, K. (2014). Excessive Internet use and personality traits. *Current Behavioral Neuroscience Reports*, *1*(1), 19-26.

Fraenkel, J., Wallen, N. ve Hyun, H. (2012). *How to design and evaluate research in education. 8th edition*. Columbus, OH: McGraw-Hill.

Furnell, S. (2008). End-user security culture: a lesson that will never be learnt? *Computer Fraud ve Security*, 4, 6-9.

Glass, R., Prichard, J., Lafortune, A. ve Schwab, N. (2013). The influence of personality and Facebook use on student academic performance. *Issues in Information Systems*, *14*(2), 119-126.

Goldberg, L. R. (1990). An alternative "description of personality": The big-five factor structure. *Journal of Personality and Social Psychology*, *59*(6), 1216-1229.

Goodrich, M. T. ve Tamassia, R. (2011). *Introduction to computer security*. Pearson.

Gökmen, Ö. F. ve Akgün, Ö. E. (2015). Bilgisayar ve Öğretim Teknolojileri Eğitimi öğretmen adaylarının bilişim güvenliği bilgilerinin çeşitli değişkenlere göre incelenmesi. *Çukurova University. Faculty of Education Journal*, *44*(1), 61.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J. ve Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, *73*, 345-358.

Gravetter, F. ve Wallnau, L. (2014). *Essentials of Statistics for the Behavioral Sciences. 8th Edition*. Wadsworth, Belmont, CA.

Gustavsson, J. P., Jönsson, E. G., Linder, J. ve Weinryb, R. M. (2003). The HP5 inventory: definition and assessment of five health-relevant personality traits from a five-factor model perspective. *Personality and Individual Differences*, *35*(1), 69-89.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), 1-18.

Halevi, T., Lewis, J. ve Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. *Proceedings of the 22nd International Conference on World Wide Web* içinde (ss. 737-744).

Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N. ve Chen, J. (2016). Cultural and psychological factors in cyber-security. *Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services* içinde (ss. 318-324).

Hekim, H. ve Başıbüyük, O. (2013). Siber suçlar ve Türkiye'nin siber güvenlik politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi*, 135-158.

Internet World Stats (2018). *Internet and world stats: Usage and population statistics*. Erişim adresi: https://www.internetworldstats.com/stats.htm

ISCTurkey (2018). *Uluslararası bilgi güvenliği ve kriptoloji konferansı*. Erişim adresi: http://www.iscturkey.org

John, O. P. ve Srivastava, S. (1999). The Big Five trait taxonomy: History, measurement, and theoretical perspectives. *Handbook of personality: Theory and research*, *2*, 102-138.

John, O. P. ve Gross, J. J. (2004). Healthy and unhealthy emotion regulation: Personality processes, individual differences, and life span development. *Journal of Personality*, *72*(6), 1301-1334.

John, O. P. ve Naumann, L. P. (2010). Surviving two critiques by Block? The resilient big five have emerged as the paradigm for personality trait psychology. *Psychological Inquiry*, *21*(1), 44-49.

Karacı, A., Akyüz, H. İ. ve Bilgici, G. (2017). Üniversite öğrencilerinin siber güvenlik davranışlarının incelenmesi. *Kastamonu Eğitim Dergisi*, *25*(6), 2079-2094.

Karaoğlan Yılmaz, G., Yılmaz, R. ve Sezer, B. (2014). Üniversite öğrencilerinin güvenli bilgi ve iletişim teknolojisi kullanım davranışları ve bilgi güvenliği eğitimine genel bir bakış. *Bartın Üniversitesi Eğitim Fakültesi Dergisi*, *3*(1), 176-199.

Karim, N. S. A., Zamzuri, N. H. A. ve Nor, Y. M. (2009). Exploring the relationship between Internet ethics in university students and the big five model of personality. *Computers ve Education*, *53*(1), 86-93.

Kaspersky Labs (2017). *Kaspersky security bulletin. Overall statistics for 2017*. Erişim adresi: https://securelist.com/ksb-overall-statistics-2017/83453

Kaspersky (2018). *Safety 101: Types of known threats*. Erişim adresi: https://support.kaspersky.com/viruses/general/614

Kayış, A. R., Satıcı, S. A., Yılmaz, M. F., Şimşek, D., Ceyhan, E. ve Bakioğlu, F. (2016). Big five-personality trait and internet addiction: A meta-analytic review. *Computers in Human Behavior*, *63*, 35-40.

Keser, H. ve Güldüren, C. (2015). Bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *Kastamonu Eğitim Dergisi*, *23*(3), 1167-1184.

Kim, E. J., Namkoong, K., Ku, T. ve Kim, S. J. (2008). The relationship between online game addiction and aggression, self-control and narcissistic personality traits. *European Psychiatry*, *23*(3), 212-218.

Landers, R. N. ve Lounsbury, J. W. (2006). An investigation of Big Five and narrow personality traits in relation to Internet usage. *Computers in Human Behavior, 22*(2), 283-293.

Leszczyna, R. (2013). Cost assessment of computer security activities. *Computer Fraud & Security*, 7, 11-16.

Lounsbury, J. W. ve Gibson, L. W. (2009). *Personal Style Inventory: A personality measurement system for work and school settings*. Knoxville, TN: Resource Associates Inc.

Lounsbury, J. W., Steel, R. P., Loveland, J. M. ve Gibson, L. W. (2004). An investigation of personality traits in relation to adolescent school absenteeism. *Journal of Youth and Adolescence, 33*(5), 457-466.

Lynam, D. R. ve Miller, J. D. (2015). Psychopathy from a basic trait perspective: The utility of a five-factor model approach. *Journal of Personality, 83*(6), 611-626.

Mamonov, S. ve Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, 83, 32-44.

McBride, M., Carter, L. ve Warkentin, M. (2012). *Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies*. Erişim adresi: http://sites.duke.edu/ihss/files/2011/12/CyberSecurityFinalReport-Final_mcbride-2012.pdf

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. ve Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, 69, 151-156.

McCrae, R. R. ve Costa, P. T. (1987). Validation of the five-factor model of personality across instruments and observers. *Journal of Personality and Social Psychology*, *52*(1), 81-90.

McCrae, R. R. ve Costa, P. T. (1997). Personality trait structure as a human universal. *American Psychologist, 52*(5), 509.

McCrae, R. R. ve John, O. P. (1992). An introduction to the five-factor model and its applications. *Journal of Personality*, *60*(2), 175-215.

Mishna, F., Khoury-Kassabri, M., Gadalla, T. ve Daciuk, J. (2012). Risk factors for involvement in cyber bullying: Victims, bullies and bully–victims. *Children and Youth Services Review*, *34*(1), 63-70.

Moore, R. (2014). *Cybercrime: Investigating high-technology computer crime*. Routledge.

NICCS (2018). *Glossary*. Erişim adresi: https://niccs.us-cert.gov/glossary

Öğütçü, G., Testik, Ö. M. ve Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security, 56*, 83-93.

Pabian, S., De Backer, C. J. ve Vandebosch, H. (2015). Dark Triad personality traits and adolescent cyber-aggression. *Personality and Individual Differences, 75*, 41-46.

Pagani, M. (2005). *Encyclopedia of multimedia technology and networking*. IGI Global.

Peltier, T. R. (2006). Social engineering: Concepts and solutions. *Information Systems Security*, *15*(5), 13-21.

Pervin, L. A. ve John, O. P. (2013). *Personality: Theory and research* (12th ed.). Oxford: John Wiley and Sons.

Pusey, P. ve Sadera, W. A. (2011). Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. *Journal of Digital Learning in Teacher Education*, *28*(2), 82-85.

Rahim, N. H. A., Hamid, S., Mat Kiah, M. L., Shamshirband, S. ve Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes, 44*(4), 606-622.

Rezgui, Y. ve Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security, 27*(7-8), 241-253.

Roberts, B. W., Luo, J., Briley, D. A., Chow, P. I., Su, R. ve Hill, P. L. (2017). A systematic review of personality trait change through intervention. *Psychological Bulletin, 143*(2), 117.

Sasse, M. A., Brostoff, S. ve Weirich, D. (2001). Transforming the 'weakest link'-a human/computer interaction approach to usable and effective security. *BT Technology Journal, 19*(3), 122-131.

Servidio, R. (2014). Exploring the effects of demographic factors, Internet usage and personality traits on Internet addiction in a sample of Italian university students. *Computers in Human Behavior,* 35, 85-92.

SGEP (2018). *Siber güvenlik eğitim portalı*. Erişim adresi: https://egitim.sge.gov.tr

Shaw, R. S., Chen, C. C., Harris, A. L. ve Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education, 52*(1), 92-100.

Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., LaRose, R. ve Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior, 48*, 199-207.

Shropshire, J., Warkentin, M., Johnston, A. ve Schmidt, M. (2006). Personality and IT security: An application of the five-factor model. *AMCIS 2006 Proceedings* içinde (ss. 3443-3449).

Sithira, V. ve Nguwi, Y. Y. (2014). A study on the adolescent online security issues. *International Journal of Multidisciplinary and Current Research, 2*, 596-601.

Smidt, W. (2015). Big Five personality traits as predictors of the academic success of university and college students in early childhood education. *Journal of Education for Teaching*, *41*(4), 385-403.

Smrtnik-Vitulić, H. ve Zupančič, M. (2011). Personality traits as a predictor of academic achievement in adolescents. *Educational Studies, 37*(2), 127-140.

Standage, T. (2002). The weakest link. *The Economist, 365,* 11-16.

STATISTA. (2018). *E-commerce worldwide-Statistics ve facts*. Erişim adresi: https://www.statista.com/topics/871/online-shopping

Subramaniam, S. R. (2017). Cyber security awareness among Malaysian pre-university students. E-*Proceeding of the 6th Global Summit on Education*, 1-14.

Sussman, S., McCuller, W. J. ve Dent, C. W. (2003). The associations of social self-control, personality disorders, and demographics with drug use among high-risk youth. *Addictive Behaviors, 28*(6), 1159-1166.

Sümer, N., Lajunen, T. ve Özkan, T. (2005). Big five personality traits as the distal predictors of road accident involvement. Underwood, G. (Yay. haz.). *Traffic and Transport Psychology, (Chapter 18)* içinde. USA: Elsevier Ltd.

Svendsen, G. B., Johnsen, J. A. K., Almås-Sørensen, L. ve Vittersø, J. (2013). Personality and technology acceptance: The influence of personality factors on the core constructs of the Technology Acceptance Model. *Behaviour & Information Technology, 32*(4), 323-334.

Tekerek, M. ve Tekerek, A. (2013). A research on students' information security awareness. *Turkish Journal of Education, 2*(3), 61-70.

TCK (2018). *Türk Ceza Kanunu.* Erişim adresi: http://www.mevzuat.gov.tr/MevzuatMetin /1.5.5237.pdf

Thompson, N. McGill, T. J. ve Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, 70, 376-391.

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J. ve Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers ve Security, 59*, 138-150.

TÜİK (2018). *Hane halkı bilişim teknolojileri kullanım araştırması, 2016*. Erişim adresi: http://www.tuik.gov.tr/PreHaberBultenleri.do?id=21779

Uffen, J., Guhr, N. ve Breitner, M. (2012). Personality traits and information security management: An empirical study of information security executives. *International Conference on Information Systems* içinde (ss. 549-566).

Venkatesh, V., Morris, M. G., Davis, G. B. ve Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS quarterly*, 425-478.

Wagner, A. E. ve Brooke, C. (2007). Wasting time: The mission impossible with respect to technology-oriented security approaches. *Electronic Journal of Business Research Methods, 5*(2), 117-124.

Warrington, C. (2017). *A study of personality traits to explain employees' information security behavior among generational cohorts* (Yayımlanmamış doktora tezi). Capella University, Minneapolis, Amerika Birleşik Devletleri.

Woszczynski, A. B., Roth, P. L. ve Segars, A. H. (2002). Exploring the theoretical foundations of playfulness in computer interactions. *Computers in Human Behavior, 18*(4), 369-388.

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q. ve Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *Computers in Human Behavior,* 84, 375-382.

Yenilmez, K. (2008). Open primary education school students' opinions about mathematics television programmes. *Turkish Online Journal of Distance Education, 9*(4), 176-189.

Zhao, H. ve Seibert, S. E. (2006). The Big Five personality dimensions and entrepreneurial status: A meta-analytical review. *Journal of Applied Psychology*, *91*(2), 259-271.

Extended Abstract

Introduction

The data obtained from various studies reveal that the usage of internet is increasing rapidly. Although the Internet provides benefits for the society, it is also a known problem that people face various risks and threats by using the internet. By using the internet, individuals can conceal their identities more easily, and so cybercrimes committed on the internet can become easier and widespread (Moore, 2014). Therefore, every individual who uses the internet can be at risk of being exposed to a number of crimes committed online (Chen, Beaudoin & Hong, 2017). For this reason, cyber security is crucial to prevent negative consequences of cybercrimes (Furnell, 2008). In the literature, it has been emphasized that awareness of cyber security for individuals should be given priority over technological investments in order to ensure security in the cyber area (Keser & Güldüren, 2015). For this reason, it is recommended to conduct studies focusing on human-based variables in cyber security. In this regard, this study was carried out to investigate the relationship between cyber security behaviors of university students with big five personality traits, namely openness to experience, conscientiousness, agreeableness, neuroticism and extroversion. In addition, it was also investigated whether the students' cyber security behavior levels differ according to gender, grade, department, status of receiving information security training and weekly internet use.

Method

In this study, it was aimed to reveal the existing situation of university students' cyber security behaviors and big five personality traits and to examine the relationship between these two variables. In addition, whether university students' cyber security behaviors are differed according to various variables were also examined. For this reason, descriptive research model was used in the study (Fraenkel, Wallen & Hyun, 2012). The participants of this study consisted of 420 students from different universities, departments and grades. In this study, three data collection tools were used to collect data. These tools are Personal Information Form developed by the researchers, Personal Cyber Security Provision Scale and Big Five Personality Traits Scale. In order to decide which statistical methods to use in the analysis of the data, normality test was performed for the dependent variables in the study. For the normality test, the skewness and kurtosis values of the variables are examined. Skewness and kurtosis values indicated the normal distribution of the data. Therefore, the use of parametric tests was considered appropriate for the analysis of data in this study. As a result, Pearson correlation coefficient, independent samples t-test and one-way analysis of variance (ANOVA) were used to analyze the data.

Results

Findings from the study showed that students' levels of cyber security behavior were at an acceptable level. Moreover, while students considered themselves as agreeable, conscientious, and open to experience, they remained neutral in deciding whether they were extroverted and neurotic. Findings also showed that the students' cyber safety behaviors showed a significant relationship with all five factor personality dimensions, namely, openness to experience, conscientiousness, agreeableness, neuroticism and extroversion. Openness to experience has been identified as the personality trait with strongest relationship with cyber security behaviors, whereas extroversion has the weakest. In addition, the students from CEIT and computer programming departments, those in the 3rd and 4th grades, those who received information

security training and those using the internet 6-10 hours weekly were found to be more adequate in terms of cyber security behavior levels.

Discussion and Conclusions

One of the findings of the study is that university students' cyber security behaviors were at an acceptable level. The scores from the whole scale as well as sub-dimensions indicated that students often exhibit cyber security behaviors in their daily lives. According to this, it was seen that university students gave importance to privacy protection, avoiding unsafe, taking precautions, protecting payment information and leaving no digital footprint. This finding is parallel to some of the study findings (Karacı, Akyüz & Bilgici, 2017; Pusey & Seadra), while there are other studies that do not support this finding (Akgün & Topal, 2015; Tekerek & Tekerek, 2013). Another finding revealed that students considered themselves as agreeable, conscientious, and open to experience. However, they could not decide whether they were extroverted and neurotic individuals.

Correlational analysis resulted that all personality traits showed significant relationship with students' cyber security behaviors. In addition, openness to experience had the highest level of relationship, whereas the extroversion had the lowest one. In the light of these findings about personality traits along with the supportive evidences from the literature, it can be deduced that individuals who are open to experience (McBride, Carter & Warkentin, 2012; McCormac et al., 2017), conscientious (Gratian et al., 2018; Halevi et al., 2016; McCormac et al., 2017), emotionally stable (McCormac et al., 2017), agreeable (McCormac et al., 2017) and extrovert (Gratian et al., 2018) perform cyber security behaviors in their daily lives in the more desired and acceptable level.

Results also reveal that gender did not play a significant role in cyber security behaviors of university students. Therefore, it can be stated that male and female students are equal in cyber security behaviors. This finding was supported by several studies (Gökmen & Akgün, 2015; Karacı, Akyüz & Bilgici, 2017; Subramaniam, 2017; Yan et al., 2018). However, there are also studies in which gender was found to be significant variable differentiating cyber security behaviors in favor of males (Akgün & Topal, 2015) or females (Tekerek & Tekerek, 2013).

Another finding is that junior and senior students were more successful in cyber security in relation to freshman, sophomore and associate degree students. In addition, computer related departments like CEIT and computer programming were also found to be more careful about cyber security behaviors. In addition to these, students who previously received training on information security were significantly scored higher on the cyber security behaviors. For this reason, it is possible to state that information security trainings contribute individuals on cyber security issues. This finding is supported by the research conducted by Karacı, Akyüz and Bilgici (2017) on university students. Lastly, weekly internet use time was examined if it is an effective variable on cyber security behaviors. Findings showed that students using the internet 6-10 hours weekly were found to be more adequate in terms of cyber security behavior levels.

In the light of the findings of this study, it is suggested to emphasize the importance of cyber security in the undergraduate departments that are not closely related to the computer domain. In addition, training and activities can be organized for students at associate degree level to raise their awareness about cyber security behaviors. Moreover, it can be suggested that the cyber security issues need to be studied effectively in the university curricula. In addition to curricular interventions, some extracurricular activities such as online awareness-raising activities for cyber security, face to face trainings and conferences can be organized. Furthermore, activities on developing personality traits such as openness to experience, conscientiousness, agreeableness and extroversion and on suppressing personality traits such as neuroticism can help individuals perform better on cyber security behaviors.

It is also possible to provide recommendations for future research. This study can be repeated in a context where the number of students is higher and the departments are more diversified, whereby more valid and reliable findings can be achieved. In addition, participants in this study are limited to university students. In this respect, a study involving students at primary and high school level can be carried out so that the findings can be evaluated comparatively according to different educational levels.