Yönetim, Ekonomi ve Pazarlama Araştırmaları Dergisi
2021, 5(3): 130-150
DOI: 10.29226/TR1001.2021.261
ISSN: 2587–0785 Dergi web sayfası: https://www.yepad.org

ARAŞTIRMA MAKALESİ

Tüketicilerin Sosyal Mühendislik ve Siber Güvenlik Farkındalıklarının Online Alışveriş Niyetleri Üzerindeki Etkisinin Ölçülmesi

Bilim uzmanı, Gülcihan Aydaner, Bandırma Onyedi Eylül Üniversitesi, Uluslararası Ticaret ve Lojistik Ana Bilim Dalı, e-posta: gulcihan.aydaner@gmail.com
ORCID ID: 0000-0003-0244-7159

Doç. Dr. Özer Yılmaz, Bandırma Onyedi Eylül Üniversitesi, Uluslararası Ticaret ve Lojistik Bölümü, e-posta: oyilmaz@bandirma.edu.tr
ORCID ID: 0000-0002-8207- 8682

Doç. Dr. Ufuk Çelik, Bandırma Onyedi Eylül Üniversitesi, Yönetim Bilişim Sistemleri Bölümü, e-posta ucelik@bandirma.edu.tr
ORCID ID: 0000-0003-3063-6272

Öz

Bu çalışmada; tüketicilerin online alışverişlerinde siber güvenlik ve sosyal mühendislik farkındalıklarının ölçülmesi amaçlanmaktadır. Çalışma için öncelikle anket formu oluşturulmuş ve oluşturulan form ile 18-21 Şubat 2019 tarihleri arasında Bandırma Onyedi Eylül Üniversitesi Merkez Kampüsünde eğitim gören 693 öğrenciden kolayda örnekleme tekniği ile veri toplanmıştır. Verilerin analizinde tanımlayıcı istatistikler ve Yapısal Eşitlik Modellemesinden yararlanılmıştır. Yapılan analizler sonucunda tüketicilerin siber güvenlik farkındalıklarının hem online alışveriş niyetleri hem de sosyal mühendislik farkındalıkları üzerinde pozitif yönlü ve anlamlı etkisinin olduğu; sosyal mühendislik farkındalıklarının ise online alışveriş üzerinde anlamlı etkisinin olmadığı yönünde bulgulara ulaşılmıştır. Çalışmada ayrıca tüketicilerin, siber güvenlik ve sosyal mühendislik farkındalık karneleri çıkarılmıştır. Karneler, tüketicilerin internet sitelerinde, siber tehditleri ihmâl ettiklerini ve görmezden geldiklerini göstermektedir.

Anahtar Kelimeler: Siber Güvenlik, Sosyal Mühendislik, Online Alışveriş, Online Güvenlik, Dijital Vatandaşlık.
Makale Gönderme Tarihi: 09.02.2021
Makale Kabul Tarihi: 17.04.2021

Önerilen Atıf: Aydaner, G., Yılmaz, Ö., Çelik, U. (2021). Tüketicilerin Sosyal Mühendislik ve Siber Güvenlik Farkındalıklarının Online Alışveriş Niyetleri Üzerindeki Etkisinin Ölçülmesi, *Yönetim, Ekonomi ve Pazarlama Araştırmaları Dergisi*, 5(3), 130-150.

***Bu makale Gülcihan AYDANER'İN yüksek lisans tezinden üretilmiştir.*

Journal of Management, Economic and Marketing Research
2021, 5(3): 130-150
DOI: 10.29226/TR1001.2021.261
ISSN: 2587–0785 Journal Homepage: https://www.yepad.org

RESEARCH PAPER

Measuring The Effect Of Consumers' Social Engineering and Cyber Security Awareness on Online Shoppıng Intention

Scientists, Gülcihan Aydaner, Bandırma Onyedi Eylül University, International Trade and Logictic Departure, e-mail: gulcihan.aydaner@gmail.com
ORCID ID: 0000-0003-0244-7159

Assoc. Prof. Dr. Özer Yılmaz, Bandırma Onyedi Eylül University, International Trade and Logictic Departure, e-mail: oyilmaz@bandirma.edu.tr
ORCID ID: 0000-0002-8207- 8682

Assoc. Prof. Dr. Ufuk Çelik, Bandırma Onyedi Eylül University, Management Information Systems Departure, e-mail: ucelik@bandirma.edu.tr
ORCID ID: 0000-0003-3063-6272

Abstract

The aim of this study is to measure the sosyal engineering and cyber secrity awareness of online shoppers. The survey tool was used in the research The surveys were conducted on 693 students who has studying in Bandırma Onyedi Eylul University on February 18-21 2019. The data were collected using the convenience sampling technique. Descriptive statistics and Structural Equation Modeling were used in the analysis of the data. The results of Structural Equation Modelling shows that consumer's cyber security awareness has a positive and significant effect on both online shopping intentions and social engineering awareness. Another finding obtained in the study is social engineering awareness does not have a significant effect on online shopping intentions. In addition, cyber security and social engineering awareness reports of consumer were created in the study. Reports show that consumers neglect and ignore cyber threats on their websites.

Keywords: Cyber Security, Social Engineering, Online Shopping, Online Security, Digital Citizenship
Received: 09.02.2021
Accepted: 17.04.2021

Suggested Citation: Aydaner, G., Yılmaz, Ö., Çelik, U. (2021). Measuring The Effect Of Consumers' Social Engineering and Cyber Security Awareness on Online Shoppıng Intention, *Yönetim, Ekonomi ve Pazarlama Araştırmaları Dergisi,* 5(3), 130-150.

GİRİŞ

Günümüz teknolojisinde elektronik platformlardan sunulan mal ve hizmetleri (internet bankacılığı, e-ticaret, e-fatura, e-bilet, e-devlet vs.) kullanan tüketicilerin sayısı her geçen gün artmaktadır. Bu durum beraberinde kötü niyetli saldırganların bu platformlara illegal erişim isteklerinin günden güne artmasına neden olmaktadır (Gülmüş, 2010:3). İnternet yoluyla ticaretin başladığı zamanlardan günümüze kadar geçilen sürede ortaya çıkan güvenlik sorunları, tüketicilerin davranışlarında belirgin değişikliğe neden olmuştur. E-ticaret sitelerinde yaşanan güvenlik ihlâlleri nedeniyle tüketicilerin mali ve son derece hassas kişisel bilgileri manipüle edilir hale gelmiştir (Suh ve Han, 2003:155). Online ticaretin gelişimiyle birlikte sahte banka web sitelerinin oluşturulması neticesinde birçok kişi mağdur edilmiştir. Teknoloji şirketlerinin yaptıkları araştırmalar ile 2020 yılının ilk yarısında 1,7 milyon sahte site aracılığıyla, kimlik avı saldırılarının ve dolandırıcılık faaliyetlerinin kayıtlara geçtiği tespit edilmiştir. Günde 18 binden fazla sahte web sitesinin kurulduğu, üstelik bu sitelerinin çoğunluğunun markalara ait olmasının endişe verici olduğu belirtilmektedir. (Tursun, 2020). Bilişim suçlarının büyük bir çoğunluğu, insanlar üzerinden gerçekleşen aldatmaca yani sosyal mühendislik saldırıları ile siber saldırıların birlikte kullanılması sonucu ortaya çıkmaktadır. Bu saldırıları etkisiz hale getirebilmek ise insan faktörü üzerinde güvenli davranış bilincine ve farkındalığa dayanmaktadır (Şahinaslan, 2013:7). Bu kapsamda, bilişim suçlarına yönelik atılacak en etkili adım ise online platformlarda alışveriş yapan tüketicilerin bilinçlendirilmesi olacaktır.

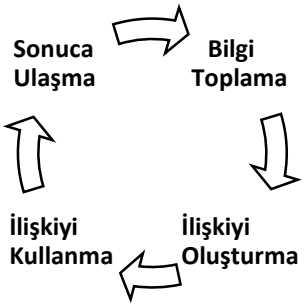
İnsanların büyük çoğunluğu online ağlarda hak ihlâllerinin teknik yollardan olduğunu düşünmektedir. Oysa teknik önlemlerle asla engellenemeyecek sosyal mühendislik saldırıları, online sistemleri istismar etmenin en iyi yollarından biridir (Tosun,2015:8,15). Online sistemlerde gerçekleştirilen çeşitli siber saldırı ve sosyal mühendislik aldatmaca yöntemleri ile tüketicilere çeşitli tuzaklar kurulup, kullanıcıların kritik önem düzeyine sahip kişisel bilgileri ele geçirilerek tüketiciler dolandırıcı sitelere yönlendirebilmektedirler (Şahinaslan ve diğerleri 2013). Bu noktada teknolojinin getirilerini doğru ölçüp değerlendirmek için gerekli araçlara ve bilgiye sahip olmamız gerekmektedir. (Frischmann 2014, 2-3). Bu çalışma ile online alışveriş yapan tüketicilerin; siber dünyadaki güvenlik kanaatleri, online gizlilik ve güvenlik farkındalıkları ortaya konulmaya çalışılmıştır. Ayrıca online tüketicilerin; siber güvenlik farkındalıkları ile sosyal mühendislik farkındalıkları ve online alışveriş niyetleri arasındaki ilişki ve bu ilişkinin hangi seviyede olduğu tespit edilmeye çalışılmıştır.

KAVRAMSAL ÇERÇEVE

Sosyal Mühendislik

İnsanların çoğunluğu, birçok konuda kandırılma veya aldatılma olasılığının çok düşük olduğunu düşünmektedir. Konu güvenlik olduğunda akıllara ilk gelen genellikle teknik güvenlik tedbirleridir. Oysaki bilgi güvenliğinin sağlanmasında kilit nokta insan faktörüdür. İnsan faktörü, güvenlikte en zayıf halkadır (Mitnick ve William, 2017). Sosyal mühendislik kavramında saldırgan, insan faktörünü ileri düzeyde kullanan saldırı tekniklerinde, kişiyi etkileme ve ikna etme yoluyla normal şartlarda kişilerin gizlemeleri ve paylaşmamaları gereken bilgileri ustalıkla ele geçirebilmektedir. Tüm gizli ve kamuya açılmaması gereken kişisel verileri ve bilgileri ele geçirme sanatına sosyal mühendislik denilmektedir (Tübitak Bilgem,2018). Başka bir ifadeyle sosyal mühendislik kimlik hırsızlığıdır. Hedefte bulunan şahsa ait kişisel bilgilerin, başkaları tarafından yetkisiz kullanılması suretiyle yapılan dolandırıcılık yöntemidir (Gündüz ve Resul 2016:9,18).Sosyal mühendisler günümüzde statik ortamları (disk,teyp, cd, dvd vb.) kullanarak veya göndericiden alıcıya ulaşan dinamik ortamdaki verileri gizlilik kurallarını ihlal ederek ele geçirmektedirler. Saldırganlar yetkileri olmayan gizli bilgilere pek çok illegal yolla erişebilmektedir. Örnek olarak, şifreli dosyaların bulunduğu veri tabanlarının çalınması veya bilgisayar başında çalışan bir kullanıcının fark etmeyeceği bir şekilde gözetlenerek, şifre ve benzeri bilgilerinin ele geçirilmesi sosyal mühendislik saldırı tiplerinden bazılarıdır (Göz ve Allahverdi, 2011:51). Başka bir sosyal mühendislik saldırısı olan kimlik avı saldırısında, saldırgan güvenilir bir üçüncü tarafın kimliğine bürünerek kullanıcının hassas bilgilerini ele geçirmeye çalışır (Jagatic ve diğerleri 2007:94-100). İnsanların özel hayatlarını sosyal ağlarda

paylaşmaya istekli olmaları sosyal mühendislerin iştahını kabartmaktadır. Hedefinde bulunan kişiye arkadaşlık isteği göndermek suretiyle online arkadaşlık kuran bir sosyal mühendis, kurbanının eğitim durumu, yaşı, mesleği, çalıştığı kurumu ve hobileri hakkında bilgi sahibi olduğunda taktik değiştirerek kişiye göre kendini güncelleyecek ve saldırıya geçecektir (Tosun 2015:8-15). Bir sosyal mühendisin kişiye göre kendisini nasıl güncelleyeceği şekil 1 ile görselleştirilmiştir.



Şekil 1: Sosyal Mühendislik Saldırılarının Yaşam Döngüsü

Kaynak: Gündüz ve Daş 2016

Sosyal mühendislerin kişilere göre kendilerini güncellemelerinde en iyi kullandıkları platformlar sosyal ağlardır. İnsanların sosyal ağlarda; konum, durum, fotoğraf ve iş ile aile hayatları hakkında farkında olarak ya da olmayarak yapmış oldukları paylaşımlar bireylerin, sosyal ve iş hayatlarıyla ilgili birçok bilgiyi ortaya sermektedir. Sosyal ağları kişisel çıkarları uğrana istismar eden kişilerin sayıları her geçen gün artmaktadır. Bu istismarın en önemli sebebi ise bilişim korsanlarının çok istemelerine rağmen ulaşamadıkları bilgilerin, sosyal ağlarda kullanıcılar tarafından bizzat ifşa edilip kolaylıkla ele verilmesidir. Sosyal ağlarda alınması gereken güvenlik tedbirleri incelendiğinde konu; sosyal çözümler, teknik çözümler ve yasal çözümler olmak üzere üç başlık altında incelenmektedir (Yavanoğlu, Sağıroğlu ve Çolak, 2012: 19).

Özellikle son yıllarda sosyal ağların artan popülaritesi ve yaygın kullanımı, sosyal ağ platformları arasında hesapların birleştirilmesi fikrini doğurmuştur. Müngen ve diğerlerinin 2020 yılında hazırlamış oldukları ; "Çoklu Sosyal Ağlarda Aynı Kullanıcıları Belirleme Yöntemi" isimli çalışmaları göstermiştir ki çoklu sosyal ağlardaki veriler tek bir uzayda birleştirilebilmektedir. Böylelikle çoklu sosyal ağ kullanımının önü açılmıştır (Müngen ve diğerleri, 2020;1-12). Bu çalışmanın sonucu, sosyal ağların kullanımının gün geçtikçe gelişerek değişeceğini ifade etmektedir. Bu değişimin nasıl gerçekleşeceğinin öngörüldüğü başka bir çalışmada, sosyal ağlarda kullanıcıları birbirine bağlayan Web 2.0 teknolojisinden, Web 3.0 (semantik web) teknolojilerine geçildiği vurgulanmaktadır. Web 3.0 teknolojisi ağ üzerindeki bilgisayarların birbiriyle etkileşimini ifade etmektedir. Bilgiyi organize etme ve kolektif yapay zekaya sahip olma niteliği taşıyan bu teknoloji, artırılmış gerçeklik özelliği ile sosyal ağlarda web yapısını çok daha ileri seviyelere taşıyacaktır (Koçyiğit ve Koçyiğit, 2018: 45-47). Bu noktada özellikle sosyal ağlarda kişisel ve finansal verilerin ele geçirilmesi sanatı olarak tanımlanan sosyal mühendislik saldırılarında artış yaşanacağı kolaylıkla öngörülebilmektedir. Sosyal mühendislik alanında yapılan son çalışmalar mevcut saldırıları algılama tekniklerinde, derin öğrenme yönteminin kullanılabileceğini ileri sürmektedir. Hibrit ve Oltalama kelimelerinin birleşiminden türetilen h-olta derin öğrenme yönteminin kullanılması, özellikle kimlik avı saldırıları ve e-posta sistemlerinin tahmin edilmesinde yüksek doğruluk payına sahiptir. Fakat bu sistemler kabul edilebilir hızda ve düşük hata oranları ile üretilmeye çalışılmalıdır. Çünkü sosyal mühendislik saldırılarının tespit edilmesinde hesaplama süreleri tam anlamıyla minimize edilememektedir. Bunun için daha verimli algoritmalar yazılmalıdır. Bu nedenlerle sosyal mühendislik saldırılarına karşı, insanların farkındalıklarının arttırılması, yapılması gereken en önemli çalışma olacaktır (Ahi, 2020:91).

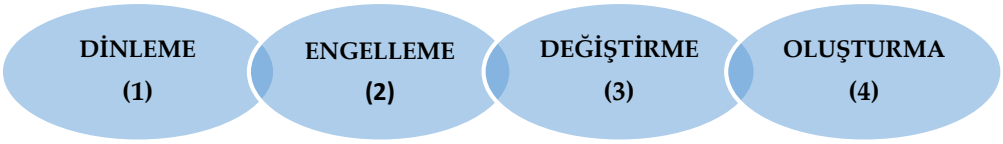
Sosyal mühendislik saldırılarında en kestirme yol sosyal ağları kullanmaktır. Son çalışmalar Türkiye'de yaşayan bireylerin sosyal medya üzerinde konum vb. bilgileri paylaşma konusunda yeterli farkındalığa sahip olmadıklarını göstermektedir (Aslan vd., 2020:1-8). Oysaki önemsiz gibi gözüken

konum bilgisinin sosyal ağlarda paylaşılması, çok basit bir öngörüyle hırsızlara ve dolandırıcılara davetiye çıkarmaktan farksızdır. İnternette paylaştığımız her bilginin ve verinin önemi toplumsal düzeyde kavranamadığı takdirde yazılı ve görsel medyada izlediğimiz dolandırıcılık haberleri her geçen gün artmaya devam edecektir. Bu noktada farkında olmayarak yapılan her paylaşım kişisel veri güvenliğimizi tehdit etmektedir. Kişisel veri güvenliği kişilerin mahremiyetleri olarak tanımlanan özel alanlarıdır. Dolayısıyla özgürlüğümüzdür. Bu noktada bireylerin kendi hayatları üzerindeki hakimiyet hakları, kişisel verileri üzerinde kontrol ve denetim haklarına sahip olmalarıyla mümkündür."Kişisel verilerin korunması kişinin kendisinin korunmasıdır" (Bilir, 2021:178). Yapılan çalışmalar kişisel verilere yönelik artan saldırıların en önemli sebebinin farkındalık eksikliği olduğunu göstermektedir (Ahn, Shehab ve Sguicciarini, 2011:10).

Siber Güvenlik

Çağımızda siber güvenlik kavramının önemi, küresel bir konu haline gelmiştir. Bugün elliden fazla ülke kendi siber güvenlik strateji belgesini ana hatlarıyla yayınlamıştır. Bu stratejiler özetle siber uzayda resmi bir duruş olarak değerlendirilebilir. Uluslararası Telekomünikasyon Kurumu, Union (ITU) siber güvenlik kavramını özetle; araçlar ve politikalardan oluşan bir güvenlik topluluğu olarak tanımlamaktadır (Solms ve Niekerk, 2013:97). Siber saldırıların kaynakları hakkında FBI ve Cybercrime Bilgisayar Güvenliği Enstitüsü tarafından yapılan ortak çalışma sonucunda güvenlik ihlallerinin %71'inin içerdekiler tarafından gerçekleştirildiği ortaya çıkarılmıştır (Byres ve Lowe, 2004:213,218). İçerdekilerden kaynaklanan kurumsal düzeyde siber güvenlik risklerinin %71 düzeyinde olması risklerin aslında sosyal mühendislik saldırılarından kaynaklandığını ortaya koymaktadır. Bu nedenle siber güvenlik kavramında teknik risklerin yanında bilişsel düzeyde farkındalık riskleri de önemli yer tutmaktadır.

Günümüzde siber savaş ve saldırılar sırasında uyulması gereken hukuk kurallarını düzenleyen hiçbir bağlayıcılığı ve caydırıcılığı olmayan sadece referans kaynak niteliği taşıyan Tallin El Kitabı dışında uluslararası alanda yapılmış bir çalışma bulunmamaktadır (Çeliktaş, 2016). AB'nin siber güvenlik politikaları büyük oranda kurumsallaşma merkezli gelişmektedir. Fakat bütüncül tutarlı bir politikası bulunmamaktadır. AB her ne kadar tutarlı olmaya çalışsa da somut anlamda bunu başaramamıştır. Bu nedenle siber güvenliğin sağlanması hususunda AB'nin dönüşüme ihtiyacı vardır (Köksoy, 2020:668). Avrupa birliği siber dünyaya ayak uydurmayı sözleşmeden ziyade yasa ile güvence altına almaya çalışarak güvenlik açıklarıyla ilgili birtakım cezai yaptırımlar öngörmüş ancak hangi güvenlik açığına karşı nasıl bir cezai yaptırım uygulanacağını detaylı açıklamaması sebebiyle yasaları çerçeve olarak kalmış ve detaylı bir yasaları olmamıştır (Nezgıtlı ve Benzer, 2020:18). Avrupa komisyonu siber suçları üç şekilde tanımlamıştır. İlki elektronik haberleşme ve bilgi sistemleri üzerinden işlenen dolandırıcılık ve sahtecilik suçu şeklinde tanımlanmaktadır. İkinci tanım; yasadışı içeriğin elektronik ortam üzerinden yayılmasıdır. Irkçılık, nefret söylemleri ve cinsel çocuk istismarı gibi suçlar, siber suç türlerine örnektir. Üçüncü tanımlama ise; bilgi sistemleri hizmetinin aksatılması, durdurulması veya hacklenmesidir (Anderson ve diğerleri 2013:265,300). İnternette gerçekleştirilen hacking teknikleri şekil 2 ile gösterilmektedir.



Şekil 2: Hacking Teknikleri

Kaynak: Berkay, 2009

İçinde bulunduğumuz dijital çağda gündemden düşmemesi ve üzerinde sıkı çalışmalar yapılması gereken bir diğer başlık devletlerin siber alanlardaki güvenlik stratejileri olmalıdır. Devletlerin bilişim sistemleri üzerindeki gücü, yeni medya araçlarını yönetebilme yeteneklerine ve teknolojik gelişmişliklerine bağlı olarak değişmektedir. Örneğin bir savaş sırasında kritik alt yapılara yönelik

siber silah olarak kullanılan Stuxnet, askeri savaş stratejilerinde öncelikle hedefte olan ülkenin iletişim sistemlerini kesmek, zayıflatmak veya enerji kaynaklarına yönelik benzer müdahalelerde bulunmak amacını taşımaktadır. Siber güvenlik stratejilerinde etkili yöntemlerin geliştirilmesi, SCADA sistemleri gibi endüstriyel kritik altyapıları hedef alan tehditleri engelleyecektir (Holat, 2021:118). Fakat ülkemizde kritik alt yapıların geliştirilmesi konusu sessizliğini korumaktadır. Amerika ve Avrupa'da kritik alt yapıların korunması sürekli gündemde kaldığı için konu daha hızlı çözülmektedir. Türkiye'de kritik alt yapıların korunmasına yönelik gelişimi etkileyen kurumsal ve yasal boşluklar bulunmaktadır. Bu nedenle Avrupa ve Amerika'dan bu alanda geridedir. Bu nedenle kritik alt yapıların güvenliğine ilişkin politikalar geliştirilmeli ve bu politikaların başarısı analiz edilmelidir (Düveroğlu,2020:115-119)

Türkiye'nin siber güvenlik öngörüsünün, alanında uzman kişilerle yapılan odak grup toplantıları ve anketleriyle çalışıldığı bir doktora tezinde ortaya çıkan sonuçlara göre; Türkiye, ilk 10'da yer alan siber saldırgan ülkeler arasında yer almayacaktır. Ancak siber saldırının hedefleri arasında bulunan ülkeler arasında 4. sırada yer almaktadır. Türkiye'de 61 aktif teknoloji geliştirme bölgesinin bulunduğu tespit edilmiştir. Yazar, siber güvenlikte, teknoloji öngörü çalışmalarının yapılmasının hayati önem taşıdığı sonucuna ulaşmıştır. Teknoloji öngörü çalışmaları, siber güvenlikte bir vizyona sahip olmanın ve kararlı bir şekilde bu alana yatırım yapmanın başlangıç noktasıdır. Tezde yapılan SWOT analizine göre Türkiye'nin siber güvenlikte zayıf yönleri, güçlü yönlerinden fazladır (17 güçlü yön, 31 zayıf yön) bununla birlikte fırsatlar tehditlerden daha fazladır (56 fırsat, 15 tehdit).Yapılan STEEPLE analizinde ise siber güvenlikte 85 faktör sıralanmıştır. Bu faktörlerin 17'si sosyal, 30'u teknolojik,14'ü ekonomik, 14'ü politik, 5'i yasal ve 2'si etik faktörlerdir. (Çiftçi,2019:155-163). STEEPLE analizinin sonuçları göstermektedir ki siber güvenlik kavramı çok boyutlu ve disiplinler üstü bir bilim dalıdır.

Online Alışveriş

Son yıllarda yapılan araştırmalar insanların geleneksel alışveriş yöntemlerinden giderek uzaklaştıklarını göstermektedir. Tüketiciler artık online platformlardan alışveriş yapmayı hem daha az zahmetli hem daha hızlı, hem de daha eğlenceli bulduklarını ifade etmektedirler. Online alışveriş sitelerinin, tüketicilere 7 gün 24 saat hizmet sunması ve online pazarlama politikalarının tüketicilerin ihtiyaçlarına cevap verecek şekilde güncellenmesi, online alışverişlere talebi arttırmıştır (Rahman, 2018:8-9). Online turizm pazarlamasında Güney Kore'de yapılan bir araştırma algılanan güvenlik unsurunun talebi etkilemede en önemli unsur olduğunu ortaya koymaktadır (Ja Kim, Chung ve Ki Lee, 2011:264).

Avrupa'da online işletmeler pazarlamada başarılı olabilmek için 5C stratejisini kullanmaktadırlar. 5C stratejisi şu şekilde özetlenir (Angeli ve Kundler, 2006:623-624).

- Müşterinin sitede geçirdiği zamanı, sitenin içeriği %33 oranında arttırmaktadır.
- Sitenin müşterine kolaylıkla sipariş verme imkânı sağlaması, ticari ilişkilerini %33 oranında arttırmaktadır.
- Sitenin, müşterileri arasındaki fikir alışverişlerini desteklemesi, başarıyı %11 oranında arttırmaktadır.
- Sitenin, danışmanlık hizmeti vermesi, güveni ve yeterliliği %11 oranında arttırmaktadır.
- Potansiyel müşterilere reklam ile ulaşma başarıyı %11 oranında arttırmaktadır.

Online ticari işletmelerin, ödeme mekanizmaları, web sitelerinin tasarımı, tüketici hizmetleri, lojistik destekleri önemli etkiye sahip olsa da tüketicilerin online alışverişlerinde dikkatli olmaları gereken ana konu, online platformlarda ki güvenlik ihlâllerinden ve beklenmeyen teknik hatalardan korunmaktır (Turban ve diğerleri, 2018:362-364) Bu noktada online tüketicilerin üzerine düşen görev ise online platformlarda güvenlik risklerini iyi yönetebilmeleri için yüksek bilinç düzeyi ve yeterli bilgi birikimine sahip olabilmeyi öğrenmeleri olacaktır (Bahadur, Chan, Weber 2002:262-264). Online alışverişlerde tüketicileri en çok korkutan konulardan bir diğeri ise internette kişisel bilgilerinin gizliliğinin tehlikede olmasıdır. Fakat online alışveriş siteleri için kişisel bilgiler, pazarlamanın ana

araçları arasındadır. Bu nedenle bu tür bilgiler diğer online ticaret siteleriyle paylaşılmaktadır. Bu noktada kişisel bilgilerin online alışveriş siteleri arasındaki ikincil paylaşımı, online alışveriş sitelerinin sağlayıcılarıyla, online tüketiciler arasında ciddi düzeyde çatışma yaratmaktadır. Ayrıca internetin getirdiği veri ambarı fırsatları ve veri madenciliği operasyonları günümüzde hiç olmadığı kadar istismar edilmektedir (Hoffman, Novak ve Peralta, 1999:83). Online platformlardaki tüm bu risklerin yanında Covid-19 salgınıyla mücadele sürecinde ülkemizde yapılan son araştırmalar göstermektedir ki online alışverişlerde %64,5 oranında değişim yaşanmıştır (Danışmaz, 2020:89). Başka bir çalışmada ise aksi yönde sonuçlara ulaşılmıştır. Tüketici güvenini ölçen 2020 yılında yapılmış araştırmada, küresel pandemiyle birlikte artan online alışverişlere rağmen, yüz yüze alışverişlerle kıyaslandığında, online alışverişlere güvenilmediği sonucuna ulaşılmıştır. Ayrıca online alışveriş sitelerinin iade işlemlerini kolaylaştırması, sorunsuz ve hızlı teslimat yapması, online alışverişlerde devlet desteği gibi faktörlerin online alışverişlere olan güveni arttıracağı tespit edilmiştir (Akçacı ve Kurt, 2020: 414).

Literatürdeki Mevcut Araştırmalar

Sosyal mühendislik, siber güvenlik ve online alışveriş ile ilgili literatürde yer alan bazı araştırmalar Tablo 1 ile görselleştirilmiştir.

Tablo 1: Geçmiş Yıl Çalışmaları

Araştırma	Araştırmanın Konusu ve Örneklemi	Araştırmanın Bulguları
Aksoğan ve diğerleri, 2018	*Siber Güvenlik:* İletişim fakültesinde öğrenim gören 368 öğrencinin siber güvenlik farkındalıkları ölçülmüştür.	Öğrencilerin büyük çoğunluğunun siber güvenlik farkındalıklarının düşük olduğu tespit edilmiştir.
Yılmaz, 2018	*Online Alışveriş:* Tüketicilerin online alışveriş niyetlerinin teknoloji kabul modeli bağlamında incelendiği bir araştırmada 355 kişiden veri toplanmıştır.	Online alışveriş sitelerinde, algılanan kullanım kolaylığının hem algılanan fayda hem de online alışveriş niyetini pozitif yönlü etkilediğine, algılanan ürün riskinin ise hem online alışveriş niyetini hem de algılanan faydayı negatif yönlü etkilediğine dair bulgulara ulaşılmıştır.
Barışkan, 2017	*Sosyal Mühendislik ve Siber Güvenlik:* 18-23 yaş arası katılımcılara uygulanan ankette bireylerin sosyal mühendislik ve siber güvenlik saldırılarına ne düzeyde açık oldukları sorgulanmıştır.	Katılımcıların büyük çoğunluğunun siber güvenlikte giriş seviyesinde bilgiye sahip oldukları ve çok azının sosyal mühendislik saldırılarından haberdar oldukları tespit edilmiştir.
El-Hassan, 2016	*Online Alışveriş:* 301 kişiden elde edilen verilere göre, (Maribor Üniversitesinden (Slovenya) 101 anket, Mersin Üniversitesinden 200 anket)	İki ülke arasında tüketicilerin seyahat sektöründe online alışveriş niyetlerinin şekillenmesinde en etkili olan faktörlerin güvenlik, güven ve kullanım kolaylığı olduğu tespit edilmiştir.
Tosun, 2015	*Sosyal Mühendislik:* 3994 kişiye sosyal mühendislik saldırı tekniklerinden kimlik avı ve kişisel iletişim kurma yoluyla gerçekleşen sosyal mühendislik saldırıları uygulanmıştır.	Kişiye hangi saldırıda bulunulacağı eğer doğru tespit edilirse %59,5 oranında başarı sağlanmaktadır. Saldırılarda insanların korku, dikkatsizlik, yardım ve konfor bölgesi gibi zafiyetleri kullanılmıştır. Korku zafiyeti baskındır.

Dai ve diğerleri 2015	*Sosyal Mühendislik ve Siber Güvenlik:* Bireylerin bilgi güvenliği farkındalıklarını değerlendirmek için 12 sağlıklı yetişkinin üzerinde, online finansal ödemelerinde elektro fizyolojik sinyallerin tepkisine ilişkin deneysel bir çalışma yürütülmüştür. Deneklerin cep telefonlarına sahtekârlık metin mesajları ve online ödemelerde kullanılan sahtekârlık mesajları atılmıştır.	EEG sinyallerinin değerlendirme için iyi bir yöntem olduğuna karar verilmiştir.Bireylerin sinyallere verdikleri reaksiyonlarda EEG sinyallerini kullanmak doğru bir yöntemdir.
Budak, 2015	*Siber Güvenlik:* Erzurum'da mesleki ve teknik liselerdeki öğrencilerin siber suç farkındalıkları araştırılmıştır.	Öğrencilerin internette siber saldırılara uğramaları ile siber suçları algılama ve aldıkları önlemler arasında anlamlı bir farklılık tespit edilmemiştir. Öğrencilere yapılan siber saldırılar, siber güvenlik farkındalıklarını etkilememiştir.

YÖNTEM

Bilişim suçlarının büyük çoğunluğu insanlar üzerinden gerçekleşen aldatmaca yani sosyal mühendislik saldırıları ile siber saldırıların birlikte kullanılması sonucu ortaya çıkmaktadır. Bu saldırıları etkisiz hale getirebilmek insan faktörü üzerinde güvenli davranış bilincine ve farkındalığa dayanır (Şahinaslan, 2013:7-78). Bilişim suçlarına yönelik atılacak en etkili adım ise online platformlarda alışveriş yapan tüketicilerin bilinçlendirilmesidir.

Bu çalışmanın iki amacı bulunmaktadır. İlk amaç genç tüketicilerin siber güvenlik ile sosyal mühendislik farkındalıklarının online alışveriş niyetleri üzerinde, etkili olup olmadığının ortaya çıkarılmasıdır. İkinci amaç ise sosyal mühendislik ile siber güvenlik farkındalığı arasında anlamlı bir ilişki olup olmadığının tespit edilmesi ve eğer bir ilişki varsa bu ilişkinin yüzdelik oranının ortaya çıkarılmasıdır.

Bu amaçlar doğrultusunda araştırmada cevabı aranan araştırma soruları şu şekildedir:

1) Genç tüketicilerin siber güvenlik ile sosyal mühendislik farkındalıkları online alışveriş niyetlerini etkiler mi?
2) Genç tüketicilerin siber güvenlik farkındalıkları ile sosyal mühendislik farkındalıkları arasında anlamlı bir ilişki var mı?

Araştırma soruları kapsamında ve ilgili literatür incelemeleri sonucunda, çalışmada 3 hipotez ileri sürülmektedir. Bu hipotezler:

H1 Tüketicilerin siber güvenlik farkındalıkları, sosyal mühendislik farkındalıklarını pozitif yönde etkilemektedir.

H2 Tüketicilerin siber güvenlik farkındalıkları, online alışveriş niyetlerini pozitif yönde etkilemektedir.

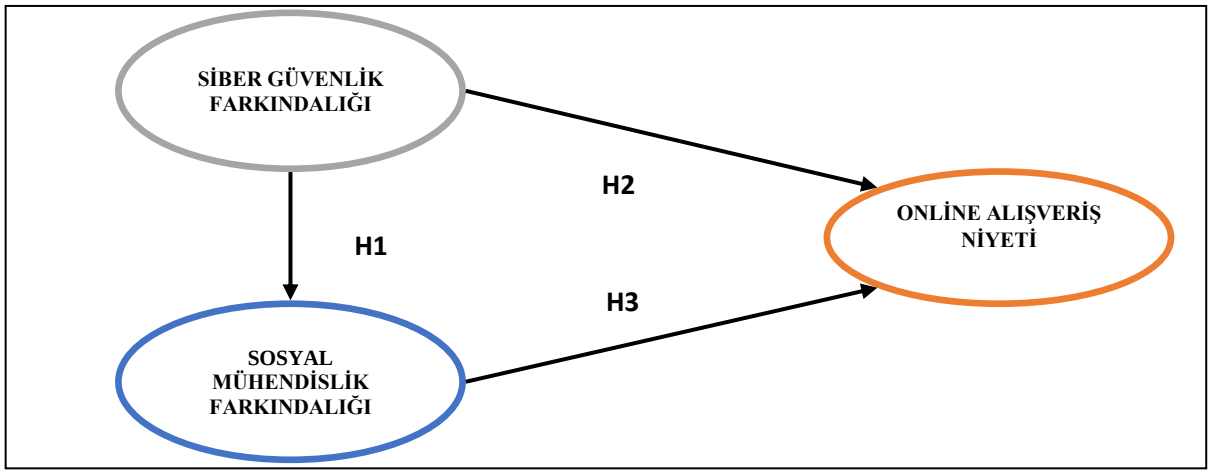
H3 Tüketicilerin sosyal mühendislik farkındalıkları, online alışveriş niyetlerini pozitif yönde etkilemektedir.

Veri Toplama Araçları ve Araştırma Modeli

Araştırmanın uygulama bölümüne geçilmeden önce, araştırma modelini ve amacını belirlemek amacıyla literatür taranmış, gerekli olan hipotezler hazırlanmış ve hazırlanan hipotezler ile Şekil 3 ile gösterilen araştırma modeli tasarlanmıştır. İlgili hipotezlerin test edilmesi için anket formu oluşturulmuştur. Anket formunun oluşturulmasında; sosyal mühendislik, siber güvenlik ve online alışveriş çalışmaları ile ilgili konularda, geçmiş yıl çalışmalarından yararlanılmıştır.

Araştırmada veri toplama işleminin yapılabilmesi için 15 Ocak 2019 tarihinde Bandırma Onyedi Eylül Üniversitesi Sosyal ve Beşeri Bilimler Etik kuruluna başvurulmuş ilgili kurulun 21 Ocak 2019 tarihli Etik Kurul kararıyla, yapılacak çalışmanın uygun olduğuna karar verilmiştir. Alınan etik kurul kararı ile birlikte 24.01.2019 tarihinde Bandırma Onyedi Eylül Üniversitesi Rektörlüğüne, uygulamanın Bandırma Onyedi Eylül Üniversitesi öğrencileri üzerinde uygulanabilmesi için izin başvurusunda bulunulmuş ve Rektörlüğün 06.02. 2019 tarihli yazısı ile çalışmaya izin verilmiştir. İlgili izinlerin alınması ile oluşturulan anket formu 18-21 Şubat tarihlerinde Bandırma Onyedi Eylül Üniversitesinin merkez kampüsünde bulunan fakültelerde öğrenim gören öğrencilere uygulanmıştır. Uygulama sonucunda 693 anket geri dönmüştür. Yapılan inceleme sonucunda 29 anket değerlendirmeye uygun bulunmamış ve örneklemden çıkarılmıştır. Kalan 664 katılımcı araştırmanın örneklemi olmuştur.

Katılımcıların siber güvenlik ve sosyal mühendislik farkındalıkları ile online alışveriş niyetleri hakkındaki davranışlarını ölçmeye yönelik 19 değişkenden oluşan 5'li likert ölçekli (1- Hiç Katılmıyorum, 2- Katılmıyorum, 3- Ne Katılıyorum Ne Katılmıyorum, 4- Katılıyorum, 5- Kesinlikle Katılıyorum) anket uygulanmıştır. Ölçekte 8 değişken; genç tüketicilerin siber güvenlik farkındalıklarını, 7 değişken; genç tüketicilerin sosyal mühendislik farkındalıklarını, 4 değişken ise genç tüketicilerin online alışveriş niyetlerini ölçmeye yönelik hazırlanmıştır. Siber güvenlik farkındalığının ölçülmesinde 8 önermeli likert ölçekli ankette; Kocadağ 2012, Öztürk 2015, ve Budak 2015 tarafından geliştirilen anketlerden, sosyal mühendislik farkındalığının ölçülmesinde kullanılan 7 önermeli likert ölçekli ankette; Tanrıkulu, Kınay ve Arıcak 2011 tarafından geliştirilen anketlerden, online alışveriş niyetinin ölçülmesinde kullanılan 4 önermeli likert ölçekli ankette ise; Rodriguez ve Trujillo 2013, Taylor ve Todd 1995 tarafından geliştirilen anketlerden faydalanılmıştır. Ankette ayrıca katılımcılara, tanımlayıcı verilerin ölçülmesi maksadı ile çoktan seçmeli sorular yöneltilmiştir. Araştırma hipotezleri ile oluşturulan araştırma modeli Şekil 3 'te görülmektedir.



Şekil 3 : Araştırma Modeli: Online Alışveriş Güvenlik Modeli (OAGM)

BULGULAR

Katılımcılara ilişkin tanımlayıcı verilerin oluşturulmasında, SPSS Versiyon 24 programından yararlanılmıştır. Katılımcılara ait tanımlayıcı istatistikler Tablo 2'de gösterilmektedir.

Tablo 2: Katılımcılara Ait Tanımlayıcı İstatistikler

Cinsiyet	Sayı	Yüzde	Yaş	Sayı	Yüzde
Kadın	340	51,2	18 ve 25 yaş	640	96,3
Erkek	324	48,8	25-30 yaş	21	3,2
			30 ve üzeri	3	0,5

Toplam	664	100	**Toplam**	664	100
Bölüm	**Sayı**	**Yüzde**	**Bölüm (devam)**	**Sayı**	**Yüzde**
İktisat	193	29,1	Ekonometri	36	5,4
Maliye	61	9,2	Medya ve İletişim	27	4,1
Hemşirelik	60	9	Mühendislik ve Doğa Bilimleri	23	3,5
Denizcilik İşletmeleri	60	9	Yönetim ve Bilişim Sistemleri	23	3,5
Siyaset Bil. ve Kamu Yönetimi	54	8,1	Çalışma Eko. ve End. İlişki.	19	2,9
Uluslararası Tic. ve Loj.	54	8,1	Akıllı Ulaşım Sistemleri	2	0,3
İşletme	52	7,8	**Toplam**	664	100

Tablo'da görüldüğü üzere katılımcıların çoğunluğunu (%96'3) 18-25 yaş arası katılımcılar oluşturmaktadır. Cinsiyet açısından bakıldığında katılımcılar çoğunluğunun kadın katılımcıların (%51,2) oluşturduğu görülmektedir. Katılımcıların bölümlerine göre dağılımı incelendiğinde, ilk sırada iktisat bölümünde okuyan katılımcıların (%29,1), ikinci sırada ise %9,2 ile Maliye bölümünde okuyan katılımcıların yer aldığı anlaşılmaktadır.

Genel Değerlendirme Anketinden Elde Edilen Bulgular

Genel değerlendirme anketinde genç katılımcıların, siber güvenlik ve sosyal mühendislikte bilgi güvenliği farkındalıklarını tespit etmeye ve online alışveriş niyetlerini ölçmeye yönelik, demografik sorular dahil 20 soruluk anket uygulanmıştır. Soruların hazırlanmasında; Barışkan 2017, Dönmez 2015, Ateş 2016 ve Çakmak 2011 tarafından geliştirilen anketlerden faydalanılmıştır. Katılımcıların, bireysel siber güvenlik ve sosyal mühendislik farkındalık karnelerinin çıkartıldığı ankette, genel raporlama Tablo 3 ile detaylı olarak görselleştirilmiştir. Genel değerlendirme anketinde genç katılımcıların istatistiksel verileri ışığında özetle aşağıdaki bulgulara ulaşılmıştır;

- ✓ Genç katılımcıların %89,5'i güvenli internet kullanımı konusunda eğitim almamıştır.
- ✓ Genç katılımcıların %70,3'sinin bilgi güvenliği hakkında bilgi sahibi olmadıkları ve çok az bilgi sahibi oldukları tespit edilmiştir.
- ✓ Genç katılımcıların %73'ü bilgisayarları saldırıya uğradığında neler yapılması gerektiğini bilmemektedir.
- ✓ Genç katılımcıların %81,8'i oltalama (phishing) ataklarından haberdar değildir.
- ✓ Genç katılımcıların %64'ü sosyal ağlarda tanımadıkları insanlarla arkadaşlık kurmaktadır.
- ✓ Genç katılımcıların %57,8'i E-posta ile gelen ekleri açarken dikkatli davranmamaktadır.
- ✓ Genç katılımcıların %44,7'si sosyal medya hesaplarında akrabalarını deşifre etmektedir.
- ✓ Genç katılımcıların %41,9'unun çevresinde, internet kaynaklı bilgi hırsızlığı, rahatsız edilme ve e-dolandırıcılık yaşayan bir kimse olmuştur.
- ✓ Genç katılımcıların %43,7'si arama motorlarında sosyal ağ profillerini gizlememektedir.
- ✓ Genç katılımcıların %22,1'i sosyal ağlarda paylaştıkları verilerin birileri tarafından kayıt altına alındığı bir durumla karşılaşmıştır.
- ✓ Genç katılımcıların %76,1'i bilgisayarının saldırıya uğradığını veya bilgisayarına virüs vb. zararlı yazılım bulaştığını fark etmektedir.
- ✓ Genç katılımcıların %81,2'si internet alışverişlerinde 3D secure (cep telefonuna doğrulama mesajı) kullanmaktadır.

Tablo 3: Genç Tüketicilerin Bireysel Siber Güvenlik ve Sosyal Mühendislik Farkındalık Karneleri

İfade	**Sayı**	**Yüzde**	**İfade**	**Sayı**	**Yüzde**

1.Güvenli internet kullanımı konusunda bir eğitim aldınız mı?			**2.Bilgi güvenliği hakkında ne kadar bilgi sahibisiniz?**		
Evet	65	9,8	Yeteri kadar biliyorum.	197	29,7
Hayır	594	89,5	Çok az bir bilgim var.	367	55,2
Cevapsız	5	0,7	Herhangi bir bilgim yok.	100	15,1
3.Bilgisayarınız saldırıya uğradığında neler yapmanız gerektiğini biliyor musunuz?			**4.Bilgisayarınızın saldırıya uğradığını / zararlı yazılımların bulaştığını anlar mısınız?**		
Evet ne yapmam gerektiğini biliyorum	178	26,8	Evet anlarım	505	76,1
Hayır bilmiyorum	485	73	Hayır anlayamam	157	23,6
Cevapsız	1	0,2	Cevapsız	2	0,3
5.Çevrenizde internet kaynaklı bir sorun (bilgi hırsızlığı, rahatsız edilme, e-dolandırıcılık yaşayan kimse oldu mu?			**6.E-posta ile gelen ekleri açarken nasıl davranırsınız?**		
Evet	278	41,9	Beklediğim kişiden geldiğine emin olurum.	279	42
Hayır	383	57,7	Bildiğim yerden geldiyse güvenliğe dikkat etmem.	245	36,9
Cevapsız	3	0,4	Dikkat etmem.	139	20,9
			Cevapsız	1	0,2
7.Oltalama (phishing) ataklarını duydunuz mu?			**8.Sosyal medyada hiç kimseyi akrabanız olarak gösterdiniz mi? Evet ise bu bilgi herkese açık mı?**		
Evet duydum	112	16,9	Evet, gösterdim. Bilgi herkese açık	82	12,3
Hayır duymadım	543	81,8	Evet ama sadece arkadaşlarım görüyor	215	32,4
Cevapsız	9	1,3	Hayır, göstermedim	365	55
			Cevapsız	2	0,3
9.Google'dan arandığında sosyal ağ profiliniz çıkıyor mu?			**10.Tanımadığınız birini sosyal ağlarda arkadaş olarak eklediniz mi?**		
Evet	291	43,7	Evet	425	64
Hayır	369	55,6	Hayır	236	35,5
Cevapsız	4	0,7	Cevapsız	3	0,5
11.Sosyal ağda paylaştığınız verilerin, birileri tarafından kayıt altına alındığı bir durumla karşılaştınız mı?			**12.İnternetten alışveriş yapıyorum.**		

Evet	147	22,1	Evet	560	84,3
Hayır	511	77	Hayır	104	15,7
Cevapsız	6				
13.İnternette yaptığınız alışverişlerde 3D secure (cep telefonuna doğrulama mesajı) kullanmaya dikkat ediyor musunuz?			**14.İnternetten alışveriş yapma deneyiminiz ne kadardır?**		
Evet	540	81,2	1-5 kez	163	24,4
Hayır	122	18,4	5-10 kez	146	22
Cevapsız	2	0,4	10 ve üzeri	306	46,2
			Hiç	49	7,4
15.İnternette bir kerede en fazla ne kadarlık alışveriş yapmayı düşünürsünüz?			**16.İnternet alışverişlerinizin 5 yıl içerisinde tüm alışverişlerinizin yaklaşık ne kadarını oluşturacağını düşünüyorsunuz?**		
En fazla 100 TL	316	47,6	%5 ten az	88	13,3
100 ve 500 TL aralığında	263	39,6	% 5-10 arası	116	17,5
500ve 1000 TL aralığında	32	4,8	%10-20 arası	162	24,4
1000 TL den fazla	52	7,8	% 20'den fazla	297	44,6
Cevapsız	1	0,2	Cevapsız	1	0,2

Genel değerlendirme anketinden elde edilen veriler ışığında, karne notları katılımcıların verdikleri yanıtların yüzdelik oranlarına göre; "Başarılı", "Başarısız" ve "Ortalama" seviyeleri olmak üzere üç ayrı seviyede değerlendirilmiştir. Karne notunun "Başarılı" olması genç tüketicinin ilgili soru hakkında yeterli düzeyde bilgiye sahip olduğunu, "Ortalama" olması, genç tüketicinin ilgili soru hakkında ortalama düzeyde bilgi birikimine sahip olduğunu, "Başarısız " olması ise genç tüketicilerin ilgili soru hakkında yetersiz olduğunu ifade etmektedir. Katımcıların karneleri aşağıdaki gibi raporlanmıştır.

- ✓ 1. 2. ve 3. Sorulara verilen cevaplar katılımcıların siber saldırılara açık olduklarını göstermektedir. Verdikleri yanıtlarla yüksek oranda ***BAŞARISIZ*** olmuşlardır. Üniversite öğrencilerinin güvenli internet kullanımı ve bilgi güvenliği konularında eğitimlere ihtiyaç duydukları görülmektedir.
- ✓ 4. Soruya verdikleri yanıtlarda yüksek oranda ***BAŞARILI*** olmuşlardır. Katılımcıların büyük çoğunluğu bilgisayarlarının saldırıya uğradığını veya zararlı yazılım bulaştığını fark edebilmektedir.
- ✓ 5. Soruda internet kaynaklı dolandırıcılık ve rahatsız edilme yaşayan katılımcıların oranının %41,9 olduğu görülmektedir. Bu oran çok yüksektir. Fakat %57,7 oranında bu tür vakalarla karşılaşma yaşanmadığı için ***ORTALAMA*** düzeyde farkındalık olduğu söylenebilir.
- ✓ 6. ve 7. Sorular katılımcıların sosyal mühendislik saldırılarına açık olduklarını göstermektedir. Özellikle oltalama (phishing) ataklarının %81,8 oranında hiç duyulmamış olmasıyla yüksek oranda ***BAŞARISIZ*** olmuşlardır.
- ✓ 8. ve 9 sorularda sosyal ağlarda, akrabaların deşifre edilmemesi ve sosyal ağ profillerinin arama motorlarında gizlenmesi konusunda anket katılımcılarının %55'inin bilinçli olduğu görüldüğünden ***ORTALAMA*** düzeyde farkındalık tespit edilmiştir.

- ✓ 10. Soruda katılımcıların %64'ünün sosyal medyada tanımadıkları insanları arkadaş olarak eklemeleri sosyal mühendislik saldırılarına açık olduklarını yinelemektedir. Katılımcılar verdikleri yanıtlarla **B*AŞARISIZ*** olmuşlardır. Bilinçli sosyal medya kullanım farkındalığı yoktur.
- ✓ 11. ve 13. Sorulara verilen yanıtlarda katılımcılarda yüksek oranda farkındalık tespit edildiğinden ***BAŞARILI*** olmuşlardır. Katılımcıların %81,2 oranında online alışverişlerinde 3D Secure kullanmaya dikkat etmeleri önemli bir farkındalıktır. 12.soruda katılımcıların büyük çoğunluğu sosyal ağlarda paylaştıkları verilerin birileri tarafından kayıt altına alındığı bir durumla henüz karşılaşmadıklarını ifade etmişlerdir. Bu sonuç şuanda internette bilgi hırsızlığının çok ilerlemediğini gösterse de %22 oranında katılımcının evet yanıtını vermesi, kişisel verilerin korunması konusunda bilinçlendirme eğitimlerine ihtiyaç olduğunu göstermektedir.

Genel değerlendirme anketinde üç adet önemli bulgu tespit edilmiştir. Bunlardan ilki; genç tüketicilerin büyük çoğunluğu, siber saldırılara ve sosyal mühendislik saldırılarına açıklardır ve bilgi güvenliği eğitimlerine ihtiyaç duymaktadırlar. İkinci olarak; genç tüketicilerin, siber güvenlik ve sosyal mühendislik farkındalıklarının, online alışveriş niyetleri üzerindeki etkisinin zayıf olduğu tespit edilmiştir. Başka bir ifadeyle, online platformlarda siber güvenlik ve sosyal mühendislik risklerini ihmâl eden, "*benim başıma gelmez*" anlayışına uygun hareket ettikleri rahatlıkla söylenebilir. Üçüncü bulgu ise genç tüketicilerin %47,7'si önümüzdeki 5 yıl içerisinde online alışverişlerine %20'den fazla bütçe ayıracaklarını öngörmektedirler.

Ölçeğin Güvenilirlik ve Geçerlilik Analizleri

Araştırmanın güvenilirlik analizinde, Cronbach's Alpha, sorular arası korelasyona bağlı uyum değeri kullanılmıştır. Cronbach's Alpha değerinin 0,70 ve üstünü göstermesi durumunda ölçeğin güvenilir olduğu kabul edilir. Fakat soru sayısı az olduğunda bu sınır 0,60 değeri ve üstü olarak kabul edilmektedir (Durmuş, Yurtkoru ve Çinko, 2016: 89). Bu doğrultuda ölçek güvenilirliğinin tespiti için Cronbach Alpha katsayısından yararlanılmasına karar verilmiştir. Ölçeğin güvenilirlik analizleri Tablo 4 ile gösterilmektedir. Yapılan güvenilirlik analizleri sonucunda ölçeğin güvenilir olduğu görülmüştür. İlk güvenilirlik analizinde siber güvenlik farkındalığı ölçeğinde bulunan 6. soru güvenilirliği düşürdüğü için değerlendirme dışı bırakılmıştır. Ankette yer alan tüm aralıklı/oransal sorulara ilişkin güvenilirlik değeri 0,767 bulunmuştur.

Tablo 4: Ölçeğe İlişkin Güvenilirlik Analizi Sonuçları

Boyut	İfade Sayısı	Alfa Katsayısı
Siber Güvenlik Farkındalığı	7	0,646
Sosyal Mühendislik Farkındalığı	7	0,776
Online Alışveriş Niyeti	4	0,880
SERVEQUAL TOPLAM	18	0,767

Verilerin analizinde ve ortaya çıkarılan Online Alışveriş Güvenlik Modelinin oluşturulmasında Yapısal Eşitlik Modellemesinden (YEM) yararlanılmıştır. Yapısal eşitlik modellemesi, istatistiksel bağımlılıkla açıklanabilen modellerde, hipotezlerin içinde bulunan değişkenlerin sebep sonuç ilişkisini açıklayarak teorik olan modellerin bir bütün halinde test edilmesine olanak sağlayan en etkili model test etme ve geliştirme yöntemlerinden biridir (Özkırış, 2010: 50).

YEM ile araştırmacı tarafından geliştirilen hipotezler, sayısal veriler yardımıyla test edilmektedir (Schumacker ve Lomax, 2004: 2). YEM analizi iki farklı istatistiksel parametre olarak kullanılan psikoloji ve psikometri alanlarında gelişen faktörlerin melez, yani karma analizidir (Çokluk,

Şekercioğlu ve Büyüköztürk, 2010: 253). Davranış bilimlerinde bilim insanları genellikle ölçülmesi mümkün olmayan teorik yapılar üzerinde çalışırlar. Bu yapılara gizil faktörler denilir. YEM, analizi diğer analizlerden farklı olarak gözlemlenen gizil eksojen ve gizil endojen değişkenleri üzerinde çalışır (Byrne, 2010: 4). Yapısal Eşitlik Modellemesi iki parçadan oluşmaktadır. Bunlardan ilki gözlenen değişkenleri, gizil değişkenlere bağlayarak uygulanan, "doğrulayıcı faktör analizini" kullanan "ölçme modeli"dir. İkincisi ise gizil değişkenleri birbirlerine eşitlik sistemi ile eş zamanlı bağlayarak uygulamaya alınan "yapısal model"dir (Çokluk, Şekercioğlu ve Büyüköztürk, 2010: 261). Bu çalışmada doğrulayıcı faktör analizi ile kullanılan ölçme modeli kullanılmıştır. Doğrulayıcı faktör analizi ile ölçme modeline geçildiğinde, verilerde boş verilerin yer aldığı fark edilmiştir. Yapısal eşitlik boş veriyle çalışmamaktadır. Bu sebeple boş veriler SPSS paket programı yardımıyla EM (Expectation Maximization) algoritması kullanılarak doldurulmuş, ilaveten hatalı girilen veriler düzeltilmiştir. Verilerin hem yapı geçerliliklerini test etmek için hem de hipotez testleri öncesi modeli uygun bir yapıya sokabilmek için öncelikle doğrulayıcı faktör analizi (AMOS 22 paket programı yardımıyla) yapılmıştır. Analiz öncesi verilerin hem ifade bazında hem de çoklu bazda normallik değerleri incelenmiştir. Verilerin çoklu normal dağılım göstermediği (katsayı= 41.843) anlaşıldığından, analizlerde GLS (Generalized Least Square) tahmincisinin tercih edilmesine karar verilmiştir. Yapılan ilk DFA analizi sonucunda modelde yer alan 4 ifadeye ilişkin yük değerlerinin düşük olduğu ve yapı güvenilirliğini düşürdüğü anlaşılmış (Bkz, tablo 5) bu değişkenler analizden çıkarılarak DFA analizi tekrar edilmiştir. Tablo 5'de ilk doğrulayıcı faktör analizinin sonuçları görülmektedir.

Tablo 5: İlk DFA (doğrulayıcı faktör analizi) Sonucu Modelden Çıkarılan Değişkenler

Yapı	İfadeler	Kısaltma	Yük Değeri
Siber güvenlik farkındalığı	İhtiyaç duyduğumda ücretsiz yazılımları bilgisayarıma indirebilir veya kurabilirim.	sgf3	,217
Siber güvenlik farkındalığı	Bilinmeyen kişi ve adreslerden gelen mailleri herhangi bir güvenlik açığı oluşmaması için okumayarak kimlik avı ve dolandırıcılık ile ilgili yerlere şikayet ederim.	sgf2	,390
Sosyal mühendislik farkındalığı	Yaptığım her şeyi sosyal medyada paylaşmayı sevmem.	smf7	,246
Siber güvenlik farkındalığı	Bilgisayarımda lisansız yazılım kullanmaktan çekinirim.	Sgf 6	Güvenilirlikte Çıkarıldı
Sosyal mühendislik farkındalığı	İnternette tanımadığım insanlarla iletişim kurmam.	smf4	,268

İlk doğrulayıcı faktör analizinden çıkarılan değişkenlerden sonra ikinci doğrulayıcı faktör analizine geçilmiştir. İkinci DFA analizi sonucunda, tüm ifadelere ilişkin yük değerlerinin 0,4 ve üstünde olduğu anlaşılmıştır. Tablo 6'da ikinci DFA sonuçları görülmektedir. Ortaya çıkan sonuç ile DFA modeline ilişkin uyum iyiliği değerlerinin ölçümüne geçilmiştir.

Doğrulayıcı faktör analizine ilişkin uyum iyiliği değerleri ve testleri ile model ve veriler arasındaki uygunluk, farklı uyum endeksleri ile kontrol edilmektedir. (Yücenur, Demirel, Ceylan ve Demirel, 2011: 163). Yapısal eşitlik modelinde (YEM) uyum iyiliği indeksleriyle ortaya çıkan verilerle, modelin ne kadar iyi açıklandığı ispat edilir. Uyum iyiliği testleriyle, modelin kabul veya reddedilmesine karar verilir. Fazla sayıda uyum iyiliği limit değerleri olmakla birlikte, her uyum iyiliği indeksinde kritik limit değerleri bulunmaktadır. Uyum iyiliği indeksleri henüz gelişme aşamasında olduğundan bazı uyum iyiliği indekslerinin kritik limitlerin altında kalması normal kabul edilmektedir. (Özkırış, 2010: 51).

Tablo 6: İkinci DFA (doğrulayıcı faktör analizi) Sonuçları

Yapı	İfadeler	İfadelerin Kısaltmaları			Yük Değeri
Siber güvenlik	Bilgileri dijital ortamda nasıl güvende tutmam	sgf8	<---	SGF	,562

farkındalığı	gerektiğini biliyorum.				
Siber güvenlik farkındalığı	İnternet şifrelerimin güvenlik seviyelerini önemserim.	sgf7	<---	SGF	,603
Siber güvenlik farkındalığı	İhbarda bulunacağım hat, web sitesi ve yasal kurumları bilirim.	sgf5	<---	SGF	,509
Siber güvenlik farkındalığı	Web sitelerinin yardım gizlilik ve güvenlik gibi bölümlerinin olduğunu biliyorum ve kullanıyorum.	sgf4	<---	SGF	,508
Siber güvenlik farkındalığı .	Herkesin erişimine açık bilgisayarlarda herhangi bir şifre gerektiren işlem yapmamaya özen gösteririm.	sgf1	<---	SGF	,427
Sosyal mühendislik farkındalığı	Sosyal paylaşım sitelerinde bilgilerim herkese açık değildir.	smf6	<---	SMF	,515
Sosyal mühendislik farkındalığı	İnternete girdiğimde internetin aynı zamanda başkalarına zarar vermek amacıyla kullanılabileceğini aklımda tutarım.	smf5	<---	SMF	,575
Sosyal mühendislik farkındalığı	Sanal ortamlardayken bir bilgisayar korsanının benim içinde tehlike oluşturabileceğini göz önünde bulundururum.	smf3	<---	SMF	,725
Sosyal mühendislik farkındalığı	Sosyal paylaşım sitelerinde (Facebook, Twitter vb.)özel bilgilerimin başkaları tarafından kötü amaçlı olarak kullanılabileceğini göz önünde bulundururum.	smf2	<---	SMF	,841
Sosyal mühendislik farkındalığı	İnternete girerken bilgilerimin başkaları tarafından çalınabileceğini göz önünde tutarım.	smf1	<---	SMF	,719
Online alışveriş niyeti	Gelecekte internet üzerinde alışveriş yapmaya devam etme niyetindeyim.	oan1	<---	OAN	,713
Online alışveriş niyeti	Her zaman internet üzerinden alışveriş yapmak için çaba göstereceğim.	oan2	<---	OAN	,847
Online alışveriş niyeti	İnternet üzerinden alışveriş yapmak hayatımı daha cazip hale getirir.	oan3	<---	OAN	,894
Online alışveriş niyeti	İnternet üzerinden alışveriş yapmayı arkadaşlarıma tavsiye ederim.	oan4	<---	OAN	,834

Yapısal eşitlik modelinde kullanılan uyum iyiliği değerlerine ilişkin değerler Tablo 7 ile toplu olarak gösterilmiştir.

Tablo 7: Uyum İyiliği Değerleri

Uyum İyiliği	Değer	Model Uyumu
X^2/Df	288,972/74=3,905	Uyumlu
GFI	0,938	Uyumlu
AGFI	0,912	Uyumlu
RMR	0,999	Uyumlu Değil
RMSEA	0,066	Uyumlu
CFI	0,696	Uyumlu Değil

Tablo 7'de gösterilen uyum iyiliği değerleri incelendiğinde, RMR ve CFI değerlerine göre model uyumunun düşük olduğu görülmektedir. Bununla birlikte yapıların x2/df, GFI, AGFI ve RMSEA değerlerine göre kabul edilebilir düzeyde uyum gösterdiği (Yılmaz, 2014: 138) anlaşılmıştır. Yapılar

uyum değerlerinin büyük çoğunda kabul edilebilir düzeyde uyum gösterdiği için modelin genel olarak uyumlu olduğuna karar verilmiş ve hipotez testlerine geçilmiştir.

Hipotez Testleri

İlgili hipotezlerin test edilmesinde GLS tahmincisine dayanan Yapısal Eşitlik Modellemesinden yararlanılmıştır. Yapılan hipotez testleri neticesinde elde edilen sonuçlar Tablo 8 ile gösterilmektedir.

Tablo 8: Hipotez Testi Sonuçları

İlişki	Katsayı	Standart Hata	Anlamlılık (p)	R2 (Belirleme katsayısı)	SONUÇ
SMF <-- SGF	,883	,093	,000	0,65 (%65)	DESTEKLENDİ
OAN <-- SGF	,328	,158	,039	0,05 (%5)	DESTEKLENDİ
OAN <-- SMF	-,058	,135	,666	-	DESTEKLENMEDİ

Yapılan testler sonucunda; siber güvenlik farkındalığı değişkeninin hem sosyal mühendislik farkındalığı değişkeni üzerinde hem de online alışveriş niyeti değişkeni üzerinde pozitif yönlü ve anlamlı etki gösterdiği görülmüştür. Hipotez testleri sonucunda görüldüğü gibi bu değişkenler arasındaki değerler p<,05 koşulunu sağladığı için H1 ve H2 hipotezleri desteklenmiştir. H1 ile genç tüketicilerin siber güvenlik farkındalığında meydana gelecek bir birimlik artışın, genç tüketicilerin sosyal mühendislik farkındalığında 0,883 birim artış yaratmakta olduğu raporlanmıştır. H2 ile genç tüketicilerin siber güvenlik farkındalığında meydana gelecek bir birimlik artışın, genç tüketicilerin online alışveriş niyetlerinde 0,328 birim artış yaratmakta olduğu raporlanmıştır.

Genç tüketicilerin sosyal mühendislik farkındalıklarında, meydana gelen değişimin %65'lik kısmı genç tüketicilerin siber güvenlik farkındalıklarında meydana gelen değişim tarafından açıklanmaktadır (R^2=0,65). Bununla birlikte genç tüketicilerin sosyal mühendislik farkındalıklarının, online alışveriş niyetleri üzerinde anlamlı bir etkisi bulunmamaktadır. Bu nedenle H3 hipotezi ret edilmiştir. Genç tüketicilerin online alışveriş niyetlerinde meydana gelen değişimin %5'lik kısmı, genç tüketicilerin siber güvenlik farkındalıkları tarafından açıklanmaktadır. (R^2=0,05). Bu düşük bir açıklama oranıdır. Ancak tüketicilerin online alışveriş niyetini etkileyen birçok faktör olduğu düşünüldüğünde bu sonucun kabul edilebilir olduğu rahatlıkla ifade edilebilir. Çünkü yapılan analizler online alışveriş niyetini etkileyen tüm faktörlerden sadece güvenlik faktörünü değerlendirmeye almıştır.

Özetle; "Genç tüketicilerin siber güvenlik farkındalıkları (SGF), sosyal mühendislik farkındalıklarını (SMF) pozitif yönde etkilemektedir" H1 hipotezi kabul edilmiştir. "Genç tüketicilerin siber güvenlik farkındalıkları (SGF) online alışveriş niyetlerini (OAN) pozitif yönde etkilemektedir" H2 hipotezi kabul edilmiştir. Araştırma sonucunda ulaşılan bir başka bulgu, sosyal mühendisliğin, online alışveriş niyetini etkilemediğidir. Bu nedenle "Genç tüketicilerin sosyal mühendislik farkındalıkları (SMF), online alışveriş niyetlerini pozitif yönde etkilemektedir (OAN)"H3 hipotezi reddedilmiştir.

TARTIŞMA, SONUÇ VE ÖNERİLER

Çağımızın kâbusu siber güvenliktir. Bu çalışma ile genç tüketicilerin, sosyal mühendislik ile siber güvenlik farkındalıklarının online alışveriş niyetleri üzerindeki etkisi ölçülmüştür. Bilgi güvenliğinin disiplinler üstü bir bilim dalı olduğu bilinciyle yapılan bu çalışma ile özgün bir model olan Online Alışveriş Güvenlik Modeli (OAGM) oluşturulmuştur. Modelde siber güvenliğin tamamen teknik bir konu olmadığı, teknolojik ve teknik zafiyetlerden bilinenin aksine yüksek oranda etkilenmediği ispatlanmıştır.

Ortaya çıkan sonuçlara göre; siber güvenlik farkındalığının ana iskeletini %65 oranında sosyal mühendislik farkındalığı oluşturmaktadır. Kalan %35 'lik dilim, siber güvenlik farkındalığında teknik risk unsurları olarak tanımlanan yazılımsal ve donanımsal risk unsurlarıyla ilgili olup, teknik risk unsurlarının en fazla %35 düzeyine kadar yükselebileceğini ifade etmektedir. Daha öz bir ifadeyle, siber güvenlikte sadece %35'lik dilim teknik güvenlik zafiyetleri olarak bilinen yazılımsal ve donanımsal teknik risk faktörleriyle ilgili olup kalan %65'lik dilim güvenlik zincirinin en zayıf halkası olan insanın, sosyal mühendislik farkındalığıyla ilgilidir. Bu veriler ışığında siber güvenlik farkındalığının ana iskeletini %65 'lik dilimle sosyal mühendislik farkındalığının oluşturduğu tespit edilmiştir. Genç tüketicilerin siber güvenlik farkındalıkları, sosyal mühendislik farkındalıklarını pozitif yönde etkilemektedir" H1 hipotezi %65 payla, çok güçlü bir oranla kabul edilmiştir. Bu noktada, siber güvenlik denilince akıllara öncelikle sosyal mühendislik faaliyetleri gelmelidir ve bu doğrultuda eğitimler verilmelidir. H1 hipotezi ile açıklanan oranlar, siber güvenliğin bir teknoloji sorunu olmadığını, insan ve yönetim sorunu olduğunu ispatlamıştır.

Araştırmada kabul edilen ikinci hipotez; "Genç tüketicilerin siber güvenlik farkındalıkları, online alışveriş niyetlerini pozitif yönde etkilemektedir" H2 hipotezidir. Genç tüketicilerin online alışveriş niyetlerinde meydana gelen değişimin %5'lik kısmı tüketicilerin siber güvenlik farkındalıkları tarafından açıklanabilmektedir. %5'lik kabul oranı düşük bir orandır. Bu durum iki şekilde açıklanabilir. Birincisi; genç tüketicilerin, online ortamlarda alışveriş yaparken siber güvenlik risklerini ihmâl etmelerinden kaynaklanmaktadır. Özetle genç tüketiciler, online (çevrimiçi) ortamlarda karşılaşabilecekleri siber saldırı ve tehlikelerden haberdar değillerdir ve benim başıma gelmez anlayışıyla umursamaz bir tavır sergilemektedirler. Dolayısıyla genel anlamda kabul edilebilir bir siber güvenlik farkındalığı yoktur. İkincisi; tüketicilerin online alışveriş niyetlerini etkileyen birçok faktör bulunmaktadır. Konu literatürde "Teknoloji Kabul Modeli", (TKM) olarak çalışılmıştır. TKM ilk olarak 1986 yılında Davis tarafından kullanılmıştır. Model e-ticaret web sitelerinin verimliliğinin değerlendirilmesinde tüketici niyetlerini açığa çıkartmaktadır (Davis, 1986; Davis, 1989; Lingyun and Dong, 2008; Klopping and Mckinney, 2004). Teknoloji Kabul Modeli, online kullanıcıların teknolojiyi nasıl benimsediklerini ve kullandıklarını modelleyen bilgi ve bilişim sistemleri teorisidir. Bu modelde tüketicilerin online alışveriş niyetlerindeki tutum ve davranış değişliği genel anlamda ve çok geniş bir yelpazede değerlendirilebilmektedir. Oysa bu çalışmada genç tüketicilerin online alışveriş niyetlerinde yalnızca güvenlik faktörleri olarak tanımlanan; sosyal mühendislik ve siber güvenlik farkındalıklarına odaklanıldığından online alışveriş niyetlerini etkileyen diğer alt boyutlar ihmâl edilmiştir. Teknoloji Kabul Modelinde yer alan tüm faktörler değerlendirmeye alındığında aslında siber güvenlik farkındalığının, online alışveriş niyetini %5'lik orandan çok daha yüksek oranda etkileyeceği yorumu kolaylıkla yapılmaktadır.

Elde edilen bulgulara dayanılarak şu tavsiyelerde bulunulmaktadır:

- Araştırmada elde edilen verilere göre tüketiciler, online alışveriş niyetlerinin artacağını ifade etmişlerdir. Ayrıca tüketicilerin online platformlarda kabul edilebilir düzeyde online güvenlik farkındalıklarının olmadığı ortaya çıkmıştır. Bu sonuçlarla dijital vatandaşlığın geliştirilmesi kapsamında; siber güvenlik farkındalığı, sosyal mühendislik farkındalığı, bilgi güvenliği farkındalığı, kişisel verileri koruma farkındalığı, bilgi okuryazarlığı, sosyal medya ağı okuryazarlığı ve dijital okuryazarlık vb. eğitimler tüm üniversitelerde yaygınlaştırılmalıdır.
- Ülkemizde ulusal veri koruma otoritesi, Kişisel Verileri Koruma Kurumudur (KVKK). Veri gizliliğinde ulusal ve uluslararası standartların sağlanması amacıyla özellikle bankacılık, finans, sağlık kuruluşları, sosyal medya ağları ve online ticaret siteleri üzerinde, kişisel veri güvenliğinin sağlanması adına denetimler daha sıkı gerçekleştirilmelidir. Çağımızda veri güvenliği demek milli güvenlik demektir. Bu sebeple milli güvenlik politikalarımız ulusal veri güvenliğimizi kapsayacak şekilde güncel tutulmalıdır. İçinde bulunduğumuz dijital çağda ulusal alanda veri güvenliklerini koruyabilen ülkeler, uluslararası alanda ekonomik bağımsızlıklarını koruyabileceklerdir.

- Bilişim üzerine ihtisaslaşmış, Bilişim İhtisas Mahkemeleri'nin kurulması için alt yapı çalışmalarına başlanılmalı ve zaman kaybedilmeden hayata geçirilmelidir. Gerekli hukuki alt yapı oluşturulmadığı takdirde tüm çalışmalar sonuçsuz kalacaktır.
- Hukuk, iktisadi ve idari bilimler fakültelerinin tamamında tüm öğrencilere seçmeli ders olarak algoritma, kodlama ve yazılım dersleri önerilebilmeli ve tüm öğrenciler bu dersleri almaya teşvik edilmelidir.
- Siber güvenlik ve sosyal mühendislik farkındalıklarının oluşturulmasına yönelik vatandaşlarımızı bilinçlendirecek kamu spotlarına yeteri kadar yer verilmelidir.
- Teknolojik gelişim ve yenilenmeyle birlikte siber güvenlik uzmanlarına olan ihtiyaç artmaktadır. Bu noktada siber güvenlik açığının oluşmaması için yeterli düzeyde siber güvenlik uzmanı yetiştirilmelidir. (Aydaner,2019: 97-131).

Bu araştırmanın sınırlılığı genç tüketiciler üzerinde çalışılmış olmasıdır. Çalışmada katılımcılar 18-25 yaş aralığında, üniversite öğrencilerinden oluşan genç nüfusu temsil etmektedir. Orta yaş ve yaşlı nüfus araştırma grubuna dahil değildir. Bu durum hem sınırlılık hem de avantaj olarak değerlendirilebilir. Çünkü internet üzerinde en aktif olan, interneti en etkili kullanan ve siber alanlardaki riskleri en iyi kavrayan yaş aralığı 18-25 yaş aralığındaki genç nüfustur. Fakat 7 den 77'ye tüm vatandaşların internete erişimi ve internetle etkileşimi günden güne arttığından tüm nüfusun fotoğrafının çekilebilmesi ve genel bir çerçeve oluşturulabilmesi adına, bundan sonraki çalışmalarda araştırmacılara orta yaş ve yaşlı nüfusu kapsayacak şekilde çalışmalar yapmaları tavsiye edilir.

Beyan

Makalenin tüm yazarlarının makale sürecine verdikleri katkı eşittir. Yazarların bildirmesi gereken herhangi bir çıkar çatışması yoktur.

KAYNAKÇA

Ahi, Ş.(2020). *Gelişmiş Sosyal Mühendislik Saldırıları Analizi ve Tespiti*. Yayınlanmış Yüksek Lisans Tezi. Gebze Teknik Üniversitesi Fen Bilimleri Enstitüsü, Kocaeli.

Ahn, G. J., Shehab, M. ve Squicciarini, A. (2011). Security and privacy in social networks. *IEEE Internet Computing*, 15(3), 10-12.

Akçacı, T. ve Kurt, F. B. (2020). Online Süpermarket Alışverişinde Tüketici Güven Faktörü. *Dicle üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 10(20), 414-433.

Aksoğan, M., Bayer, H., Gülada, M. O. ve Çelik, E.(2018). İletişim Fakültesi Öğrencilerinin Siber Güvenlik Farkındalığı: İnönü Üniversitesi Örneği.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ve Savage, S. (2013**).** Measuring the cost of cybercrime İçinde: *The economics of information security and privacy* (pp. 265-300). Springer, Berlin, Heidelberg.

Angeli, S. ve Kundler, W. (2006). *Der Online Shop Handbuch für Existenzgründer*. Pearson Education Deutschland GmbH, Printed in Germany. Pp.623-624.

Aslan, T., Aktaş, B., ve Akbıyık, A. (2020) Kullanıcıların Bilgisayar Güvenliği Davranışını İnceleme: Siber Hijyen. *7. Uluslararası Yönetim Bilişim Sistemleri Konferansı*. Sağlık Bilişimi Analitiği. 9-11 Aralık, Bakırçay Üniversitesi, İzmir

Ateş, E.C. (2016). *Üniversite öğrencilerinin sosyal ağlara ilişkin tutumlarının suç ve suçla mücadele açısından değerlendirilmesi*. Yayınlanmış Yüksek Lisans Tezi. Ondokuz Mayıs Üniversitesi Fen Bilimleri Enstitüsü, Samsun.

Aydaner, G. (2019). *Genç Tüketicilerin Sosyal Mühendislik ile Siber Güvenlik Farkındalıklarının Online Alışveriş Niyetleri Üzerindeki Etkisinin Ölçülmesi*. Yayımlanmış Yüksek Lisans Tezi. Bandırma Onyedi Eylül Üniversitesi, Sosyal Bilimler Enstitüsü, Balıkesir.

Bahadur. G, Chan. W ve Weber, C. (2002). *Privacy Defended Protecting Yourself Online*. First Printed, Que Publishing, U.S.A.

Barışkan, M. A. (2017). *Türkiye' de Siber Güvenlik Bilinci ve Sosyal Mühendislik Ataklarına Karşı Savunma Önlemlerinin Geliştirilmesi*. Yayınlanmış Yüksek Lisans Tezi, İstanbul Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Bilir, F. (2021) Kişisel Verilerin Korunması Kişinin Kendisinin Korunmasıdır. *TRT Akademi Dergisi*, *6*(11), 172-181.

Budak, Ö.S. (2015). *Bilişim Öğrencilerinin Siber Suç Farkındalığı: Erzurum İli Mesleki ve Teknik Liseler Örneği*. Yayınlanmış Yüksek Lisans Tezi. Atatürk Üniversitesi, Eğitim Bilimleri Enstitüsü. Erzurum.

Byres, E., & Lowe, J. (2004). The myths and facts behind cyber security risks for industrial control systems. *In Proceedings of the VDE Kongress* 116, 213-218.

Byrne, B. M. (2010). *Structural Equation Modeling with AMOS: Basic Concepts, Applications and Programming*, Second Edition. New York: Routledge Taylor and Francis Group;

Çakmak, E. (2011). *Consumer Trust in the Online Environment,* Yayınlanmış Yüksek Lisans Tezi. Boğaziçi Üniversitesi. Sosyal Bilimler Enstitüsü, İstanbul

Çeliktaş, B (2016). *Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme*. Yayınlanmış Yüksek Lisans Tezi. Karadeniz Teknik Üniversitesi, Sosyal Bilimler Enstitüsü. Trabzon

Çifci, H. (2019). *Teknoloji öngörüsü ve modellemesi: Türkiye'nin siber güvenlik öngörüsü 2040*. Yayımlanmış Doktora Tezi. Orta Doğu Teknik Üniversitesi. Sosyal Bilimler Enstitüsü, Ankara.

Çokluk, Ö. Şekercioğlu, G. ve Büyüköztürk, Ş. (2010). *Sosyal Bilimler İçin Çok Değişkenli İstatistik: SPSS ve Lisrel Uygulamaları*, Ankara: Pegem Akademi.

Dai. Y, Han. D, Han. T ve Dai. X.(2015) Explore Awareness of Information Security: Insights from Cognitive Neuromechanism. *Computational Intelligence and Neuroscience,* 2015 (1), 1-8

Davis, F.D. (1986) *A technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results*, Yayınlanmamış Doktora Tezi**,** Massachusetts Institute of Technology, Cambridge, MA.

Davis, F.D. (1989), Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology, *MIS Quarterly***,** 13(3), 319-340.

Dönmez, O. (2015). *Sınıf Öğretmeni Adaylarının Çocukların Karşılaştığı Çevrimiçi Risklere Yönelik Algılarının Çeşitli Değişkenler Açısından İncelenmesi*. Yayınlanmış Doktora Tezi. Anadolu Üniversitesi, Eğitim Bilimleri Enstitüsü, Eskişehir.

Durmuş. B, Yurtkoru, S. Çinko, M. (2016). *Sosyal Bilimlerde SPSS'le Veri Analizi*, 6. Baskı, İstanbul, Beta Basım Yayım Dağıtım A.Ş.

Düveroğlu, E.(2020). *Kritik Altyapı Siber Güvenlik Politikalarının Karşılaştırılmalı Analizi. ABD, AB ve Türkiye'den En İyi Uygulamalar*. Yayımlanmış Yüksek Lisans Tezi. İhsan Doğramacı Bilkent Üniversitesi, Ekonomi ve Sosyal Bilimler Enstitüsü. Ankara.

Escobar-Rodríguez, T. ve Carvajal-Trujillo, E. (2013). Online drivers of consumer purchase of website airline tickets. *Journal of Air Transport Management***,** 32, 58–64.

Frischmann, B. (2014). Human-focused Turing tests: A framework for judging nudging and techno-social engineering of human beings. *Cardozo Legal Studies Research Paper No. 441*

Tursun, G. (2020). *Günde 18 binden fazla sahte web sitesi oluşturuluyor,* Global Tech Magazine 4 Aralık 2020 Sayısı Çevrimiçi: https://www.globaltechmagazine.com/2020/12/04/gunde-18-binden-fazla-sahte-web-sitesi-olusturuluyor/ Erişim Tarihi: 06.12.2020

Göz, A. ve Allahverdi, M. (2011). Kurumsal Bilgi Güvenliği Ve Muhasebe Bilgi Sistemi. *Muhasebe ve Vergi Uygulamaları Dergisi (MUVU)/Journal Of Accounting & Taxation Studies*, 4(3). 47-64

Gülmüş, M.(2010) *Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği*. Yayınlanmış Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Gündüz, M. Z. ve Resul, D. (2016). *Sosyal Mühendislik Yaygın Ataklar ve Güvenlik Önlemleri***.** ISCTURKEY, *9*, 11-18 .

Hoffman, D., Novak, T. P., ve Peralta, M. (1999). Building consumer trust online**.** *Communications of the ACM*, *42*(4), 80-85.

Holat, O. (2021) Yeni medya ve siber savaş kavramları bağlamında Stuxnet saldırısı örneğinin incelenmesi. *Abant Kültürel Araştırmalar Dergisi*, *6*(11), 105-121.

Jagatic, T., Nathaniel, A.J., Jakobsson, M. and Menczer, F. (2007**).** Social Phishing**.** *Communications of the ACM*, *50*(10), 94-100

Kim, M. J., Chung, N., and Lee, C. K. (2011). The effect of perceived trust on electronic commerce: Shopping online for tourism products and services in South Korea. *Tourism Management***,** 32(2), 256-265.

Kocadağ, T. (2012). Öğretmen adaylarının dijital vatandaşlık düzeylerinin belirlenmesi. Yayımlanmamış Yüksek Lisans Tezi, Karadeniz Teknik Üniversitesi, Eğitim Bilimleri Enstitüsü, Trabzon.

Koçyiğit, M., ve Koçyiğit, A. (2018) Değişen ve Gelişen Dijital İletişim: Yazılabilir Web Teknolojisi (Web 2.0). İçinde: Dijital Kültür ve İletişim, Konya: Literatürk Academia Yayıncılık.

Köksoy, F. (2020). Avrupa Birliği'nin Siber Güvenlik Politikası: Kurumsalcılık mı Tutarlılık mı?. *Güvenlik Stratejileri Dergisi*, *16*(35), 635-674.

Lingyun, Q. and Dong, L. (2008). Applying TAM in B2C E-Commerce Research: An Extended Model, *Tsinghua Science & Technology*, 13(3), 265-272.

Lopping, I. M. and Mckinney, E. (2004), Information Technology, *Learning, and Performance Journal*, 24(1), 35-47.

Mitnick. D. K., and Simon L. W (2017) *Aldatma Sanatı, Bilgi Güvenliğinde İnsan Faktörünün Kontrolü*. 8. Basım . Ankara: ODTÜ Yayıncılık

El-Hassan, M. (2016). *Hizmet Sektöründe Online Alışveriş Davranışını Etkileyen Faktörler: Seyahat Sektörü (Türkiye ve Slovenya Karşılaştırması)*. Yayınlanmış Yüksek Lisans Tezi. Mersin Üniversitesi Sosyal Bilimler Enstitüsü, Mersin.

Müngen, A. A., Bulut, B., ve Mehmet, K. A. Y. A. (2020). Çoklu Sosyal Ağlarda Aynı Kullanıcıları Belirleme Yöntemi. *Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi*, *11*(3), 1043-1054.

Nezgitli, S., ve Benzer, R. (2020). Avrupa Birliği Siber Güvenlik Kanunu. *Journal of Information Systems and Management Research*, *2*(1), 10-17.

Özkırış, B. (2010). *Tüketicinin İmajı ile Marka İmajı Arasındaki Uyumun, Marka Sadakati Üzerine Etkileri.* Yayınlanmamış Doktora Tezi. Gebze Yüksek Teknoloji Enstitüsü, Sosyal Bilimler Enstitüsü, Kocaeli.

Öztürk, M. (2015). *Ortaokul Öğrencilerinin Dijital Vatandaşlık Düzeyleri*. Yayınlanmış Yüksek Lisans Tezi. Kastamonu Üniversitesi, Sosyal Bilimler Enstitüsü, Kastamonu.

Rahman, K. M. (2018). A Narrative Literature Review and E-Commerce Website Research**.** *EAI Endorsed Transactions on Scalable Information Systems,* 5(17), 1-11.

Schumacker, R. E and Lomax, R. G. (2004). *A Beginner's Guide to Structural Equation Modeling, Second Edition*. Lawrence Erlbaum Associates. U.S.A

Suh, B. and Han, I. (2003). The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce. *International Journal of Electronic Commerce,* 7(3), 135-161

Şahinaslan, Ö., Şahinaslan, E., Borandağ, E., ve Şahinaslan, A. M. (2013). Güvenli Bir Toplumun İçin Son Kullanıcı Siber Güvenliği, *XV. Akademik Bilişim Konferansı Bildirileri*, 1081-1085.

Şahinaslan, Ö.(2013). *Siber Saldırılara Karşı Kurumsal Ağlarda Oluşan Güvenlik Sorunu ve Çözümü Üzerine Bir Çalışma*. Yayımlanmış Doktora Tezi. Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Edirne.

Tanrıkulu, T., Kınay, H. ve Arıcak, O. T. (2011). Siber Zorbalığa İlişkin Duyarlılık Ölçeği. *XI. Ulusal Psikolojik Danışma ve Rehberlik Kongresi Bildiri Özetleri Kitabı. 338-339.* İzmir

Taylor, S., and Todd, P. A. (1995). Understanding İnformation Technology Usage: A Test Of Competing Models. *Information Systems Research*, 6(2), 144-176.

Tellï Danışmaz, A. (2020). Covıd-19 Salgınının Tüketicilerin Online Alışveriş Tercihine Etkisi, *Sosyal Bilimler Araştırma Dergisi*, 9(2), 83-90.

Tosun, A (2015). *İnsan Zafiyetlerini İstismar Ederek Yapılan Sosyal Mühendislik Saldırılarının Siber Güvenlik İle İlişkilendirilmesi: Türkiye Örneği*. Yayınlanmış Yüksek Lisans Tezi. Orta Doğu Teknik Üniversitesi, Enformatik Enstitüsü. Ankara.

Turban, E., Outland, J., King, D., Lee J.K., Liang T.P. and Turban, D. C. (2018). *Electronic Commerce 2018 A Managerial and Social Networks Perspective* Ninth Edition, Springer International Publishing, Switzerland.

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

Yavanoğlu, U., Sağıroğlu, Ş., ve Çolak, İ. (2012). Sosyal ağlarda bilgi güvenliği tehditleri ve alınması gereken önlemler. *Politeknik Dergisi*, *15*(1), 15-27.

Yılmaz, Ö. (2018). Tüketicilerin Online Alışveriş Niyetlerinin Teknoloji Kabul Modeli Bağlamında İncelenmesi. *Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi*, 20 (3),331-346. DOI: 10.32709/akusosbil.478718.

Yılmaz, Ö. (2014). *İlişkisel Pazarlama Faaliyetlerinin Ağızdan Ağıza İletişim (WOM) Yaratma Üzerine Etkisi: Bankacılık Sektörüne İlişkin Bir Alan Araştırması.* Yayınlanmamış Doktora Tezi, Balıkesir Üniversitesi, Sosyal Bilimler Enstitüsü, Balıkesir.

Yücenur, G.N., Demirel N.Ç., Ceylan, C. ve Demirel T. (2011). Hizmet Değerinin Müşterilerin Davranışsal Niyetleri Üzerindeki Etkisinin Yapısal Eşitlik Modeli ile Ölçülmesi**.** *Doğuş Üniversitesi Dergisi*, 12(1), 156-168.