SİBER SUÇ KORKUSUNUN İNTERNET KULLANICILARININ DAVRANIŞSAL ADAPTASYONLARI, KİŞİSEL VERİLERİN PAYLAŞIMI KARARLARI VE GÜVENLİK TEDBİRLERİNİ UYGULAMA NİYETLERİ ÜZERİNDEKİ ETKİLERİNİN ÖLÇÜLMESİ

ÖZ

Bu ampirik çalışma, siber suç korkusunun İnternet kullanıcılarının çevrimiçi alışveriş davranışlarını, çevrimiçi güvenlik önlemlerini, şifre yönetimi stratejilerini ve çevrimiçi kişisel veri paylaşımı kararlarını nasıl etkilediğini incelemektedir. Siber suç korkusunun öngörücülerini araştırmak bu çalışmanın bir diğer hedefidir. Bu amaçla, İngiltere ve Galler 2014/2015 Suç Araştırması'nın veri setini analiz edilmiştir. Bu çalışma, korkuya neden olan olaylara maruz kaldıklarında bireylerin davranışsal adaptasyonlarını açıklayan yaklaşım-kaçınma paradigmasını teorik ve kavramsal bir çerçeve olarak kullanmıştır. İki değişkenli analiz sonuçları, siber suç korkusunda cinsiyet farklılıklarının olmadığını göstermektedir. Bu bulgu, kadınların daha korkulu olduğunu savunan suç korkusu çalışmalarının mevcut sonuçlarıyla çelişmektedir. Yaş ve sosyal statü (eğitim ve gelir) ile siber suç korkusu arasında istatistiksel olarak anlamlı bir ilişki bulunduğu ortaya çıkmıştır. Yüksek gelir ve yüksek eğitim seviyesine sahip İnternet kullanıcılarının, önemli derecede yüksek siber suç korkusuna sahip oldukları tespit edilmiştir. Ayrıca, yaşlı İnternet kullanıcılarının, orta yaşlı ve daha genç İnternet kullanıcılarına kıyasla siber suçlardan daha çok korktukları görülmüştür. Çok değişkenli analiz, İnternet kullanıcılarının yüksek siber suç korkusu düzeylerine rağmen çevrimiçi alışverişe devam ettiklerini ve yaklaşım-kaçınma stratejilerini kullandıklarını göstermiştir. Bu sonuç, suç korkusunun kaçınma davranışını teşvik ettiğini ileri süren yaklaşma-kaçınma paradigması ile çelişmektedir. Araştırma sonuçlar genç İnternet kullanıcıları çevrimiçi alışveriş konusunda daha temkinli davrandıklarını göstermektedir. Bu bulgu çalışmanın alana bir başka yeni ve önemli bir katkısıdır, çünkü mevcut araştırma genç kullanıcıları içgüdüsel alıcı olarak tasvir etmektedir. Ayrıca, araştırma sonuçları siber suç korkusunun çevrimiçi kişisel verileri paylaşma davranışını sınırladığını göstermektedir. Analiz sonuçlarına göre siber suç korkusu daha yüksek olan internet kullanıcıları kişisel verilerini çevrimiçi paylaşmaktan kaçınmaktadır. Son olarak, siber suç korkusu çevrimiçi koruma önlemlerinin uygulanmasını teşvik ettiği tespit edilmiştir.

Anahtar Kelimeler: Siber suçlar, siber suç korkusu, davranışsal adaptasyon, başa çıkma, güvenlik.

GİRİŞ

Son araştırmalar, siber suçun dünyadaki en hızlı büyüyen suç olduğunu (CNBC, 2017) ve hem bireyler hem de çevrimiçi yatırımcılar için önemli bir tehdit oluşturduğunu göstermektedir (Anderson, Barton, Bölme, Clayton, Ganán, Grasso, Levi, Moore ve Vasek, 2019). RiskIQ tarafından yayınlanan rapora göre, siber suçların 2018 yılında küresel ekonomiye her dakika 2,9 milyon $ maliyeti vardır (RiskIQ, 2019). Accenture ve Ponemon Institute tarafından yapılan bir başka araştırma ise, siber suçların kuruluşlara ortalama maliyetinin yaklaşık 13 milyon dolar olduğunu tahmin etmektedir (Accenture, 2019). Siber uzayı terörist maksatlarla kullanımı siber suç korkusunu arttıran başka bir etken olarak karşımıza çıkmaktadır (Başaranel, 2017). Siber suçların bu olumsuz imajı kamuoyunun endişesini ve kaygısını artırmaktadır. Bu durum "kişisel tehdit değerlendirmesi ve siber suçluların mağduru olunması durumunda uğranılacak hasarı en az indirgemenin değerlendirme" olarak tanımlanan siber suç korkusunu şiddetlendirmektedir (Bernik, Dobovšek ve Markelj, 2013). Ampirik araştırmalarda sunulan rakamların yanı sıra, siber suç vakalarının medyada temsil edilmesi şekli de siber suç korkusunu artırmaktadır (Riek, Böhme ve Moore, 2014; Wall, 2015). Finansal kayıp için geri ödeme alamayan müşterilerin dramatik hikayeleri (Clough, 2011; van der Meulen, 2013) veya önemli veri ihlalleri ile sonuçlanan uç örnekler gibi dikkat çekici olaylar siber suç korkusunu şiddetlendirmektedir. Bu ampirik çalışma, siber suç korkusunun İnternet kullanıcılarının çevrimiçi alışveriş yapma alışkanlıkları, çevrimiçi güvenlik önlemlerini, şifre yönetimi stratejileri ve çevrimiçi gizlilik hesabını nasıl etkilediğini incelemektedir. Siber suç korkusunun belirleyici unsurlarının incelenmesi, bu çalışmanın bir diğer hedefidir.

Araştırmalar, medya tarafından sunulan siber suçların olumsuz imajının İnternet kullanıcılarının çevrimiçi davranışları ve güvenlik önlemleri üzerinde etkili olduğunu göstermektedir. Böhme ve Moore (2012) tarafından yapılan araştırmalar, siber suç vakalarıyla ilgili haberlere maruz kalmanın İnternet kullanıcılarının çevrimiçi bankacılık hizmetlerini kullanma niyetlerini azalttığını bulmuştur. Benzer şekilde Putnik ve Boskoviç (2015) medyanın, öğrencilerin siber suç risk algısı üzerinde eğitim programlarından daha önemli bir etkiye sahip olduğunu göstermiştir. Ayrıca, medyada uzmanlık eksikliği de ekonomik siber suç imajını etkilemektedir. Bu kapsamda alınacak siber güvenlik önlemlerinin, organizasyonların yer aldığı sektör içerisinde rakiplerine karşı üstünlük kurmalarına yardımcı olan ve önemli bir güç unsuru konumunda olan kurumsal itibar değerini de olumlu yönde etkileyeceği değerlendirilmektedir (Güleryüz ve Dalkılıç, 2019). İngiltere'deki siber suç davalarının medyada yer almasını inceleyen Hernandez-Castro ve Boiten (2014), Guardian veya The Times gibi ulusal düzeydeki gazetelerin siber suçlarla ilgili daha önce yayınladıkları anketlerinde yer alan rakamları yanlış yorumladıklarını savunmaktadır.

Ayrıca, Wall (2010) bilim kurgu filmleri ve romanlarını siber suçların kamusal imajını şekillendiren kaynaklardan biri olarak belirtmektedir. Wall İtalyan İşi, Die Hard veya Matrix gibi filmlerin çarpık bir siber suç resmi oluşturduğunu ve yanlış bir "her şeye gücü yeten süper hackerlar" algısına yol açtığını öne sürmektedir (Wall, 2011, s.13). Bilimsel araştırma sonuçları Wall'ın bu önermesini doğrular niteliktedir. Örneğin, lisans öğrencilerinin

siber suçlarla ilgili algılarını araştıran Bidgoli, Knijnenburg ve Grossklags (2016), görüştükleri her on kişiden altısının siber suçlarla ilgili bilgilerinin kaynağı olarak film, TV şovu ve çevrimiçi haberler olduğunu bulmuştur.

Siber Suç Korkusunun Öngörücüleri

Geçmiş geleneksel suç korkusu ve siber suç korkusu araştırmaları çoğunlukla suç korkusunun belirleyicilerini ortaya koymayı amaçlamaktaydı. Cinsiyet, yaş, eğitim ve gelir öncelikle suç korkusuyla ilişkilendirilen demografik özelliklerdir (Warr, 2000; May, Rader ve Goodrum, 2010; Gutt ve Randa, 2016). Geleneksel suç araştırmaları, kadınların sürekli olarak siber suçlardan daha fazla korktuklarını bildirilmiştir (Fisher ve Sloan, 2003; van Eijk, 2017). Ancak, siber suç korkusu araştırmaları, kadınların çevrimiçi kişilerarası suçlardan daha fazla korkarken (Pereira ve Matos, 2016; Virtanen, 2017), kötü amaçlı yazılım enfeksiyonu veya çevrimiçi kimlik hırsızlığı korkusunda cinsiyet farkı olmadığını ortaya koymuştur (Roberts, Indermaur ve Spiranovic, 2013; Yu, 2014). Hedeflerin cinsiyeti ile ilgili bilgi eksikliği, geleneksel suç korkusu araştırmaları ile siber kaynaklı suç korkusu araştırma sonuçları arasındaki tutarsızlığın bir açıklaması olabilir.

Önceki geleneksel suç korkusu araştırmaları yaşlı bireylerin daha korkulu olduklarını ortaya koymuştur (Moore ve Shepherd, 2006; Boateng, 2016). Bununla birlikte, siber suç korkusu araştırmaları tutarsız sonuçlar ortaya koymuştur. Virtanen (2017) genç yaşın siber suç korkusunun bir belirleyicisi olduğunu bildirirken, Lee, Choi, Choi, ve Englander (2019) yaşlı İnternet kullanıcılarının siber suçlardan daha korktuğunu keşfetmiştir. Öte yandan, diğer bazı çalışmalar siber suç korkusunda yaş farkının olmadığını göstermiştir (Henson, Reyns ve Fisher, 2013; Roberts vd., 2013).

Sosyal statü (eğitim düzeyi ve gelir) ve siber suç korkusu arasındaki ilişkiyi inceleyen çalışmalar, daha düşük sosyal statüye sahip olanların siber suçtan daha çok korktuklarını göstermiştir (Roberts vd., 2013; Virtanen, 2017; Brands ve van Wilsem, 2019). Ancak, geleneksel suç korkusu ve siber suç korkusu belirleyicilerini karşılaştıran Maddison ve Jeske (2014), eğitim ve siber suç korkusu arasında anlamlı bir ilişki bulamamıştır.

Siber Suç Korkusunun Davranışsal Adaptasyonlara, Güvenlik Niyetlerine ve Kişisel Veri Paylaşımı Kararlarına Etkisi

Kişisel veri paylaşımı kararı, bireylerin kişisel verilerini paylaşmanın ödülleri ve olumsuz sonuçları ile ilgili olan öz değerlendirmeleridir (Culnan ve Armstrong, 1999). Beklenen ödüller ve gizlilik endişeleri bu yaklaşımın iki odak noktasıdır (Dienlin ve Metzger, 2016). Kişisel veri paylaşımı kararı perspektifi, algılanan ödüller ve algılanan kişisel verileri paylaşma riskleri arasındaki karşılaştırmanın, bireylerin kişisel verilerini paylaşma kararlarını belirlediğini ileri sürülmektedir (Krasnova, Veltri & Günther, 2012). Sosyal ağ siteleri (SAS) üzerinden kişisel verilerini paylaşma davranışı hakkında yapılan araştırmalar, kişisel verileri paylaşma hakkındaki algılanan riskler (Salleh, Hussein, Mohamed, Karim, Ahlan ve Aditiawarman, 2012; Salleh, Hussein, Mohamed ve Aditiawarman, 2013) ve beklenen faydanın (Youn, 2005; Howe, Ray, Roberts, Urbanska ve Byrne, 2012) kişisel verilerin paylaşımı kararını etkilediğini göstermiştir. Siber suç korkusunun İnternet kullanıcılarının kişisel veri paylaşımı kararını nasıl etkilediği siber suçlar literatüründe henüz araştırılmamıştır. Bu çalışma literatürdeki bu boşluğu ele almaktadır.

Suç korkusunun bireyin sosyal hayatı ve psikolojisi üzerinde olumsuz etkileri olabileceği ileri sürülmektedir (Skogan, 1986). Suç korkusu literatürü temel olarak suç korkusu ve siber suç korkusunun belirleyicilerini bulmaya odaklanmıştır, bu nedenle suç korkusunun olumsuz etkileri yeterince incelenmiştir. Çevrimiçi alışveriş davranışı üzerine yapılan ampirik araştırmalar, yüksek suç korkusu ve algılanan mağduriyet riski yüksek olan İnternet kullanıcılarının çevrimiçi alışveriş yapma olasılığının daha düşük olduğunu göstermiştir (Forsythe, Liu, Shannon ve Gardner, 2006; Chang ve Wu, 2012; Dai, Forsythe ve Kwon, 2014). Geçmiş olumsuz çevrimiçi deneyimlerin, İnternet kullanıcılarının bilgisayar güvenlik yazılımı kullanma (Claar ve Johnson, 2012), güvenlik önlemlerini uygulama (Thompson ve Gibbs, 2016; Tsai, Jiang, Alhabash, LaRose, Rifon ve Cotten, 2016) ve şifre oluşturma yönergelerine uyma (Mwagwabi, 2014) gibi güvenlik tedbirlerini uygulama davranışları üzerinde etkili olduğunu bulunmuştur.

Brand ve van Wilsem (2019) finansal suç korkusu ile koruyucu davranış arasındaki ilişkiyi yakın zamanda araştırmıştır. Buldukları sonuçlar, kadınların ve yaşlıların çevrimiçi mali suçlardan daha çok korktuklarını göstermektedir. Bununla birlikte, yüksek öğrenimi olan bireylerde daha düşük finansal suç korkusu bildirmişlerdir. Sonuçlar ayrıca, yoğun bir finansal suç korkusu olan İnternet kullanıcılarının çevrimiçi bankacılık kullanma ve çevrimiçi satın alma olasılıklarının daha düşük olduğunu ortaya koydu.

Jansen ve van Schaik (2018) tarafından yapılan araştırma, kötü amaçlı yazılım ve kimlik avı girişimlerinin İnternet kullanıcılarının başa çıkma tepkileri üzerindeki etkisini incelemiştir. Bulguları, kimlik avı ve kötü amaçlı yazılım kurbanlarının virüsten koruma programı yükleme, çevrimiçi bankacılık hesaplarını daha sık kontrol etme veya kimlik avı e-postaları konusunda daha dikkatli olma gibi bazı davranışsal değişiklikler geçirdiğini ortaya koymaktadır. Ancak, sonuçların genelleştirilebilir olmaması bu araştırmanın ana sorunudur, çünkü araştırmacılar bu çalışmada Hollanda'da yapılan 30 yarı yapılandırılmış görüşmeyi kullanmışlardır. Bu mevcut ampirik çalışma, İngiltere ve Galler'in ulusal temsili bir örneğini kullanarak anılan araştırmayı genişletmektedir.

Şifre yorgunluğu, birden fazla çevrimiçi hesap için aynı şifrenin tekrar tekrar kullanılması anlamına gelir (Corre, Barais, Sunyé, Frey ve Crom, 2017). Parola yorgunluğu, e-cüzdanlar gibi finansal hesaplar da dahil olmak üzere çok sayıda çevrimiçi hesaba sahip olmanın bir sonucudur. Örneğin, Das, Bonneau, Caesar, Borisov ve Wang (2014) kullanıcıların yaklaşık yarısına yakınının farklı çevrimiçi hesaplar için aynı şifreyi uyguladığını bulmuştur. Önceki siber suç mağduriyet çalışmaları, aynı şifreyi farklı hesaplarda kullanmanın mağduriyet riskini arttırdığını (Button, Nicholls, Kerr ve Owen, 2014), şifre ve güvenlik yönergelerine uymanın bilgisayar korsanlığı girişimlerine karşı etkin korunma sağladığını göstermiştir (Mwagwabi vd., 2014). Ancak, siber suç korkusunun şifre yönetimi stratejileri üzerindeki etkisi henüz ele alınmamıştır. Bu çalışma literatürdeki bu boşluğu doldurmaktadır.

Teorik Altyapı

Bu çalışma, siber suç korkusunun İnternet kullanıcılarının çevrimiçi davranışları ve güvenlik niyetleri üzerindeki etkisini araştırırken Yaklaşım ve Kaçınma vasıtasıyla Başa Çıkma Paradigmasını (Lazarus ve Folkman, 1984; Roth ve Cohen, 1986) uygulamaktadır. Başa çıkma, "kişinin öz kaynaklarını aşan iç ve/veya talepleri yönetmek için

sürekli değişen bilişsel ve davranışsal çabalar" olarak tanımlanmaktadır (Lazarus ve Folkman, 1984: 612). Yaklaşım ve Kaçınma vasıtasıyla Başa Çıkma Paradigması, bireylerin korku uyandıran durumların olumsuz duygusal etkilerinin üstesinden gelmek için problem odaklı (yüzleşme) veya duygu odaklı (kaçınma) başa çıkma stratejileri uyguladığını ortaya koymaktadır (Roth ve Cohen, 1986; Lazarus, 2006). Sorun odaklı başa çıkma stratejileri, sorunla yüzleşmeyi ve sorunlara çözüm aramayı içeren aktif stratejilerken, duygu odaklı başa çıkma stratejileri, tehdidi görmezden gelmek veya sorun hakkında düşünmekten kaçınmak gibi pasif eylemlerdir (Arachchilage ve Love, 2014). Bu çalışmada internet kullanıcılarının siber suç korkusuna karşı başa çıkma tepkilerini anlamak için başa çıkma paradigması kullanılmıştır. Siber suç korkusunun davranış üzerine etkileri, çevrimiçi alışveriş ile ilişkili dört çevrimiçi faaliyet ile ölçülmüştür. İnternette ürün satın almaktan kaçınmak, duygu odaklı (kaçınma) başa çıkma stratejilerinin dolaylı ölçüm değişkenleri olarak belirlenmişken, yalnızca güvenli web sitelerinden ürün satın almak, güvenlik işaretlerini kontrol etmek ve sadece iyi bilinen ya da güvenilir siteleri kullanmak, problem odaklı (yüzleşme) başa çıkma stratejileri için dolaylı ölçüm değişkenleri olarak belirlenmiştir. Kişisel verilen paylaşımı da yaklaşımla başa çıkma stratejilerinin dolaylı değişkeni olmuştur. Ayrıca, güvenli bilgisayarlara ve çevrimiçi hesaplara uygulanan çevrimiçi güvenlik önlemleri, yaklaşımla başa çıkma stratejileri için dolaylı değişken seçilmiştir.

Mevcut Çalışma

Önceki bilimsel araştırma sonuçları ve teorik bilgiler ışığında şekillenen bu ampirik araştırma, siber suç korkusunun belirleyicilerini araştırmaktadır. Çalışma özellikle siber suç korkusunun bireylerin çevrimiçi alışveriş davranışı, kişisel veri paylaşımı kararı, şifre yönetimi ve bilgisayar güvenliği önlemleri üzerindeki etkisini incelemektedir.

Varsayımlar

Önceki çevrimiçi ve çevrimdışı suç araştırmaları korkusunun sonuçlarına dayanarak beş hipotez öne sürülmüştür. Önceki tüketici davranışı araştırmaları(Böhme ve Moore, 2012; Riek vd., 2014; Riek, Bohme ve Moore, 2016) ve siber suç/kimlik hırsızlığı korkusu çalışmaları (Hille, Walsh ve Cleveland, 2015; Jordan, Leskovar ve Marič, 2018; Brands ve van Wilsem, 2019) korkusu/algılanan mağduriyet riskinin çevrimiçi alışveriş davranışı, alışveriş niyeti ve çevrimiçi koruma önlemleri ile olumlu bir şekilde ilişkili olduğunu ileri sürmüştür. Bu nedenle, bu çalışma şunları varsayımları yapmaktadır:

H1: Siber suç korkusu, alışverişten kaçınma davranışı ve güvenli alışveriş yapma davranışı arasında pozitif bir ilişki vardır.

H2: Siber suç korkusu ve İnternet kullanıcılarının bilgisayar güvenlik önlemlerini uygulama niyetleri arasında pozitif bir ilişki vardır.

H3: Siber suç korkusu ve İnternet kullanıcılarının şifre yönetimi stratejileri arasında pozitif bir ilişki vardır.

Gizlilik endişelerinin çevrimiçi olarak paylaşılan bilgi miktarını ve türünü azalttığı iddia edilmektedir (Krasnova vd., 2012; Dienlin ve Metzger, 2016; Trepte vd., 2017). Bu araştırma sonuçlarına dayanarak, şu varsayım yapılmıştır:

H4: Siber suç korkusu ve gizlilik endişeleri arasında pozitif bir ilişki vardır.

Önceki araştırmalar, internet kullanıcılarının demografik özellikleri ile siber suç korkusu arasındaki ilişkiyi göstermiştir (Maddison ve Jeske, 2014; Virtanen, 2017; Lee vd., 2019). Dolayısıyla şu varsayım yapılmıştı:

H5: Demografik özellikler (yaş, cinsiyet, eğitim ve gelir düzeyi) ve siber suç korkusu arasında anlamlı bir ilişki vardır.

YÖNTEM

Analizin ilk bölümü, İnternet kullanıcılarının demografik özellikleri ile siber suç korkusu arasındaki ilişkiyi incelemeyi amaçlamaktadır. Bu amaçla durumsallık tabloları ve Ki-kare testleri beşinci hipotezi test etmek maksadıyla kullanılmıştır (H5). İki kategorik değişken arasındaki ilişkiyi değerlendirmek için daha uygun bir test olduğu için Pearson'un Ki-kare testi rapor edilmiştir (Blaikie, 2003; Malhotra ve Birks, 2012). Pearson'un Ki-kare testi, gözlemlenen ve beklenen değerler arasındaki farkın istatistiksel olarak anlamlı olup olmadığını değerlendirmek için yapılan bir bağımsızlık testidir (Russo, 2004). Bu test, İnternet kullanıcılarının demografik özellikleri ile siber suç korkusu arasındaki ilişkilerin varlığını incelemek için kullanılmıştır. SPSS Nicel Analiz yazılımı durumsallık tabloları (Contingency tables) ve istatistiksel testler (Ki-kare) oluşturmak için kullanılmıştır. Ki-kare testi ile hipotezi test etmek için varsayılan anlamlılık düzeyi 0,05 (α = 0,05 olarak ayarlanmıştır, çünkü bu anlamlılık seviyesi hipotezleri test etmek için daha uygundur (Churchill ve Doerge, 1994; Payton, Greenstone ve Schenker, 2003).

Analizin ikinci kısmı araştırma sorusunu ele almaya ve hipotezleri (H1, H2, H3, H4) ikili lojistik regresyon analizleriyle test etmeye çalışmıştır. Varsayılan anlamlılık seviyesi 0.05 (α = 0.05) hipotezleri test etmek için eşik olarak belirlendi. İkili lojistik regresyon analizi, diğer tüm bağımsız değişkenleri sabit tutarken bağımsız değişkenlerin bağımlı değişkenler üzerindeki etkisini incelemek için kullanılan daha karmaşık bir istatistiksel araçtır (Field, 2009; Denis, 2015). Daha yorumlanabilir sonuçlar vermesi, bağımsız değişkenlerin bağımlı değişken üzerindeki etkisini araştırırken ikili lojistik regresyon kullanmanın avantajlarından birisidir (Engel & Keen, 1994; Pituch ve Stevens, 2016). İkili lojistik regresyon analizi, bağımsız değişkende meydana gelen bir birim değişikliğin bağımlı değişken üzerindeki etkisinin ne olduğunu yorumlamamıza olanak veren olasılık oranları (Exp (B)) verir (Verma, 2012). İkili lojistik regresyon, kriminoloji araştırmalarında en yaygın olarak uygulanan istatistiksel testlerden biridir, çünkü bu alandaki anahtar kavramların çoğu doğada ikili yapıdadır (örn. Mağduriyete karşılık mağdur olmama, suç korkusunun varlığına karşılık suç korkusunun yokluğu) (Britt ve Weisburd, 2010; Speelman, 2014. Siber suç araştırmaları ikili lojistik regresyon analizinin bu yaygın kullanımı için bir istisna değildir. Örneğin, ikili lojistik regresyon analizi siber suç mağduriyeti (Marcum, Higgins, Ricketts ve Wolfe, 2014; Reyns, 2015; Reyns, Fisher, Bossler ve Holt, 2019), DRDos saldırıları (Hyslip ve Holt, 2019), dijital korsanlığın nedenleri (Holt ve Morris, 2009) ve siber zorbalık (Navarro ve Jasinski, 2013) gibi konuları içeren çok sayıda araştırmada kullanılmıştır.

ANALİZ

İngiltere ve Galler Suç Araştırması (Crime Survey for England and Wales-CSEW) veri seti 2014/2015 (Office for National Statistics, 2016) şu araştırma sorusunu ele almak için kullanılmıştır: "Siber suç korkusu İnternet kullanıcılarının davranış ve güvenlik adaptasyonlarını nasıl etkiler?" Eskiden Britanya Suç Araştırması (British Crime Survey-BCS) olarak bilinen CSEW, İngiltere ve Galler'deki suçun derecesini ölçen bir mağduriyet anketidir. Anket 2001'den beri birer yıllık periyotlarla yürütülmektedir. Bu yüz yüze anket, katılımcıların son 12 ay içinde gerçekleşen suç deneyimlerinin yanında, suça karşı tutumları ve suç eğilimleri hakkındaki algıları ile ilgili sorular sormaktadır.

CSEW, katılımcıları seçerken çok aşamalı küme örnekleme prosedürünü kullanır. İngiltere ve Galler'de ikamet eden kişilerin posta kodu adres dosyası (Postcode address file-PAF) popülasyonu örneklemek için kullanılmaktadır (Maxfield ve Babbie, 2015). Her bir polis gücü bölgesi için en az 650 kişi araştırmaya dahil edilmektedir. CSEW 2014/2015, İngiltere ve Galler'de yaşayan 50.000 yetişkini davet etmiş ve ankete 35.000 yetişkin katılmıştır (Office for National Statistics, 2016b). Anket formatı, alt örneklemlerin yanı sıra tüm katılımcılara sorular soran takip modüllerini ve kendi kendine tamamlama modüllerini içerir ki, bu da tüm anket sorularının katılımcıların tamamına sorulmadığı anlamına gelir. Mesela, tüm katılımcılara kitlesel pazarlama dolandırıcılığı soruları sorulurken, rastgele seçilen ve toplam sayının %25'ine karşılık gelen katılımcılara çevrimiçi güvenlik soruları ve yine rastgele seçilen katılımcıların %75'ine banka kartı dolandırıcılığı soruları sorulmuş (CSEW Technical Report, 2015).

Bağımlı Değişkenler

Bu çalışma, kimlik hırsızlığı korkusu ile siber suç korkusunun İnternet kullanıcılarının çevrimiçi alışveriş davranışı, kişisel verilerin paylaşımı, şifre yönetimi ve bilgisayar güvenliği önlemleri üzerindeki etkisini incelemektedir. CSEW 2014/2015, Çevrimiçi Güvende Kalma Modülü bölümünde katılımcılara: "Son 12 ay içinde kendinizi çevrimiçi güvende tutmak için bu kartta listelenen şeylerden herhangi birini yaptınız mı?" sorusu ile Finansal Kayıp ve Sahtekarlık Modülünde katılımcıların çevrimiçi koruma önlemlerini ölçmek için "Birinin banka hesabı, elektronik cüzdan hesabı veya kredi kartı hesap bilgilerinizi ele geçirmesini önlemek için genellikle bu kart üzerindeki herhangi bir şeyi yapıyor musunuz?" sorularını sormuştur. Tüm değişkenler ikiye ayrılmıştır (0 = Hayır, Evet = 1).

Alışveriş Davranışı: Dört çevrimiçi davranış, çevrimiçi alışveriş davranışı için dolaylı tedbir değerlendirme kriteri olarak kullanıldı. İnternetten ürün satın almaktan kaçınmak, kaçınma-baş etme stratejilerini ölçmek için kullanılırken; yalnızca güvenli örün sitelerinden ürün satın almak, bir sitenin çevrimiçi satın almadan önce güvenli olduğunu gösteren işaretleri kontrol etmek, yalnızca iyi bilinen veya güvenilir örün sitelerini kullanmak başa çıkma stratejileri yaklaşımı için dolaylı değerlendirme kriteri olarak kullanıldı.

Kişisel Verilerin Paylaşımı: Kişisel veri paylaşımı kararı perspektifi, algılanan faydalar ve algılanan kişisel verileri paylaşma riskleri arasındaki mukayesenin bireylerin kişisel verilerini paylaşma kararlarını belirlediğini öne sürmektedir (Krasnova vd., 2012). Kişisel verileri paylaşmanın yararlarını algılayan İnternet kullanıcıları, kişisel verileri korumak için alınan önlemlerin korunması konusunda daha az endişe duyabilirler. 'Sadece bilinen kişileri sosyal ağlarda arkadaş olarak eklemek' ve 'sosyal ağlarda kişisel ayrıntılar koyma konusunda dikkatli olmak' gibi iki çevrimiçi davranış, kişisel verileri çevrimiçi paylaşma konusunda dolaylı değerlendirme kriteri olarak kullanıldı.

Bilgisayar Güvenlik Önlemleri: Dört çevrimiçi güvenlik davranışı; 'şüpheli e-postaları açmadan silme', 'yalnızca bilinen dosyaları veya programları indirme', 'örün sitesi hesap ayarlarını düzenleme' ve 'virüs veya diğer kötü amaçlı yazılımlar için düzenli olarak bilgisayar taraması yapmak' internet kullanıcılarının çevrimiçi koruma önlemlerini ölçmek için kullanılmıştır.

Şifre Yönetim: 'Karmaşık parola kullanma' ve 'değişik hesaplar için farklı şifreler kullanma' parola yönetimi stratejilerinin dolaylı ölçüm değişkenleri olarak kullanılmıştır. 'Karmaşık parolalar kullanma' ve 'her farklı çevrimiçi hesap için farklı bir parola kullanma' değişkenleri, parola yönetiminin dolaylı değerlendirme kriterleri olarak kullanılmıştır.

Bağımsız Değişkenler

Siber Suç Korkusu: Siber suç korkusu "kişisel tehlikenin değerlendirilmesi ve birisinin siber suçluların kurbanı olması durumunda zarar verici sonuçların azaltılmasının maliyetinin tahmini" olarak tanımlanır (Bernik vd., 2013, p. 9). Bu çalışmanın temel amacı, siber suç ve kimlik hırsızlığı korkusunun bireylerin güvenlik niyetleri üzerindeki etkisini anlamaktır. CSEW 2014/2015, siber suç korkusunun kapsamını çok endişeli olmaktan hiç endişelenmemeye kadar dört puanlık bir ölçekte ölçmek için katılımcılara 'Çevrimiçi suçun mağduru olmaktan ne kadar endişelisiniz' diye sormaktadır. Siber suç korkusunun varlığının ve yokluğunun etkisini değerlendirmek için; bu değişken, iki değişkenli bir değişken elde etmek için farklı bir değişken olarak yeniden kodlanmıştır. 'Çok endişeli' ve 'endişeli,' 'endişeli' olarak kodlanırken; 'çok endişeli değil' ve 'hiç endişeli değil,' 'endişeli değil' olarak kodlandı.

Demografik Özellikler: Daha önceki geleneksel suç korkusu ve siber suç korkusu çalışmaları, demografik özelliklerin suç korkusuyla ilişkili olduğunu önermekteydi. Önceki araştırmalara dayanarak; cinsiyet, yaş, eğitim düzeyi ve yıllık hane geliri bağımsız değişkenler olarak analizlere dahil edilmiştir. Katılımcıların yaşları üç kategoriye ayrılmıştır: (1) 30 yaş altı, (2) 30-59 yaş arası ve (3) 60 yaş üstü. Katılımcıların eğitim düzeyleri üç kategoriye ayrılmıştır: (1) A seviyesi veya üstü, (2) A seviyesi altı ve (3) Nitelik yok. Yıllık hane geliri yedi gruba ayrılmıştır: (1) 10.000 £ altında (2) 10.000 £- 19.999 £ (3) 20.000 £- 29.999 £ (4) 30.000 £- 39.999 £ (5) 40.000 £- 49.999 £ (6) 50.000 £- 69.999 £ (7) 70.000 £'dan fazla.

Tablo 1. Kavramların Ölçülmesi (Bağımlı Değişkenler)

Değişkenler	Aralık
Bağımlı Değişkenler	
Çevrimiçi Alışveriş Davranışı	
İnternetten ürün satın almaktan kaçınma (1=evet)	0-1
Sadece güvenli örün sitelerinden ürün satın alma (1=evet)	0-1
Çevrimiçi satın almadan önce bir sitenin güvenli olduğuna dair işaretlerin kontrol edilmesi (1=evet)	0-1
Sadece iyi bilinen veya güvenilir örün sitelerinin kullanılması (1=evet)	0-1
Kişisel verilerin Paylaşımı	
Sosyal ağlarda yalnızca bilinen kişilerin arkadaş olarak eklenmesi (1=evet)	0-1
Sosyal ağlara kişisel bilgileri koymada dikkatli olma (1=evet)	0-1
Bilgisayar Güvenliği Tedbirleri	
Şüpheli e-postaları açmadan silme (1=evet)	0-1
Sadece bilinen dosyaları ve programları indirme (1=evet)	0-1
Örün sitesi hesap ayarlarını düzenleme (1=evet)	0-1
Bilgisayarı düzenli olarak virüs veya diğer kötü amaçlı yazılımlara karşı tarama (1=evet)	0-1
Şifre Yönetimi	
Karmaşık şifreler kullanma (1=evet)	0-1
Her farklı çevrimiçi hesap için farklı bir şifre kullanma (1=evet)	0-1

Tablo 2. Kavramların Ölçülmesi (Bağımsız Değişkenler)

Değişkenler	Aralık
Bağımsız Değişkenler	
Siber suç korkusu (1=evet)	0-1
Yaş	
30 yaş altı (1=evet)	1-3
30-59 yaş arası (2=evet)	1-3
60 yaş üstü (3=evet)	1-3
Cinsiyet	
Erkek (1=evet)	0-1
Eğitim	
Nitelik yok (1=evet)	1-3
A-seviyesi altı (2=evet)	1-3
A-seviyesi veya üzeri (3=evet)	1-3
Gelir	
£10,000 altı (1=evet)	1-7
£10,000-£19,999 (2=evet)	1-7
£20,000-£29,999 (3=evet)	1-7
£30,000-£39,999 (4=evet)	1-7
£40,000-£49,999 (5=evet)	1-7
£50,000-£69,999 (6=evet)	1-7
£70,000 üzeri (7=evet)	1-7

BULGULAR

İki Değişkenli Analiz Bulguları

Analiz sonuçları yaş, eğitim düzeyi, gelir seviyesi ve siber suç korkusu arasında pozitif ilişkiler olduğunu göstermiştir (H5) (Tablo 3). Daha yaşlı kullanıcılar, genç ve orta yaşlı kullanıcılara kıyasla daha yüksek siber suç korkusu yaşadıklarını bildirmiştir. Benzer şekilde, daha eğitimli ve daha yüksek gelire sahip olanlar da yoğun siber suç korkusu olduğu tespit edilmiştir. Ek olarak, sonuçlar cinsiyet ile siber suç korkusu arasında anlamlı bir ilişkinin olmadığını göstermiştir.

Demografik özellikler ve siber suç korkusu arasındaki ilişkileri inceleyen iki değişkenli analiz sonuçları Tablo 2'de gösterilmektedir. Değişkenlerin dağılım sıklığını gösteren durum tabloları ve değişkenler arasındaki ilişkilerin istatistiksel anlamlılık derecesi ölçmede kullanılan Ki-kare test sonuçları rapor edilmiştir. Analiz sonuçları yaş, eğitim düzeyi, siber suç geliri ve korkusu arasında istatistiksel olarak anlamlı ilişkilerin varlığını göstermektedir. Yaşla ilgili olarak, yaşlı kullanıcılar genç ve orta yaşlı kullanıcılara kıyasla daha yüksek oranda siber suç korkusu bildirmişlerdir. Yaşlı katılımcıların yaklaşık %46'sı endişe duyarken, genç kullanıcıların sadece %30'u siber suç korkusu yaşadıklarını belirtmiştir ($\chi2 = 85,349$, $p \leq 0.001$). İki değişkenli analiz sonuçları, daha eğitimli İnternet kullanıcılarının siber suçların kurbanı olmaktan daha korktuklarını da göstermektedir. Eğitim düzeyinin siber suç korkusu karşısındaki dağılımları pozitif bir ilişki eğilimi göstermektedir (sırasıyla %44,8; %43,3 ve %36,2 ve $\chi2 =15,997$, $p \leq 0,01$. Benzer şekilde, yüksek gelire sahip olanlarda yüksek oranda siber suç korkusunun varlığına rastlanmıştır ($\chi2 =19,964$, $p \leq 0.01$. Ek olarak, sonuçlar cinsiyet ile siber suç korkusu arasında istatistiksel olarak anlamlı bir ilişkinin olmadığını göstermiştir. Erkeklerin %44'ü siber suç korkusu bildirirken, kadınların %43'ü siber suçlardan endişe duymaktadır ($\chi2 =0,075$, $p \leq 0.05$). Bu bulgu, önceki geleneksel suç korkusu ve siber suç korkusu çalışmalarının siber suç korkusundaki cinsiyet farklılıklarını önermesinden dolayı önemlidir.

Genel olarak, siber suç korkusundaki cinsiyet farklılıklarının olmaması nedeniyle iki değişkenli analiz sonuçları, demografik özellikler ile siber suç korkusu arasında bir ilişki olduğunu öne süren beşinci hipotezi kısmen desteklemektedir. Bir sonraki bölümde çok değişkenli analiz sonuçları sunulmaktadır.

Tablo 3. İki Değişkenli Analiz Sonuçları

Değişkenler		Siber Suç Korkusu		*Ki-kare Testi*
		Durumsallık Tablosu		
		Endişeli		
		Hayır	Evet	
Yaş				
	16-29	70,20%	29,80%	
	30-59	53,60%	46,40%	85,349***
	60+	54,40%	45,60%	
Cinsiyet				
	Erkek	56,40%	43,60%	0,075
	Kadın	56,70%	43,30%	
Eğitim				
	A seviyesi veya üzeri	55,20%	44,80%	
	A seviyesi altı	56,70%	43,30%	15,997***
	Nitelik yok	63,80%	36,20%	
Gelir				
	£10,000 altı	63,10%	36,90%	
	£10,000-£19,999	58,50%	41,50%	
	£20,000-£29,999	56,90%	43,10%	
	£30,000-£39,999	55,40%	44,60%	19.964**
	£40,000-£49,999	55,50%	44,50%	
	£50,000-£69,999	52,80%	47,20%	
	£70,000 üzeri	49,30%	50,70%	
	Toplam	**56,50%**	**43,50%**	

*=p ≤0.05, **=p ≤0.01, ***=p ≤0.001

Çok Değişkenli Analiz Bulguları

Siber suç korkusunun bireylerin çevrimiçi alışveriş davranışı, kişisel verilerin paylaşımı, bilgisayar güvenlik önlemleri ve şifre yönetimi üzerindeki etkisini incelemek için bir dizi ikili lojistik regresyon analizi yapılmıştır. Demografik özellikler, yaş, cinsiyet, eğitim ve gelir regresyon modellerine kontrol değişkeni olarak dahil edilmiştir.

Online Alışveriş Davranışı

Siber suç korkusunun dört tür çevrimiçi davranış üzerindeki etkisi ikili lojistik regresyon modelleri ile incelenmiştir. Siber suç korkusunun, alışverişten kaçınma davranışı ve alışverişten korunma önlemleri arasında pozitif bir ilişkili olacağı varsayılmıştır (H1). Analiz sonuçları bu varsayımı desteklemektedir. Tablo 4'te görülebileceği gibi, siber suç korkusu üç güvenli alışveriş davranışını (yalnızca güvenli web sitelerinden ürün satın alma, bir web sitesinin güvenli olduğunu gösteren işaretleri kontrol etme ve sadece iyi bilinen veya güvenilir web sitelerinden satın alma) pekiştirmektedir. Siber suç korkusunun, yalnızca güvenli web sitelerinden ürün satın alma olasılığını %48 oranında, çevrimiçi satın almadan önce güvenlik işaretlerini kontrol etme olasılığını %30 oranında ve iyi bilinen veya güvenilen siteleri kullanma olasılığını %25 oranında arttırdığı gözlemlenmiştir (Exp. (B) = 1.478; 1.310 ve 1.247 sırasıyla).

Kaçınma davranışı ile ilgili olarak, siber suç korkusun varlığının İnternet kullanıcılarının çevrimiçi alışveriş yapmalarını engellemediği tespit edilmiştir. Siber suçlardan korkan katılımcıların çevrimiçi alışverişten kaçınma olasılıkları %15 daha az olduğu görülmüştür (Exp. (B) = 0.849). Genç kullanıcıların çevrimiçi alışverişten kaçınma olasılığı diğer yaş gruplarına kıyasla daha düşük çıkmıştır. Orta yaşlı İnternet kullanıcılarının alışverişten kaçınma olasılıkları gençlere oranla %52 daha fazla iken, yaşlı katılımcıların genç kullanıcılara kıyasla çevrimiçi alışverişten kaçınma olasılıkları %153 daha fazla olmuştur (sırasıyla (B) = 1.525 ve 2.533). Sosyal statü de kaçınma davranışını öngörmüştür. Daha eğitimli (A düzeyi veya üstü) ve yüksek gelire sahip (30.000 £ 'dan fazla kazanan) internet kullanıcılarının kaçınma davranışında bulunma olasılıkları daha az çıkmıştır. Ayrıca, genç İnternet kullanıcılarının, orta yaşlı ve yaşlı kullanıcılara kıyasla güvenli web sitelerinden ve iyi bilinen veya güvenilir web sitelerinden satın alma olasılığının daha yüksek olduğu görülmüştür (sırasıyla (B) = 0,997 ve 0,979).

Tablo 4. Siber Suç Korkusunun Çevrimiçi Alışverişin Korunması Davranışı Üzerindeki Etkisi

	İnternetten ürün satın almaktan kaçınma	Sadece güvenli örün sitelerinden ürün satın alma	Çevrimiçi satın almadan önce bir sitenin güvenli olduğuna dair işaretlerin control edilmesi	Sadece iyi bilinen veya güvenilir siteleri kullanma
Analizdeki Değişkenler	*Exp(B)*	*Exp(B)*	*Exp(B)*	*Exp(B)*
Korku	0,849*	1,478***	1,310***	1,247***
Cinsiyet				
Erkek	0,982	1,057	1,04	0,967
Yaş				
30-59	1,525**	0,997	1,414***	0,979
60+	2,533***	0,746**	1,379***	1,055
Eğitim				
A-seviyesi altı	0,823	1,799***	1,920***	1,813***
A seviyesi veya üzeri	0,635***	2,671***	3,075***	2,640***
Gelir				
£10,000-£19,999	1,201	1,304**	0,430***	0,562***
£20,000-£29,999	0,769	1,869***	0,524***	0,649***
£30,000-£39,999	0,706**	1,785***	0,649***	0,821
£40,000-£49,999	0,338***	2,046***	0,718**	0,771**
£50,000-£69,999	0,389***	2,159***	0,825	0,84
£70,000 üzeri	0,396***	2,019***	0,941	0,933
Sabit	0,099***	0,873***	0,415***	0,902

*=p ≤0.05, **=p ≤0.01, ***=p ≤0.001

Bilgisayar Güvenliği Önlemlerini Uygulama Niyetleri

Siber Suç Korkusu ve İnternet kullanıcılarının bilgisayar güvenlik önlemlerini uygulama niyetleri arasında pozitif bir ilişki olduğu varsayılmıştır (H2). İkili lojistik regresyon analizi sonuçları, siber suç korkusunun bilgisayar güvenlik önlemlerini (şüpheli e-postaları açmadan silmek, yalnızca bilinen dosyaları veya programları indirmek, web sitesi hesap ayarlarını düzenlemek ve bilgisayarı virüsler veya diğer kötü amaçlı yazılımlar için düzenli olarak

taramak) niyeti artırdığını göstermiştir (Tablo 5). Siber suç korkusu, bilgisayarları düzenli olarak taranması olasılığını %45 oranında ve şüpheli e-postaları açmadan silme ihtimalini %50 oranında arttırdığı görülmüştür (sırasıyla (B) = 1.454 ve 1.505). Yaş grupları birbirleriyle mukayese edildiğinde, genç İnternet kullanıcılarının web sitesi ayarlarını yapma olasılıkları daha yüksekken (Exp. (B) = 0,731; 0,381), orta yaşlı ve daha yaşlı kullanıcıların şüpheli e-postaları silme eğilimleri daha yüksek çıkmıştır (Exp. (B) = 1,284; 1,227). Bu sonuç, farklı nesillerin İnternet becerilerine atfedilebilir. Web sitesi gizlilik ayarlarını değiştirmek için bir dereceye kadar İnternet bilgisi gerekir. Böylece, bu konularda daha uzman olan gençler, bu koruma önlemlerini yaşlı kullanıcılardan daha fazla uygulamaları doğal bir sonuç olarak ortaya çıkmaktadır. Öte yandan, şüpheli e-postaları açmadan silmek, istenmeyen e-postalar aracılığıyla kimlik avına karşı koruyucu bir önlemdir. Orta yaşlı ve daha yaşlı İnternet kullanıcıları, riskten kaçınmak için şüpheli e-postaları silme olasılıklarının daha yüksek olduğu görülmüştür. Ancak, şüpheli e-postaları göz ardı etmek de riskleri azaltmanın etkili bir yoludur. Büyük olasılıkla, daha genç İnternet kullanıcıları, istenmeyen e-postaları silmek yerine bunları görmemezlikten gelmeyi tercih ettiler. Son olarak sosyo-ekonomik statü tüm güvenlik önlemlerini öngörmüştür. Sosyal statüsü daha yüksek olan (gelir ve eğitim düzeyi) bireylerin çevrimiçi koruma önlemleri alma olasılığı daha yüksek çıkmıştır. Örneğin, eğitim düzeyi A düzeyi veya daha yüksek olan kullanıcıların herhangi bir niteliği olmayanlara göre, şüpheli e-postaları silme olasılığı 3,6 kat, yalnızca bilinen dosyaları indirme olasılığı 3,1 kat daha yüksek olduğu görülmüştür.

Tablo 5. Siber Suç Korkusunun Bilgisayar Güvenlik Önlemlerine Etkisi

	Açmadan silinen şüpheli e-postalar	Yalnızca indirilen bilinen dosya veya programlar	Düzeltilmiş örün sitesi hesap ayarları (ör., gizlilik ayarları)	Düzenli olarak virus veya diğer kötü amaçlı yazılımlara karşı taranmış bilgisayar
Analizdeki Değişkenler	*Exp(B)*	*Exp(B)*	*Exp(B)*	*Exp(B)*
Korku	1,505***	1,358***	1,223**	1,454***
Cinsiyet				
Erkek	0,906	1,018	0,996	1,008
Yaş				
30-59	1,284**	1,047	0,731***	0,896
60+	1,227*	0,926	0,381***	1,006
Eğitim				
A-seviyesi altı	1,856***	1,620***	1,700***	1,503***
A seviyesi veya üzeri	3,676***	3,148***	3,441***	2,277***
Gelir Düzeyi				
£10,000-£19,999	1,256**	1,263*	0,984	0,600***
£20,000-£29,999	2,082***	1,639***	1,19	0,551***
£30,000-£39,999	2,265***	1,766***	1,18	0,697**
£40,000-£49,999	2,667***	1,925***	1,293*	0,81
£50,000-£69,999	3,219***	2,076***	1,342*	0,952
£70,000 üzeri	4,321***	3,079***	1,745***	0,845
Sabit	1,406****	0,856	0,513***	0,617***

*=p ≤0.05, **=p ≤0.01, ***=p ≤0.001

Parola Yönetimi ve Kişisel Verilerin Paylaşımı

Üçüncü hipotez, siber suç korkusu ile İnternet kullanıcılarının şifre yönetimi stratejileri arasında pozitif bir ilişki olduğunu varsaymaktaydı. Tablo 5'te sunulan analiz sonuçları bu varsayımı desteklemektedir. Analiz, bireylerin siber suç korkusu düzeyine meydana gelen bir birimlik artışın, karmaşık şifre kullanımını olasılığını %37 ve farklı şifre kullanımı olasılığını %38 oranda artırdığını göstermiştir (Exp. (B) = 1.371 ve 1.376) (Tablo 5). Siber suç korkusunun varlığını bildiren kullanıcıların, karmaşık parolalar ve her çevrimiçi hesap için farklı parolalar kullanma olasılıklarının yaklaşık olarak %37 daha fazla olduğu ortaya çıkmıştır (sırasıyla (B) = 1.371 ve 1.376).

Yaş karmaşık şifreler kullanmayı öngörmektedir. Genç kullanıcıların, orta yaşlı ve yaşlı kullanıcılara kıyasla karmaşık şifreler kullanma olasılığı daha yüksek çıkmıştır (Exp. (B) = 0,709; 0,471). Bu bulgunun risk farkındalığının bir sonucu olduğu değerlendirilmektedir. Çevrimiçi tehdit hakkında daha bilinçli ve bilgili olan genç İnternet kullanıcılarının hesapları için karmaşık şifreler kullanmaları daha muhtemeldir. Son olarak, eğitimin şifre yönetimi üzerindeki etkisi ile ilgili olarak, eğitim seviyesi ile şifre yönetimi stratejilerinin uygulanması olasılığı arasında pozitif bir ilişki olduğu görülmektedir.

Ayrıca, siber suç korkusu ve İnternet kullanıcılarının kişisel verilerini paylaşma davranışı arasında negatif bir ilişki olduğu varsayılmıştı (Dördüncü hipotez). Tablo 6'te görülebileceği gibi, çok değişkenli analiz bu öneriyi desteklemektedir. Analiz sonuçları, siber suç korkusunun, sosyal medya aracılığıyla kişisel verilerin paylaşımına ilişkin farkındalığı artırdığını göstermiştir.

Siber suç korkusu yüksek olan bireylerin sosyal ağlar üzerinden kişisel verileri paylaşma konusunda dikkatli olma olasılıklarının %22 ve sosyal ağlara yalnızca bilinen kişileri ekleme olasılıklarının ise %22 daha fazla olduğu tespit edilmiştir (Exp. (B) = 1,223 ve 1,181). Genç İnternet kullanıcılarının, orta yaşlı ve yaşlı kullanıcılara kıyasla kişisel verilerin paylaşımı konusunda daha bilinçli olduğu ortaya çıkmıştır. Örneğin, orta yaşlı kullanıcıların genç kullanıcılara kıyasla sosyal ağlara bilinen kişileri ekleme olasılığının %27 daha fazla ve sosyal ağlara kişisel ayrıntıları koyarken dikkatli olma konusundaki olasılıkları ise %23 daha az olduğu görülmüştür.

Tablo 6. Siber Suç Korkusunun Kişisel Verilerin Paylaşımı ve Şifre Yönetimi Üzerindeki Etkisi

	Kişisel Verilerin Paylaşımı		Şifre Yönetimi	
	Sosyal ağlarda yalnızca bilinen kişileri arkadaş olarak ekleme	Sosyal ağ sitelerine kişisel ayrıntılar koymak konusunda dikkatli olma	Kullanılan karmaşık şifreler	Her farklı çevrimiçi hesap için farklı bir şifre kullanılması
	Exp(B)	Exp(B)	Exp(B)	Exp(B)
Analizdeki Değişkenler				
Korku	1,181**	1,223***	1,371***	1,376***
Cinsiyet				
Erkek	1,037	1,078	0,994	1,096
Yaş				
30-59	0,736***	0,777**	0,709***	1,11
60+	0,347***	0,398***	0,471***	0,96
Eğitim				
A-seviyesi altı	1,218*	1,286***	1,637***	1,457***

A seviyesi veya üzeri	1,919***	1,923***	3,303***	2,058***
Gelir				
£10,000-£19,999	1,024	1,091	1,197	0,979
£20,000-£29,999	1,193	1,234*	1,608***	1,041
£30,000-£39,999	1,215	1,411**	1,777***	1,044
£40,000-£49,999	1,314**	1,223	2,332***	1,097
£50,000-£69,999	1,300*	1,31*	2,312***	1,143
£70,000 üzeri	1,376**	1,396**	3,131***	1,177
Sabit	1,370**	1,824*	2,195***	0,553***

*=p ≤0.05, **=p ≤0.01, ***=p ≤0.001

SONUÇ ve TARTIŞMA

Bu ampirik çalışma, siber suç korkusunun İnternet kullanıcılarının çevrimiçi alışveriş koruma davranışları (yaklaşım ve kaçınma), kişisel verilerin paylaşımı ve güvenlik niyetleri üzerindeki etkisini incelemiştir. Siber suç korkusunun belirleyicileri de araştırılmıştır. Bu amaçla, İngiltere ve Galler 2014/2015 Suç Araştırması'nın ulusal temsili veri seti kullanılmıştır. Demografik özellikler, yaş, cinsiyet, eğitim ve yıllık hane geliri de analizlere dahil edilmiştir.

Bu çalışma, siber suç korkusunun öngörücüleri ve siber suç korkusunun başa çıkma tepkileri üzerindeki etkisini anlamamıza ışık tutan yeni önemli bulgular ortaya koymuştur. Önceki araştırmalar, siber suç korkusu, kaçınma davranışı ve alışveriş niyeti arasında pozitif bir ilişki olduğunu ileri sürüyordu (Hille vd., 2015; Riek vd., 2016; Brands ve van Wilsem, 2019) (H1). Ancak bu çalışmanın sonuçları, İnternet kullanıcılarının siber suçlardan korkmalarına rağmen alışverişe devam ettiklerini göstermektedir. Bu çalışmanın bir diğer yeni katkısı ise Yaklaşım/kaçınma alışverişi davranışındaki yaş farklılıklarını göstermiş olmasıdır. Genç İnternet kullanıcılarının yaklaşım alışveriş stratejilerini (güvenli örün sitelerinden satın alma ve yalnızca iyi bilinen veya güvenilir siteleri kullanma) kullanma olasılıkları yüksek çıkarken, çevrimiçi satın almadan kaçınma ihtimalleri daha düşük çıkmıştır. Bu sonuçlar, genç kullanıcıları içgüdüsel alışveriş yapan bireyler olarak tasvir eden mevcut araştırmalarla çelişmektedir (Lin vd., 2012; Wu ve Lee, 2016; Kumar vd., 2020).

Siber suç korkusunun kişisel verilerin paylaşımı davranışı üzerindeki etkisine ilişkin sonuçlar, daha yüksek endişe düzeyine sahip İnternet kullanıcılarının kişisel verileri paylaşmaktan daha fazla kaçındıklarını göstermiştir. Bu sonuç, kişisel veri paylaşmayla ilgili endişeler kişisel verileri paylaşmanın algılanan ödüllerini aştığında, bireylerin paylaşılan bilginin miktarını ve türünü kontrol etme eğiliminde olduğunu öngören kişisel veri paylaşım perspektifini desteklemektedir. (Kuo vd., 2013; Trepte vd., 2017; Gruzd vd., 2018).

Ayrıca, bu çalışmanın (Blank vd., 2014) ile uyumlu ancak (Lutz ve Strathoff, 2014; Xie ve Kang, 2015)'ın çalışmaları ile çelişen bir diğer önemli katkısı da, genç İnternet kullanıcılarının sosyal medya vasıtasıyla kendini teşhir etme davranışını kontrol etme olasılığının daha yüksek olduğunu göstermesiydi. Bu sonuç, gençlerin İnternet becerilerine atfedilebilir. Sosyal medya gizlilik ayarları hakkında daha bilgili olan genç internet kullanıcılarının gizlilik kontrollerini uygulaması daha mümkündür.

Önceki araştırmalar, daha düşük sosyal statüye (düşük eğitim ve gelir) sahip bireylerin daha yüksek derecede siber suç/kimlik hırsızlığı korkusu bildirdiğini ileri sürüyordu (Roberts vd., 2013; Virtanen, 2017; Brands ve van Wilsem, 2019). Ancak, bu çalışma eğitim, gelir ve siber suç korkusu arasında olumlu bir eğilim olduğunu göstermiştir. Daha eğitimli ve daha fazla yıllık geliri olan İnternet kullanıcıları, daha az eğitimli ve daha az kazancı olanlara kıyasla daha yüksek siber suç korkusu bildirmişlerdir. Ayrıca, daha önceki çalışmalar, kadınları suçtan daha çok korkan kişiler olarak göstermekteydi (Pereira vd., 2016; van Eijk, 2017). Bununla birlikte, bu çalışmanın sonuçları siber suç korkusunda cinsiyet farklılığını desteklememektedir. Bu sonuç kötü amaçlı yazılım enfeksiyonu ve kimlik hırsızlığı korkusunun belirleyicilerini inceleyen araştırmaların sonuçlarını desteklemektedir (Roberts vd., 2013; Yu, 2014). Çevrimiçi tehditlere karşı algılanan hassasiyet, bu sonuç için olası bir açıklama olabilir. Kadınlar çevrimiçi taciz gibi çevrimiçi kişilerarası tehditlere daha fazla maruz kalmaktadır (Kimble, 2016; Backe vd., 2018). Bunun nedeni, bireyler hakkındaki bilgilerin Sosyal ağ siteleri (SOS) üzerinden edinilme fırsatıdır. Siber tacizciler muhtemel hedeflerinin kişisel özellikleri hakkında bilgi toplama yeteneğine sahipken, finansal kazanç elde etmeyi amaçlayan çevrimiçi failler, potansiyel hedeflerin cinsiyeti ile ilgili sınırlı bilgiye sahiptir. Bu nedenle, cinsiyete dayalı çevrimiçi saldırılar yapmazlar. Bu gerçek, bireylerin siber suç korkusu ile ilgili algılarına yansımış gibi görünmektedir.

Analiz sonuçları, siber suç korkusunun alışverişten kaçınma davranışını desteklemediğini göstermektedir. Siber suç korkusu olan İnternet kullanıcıları, güvenli çevrimiçi örün sitelerinden mal satın alma gibi koruma uygulamalarını benimsedikleri görülmektedir. Çevrimiçi satış yapanlara duyulan güven, yaklaşım başa çıkma stratejilerinin siber suç korkusuyla başa çıkmada ana itici güç olarak ortaya çıkmıştır. Bu sonuç, çevrimiçi satıcıların çevrimiçi satışlarını artırmak için güven ve güvenli satın alma hissi oluşturması gerektiğini göstermektedir. Analiz sonuçları ayrıca, genç İnternet kullanıcılarının çevrimiçi alışverişten kaçınma olasılığının düşük olduğunu ve çevrimiçi satın almaya devam etmek için aktif mücadele stratejileri kullanma olasılıklarının daha yüksek olduğunu göstermektedir. Bu sonuç, İnternet kullanıcılarının çevrimiçi tehditlere ilişkin bilgilerine istinaden İnternet öz-yeterliliğinin sonucu olabilir. Çevrimiçi tehditlerle aktif olarak mücadele ile ilgili eğitim programları orta yaşlı ve yaşlı İnternet kullanıcılarına yönlendirilebilir.

Analiz, siber suç korkusunun İnternet kullanıcılarının şifre yönetimi stratejilerini benimsemesine yol açtığını ortaya koymaktadır. Siber suç korkusu olan İnternet kullanıcıları, farklı çevrimiçi hesaplar için daha karmaşık şifreler ve ayrı şifreler kullanma eğilimindedir. Orta yaşlı ve yaşlı İnternet kullanıcıları, siber suç mağduriyeti riskini artırabilecek daha az şifre yönetimi stratejileri kullandıkları tespit edilmiştir. İnternet güvenliği şirketleri ve örün siteleri, şifre doğrulaması için iki adımlı doğrulama gibi yeni yöntemler sunmaktadır. Karmaşık şifreleri ezberleme konusunda sorun yaşayan İnternet kullanıcıları bu tür ikincil şifre kimlik doğrulama yöntemlerini kullanmaya teşvik edilmelidir.

Yaklaşma-kaçınma vasıtasıyla başa çıkma paradigması, bireylerin korku uyandıran durumla aktif olarak yüzleşmek için koruyucu önlemler aldıklarını veya sorunu içselleştirdiklerini ve tehdidi görmezden geldiklerini ileri sürer (Lazarus ve Folkman, 1984). Analiz sonuçları, siber suç korkusunun yaklaşma başa çıkma stratejilerini

öngördüğünü göstermektedir. Ancak, siber suç korkusu bildiren kullanıcılar, kaçınma alışveriş davranışları uygulamadıkları görülmüştür. Bu sonuç, yaklaşıma/kaçınma davranışının uygulanmasında tek itici gücün korku olmayabileceğini göstermektedir. İnternetten alışveriş yapmanın veya daha düşük fiyatlar için mal satın alma kolaylığı gibi algılanan ödüllerin, siber suç mağduriyetine maruz kalma riskinden daha ağır bastığı görülmektedir. Gelecek siber suç korkusu çalışmaları, siber suç korkusu ile başa çıkma tepkilerini incelerken algılanan faydaların/ödüllerin aracı rolünü inceleyebilir.

TEŞEKKÜR

UK Data Archive'a araştırmada İngiltere ve Galler 2014/2015 Suç Araştırması Anketini kullanmama izin verdikleri için şükranlarımı sunarım.

ETİK METNİ

Bu makale Helsinki Deklerasyonunda yer alan Etik Kurallarına uygun olarak hazırlanmıştır. Çalışmada veri Birleşik Krallık Veri Merkezi tarafından sağlanan ikincil veri kullanıldığından etik kurulu raporuna ihtiyaç duyulmamıştır.

"Bu makalede dergi yazım kurallarına, yayın ilkelerine, araştırma ve yayın etiği kurallarına, dergi etik kurallarına uyulmuştur. Makale ile ilgili doğabilecek her türlü ihlallerde sorumluluk yazar(lar)a aittir."

KAYNAKÇA

Accenture. (2019). Ninth Annual Cost of Cybercrime Study. Available at: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study (accessed 12 Decembre 2019).

Anderson, R., Barton, C., Bölme, R., Clayton, R., Ganán, C., Grasso, T., Levi, M., Moore, T. ve Vasek, M. (2019). Measuring the Changing Cost of Cybercrime. Available at: http://orca.cf.ac.uk/122684/ (accessed 07 January 2020).

Arachchilage, N. ve Love, S. (2014). "Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective". *Computers in Human Behavior,* 38 (1): 304-312.

Backe, E. L., Lilleston, P. ve Mccleary-Sills, J. (2018). "Networked Individuals, Gendered Violence: A Literature Review of Cyberviolence". *Violence and Gender,* 5 (3): 135-146.

Başaranel, B.U. (2017). Online Terrorist Financing. M.Conway, L. Jarvis, O. Lehane, S. Macdonal ve L. Nouri (Eds.) *Terrorist's Use of the Internet: Assessment and Response*, 136, 95-108. Amsterdam: IOS Press.

Bernik, I., Dobovšek, B. ve Markelj, B. (2013). "To Fear or Not to Fear on Cybercrime". *Innovative Issues and Approaches in Social Sciences,* 6 (3): 1-17.

Bidgoli, M., Knijnenburg, B. P. ve Grossklags, J. (2016). When Cybercrimes Strike Undergraduates. Electronic Crime Research (eCrime), 2016 APWG Symposium, IEEE, pp. 1-10.

Blaikie, N. (2003). *Analyzing Quantitative Data: From Description to Explanation. London:*Sage.

Blank, G., Bolsover, G. ve Dubois, E. (2014). A New Privacy Paradox: Young People and Privacy on Social Network Sites. Prepared for the Annual Meeting of the American Sociological Association.

Boateng, F. D. (2016). "Fearfulness in the Community: Empirical Assessments of Influential Factors". *Journal of Interpersonal Violence*, 34(3): 562-562.

Böhme, R. ve Moore, T. (2012). How Do Consumers React to Cybercrime?. eCrime Researchers Summit (eCrime).IEEE.

Brands, J. ve Van Wilsem, J. (2019). "Connected and Fearful? Exploring Fear of Online Financial Crime, Internet Behaviour and Their Relationship". *European Journal of Criminology,* 2019(1): 1-22.

Britt, C. L. ve Weisburd, D. (2010). Logistic Regression Models for Categorical Outcome Variables. In: Piquero A., Weisburd D. (Eds.) Handbook of Quantitative Criminology. Springer, New York, NY, 649-682.

Button, M., Nicholls, C. M., Kerr, J. ve Owen, R. (2014). "Online Frauds: Learning from Victims Why They Fall for These Scams". *Australian ve New Zealand Journal of Criminology,* 47 (3): 391-408.

Chang, M. L. ve Wu, W. Y. (2012). "Revisiting Perceived Risk in the Context of Online Shopping: An Alternative Perspective of Decision-Making Styles". *Psychology ve Marketing,* 29 (5): 378-400.

Churchill, G. A. ve Doerge, R. W. (1994). "Empirical Threshold Values for Quantitative Trait Mapping". *Genetics,* 138 (3): 963-971.

Claar, C. L. ve Johnson, J. (2012). "Analyzing Home Pc Security Adoption Behavior". *Journal of Computer Information Systems,* 52 (4): 20-29.

Clough, J. (2011). "Cybercrime". *Commonwealth Law Bulletin,* 37 (4): 671-680.

Cnbc. (2017). Cybercrime Costs the Global Economy $450 Billion. Available at: https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html (accessed 06 August 2019).

Corre, K., Barais, O., Sunyé, G., Frey, V. ve Crom, J.-M. (2017). "Why Can't Users Choose Their Identity Providers on the Web?". *Proceedings on Privacy Enhancing Technologies,* 3: 72-86.

Culnan, M. J. ve Armstrong, P. K. (1999). "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation". *Organization Science,* 10 (1): 104-115.

Dai, B., Forsythe, S. ve Kwon, W.-S. (2014). "The Impact of Online Shopping Experience on Risk Perceptions and Online Purchase Intentions: Does Product Category Matter?". *Journal of Electronic Commerce Research,* 15 (1): 13.

Das, A., Bonneau, J., Caesar, M., Borisov, N. ve Wang, X. (2014). "The Tangled Web of Password Reuse", NDSS Conference, pp. 23-26.

Denis, D. J. (2015). *Applied Univariate, Bivariate, and Multivariate Statistics.* John Wiley ve Sons.

Dienlin, T. ve Metzger, M. J. (2016). "An Extended Privacy Calculus Model for Snss: Analyzing Self-Disclosure and Self-Withdrawal in a Representative Us Sample". *Journal of Computer-Mediated Communication,* 21 (5): 368-383.

Engel, B. ve Keen, A. (1994). "A Simple Approach for the Analysis of Generalizea Linear Mixed Models". *Statistica Neerlandica,* 48 (1): 1-22.

Field, A. (2009). *Discovering Statistics Using Spss. USA:* Sage Publications.

Fisher, B. S. ve Sloan, J. J. (2003). "Unraveling the Fear of Victimization among College Women: Is the "Shadow of Sexual Assault Hypothesis" Supported?". *Justice Quarterly,* 20 (3): 633-659.

Forsythe, S., Liu, C., Shannon, D. ve Gardner, L. C. (2006). "Development of a Scale to Measure the Perceived Benefits and Risks of Online Shopping". *Journal of Interactive Marketing,* 20 (2): 55-75.

Gruzd, A., Hernández-García, Á. (2018). "Privacy Concerns and Self-Disclosure in Private and Public Uses of Social Media". *Cyberpsychology, Behavior and Social Networking*, 21 (7): 418-428.

Gutt, T. A. ve Randa, R. (2016). "The Influence of an Empathetic Adult on the Relationship between Bullying Victimization and Fear at School". *Journal of Crime and Justice,* 39 (2): 282-302.

Guleryuz, I., ve Dalkilic Surgevil*, O. (2019).* "A Research On Determining The Effect Of Corporate Social Responsibility Projects On The Corporate Reputation." *Social Science Studies Journal,* 5(33)*,* 2089-2098.

Henson, B., Reyns, B. W. ve Fisher, B. S. (2013). "Fear of Crime Online? Examining the Effect of Risk, Previous Victimization, and Exposure on Fear of Online Interpersonal Victimization". *Journal of Contemporary Criminal Justice,* 29 (4): 475-497.

Hernandez-Castro, J. ve Boiten, E. (2014). "Cybercrime Prevalence and Impact in the UK". *Computer Fraud ve Security,* (2): 5-8.

Hille, P., Walsh, G. ve Cleveland, M. (2015). "Consumer Fear of Online Identity Theft: Scale Development and Validation". *Journal of Interactive Marketing,* 30: 1-19.

Holt, T. J. ve Morris, R. G. (2009). "An Exploration of the Relationship between Mp3 Player Ownership and Digital Piracy". *Criminal Justice Studies,* 22 (4): 381-392.

Howe, A. E., Ray, I., Roberts, M., Urbanska, M. ve Byrne, Z. (2012). "The Psychology of Security for the Home Computer User", 2012 IEEE Symposium on Security and Privacy: IEEE, pp. 209-223.

Hyslip, T. ve Holt, T. (2019). "Examining the Correlates of Failed Drdos Attacks". *Journal of Digital Forensics, Security Law,* 14 (2): 2.

Jansen, J. ve Van Schaik, P. (2018). "Persuading End Users to Act Cautiously Online: A Fear Appeals Study on Phishing". *Information ve Computer Security,* 26 (3): 264-276.

Jordan, G., Leskovar, R. ve Marič, M. (2018). "Impact of Fear of Identity Theft and Perceived Risk on Online Purchase Intention". *Organizacija,* 51 (2): 146-155.

Kimble, M. (2016), *Online Gendered Harassment and Violence: Naming the Harm and Punishing the Behavior.*Unpublished Thesis, University of Michigan, US.

Krasnova, H., Veltri, N. F. ve Günther, O. (2012). "Self-Disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture". *Business ve Information Systems Engineering,* 4 (3): 127-135.

Kumar, H., Garg, R., Kumar, P. ve Chhikara, R. (2020). A Qualitative Insight into the Personal Factors Impacting Online Impulse Behavior. *Strategies and Tools for Managing Connected Consumers.* IGI Global.pp. 279-291.

Kuo, F.-Y., Tseng, C.-Y., Tseng, F.-C. ve Lin, C. S. (2013). "A Study of Social Information Control Affordances and Gender Difference in Facebook Self-Presentation". *Cyberpsychology Behavior Social Networking,* 16 (9): 635-644.

Lazarus, R. S. (2006). "Emotions and Interpersonal Relationships: Toward a Person-Centered Conceptualization of Emotions and Coping". *Journal of Personality,* 74 (1): 9-46.

Lazarus, R. S. ve Folkman, S. (1984). *Stress, Appraisal, and Coping.* Springer Publishing Company.

Lee, S.-S., Choi, K.-S., Choi, S. ve Englander, E. (2019). "A Test of Structural Model for Fear of Crime in Social Networking Sites". *International Journal of Cybersecurity Intelligence Cybercrime,* 2 (2): 5-22.

Lin, Y.-H., Chen, C.-Y. (2012). "Adolescents'impulse Buying: Susceptibility to Interpersonal Influence and Fear of Negative Evaluation". *Social Behavior and Personality,* 40 (3): 353-358.

Lutz, C. ve Strathoff, P. (2014). "Privacy Concerns and Online Behavior–Not So Paradoxical after All? Viewing the Privacy Paradox through Different Theoretical Lenses". Available at SSRN: https://ssrn.com/abstract=2425132 (accessed 17 January 2020).

Maddison, J. ve Jeske, D. (2014). "Fear and Perceived Likelihood of Victimization in Traditional and Cyber Settings". *International Journal of Cyber Behavior, Psychology and Learning (IJCBPL),* 4 (4): 23-40.

Malhotra, N. ve Birks, D. F. (2012). *Marketing Research: An Applied Approach.* Harlow: Harlow : Financial Times/Prentice Hall.

Marcum, C. D., Higgins, G. E., Ricketts, M. L. ve Wolfe, S. E. (2014). "Hacking in High School: Cybercrime Perpetration by Juveniles". *Deviant Behavior,* 35 (7): 581-591.

May, D. C., Rader, N. E. ve Goodrum, S. (2010). "A Gendered Assessment of the ‘‘Threat of Victimization’’: Examining Gender Differences in Fear of Crime, Perceived Risk, Avoidance, and Defensive Behaviors". *Criminal Justice Review,* 35 (2): 159-182.

Moore, S. ve Shepherd, J. (2006). "The Elements and Prevalence of Fear". *British Journal of Criminology,* 47 (1): 154-162.

Mwagwabi, F., Mcgill, T. ve Dixon, M. (2014). "Improving Compliance with Password Guidelines: How User Perceptions of Passwords and Security Threats Affect Compliance with Guidelines", 47th Hawaii International Conference on System Sciences (HICSS), IEEE, pp. 3188-3197.

Navarro, J. N. ve Jasinski, J. L. (2013). "Why Girls? Using Routine Activities Theory to Predict Cyberbullying Experiences between Girls and Boys". *Women Criminal Justice,* 23 (4): 286-303.

Office for National Statistics. (2016), Crime Survey for England and Wales, 2014-2015. *UK Data Service. SN: 7889.*

Office for National Statistics. (2016b). Crime Survey for England and Wales Technical Report 2014/15. Available at: http://doc.ukdataservice.ac.uk/doc/7889/mrdoc/pdf/7889_csew_technical_report.pdf (accessed 01 July 2016).

Payton, M. E., Greenstone, M. H. ve Schenker, N. (2003). "Overlapping Confidence Intervals or Standard Error Intervals: What Do They Mean in Terms of Statistical Significance?". *Journal of Insect Science,* 3 (1): 34.

Pereira, F. ve Matos, M. (2016). "Cyber-Stalking Victimization: What Predicts Fear among Portuguese Adolescents?". *European Journal on Criminal Policy and Research,* 22 (2): 253-270.

Pereira, F., Spitzberg, B. H. ve Matos, M. (2016). "Cyber-Harassment Victimization in Portugal: Prevalence, Fear and Help-Seeking among Adolescents". *Computers in Human Behavior,* 62(1): 136-146.

Pituch, K. A. ve Stevens, J. P. (2016). *Applied Multivariate Statistics for the Social Sciences: Analyses with SAS and IBM's SPSS.* London:Routledge.

Putnik, N. ve Boskovic, M. (2015). "The Impact of Media on Students' Perception of the Security Risks Associated with Internet Social Networking-a Case Study". *Croatian Journal of Education,* 17 (2): 569-595.

Reyns, B. W. (2015). "A Routine Activity Perspective on Online Victimisation: Results from the Canadian General Social Survey". *Journal of Financial Crime,* 22 (4): 396-411.

Reyns, B. W., Fisher, B. S., Bossler, A. M. ve Holt, T. J. (2019). "Opportunity and Self-Control: Do They Predict Multiple Forms of Online Victimization?". *American Journal of Criminal Justice,* 44 (1): 63-82.

Riek, M., Bohme, R. ve Moore, T. (2016). "Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance". *IEEE Transactions on Dependable and Secure Computing,* 13 (2): 261-273.

Riek, M., Böhme, R. ve Moore, T. (2014). "Understanding the Influence of Cybercrime Risk on the E-Service Adoption of European Internet Users", Proceedings of the 13th Workshop on the Economics of Information Security (WEIS), Citeseer.

Riskiq. (2019). The Evil Internet Minute 2019. Available at: https://www.riskiq.com/infographic/evil-internet-minute-2019/ (accessed 01 Decembre 2019).

Roberts, L. D., Indermaur, D. ve Spiranovic, C. (2013). "Fear of Cyber-Identity Theft and Related Fraudulent Activity". *Psychiatry, Psychology and Law,* 20 (3): 315-328.

Roth, S. ve Cohen, L. J. (1986). "Approach, Avoidance, and Coping with Stress". *American psychologist,* 41 (7): 813.

Salleh, N., Hussein, R., Mohamed, N. ve Aditiawarman, U. (2013). "An Empirical Study of the Factors Influencing Information Disclosure Behaviour in Social Networking Sites", Advanced Computer Science Applications and Technologies (ACSAT), 2013 International Conference IEEE, pp. 181-185.

Salleh, N., Hussein, R., Mohamed, N., Karim, N. S. A., Ahlan, A. R. ve Aditiawarman, U. (2012). "Examining Information Disclosure Behavior on Social Network Sites Using Protection Motivation Theory, Trust and Risk". *Journal of Internet Social Networking ve Virtual Communities,* 2012: 1-12.

Skogan, W. (1986). "Fear of Crime and Neighborhood Change". *Crime and Justice,* 8: 203-229.

Speelman, D. (2014). "Logistic Regression". *Corpus Methods for Semantics: Quantitative Studies in Polysemy Synonymy,* 43: 487-533.

Thompson, W. E. ve Gibbs, J. C. (2016). *Deviance and Deviants: A Sociological Approach.* John Wiley ve Sons.

Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z. ve Ziegele, M. (2017). "A Cross-Cultural Perspective on the Privacy Calculus". *Social Media + Society,* 3 (1): 1-13.

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.

Van Der Meulen, N. S. (2013). "You've Been Warned: Consumer Liability in Internet Banking Fraud". *Computer Law ve Security Review,* 29 (6): 713-718.

Van Eijk, G. (2017). "Between Risk and Resistance: Gender Socialization, Equality, and Ambiguous Norms in Fear of Crime and Safekeeping". *Feminist Criminology,* 12 (2): 103-124.

Verma, J. (2012). *Data Analysis in Management with SPSS Software.* Springer Science ve Business Media.

Virtanen, S. M. (2017). "Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities". *Psychiatry, Psychology and Law,* 24 (3): 323-338.

Wall, D. S. (2010). Criminalising Cyberspace: The Rise of the Internet as a 'Crime Problem'. *In:* Jewkes, Y. ve Yar, M. (Eds.) *Handbook of Internet Crime.* Cullompton: Cullompton : Willan.pp. 88-103.

Wall, D. S. (2011). "Cybercrime and the Culture of Fear: Social Science Fiction (s) and the Production of Knowledge About Cybercrime (Revised Feb. 2011)". *Information, Communication ve Society,* 11 (6): 861-884.

Wall, D. S. (2015). The Internet as a Conduit for Criminal Activity. *In:* Pattavina, A. (Ed.) *Information Technology and the Criminal Justice System.* USA: Sage.pp. 77-98.

Warr, M. (2000). "Fear of Crime in the United States: Avenues for Research and Policy". *Criminal Justice,* 4 (4): 451-489.

Wu, P.-T. ve Lee, C.-J. (2016). "Impulse Buying Behaviour in Cosmetics Marketing Activities". *Total Quality Management Business Excellence,* 27 (9-10): 1091-1111.

Xie, W. ve Kang, C. (2015). "See You, See Me: Teenagers' Self-Disclosure and Regret of Posting on Social Network Site". *Computers in Human Behavior*. 52: 398-407.

Youn, S. (2005). "Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk–Benefit Appraisal Approach". *Journal of Broadcasting ve Electronic Media,* 49 (1): 86-110.

Yu, S. (2014). "Fear of Cyber Crime among College Students in the United States: An Exploratory Study". *International Journal of Cyber Criminology,* 8 (1): 36-46.