JOURNAL OF GASTRONOMY HOSPITALITY AND TRAVEL

ISSN: 2619-9548 **Journal homepage:** www.joghat.org

Received: 04.04.2022 Accepted: 01.06.2022

Journal of Gastronomy, Hospitality and Travel, 2022, 5(2), 588-606

Araştırma Makalesi (Research Article)

OLTALAMA SALDIRILARININ YENİ HEDEFİ OTEL WEB SİTELERİ (HOTEL WEBSITES ARE THE NEW TARGET OF PHISHING ATTACKS)

Senem YAZICI YILMAZ[1*] (orcid.org/ 000-0002-1318-3462)

Eda AVCI[2] (orcid.org/ 0000-0003-3834-7707)

[1]Muğla Sıtkı Koçman Üniversitesi, Turizm Fakültesi, Turizm İşletmeciliği Bölümü, Muğla, Türkiye

[2]Dokuz Eylül Üniversitesi, Efes Meslek Yüksekokulu, Turizm ve Otel İşletmeciliği Programı, İzmir, Türkiye

Özet

Turistler hızlı ve ucuz tatil alma ihtiyacı ile internetten alışveriş yapmaktadırlar. Bu durum ise siber suçlulara fırsatlar yaratmaktadır. Otel işletmelerinin web siteleri kopyalanmakta ve sahte tatil teklifleri elektronik posta ile müşterilere iletilmektedir. Oltalama bir çeşit dolandırıcılık yöntemi olup her geçen gün daha fazla turisti maddi zarara uğratmaktadır. Bu araştırmanın amacı otel web sitelerinin kopyalanması ile oluşturulan sahte web siteleri üzerinden gerçekleştirilen oltalama saldırılarının incelemesidir. Türkiye'de bulunan otel işletmelerinin web siteleri üzerinden gerçekleşen oltalama olayları örnek olay olarak belirlenmiştir. Araştırma nitel araştırma yöntemlerinden keşfedici örnek olay yöntemi ile gerçekleştirilmiştir. Veriler sosyal medya, çevrimiçi rezervasyon, yorum platformları, internet arama motorunda yer alan ve kullanıcılar tarafından anonimleştirilen kaynaklardan elde edilmiştir. Araştırma verileri için "turizmde oltalama, sahte otel işletmesi, sahte otel işletmesi rezervasyon, dolandırıcı otel işletmesi, siber dolandırıcı, phishing, çakma otel işletmesi sitesi, Bodrum'da sahte otel işletmesi, Antalya'da sahte otel işletmesi, Didim'de sahte otel işletmesi" anahtar kelimeleri taratılarak 89 google sayfasına, 1 Instagram profiline (dolandırılan tarafından açılmış), 15 Linkedin post, 19 şikayetvar.com post, 1 adet Tripadvisor mağdur post, 84 adet tweet, 3 gazete websitesi ve arşivi, 3 resmi kamu websiteleri ve arşiv bilgileri, 5 kitap bölümü, 5 blog sitesi/web sitesi, 3 konferans bildirisi ve 37 makaleye ulaşılmıştır. Elde edilen veri doküman analizi tekniği ile incelenmiştir. Araştırma bulguları vurdumduymazlık, dijital okuryazarlık, farkındalık ve yasal düzenleme yetersizliği olmak üzere üç kategoriye ayrılmıştır. Araştırma sonucunda söz konusu bulgular devlet, sektör ve müşteri üçgeninde değerlendirilerek oltalama saldırılarının gelecekte önlenmesi yönelik öneriler geliştirilmiştir.

Anahtar Kelimeler: Web Siteleri, Bilgi Güvenliği, Güvenlik Açığı, Oltalama, Otel İşletmeciliği

Abstract

Tourists are shopping online with the need to get a fast and cheap holiday. This creates opportunities for cybercriminals. Websites of hotel businesses are copied, and fake holiday offers are sent to customers via e-mail. Phishing is a kind of fraudulent method and is causing more and more tourists financial damage every day. The purpose of this research is to examine the phishing attacks carried out on fake websites created by copying hotel websites. Phishing incidents on the websites of hotel businesses in Turkey have been determined as a case study. The research was carried out with the exploratory case study method, one of the qualitative research methods. The data were obtained from sources such as social media, online booking, comment platforms, internet search engines and anonymized by users. For research data, "phishing in tourism, fake hotel business, fake hotel business reservation, fraudulent hotel business, cyber fraud, phishing, fake hotel business site, fake hotel business in Bodrum, fake hotel business in Antalya, fake hotel business in Didim". " keywords were searched, 89 google pages, 1 Instagram profile (opened by the defrauded), 15 LinkedIn posts, 19 complainvar.com posts, 1 TripAdvisor victim post, 84 tweets, 3 newspaper websites and archives, 3 official public websites and archive information, 5 book chapters, 5 blog sites/web sites, 3 conference papers and 37 articles were reached. The obtained data were analysed by document analysis technique. Research findings are divided into three categories as callousness, digital literacy, awareness, and lack of legal regulation. As a result of the research, the findings in question were evaluated in the triangle of the state, the sector and the customer, and suggestions were developed for the prevention of phishing attacks in the future.

Anahtar Kelimeler: Websites, Information Security, Vulnerability, Phishing, Hotel Management

* Sorumlu yazar: senemyazici@mu.edu.tr

DOİ: 10.33083/joghat.2022.153

Giriş

Sahte web siteleri ile dolandırıcılık her geçen gün artarak hem işletmenin hem de müşterilerin bilgilerini çalarak maddi ve manevi zararlar yaratmaktadır. Bilgi güvenliği bir işletmenin bilgi kaynakları ile iş devamlılığını sağlamak amacıyla tehditlerden korunması, bilginin yalnızca işletme amaçları çerçevesinde kullanılması anlamına gelmektedir (Grobler ve Louwrens, 2007). Bu bağlamda bilgi güvenliği için bütünlük, erişilebilirlik ve gizlilik ilkelerinin sağlanmış olması hayati önem taşımaktadır. Söz konusu ilkelerin ihlal edilmesi güvenlik zafiyeti meydana getirmekte (Pesen, 2015), bilginin korunamaması ise para, zaman, insan gücü ve iş fırsatlarının kaybedilmesi ve işletmenin geri dönülmesi oldukça zor bir zarara uğramasına neden olabilmektedir (Whitman ve Mattord, 2012: 75).

Otel işletmeleri web siteleri sayesinde turist ile aralarında aracıyı kaldıran ve direkt satış kanalı görevi gören bir yapı oluşmuştur. Otel web sitelerinden alışveriş yapmak gittikçe kolaylaşmıştır. Aynı zamanda turist için bu alışveriş kolaylık ve zaman tasarrufu sağlamakta ve fırsatlar yaratmaktadır. Bu nedenle birçok turist ucuz tatil reklamı ile gelen e-postalara bakmakta ve bunları fırsat olarak görmektedir ve bu nedenle bir dolandırıcılığın içinde olduklarını fark etmeyen ve bundan mağdur olan turist sayısı her geçen gün artmaktadır. Oltalama (phishing) olarak bilinen söz konusu dolandırıclık; sosyal mühendislik teorisi çerçevesinde bir bireyi ya da kuruluşu, bilişim teknolojileri aracılığıyla bir saldırgandan gelen isteğe uymaya ikna etmek için bir araç olarak sosyal etkileşimi kullanma bilimi olarak tanımlanmaktadır (Zhang vd., 2021).

Bir "ikna sanatı" olarak nitelendirilen sosyal mühendislik saldırılarının altında yatan temel amaç, sosyal etkileşimle ikna yeteneğinin kullanılmasıdır. Doğrudan ya da dolaylı iletişim kurulması ile gerçekleşen sosyal mühendislik saldırıları (Mouton, vd., 2014), araştırma, uyum, güven geliştirme, güvenden yararlanma ve bilgiyi kullanma aşamalarından oluşmaktadır. Araştırma aşamasında saldırganlar hedefleri hakkında mümkün olduğunca detaylı bilgiye ulaşmaya çalışmakta ve bir sonraki aşama olan hedefle uyum ve güven geliştirme aşamasında bu bilgileri kullanmaya odaklanmaktadır. Hedefin saldırgana güvenmesiyle birlikte güven manipüle edilerek hassas bilgiler ele geçirilmekte ve söz konusu bilgiler kullanılarak dolandırıcılık faaliyetinde başarıya ulaşılmaktadır. Sosyal iletişim yeteneği ile manipüle edilen mağdur tüm bu süreçte dolandırıldığından şüphe etmemekte ve her şeyin farkına vardığında dolandırıcılar çoktan amacına ulaşmış olmaktadır (Mitnick ve Simon, 2002).

Sosyal mühendislik saldırılarının temelinde korku, şehvet, açgözlülük, ahlaki zorunluluk ve suçluluk duygusu gibi insanların zayıf yanlarının sömürülmesi yatmaktadır. Ayrıca sosyal mühendisler, ikna kabiliyeti yüksek, yardımsever görünen, ustalıkla yalan söylenebilen, masum gibi görünen sorular arasına sıkıştırdıkları anahtar sorular ile bilgiyi elde eden profesyonellerden oluşmaktadır (Abraham ve Chengalur-Smith, 2010). Kimlik bilgileri, şifreler, kredi kartı bilgileri, şirket dokümanları gibi kritik bilgilerin elde edilmesi için insan psikolojisini hedef alan ve sağduyuyu manipüle eden sosyal mühendislik saldırıları, güçlü güvenlik önlemlerine rağmen başarılı olabilmektedir (Ghafir ve Prenosil, 2016).

Turistik satın alma davranışının en önemli aşamalarından biri olan bilgi arama aşaması bilgi ve iletişim teknolojilerinde yaşanan gelişmeler sayesinde bugün sıklıkla internet ortamında gerçekleşmektedir (Yıldırım, 2016). Turistlerin ihtiyaç duyduğu bilgiye kolay ve hızlıca ulaşmasını sağlayan internet aynı zamanda dolandırıcıların iş sahası haline de gelmiştir. İnternet ortamında güvenli bilgiye ulaşacağını düşünen turistler oltalama saldırıları nedeniyle mağdur olabilmektedir. Turistik ürünün doğası gereği satın alma öncesi deneyimlenememe özelliğine sahip olması ise bu duruma zemin hazırlamaktadır. Turistik müşteriler satın aldıkları ürünü yani bir tatili ya da otel işletmesi odasını, satın aldıktan sonra deneyimlemek zorundadır (Civelek, 2016, Kıycı vd., 2021).

Satın alma sonrası dönemde hevesle ürüne kavuşmayı bekleyen müşteri, dolandırıcılar nedeniyle büyük bir hayal kırıklığına uğramakta ve dolandırıldığını ancak otel işletmesine gittiğinde fark etmektedir. Dolandırıcılığa adı karışan otel işletmesi de durumdan ancak bu vesile ile haberdar olmaktadır. Her iki tarafın da mağdur olduğu bu süreç, şaşkınlık, üzüntü, hayal kırıklığı ve aldatılmışlık hisleri ile son bulmaktadır. Hem üretici (otel işletmesi) hem de müşteri (turist) açısından önemli kayıplara neden olan bu duruma dikkat çekilmesi ve konuya olan farkındalığın artması önem arz etmektedir. Bu nedenle araştırmada, otel web siteleri aracılığıyla gerçekleştirilmiş oltalama saldırıları incelenmiştir. Konunun derinlemesine incelenmesi ve tüm yönleri ile ele alınması amacıyla nitel yöntem ile gerçekleştirilen bu araştırmada veri toplama aşamasında örnek olay tekniğinden yararlanılmıştır. İçerik analizinin ardından, araştırma verisi ile mevcut durum ve alınan önlemler hakkındaki bilgiler sınıflandırılmıştır. Araştırma sonucunda, turistlerin oltalama saldırılarına maruz kalma ihtimallerinin düşürülebilmesi için faydalı olabilecek öneriler geliştirilmiştir.

Kavramsal Çerçeve

Bilgi Güvenliği

Dijital çağın başlangıcı olarak kabul edilen ARPANET projesi ile bilgisayarlar birbirine bağlanmış ve ilk veri transferi gerçekleştirilmiştir (Packard, 2020). 1960-1970 yıllarında bilgisayar ağı ve bu ağ üzerinden yapılabilecekler geliştirilmişse de esas değişim, 1983 yılında Tim Barner Lee tarafından internet sunucu ağı kısaca "www" olarak bilinen yapı keşfedildiğinde başlamıştır (Aldrich, 2013; Ashton, 2020). 2000 yılın ise, geleneksel yollarla yapılan iş ilişkileri, bilgi transferi ve alışveriş işlemlerinin internet ağı kullanılarak web siteleri üzerinden yapılmaya başlanması ile bir milat olarak kabul edilmektedir (Ashton, 2020). İlk yıllarda işletmeler web sitelerini ürünlerin pazarlamasında kullanmışlardır. İlerleyen yıllarda satın alma işlevinin de kullanılmaya başlanmasıyla e-ticaret kavramı doğmuştur (Kulular İbrahim, 2019).

Web siteleri işletmelerin gerçek dünyada üretilen ürünlerin internet üzerinden satışlarının gerçekleşmesini sağlamaktadır. Web siteleri alan adı ile açılır ve bu alan adlarının hem kısa hem de benzersiz olması gerekmektedir (Vinayakumar, Soman ve Poornachandran, 2018). E-ticaret amacıyla tasarlanacak olan web sitesi oluşturmanın ilk adımı benzersiz alan adını belirlemekle başlamaktadır (Lazarević, 2017). Web siteleri, ürünlerinin tanıtım, pazarlama ve satışının gerçekleştirildiği sanal dükkânlardır (Şenocak, 2009). Alan adı ise, bir kullanıcının web sitesine ulaşmak için kullandığı adrestir (Oguama, 2021).

İnternetteki tüm web siteleri, herhangi bir cihazdan ya da konumdan nasıl erişildiğini belirleyen İnternet Protokolü (IP adresi) adı verilen benzersiz bir sayı ve karakter kombinasyonundan oluşmaktadır (Brügger, 2009). Bu kombinasyonun hatırlanması zor olduğundan; alan adları tek ya da birleşik kelimeler ile ifade edilmektedir. Örnek olarak IP adresi "55.250.77.11" olan bir web sitesinde alan adı "marka" kelimesi kullanılarak adres çubuğuna "www.marka.com" olarak yazılarak kolaylıkla ulaşılmaktadır (Kulular İbrahim, 2019). Bir alan adı benzersiz ve aranabilir olmasının yanı sıra sitenin amacını da yansıtmalıdır (Oguama, 2021) ve bir alan adı seçerken göz önünde bulundurulması gereken sonsuz seçenek olmasına rağmen, alan adının kişisel ya da ticari kullanım için fark etmeksizin her zaman "özgün ve orijinal" olmasına dikkat edilmelidir (Wang vd., 2020). Bu nedenle alan adı seçerken kısa, akılda kalıcı ve bir arama tarayıcısına yazılması kolay olmasına dikkat edilmeli, markanın ya da işletmenin en önemli özellikleri düşünülmeli ve ayırt edilebilir kılmak için herhangi bir anahtar kelime, kelime öbeği ya da kelimeyi alan adı olarak seçilmelidir (Visconti, 2020).

İnternet ile yapılabilecekler yıllar içinde süratle gelişmiş, işletmeler büyük ve geniş bir coğrafyada ulaşılabilecekleri müşteriler için farklı bir pazarlama ve satış kanalı bulmuşlardır. İşletmeler ve müşteriler açısından iyi bir gelişme olan bu durum, güvenlik açıklarını da beraberinde getirmiştir. Alınan önlemler kullanıcıların bilgi güvenliğinin sağlanması için zaman zaman yetersiz kalmıştır (Wang vd. 2020). Teknolojinin ilerlemesi ve yenilikler sayesinde, web siteleri işletmeler için sadece iletişim kurma ve bilgi verme fonksiyonlarından çıkmış, ticaretin yapılabilmesine olanak tanıyan bir yapıya kavuşmuştur (Plumley, 2010). Çevrimiçi ticaret söz konusu olduğunda, internet, yüzlerce hatta binlerce potansiyel ya da eski müşteri ile iletişim kurmak ve online satış gerçekleştirmek için uygun bir platform haline dönüşmüştür. Tüm bu olumlu gelişmelerin yanı sıra, web sitelerinin açıklarını kullanılarak müşterinin haberi olmadan elde edilen veriyi ücret karşılığı satan bilgisayar korsanları artarak büyük güvenlik sorunlarına neden olmaktadır. Bilgisayar korsanları, web sitesi sahiplerini ve kullanıcıları riske atabilecek hassas bilgileri açığa çıkararak (Wang vd. 2020) ve önemli verileri çalarak (Kara, 2021) ücret karşılığı satmaktadır. Bu nedenle, müşterilerin hassas bilgilerinin yasa dışı erişime karşı korunması oldukça önemlidir. Özellikle iletişim formu bulunan ve "ad, e-posta adresi ve telefon numarası" gibi ayrıntılı müşteri bilgilerini isteyen web sitelerinin, bilgi güvenliğini sağlamak için güçlü önlemler alması gerekmektedir (Aboobucker ve Bao, 2018).

Bilgi güvenliği teknik anlamda, bilgisayar ve iletişim güvenliğini içeren bilgi teknolojileri güvenliği ve fiziksel güvenlik unsurlarından oluşmaktadır (Karimi, 2018: 33). Bu bağlamda bilgi güvenliğini tehdit eden unsurları, zararlı yazılımlar, sahte antivirüs yazılımları, servisi engelleyen saldırılar (denial of service/dos), bilişim korsanlığı (hacking), zincir e-posta ve internet aldatmacası (hoax) ve sosyal mühendislik olmak üzere altı kategoride toplamak mümkündür. Zararlı yazılımlar, casus yazılımlar (spyware), mesaj sağanakları (spam), virüsler, arka kapılar (backdoor), solucanlar (worm), tuş kaydediciler (keylogger), turva atları (trojan horse) ve botnet gibi bulaştığı cihaza hem donanım ve yazılım açısından zarar vermekle birlikte cihazdaki veriyi başkalarının ulaşımına açan kötü amaçlı yazılımlardır. Antivirüs yazılım programları bilgisayarların içinde

bulunan belgelerin korumasını sağlamayı amaçlamaktadır fakat sahte antivirüs yazılımları da bulunmaktadır. Bu yazılımlar koruyormuş gibi gözükmesine rağmen hiçbir koruma gerçekleştirmemektedir.

Bilgi güvenliğini tehdit eden ve servisi engelleyen saldırılar (denial of service/dos), sisteme virüs gibi bulaşmayan ama sistem kapasitesini aşırı zorlayarak kullanılmayacak hale getiren, diğer bir değişle sistemin çökmesine neden olan saldırılardır. Yine, izinsiz bir şekilde sisteme girerek sistemi kontrol etme yönündeki girişimleri ifade eden bilişim korsanlığı (hacking) ve bir bilgiyi güvenilir bir kaynaktan geliyormuş gibi göstererek e-posta siteminde yer alan tüm alıcılara bilginin gönderilmesini talep eden kullanıcıyı bu konuda ikna etmeye çalışan girişimleri ifade eden zincir e-posta ve internet aldatmacası (hoax) da bilgi güvenliğini tehdit eden diğer unsurlardır. Sosyal mühendislik ise, kişilerin zaaflarından yararlanarak şifre, kredi kartı numarası gibi önemli bilgileri ele geçirmeye çalışan uygulamaları ifade etmektedir. En çok kullanılan sosyal mühendislik yöntemi oltalama olarak isimlendirilen, kişilerin sahte giriş ekranları ile kandırılarak önemli bilgileri girmelerini sağladıkları dolandırıcılık yöntemidir (Ceylan, 2019: 8). Tüm bu saldırılardan işletmeyi korumak adına uygulanacak olan bilgi güvenliği yönetimi ise, işletmenin yönetim birimlerinin güvenlik planlaması, yeni bilgi ve iletişim teknolojilerinin güvenlik gereksinimleri açısından değerlendirilmesi, güvenlik operasyon merkezinin tasarlanması, güvenlikle ilgili politikaların tanımlanması, risk değerlendirmesi, güvenlik teknolojilerinin seçimi, güvenlik açığı yönetimi kanallarının değerlendirilmesi ve güvenlik izleme gibi birçok önemli görevler üstlenildiği bütünsel bir süreçtir (Vladimirov vd., 2010: 68).

Bilgi Güvenliği Tehdidi Olarak Oltalama Saldırıları

Kişilerin güvendiği ilişkileri ve psikolojik faktörleri manipüle ederek kişisel bilgilerin kötü niyetli kişilerin eline geçmesine olanak tanıyan bir dolandırıcılık türü olan oltalama, internet kullanımının artması ile giderek yaygın bir hale gelmiştir (Yuan Sun, vd., 2016). Oltalama Önleme Çalışma Grubu (APWG) 2021 yılı raporuna göre, pandemi nedeniyle iş yapış biçimlerinin uzaktan yani internet aracılığı ile gerçekleşme zorunluluğu oltalama saldırılarının iki katına çıkmasına neden olmuştur. 2021 yılında oltalama saldırılarından en çok etkilenen sektörler; SAAS / Webmail (%29,1), Finansal Kurumlar (%17,8), E-ticaret /Perakende (%13,1), Sosyal Medya (%11,0), Ödeme (%7,1), Kripto (%5,6), Lojistik /Nakliye (%3,5), İletişim (%3,5) ve diğer sektörler (%9,3) olarak belirtilmektedir. Oltalama saldırıların küresel ekonomiye olan maliyetinin giderek artarak 6 trilyon dolardan 10,5 trilyon dolara ulaşacağı öngörülmektedir (APWG, 2021). Oltalama kavramı Kimlik Avı Önleme Çalışma Grubu tarafından müşterilerin kişisel kimlik verilerini ve finansal hesap kimlik bilgilerini çalmak için hem sosyal mühendislik hem de teknik hile kullanan bir suç mekanizması olarak tanımlanmaktadır. Oltalama eylemini gerçekleştirenler teknolojik açıkları kullanmanın yanı sıra, hedeflerini aldatabilecekleri ve ikna edebilecekleri kişilerden seçmekte ve onların kimlik bilgisi ve para gibi değerli varlıklarını ele geçirmektedir (Kara, 2021).

Oltalama saldırılarını, kimlik avı dolandırıcılığı (deceptive phishing), hedefli kimlik avı dolandırıcılığı (spear phishing), kopya web sitesi dolandırıcılığı (pharming) ve klonlama (clone phishing) olmak üzere dört ana başlıkta toplamak mümkündür. Kimlik avı dolandırıcılığı, hedefteki kişilere hesabın güncellenmesi gerektiği yönünde bir e-postaya gömülü köprü gönderilmesi ile gerçekleşmektedir. İlgili köprüye tıklandığında kişisel bilgiler ve oturum açma bilgileri talep edilmekte ve bu sayede önemli bilgilere erişilebilmektedir. Hedefli kimlik avı ise bir kuruluş içindeki belirli kişi ya da grupları hedefleyen bir dolandırma yöntemidir. Burada dolandırıcılığa maruz kalan hedef daha önceden araştırması yapılmış ve özel olarak seçilmiştir. Bir diğer oltalama çeşidi olan kopya web sitesi dolandırıcılığı, DNS yani Domain ismi sistemine saldırarak hedefi istenilen başka bir web sitesine yönlendiren bir taktiktir. Bu sayede kullanıcının yine kimlik bilgileri gibi önemli kişisel bilgilerine ulaşmak hedeflenmektedir. Klonlama ile yasal olan e-postaların kopyalanması ve benzer e-postaya ekler ve köprüler eklenmesi sonucunda kötü amaçlı web sitelerine yönlendirme gerçekleşmektedir (Fowdur ve Abdool Khader, 2018). Dolandırıcılar hedeflerini sahte web sitelerine yönlendirmek için e-postanın yanı sıra SMS, sosyal medya gibi çeşitli ortamları da kullanmaktadır (Bozkır ve Aydos, 2019).

Kimlik avı önleme müdahalelerinin nihai amacı, çeşitli kimlik avı e-postalarına karşı duyarlılığı azaltmaktır. Bilgi aramanın kimlik avına yatkınlığı etkilemedeki potansiyel rolünü anlamak için öncelikle, insanları kimlik avına duyarlı kılan unsurlarla ilgili mevcut araştırmaları dikkate almak gerekmektir. Alan yazınında yer alan araştırmalar incelendiğinde, duyarlılığı etkileyen faktörleri saptamak için gerçek dünyayı yansıtan kontrollü deneysel ortamlarda gerçekleştiği dikkat çekmektedir (Salloum vd., 2021; Grilli vd., 2021). Bulgulara göre, oltalama saldırılarını etkileyen narsisizm, dürtüsel olma gibi psikolojik, yaş ve cinsiyet gibi sosyo-demografik olmak üzere çeşitli faktörler bulunmaktadır. Psikolojik ve sosyo-demografik faktörler kadar teknik beceriler de önemli bir faktör olarak görülmektedir (Sankhwar vd., 2021; Daengsi vd., 2021). Yine, çevrimiçi ortama

yönelik algılanan riskteki bireysel farklılıkların ve insanların bilgisayar güvenliği ve çevrimiçi tehditlerle ilgili sahip oldukları bilgi ve deneyim derecesi de önemli faktörler arasında yer almaktadır (Baig vd., 2021; Grilli vd., 2021). Diğer yandan söz konusu araştırmalar, özellikle uzun vadeli etkileri göstermede sınırlı kalmaktadır (Vishva ve Aju, 2022).

Devlet, sivil toplum örgütleri ve üniversiteler kimlik avına yönelik potansiyel saldırı vektörlerine dikkat çekmeye ve siber suçluların saldırılarını gerçek gibi göstermek için web sitelerini ve e-posta adreslerini taklit etme yetenekleri konusunda farkındalık yaratmaya çalışmaktadır (Mohd Zaharon vd., 2021). Kimlik avına karşı korunmak için yaygın öneriler arasında, güvenli bağlantıların üzerinde gezinmek, e-postalardaki bağlantılara tıklamamak, şüpheli e-postaları siber güvenlik birimlerine bildirmek, bilinmeyen ekleri açmamak ve kullanıcı kimlik bilgilerini sağlamak gibi tavsiyeler yer almaktadır (Daengsi vd., 2021).

İnsanların çeşitli davranışlarda bulunma niyetlerini etkileyebilecek faktörlere odaklanan Koruma Motivasyon Teorisi siber güvenlik alanında umut vaat eden teorik bir yaklaşım olarak dikkat çekmektedir (Mou vd., 2021). Ayrıca, korku çekiciliği teorisi geliştirilmiş ve sağlık alanında kullanılmaktadır (Mehraj vd., 2021). Söz konusu teorinin kimlik avı bağlamında incelenmesi alan yazınında çok fazla çalışılmış ve etkisi kabul edilmiştir (Shahbaznezhad vd., 2021; Mehraj vd., 2021; Bax vd., 2021; Mou vd., 2021). Koruma Motivasyon Teorisini oluşturan faktörler, algılanan ciddiyet ve algılanan güvenlik açığı olmak üzere iki ana grupta değerlendirilmektedir. İnsanların belirli bir tehdidi ve sonuçlarını nasıl değerlendirdiği algılanan ciddiyeti ifade ederken, bu tehditti başarılı bir şekilde yönetme yeteneğini nasıl algıladığı güvenlik açığını ifade etmektedir (Haag vd., 2021). Yüksek düzeyde tehdit ve etkinlik değerlendirmesine sahip olmak, insanların kendilerini korumaya motive olmaları için gerekli kabul edilmektedir (Shahbaznezhad vd., 2021). Kişiler hem bir tehdidi algılamalı hem de kendilerini bu tehdidi etkin bir şekilde yönetebileceklerini düşünmelidir (Vrhovec ve Mihelič, 2021). Eğer insanlar bir tehdidi yüksek buluyor ancak bu tehdidi azaltmak için etkili bir şekilde hareket edebileceklerini hissetmiyorsa, bu durum tehdidin kendisini azaltmak yerine korku duygularını azaltmaya odaklanan uyumsuz başa çıkma stratejilerinin ortaya çıkmasına neden olabilmektedir (Bax vd., 2021). Bu yaklaşımda koruyucu bir davranışta bulunmanın algılanan maliyetleri ile algılanan ödüller genel tehdit değerlendirmesini etkileyebilmektedir (Mehraj vd., 2021).

Oltalama saldırılarını önlemeye yönelik geliştirilen profesyonel uygulamalar, liste tabanlı teknikler, buluşsal tabanlı teknikler, vizyon tabanlı teknikler ve makine tabanlı teknikler olmak üzere dört kategoriye ayrılmaktadır. Google Güvenli Tarama Uygulama Ara Yüzünün kullandığı liste tabanlı teknikler, web sayfaları URL bilgilerine dayalı olarak kara ve beyaz listelere böler. Bu sayede web siteleri oltalama saldırılarına karşı korunmuş olur fakat bu tekniğin işlevsel olabilmesi için kara listenin düzenli olarak güncellenmesi gerekmektedir. Buluşsal tabanlı tekniklerde ise çeşitli makine öğrenimi yöntemi ile metin, resim ve web sayfalarının URL'sinden elde edilen bilgiler toplanıp bir karar fonksiyonu oluşturulmaktadır. Bu tekniğin liste tabanlı tekniğe göre daha az hataya olanak tanıdığı dikkat çekmektedir. Makine tabanlı teknikte web sayfalarından çıkarılan özellikler üzerinde, Rastgele Orman (random forest-RF), Lojistik Regresyon (logistic regression-LR), Çok Katmanlı Algılayıcı (multilayer perceptron-MLP), Bayes Ağı (bayesian network-BN) ve Destek Vektör Makinesi (support vector machine-SVM) gibi makine öğrenme algoritmalarının uygulanmasına odaklanılır (Eroğlu, vd., 2019). Bunlara ek olarak devletler de siber suçlar ile mücadele etmek için hukuk sistemleri içinde düzenlemeler yapmaktadır. Ne yazık ki alınan hukuksal önlemler söz konusu suçların işlenmesini engelleyememekte hatta birçoğu uluslararası boyutta gerçekleşmektedir (Damar ve Gökşen, 2018).

Otlama saldırısı hangi türde, arkasında yatan amaç ya da teori ile açıklanmaya çalışılırsa çalışılsın müşteriler ve işletmeler açısından önemli kayıpların yaşanmasına neden olmaktadır. Oltalama saldırıları nedeniyle maddi ve manevi zarar uğrayan müşteriler işletmelere olan güvenini kaybetmektedir. Bu durum ise işletmeler için paha biçilemez bir sosyal maliyet anlamına gelmektedir (Yuan Sun, vd., 2016). Elbette ki işletmelerin bu durumun önüne geçmek için uygulayabileceği bazı stratejiler bulunmaktadır. Tehditleri profesyonellerce sunulan "antiphishing" uygulamaları ile sessizce ortadan kaldırmak, kullanıcıları tehditler hakkında uyarmak ve insanları kimlik avı tuzaklarına düşmemeleri için eğitmek önerilen stratejiler arasında ön plana çıkmaktadır (Kumaraguru, vd., 2007).

Turizm İşletmelerinde Bilgi Güvenliği ve Oltalama Saldırıları

Teknolojik gelişmeler ile devlet organları ve özel sektör tarafından üretilen devasa boyutlardaki bilgiye bilgi teknolojileri aracılığı ile kolaylıkla erişilebilmekte ve bilgi işlenip aktarılabilmektedir. Dolayısıyla bilgiyi üretmek kadar onu korumak da önem arz etmektedir. Bu bağlamda 1970'li yıllardan bu yana dünya genelinde bilgi güvenliği hakkında çalışmalar yürütülmektedir. Türkiye'de ise bilgi güvenliği ile ilgili çalışmalar Avrupa

Birliği Tam Üyelik Süreci kapsamında gelişme göstermeye başlamış ve konu kişisel veriyi koruma çerçevesinde gelişmiştir (Akan, 2019: 34-36). İlgili alan yazın incelendiğinde bilgi güvenliği ile ilgili çalışmaların bilişim, bankacılık, sağlık, eğitim, kamu yönetimi vb. alanlarda şekillendiği görülmektedir. Birçok disiplin tarafından değerlendirilen konuya; teknik, yönetim bilimi, yasalar ve politikalar, örgüt, kültür, bilinçlendirme, psikoloji ve davranış gibi birçok yaklaşım bulunmaktadır (Karimi, 2018: 10).

Bilgi güvenliği konusu web siteleri üzerinden ticaret yapan ve hatta web sitelerini bir dağıtım aracı olarak kullanan turizm endüstrisi özelinde de araştırılan bir konudur. Yapılan araştırmaların seyahat ve turizm işletmeciliği, seyahat acentacılığı, konaklama işletmeciliği ve havayolu işletmeciliği çerçevesinde şekillendiği dikkat çekmektedir. Söz konusu çalışmalarda, web sitesi ve bilgi güvenliği ilişkisi (Liao ve Shi, 2017), seyahat acentalarında uygulanan bilgi güvenliği yaklaşımları (Rasulovich, vd., 2019), seyahat işletmelerinde bilgi güvenliğinin boyutları (Yağcı, vd., 2020), konaklama işletmelerinde bilgi güvenliği açığı yaratan iç ve dış kaynaklı unsurlar ve yöneticilerin farkındalık düzeyleri (Okul vd., 2018), havacılık sektöründe siber güvenlik tehditleri ve personelin farkındalık düzeyi (Akan, 2019: 88-90), turizm endüstrisinde siber güvenlik açıkları (Shabani, 2016), havayolu ödeme sisteminde dolandırıcılık (Demir, 2021) ve kişisel bilgilerin korunması (Türeli, vd., 2015) konuları ele alınmaktadır.

Diğer yandan turizm endüstrisindeki e-ticaretin dünya çapında önemli bir hale gelmesi konunun web sitesine olan güven çerçevesinde incelenmesini de sağlamamıştır. Çalışmalarda e-ticaretin turistik satın almada birçok avantaj sağladığını, bununla birlikte müşterilerin kişisel bilgilerini paylaşma konusunda endişeleri olduğunu göstermektedir. E-ticaretin kişisel veriye erişim ve korunması konusunda belirsiz yaratması önemli bir sorun olarak görülmektedir. Bu doğrultuda güven e-ticarette önemli bir unsur olarak dikkat çekmektedir (Suh ve Han, 2003). Oltalama saldıranlarında da müşteriler web sitelerine güvenmeleri sonucunda tuzağa düşmektedir (John, vd., 2019). Orijinal web sitesinin birebir aynısı ve URL uzantısının çok yakın bir kopyası müşteriyi yanılmaktadır. Turizm işletmesine ait web sitelerinin logoları taklit edilerek müşterilerin güvenini kazanma noktasında ikna edici olunmaktadır (Nedelea ve Bălan, 2010).

Seyahat, konaklama ve ulaştırma gibi ana sektörler oltalama saldırıları için büyük bir potansiyel taşımasına rağmen, bu saldırıların profesyonel anlamda daha çok havacılık sektörü tarafından engellenmeye çalışıldığı dikkat çekmektedir. Uluslararası Hava Taşımacılığı Birliği (AITA), dolandırıcılığın tespiti, önlenmesi ve yeniden değerlendirilmesi için iş birliğini önemli bir stratejik hedef haline getirmiştir. Kanada, Seyahat Dolandırıcılığını Önleme Grubu, Europol, GAAD, Interpol, Visa Europe gibi kurumlar ile oltalama saldırılarına karşı uluslararası bir mücadele gerçekleşmektedir (Demir vd., 2021). Diğer yandan, siber dolandırıcıların önemli bir hedefi olan otel işletmesi işletmelerinin web sitelerine olan oltalama saldırıları ile ilgili mevcut durum ve alınan önlemler ile ilgili akademik çalışmaların yetersiz olduğu dikkat çekmektedir.

Yöntem

Bu araştırmanın ana amacı otel web sitelerinin kopyalanması ve gerçekmiş izlenimi verilerek turistlerin oltalama saldırılarına uğramaları durumunu derinlemesine araştırmaktır. Araştırmanın amacına uygun olarak "Otellerin web siteleri neden ve nasıl kopyalanarak turistler aldatılıp, dolandırılmaktadır?" araştırma sorusuna yanıt bulunmaya ve aşağıda ifade edilen alt sorular ile ana soru detaylı bir biçimde açıklanmaya çalışılmıştır

- Otel web sitelerine yönelik oltalama saldırılılarının altında yatan güvenlik açıkları nelerdir?
- Turistler sahte web sitelerine neden ve nasıl güvenmektedir?
- Dolandırıcılığa konu olan otel işletmeleri duruma nasıl yaklaşmaktadır?
- Dolandırılan turistlerin mağduriyetleri nasıl giderilmektedir?
- Oltalama saldırılarına karşı işletmelerin ve devletin aldığı önlemler nelerdir?

Araştırmanın ana amacı doğrultusunda, oltalama saldırıları hakkında bilgilere ulaşmak ve değerlendirmek amacı ile nitel araştırma yöntemlerinden örnek olay (vaka çalışması) deseninden yararlanılmıştır. Örnek olay bütünsel ve derinlemesine bir araştırma yapılmasını sağlayan etkili bir yöntem olarak değerlendirilmektedir (Foster, 2002). Gummesson (2017) tarafından da vurgulandığı üzere, örnek olay araştırmalarında birden fazla olgu ya da olay örnek olay olarak incelenebileceği gibi, vaka geçmişi özellikle ilgi çekici olduğu için tek bir vakayla da ilgili ifadelere ve sonuçlara ulaşılabilmektedir. Yin (2011) örnek olay araştırma deseninin keşfedici, betimleyici ya da açıklayıcı olabileceğine dikkat çekmiştir. Araştırma kapsamında tek ve keşfedici örnek olay yöntemi kullanılmaktadır. Veri toplama sürecinde tek bir olaydan yani "Türkiye'de yer alan otel işletmelerinde oltalama vakalarından" yararlanılmıştır. Bu araştırma ile otel web sitelerinin kopyalanması ve turistlerin oltalama saldırıları ile dolandırılması durumu incelenmektedir. Araştırmanın en önemli özgün değeri iki farklı disiplini bir araya getirerek turizm ve siber güvenlik alan yazınına yaşanmış örnekler, yazılı bilgiler, sosyal

medya paylaşımları, haber siteleri, kamu ve özel sitelerin konu hakkında yer verdikleri bilgiler derlenerek örnek olay oluşturulması ile alan yazınına yeni bilgiler kazandırılması hedeflemektedir.

Araştırma verisi Mayıs-Eylül 2021 tarihleri arasında facebook, instagram, linkedin, tripadvisor, twitter, şikayetvar.com gibi sosyal medya, çevrimiçi rezervasyon ve yorum platformlarından ve arama motorundan elde edilmiştir. Söz konusu platformlarda yer alan ve kullanıcılar tarafından anonimleştirilen yorum, tweet, blog yazısı, köşe yazısı gibi kaynaklar ve haber kaynakları toplanmıştır. Internet üzerinden yapılan araştırma ile 89 google sayfasına, 1 instagram profiline (dolandırılan tarafından açılmış), 15 linkedin post, 19 şikayetvar.com post, 1 adet tripadvisor mağdur post, 84 adet tweet, 3 gazete websitesi ve arşivi, 3 resmi kamu websiteleri ve arşiv bilgileri, 5 kitap bölümü, 5 blog sitesi/web sitesi, 3 konferans bildirisi ve 37 makale olmak üzere toplamda 265 adet dokumana ulaşılmıştır. Veri toplama aşamasında "turizmde oltalama, sahte otel işletmesi, sahte otel işletmesi rezervasyon, dolandırıcı otel işletmesi, siber dolandırıcı, phishing, çakma otel işletmesi sitesi, Bodrum'da sahte otel işletmesi, Antalya'da sahte otel işletmesi, Didim'de sahte otel işletmesi" anahtar kelimelerinden yararlanılmıştır.

Elde edilen veri seti doküman analizi tekniği ile incelenmiştir. Dokumanlar her ne kadar zengin veri setleri olarak kabul edilse de elde edilen dokümanlara tüm süreç boyunca eleştirel bir gözle bakılmıştır (Hodder, 2000). Bu nedenle analizin ilk aşamasında dokümanlar araştırma sorusunu kapsamında değerlendirilmiş ve ilgisiz metinler veri manipüle edilmeden veri setinden ayrılmıştır. Araştırma sorusu ile doğrudan ilgili olan dokümanlara, kategoriler ve temalar oluşturulmak üzere içerik analizi uygulanmıştır. İçerik analiz ile anlamlı veri birimlerinin saptanmasının ardından kodlama işlemine geçilmiştir. Veri kodlama işleminin ardından taslak temalar belirlenmiş ve taslak temalara göre kodlar yeniden düzenlenmiştir. Analiz süreci yazarlar tarafından ayrı ayrı yürütülmüş ve kodlama çalışmaları sırasında ortaya çıkan farklı görüş ve anlaşmazlıkları gidermek için çapraz doğrulamaya özen gösterilmiştir. Tüm analiz sürecinde tarafsız davranılmasına ve verinin manipüle edilmemesine özen gösterilmiştir (Creswell, 2007). Ayrıca araştırmanın güvenirliğini desteklemek için Creswell ve Miller (2000) tarafından önerilen uzman incelemesine gidilmiştir. Araştırma verisi ve oluşturulan kodlama cetveli farklı akademisyenler tarafından ve bağımsız olarak incelenmiştir. İnceleme sonucunda önerilen kodlar ve temalar doğrultusunda araştırma verisi ortak tekrar incelenmiş ve ortak görüş doğrultusunda son şeklini almıştır. Araştırma vurdumduymazlık, dijital okuryazarlık, farkındalık ve yasal düzenleme yetersizliği olmak üzere üç kategoriye ayrılmıştır. Keşfedici örnek olay ile elde edilen araştırma bulguları doğrultusunda, bu alanda araştırma yapılıp yapılamayacağı, yeni fikirler ve hipotezler geliştirme durumu ortaya konmaya çalışılmış ve araştırma sonucunda turizm alanında oltalama konusunda yapılabilecek araştırmalara öneriler geliştirilmiştir.

Örnek Olay: Otel İşletmeleri Web Siteleri Üzerinden Oltalama Saldırıları

İş hayatının zorlukları günden güne artmıştır. Bilgi ve teknoloji çağı insanların çok fonksiyonlu ve yetenekli çalışmalarını gerektirmektedir. İş hayatının büyük şehirlere taşındığı günümüzde, kalabalık, kirli hava, trafik, stres ve ekonomik geçim zorlukları insanları psikolojik olarak zorlamaktadır. Çalışan insanların hafta sonu iki gün ya da bir gün çalışmaması onlar için tatil anlamına gelmemektedir. Aslında, izin günleri tatil amaçlı bulunduğu yerden başka bir yere gitmesi için bir fırsattır fakat yoğun tempoda çalışılan hafta sonrasında izin günü sorumluluklara bağlı olarak yapılamayan işlerin yapılması anlamına da gelebilmektedir. Ücretli yıllık izinler ise dinlenme, uzaklaşma, keşfetme, ziyaret etme amaçlı uzun süreli tatillerin yapılabildiği zaman dilimleri olmaktadır. Çalışılan kurumun kurallarına göre işe yeni başlayanlar için yıllık izin 10 ila 20 gün arasında değişebilmektedir.

Ücretli yıllık izinler çalışma yılına göre hesaplanır ve 1-5 yıl arası çalışılmış ise 14 gün; 5-10 yıl ise 20 ve 10 yıldan fazla ise 26 iş günü ücretli izin kullanabilir. Bir kişinin bir yılda 96 hafta sonu günleri çıkarıldığında 14 günlük tatile gidebilmesi için 255 gün çalışması gereklidir. Ekonomik sıkıntılar ise ailelerin ve bireylerin her yıl tatile istedikleri sürede çıkmalarını engellemektedir. Hem maliyet hem de süre açısından bakıldığında, tatile gidecek kişinin tatil kararını alırken düşünmesi gereken çok fazla faktör olduğu açıktır (Akkuş, 2018).

Turistin tatil planları hayal aşaması ile tatil hakkında aldığı bilgiler doğrultusunda başlar. Tatil hakkında bilgi edinilmesi gereken iki önemli konu vardır. Bunlardan biri ulaşım, diğeri ise oteldir. Ulaşım konusunda gidilecek yerin mesafesine göre karar verilmesine rağmen, Türk turistlerin tercihleri bireysel olarak kendilerine ait araba ile seyahat etmek yönündedir (Kazım vd., 2021). Pandemi koşulları turistlerin toplu taşımacılıktan uzaklaşmalarına neden olmuştur. Bu nedenle turistin tatil planında en önemli yeri doğru, istediği gibi, ucuz otel işletmeleri bulmak yer almaktadır (Akkuş, 2018). Bireysel olarak ulaşımını sağlayacak olan turist, otel işletmesini de kendisi bulmak istemektedir (Kıycı vd., 2020; Sezgin ve Yurtlu, 2021). Sosyal medya ve diğer imkânlar ile verilen reklamlar bu aramada önemli rol oynamaktadır.

Turistin tatil hayalinin başlaması için bazı faktörlerin oluşması gerekmektedir. Bu faktörler arasında reklamlar, promosyonlar, eş ve dost tavsiyeleri, daha önce gitmiş ve deneyim yaşamış kişilerden alınan bilgiler, belgeseller, kitaplar ve oyunlar sıralanabilir (Emen, 2019). Bu süreçte tatile gitme isteğinin doğmasında en etkili olan kişiler çocuklar ve kadınlar olmaktadır (Aymankuy ve Ceylan, 2013). İlk bilgi alındıktan ve tatil isteği oluştuktan sonraki aşama ise otel işletmesi arama sürecidir. Birçok otelin web sitesi bulunmaktadır. Turistlerin isteklerine uygun otellerin web sitelerini tek tek aramaları, bulmaları ve incelemeleri zaman almaktadır (Demir vd., 2021). Türkiye genelinde yaz tatilini geçirmek için tercih edilen destinasyonlar güney kıyı destinasyonları olmaktadır. Son 10 yıldır artan talep göz önünde bulundurulduğunda, fiyatların iç turizm için sürekli artan ve maliyetli bir hal aldığı dikkat çekmektedir (Ongun vd., 2021). Son üç yıldır pandemi ile zamanını evde geçiren yerli turistler ucuz maliyetli ve beklentilerini karşılayabilecek otelleri bulma çabası içindedir (Demir vd., 2021).

Teknolojik gelişmeler otel işletmelerinin çok kişiye kısa süreler içinde daha fazla mesaj içeriğini ulaştırmalarını sağlamış (Işılar, 2021) ve üçüncü direkt satış kanalı oluşturmuştur. Otel işletmeleri ile turistlerin arasındaki mesafenin fazla olması ise hedef kitleye ulaşılması gerekliliğini doğurmuştur. Çok büyük bir rekabet içinde olan bu sektörde tatil planı yapan kişinin kararını ilk anlarda etkilemek en önemli eylem haline gelmiştir. Otel işletmeleri satışlarını aylar öncesinden yapmakta, satışı garantilemek için özel indirimler, promosyonlar ve ödeme kolaylıkları sunmakta ve müşterilerine ulaşma çabası içinde her tür yolu ve kanalı etkinleştirmektedir. Otel işletmeleri odalarını, seyahat acentası ve tur operatörü üzerinden komisyonla, otel işletmesinin kendi satış departmanından telefon görüşmeleriyle ve kapı müşterilerine resepsiyondan olmak üzere dört rezervasyon kanalı ile satmaktadır. Söz konusu satış kanallarından web sitesi ve çağrı merkezi, turistlerin oltalama dolandırıcılığı yaşayabileceği platformlara da zemin hazırlamaktadır. Oltalama web sitesinde başlayıp telefon kanalı ile sonuçlanabilmekte ya da tam tersi de olabilmektedir.

Otel işletmesi müşterisini etkilemek ve bu satış tekniklerini kullanmak için doğrudan etkileşime geçebileceği tek yer işletmenin web sitesi olmuştur (Acar, 2021). Otel işletmeleri ile seyahat acentalarının maddi ilişkisi oldukça karmaşıktır (Eğilmezgil vd., 2021). Turist tatil ücretini seyahat acentasına ödedikten sonra, otel işletmesinin bu ücreti alması farklı bir zaman dilimini, turistin konaklaması ise daha farklı bir zaman dilimini içermektedir. Bu durum, paranın değişim zamanını kullanan kişiyi, kazanç, kar ve zarar dengelerini değiştirmektedir. Bu nedenle otel işletmeleri seyahat acentası yerine doğrudan satış kanalları olan web sitesi, telefon ve sosyal medya kanalları üzerinden satış gerçekleştirmeyi tercih etmektedir (Görgülü ve Kosova, 2021).

Otel işletmeleri için telefon ile satışın gerçekleştirilmesi çok doğal ve standart bir iş süreci olarak bilinmektedir. İşletme normal telefon numarası üzerinden (genellikle bölge telefon kodu ile aranan) arama gerçekleştiren turiste satış ofis çalışanının vereceği bilgiler ışığında satış gerçekleşir. Satışın gerçeklemesinde kişinin ve beraberinde kalacak kişilerin bilgileri ve ücretin ödenme yönteminin verilmesi yeterlidir. Sanal post ile ödeme sistemi geliştirildikten sonra kredi kartı ile ödeme gerçekleştirilmesi oldukça kolaylaşmıştır (Pilatin ve Dilek, 2021). Sanal post ile ödemeler otel işletmesinin turist ile telefonda ya da web sitesi üzerinden satış görüşmesi sonunda hem rezervasyonu gerçekleştirmesine hem de satış ücretini alarak işlemin kapatılmasına kolaylık sağlamıştır. Bu durumda birçok turist altı ay öncesinden tatil ücretini ödemiş olmaktadır. Turist için tek yapması gereken hayalini kurduğu tatilin günü geldiğinde gitmek ve otel işletmesine rezervasyonu olduğunu söyleyerek odasının verilmesini beklemektir. Otel işletmelerinin telefon numaraları müşterilerinin ulaşabilmesi için ve direkt satış kanalı olduğundan web sitelerinde paylaşılmaktadır.

Telefon numaralarının yayınlandığı sitelerde, yerel bölge kodlu telefon numaraları direkt otel işletmesinde çalışan kişiler ile irtibat kurulmasını sağlarken, 0800 ya da 0850 ile başlayan numaralarda çağrı merkezi ile irtibat kurulur. Çağrı merkezleri çalışma sistemlerinde işletmeye ait bir çağrı merkezi olabilirken, birkaç otel işletmesi ya da tek bir işletme için hizmet veren bir çağrı merkezi de olabilir. Çağrı merkezleri telefon ile satışın en önemli ayaklarından biridir. Telefon ile bilgi verilir, iptal ya da değişiklik sorunları çözülür ve satış gerçekleştirilir. Çağrı merkezlerinin lokasyonları bilinmemektedir. Yapılan işlem sırası ile arayan müşteriye otel işletmesi hakkında ücret, imkânlar, oda türleri, restoran, etkinlik gibi bilgiler vermektir. Müşterinin istediği tarihlerdeki müsaitlik durumlarına bakılır. Bu noktada satışın gerçekleşmesi için "fiyatlar gelecek hafta değişebilir. "Bu otel işletmesi çok talep görüyor odalarımız hızla doluyor, yer bulamayabilirsiniz?" gibi ikna ifadeleri kullanılır. Müşteri bu durum karşısında ucuz bir otel işletmesi odası satın aldığını düşündüğünden, kredi kartı bilgilerini vererek işlemin tamamlanmasını ister. Çağrı merkezi çalışanı bilgileri teyit eder, ödeme gerçekleşir. Müşteriye otel işletmesinde rezervasyonu olduğunu ve ödeme bilgisinin yer aldığı belge e-posta yolu ile gönderilir. Bu işlemler otel işletmesinin kendi telefon numarası ile arandığında da aynen gerçekleşir.

Otel işletmesinin ikinci direkt satış yöntemi web siteleridir. Web sitelerinde iki tür satış gerçekleşebilir. İlk satış yönteminde turist tatil bilgi ve detaylarını soru cevap şeklinde yer alan bir form doldurarak yollar. Bu işletmenin web sitesine oda envanter sistemi ile bağlantılı olmadığı durumlarda gerçekleşir. Otel işletmesi satış çalışanı gelen bilgileri inceler ve e-posta ya da telefon ile yanıt verir. İşlem e-posta ya da telefon ile satışa dönüşür, müşteri kredi kartını verir ve ödeme işlemi tamamlanır. Müşteriye otel işletmesi tarafından rezervasyonun yapıldığı ve ödemenin alındığına dair belge eposta yolu ile iletilir. Bu süreç dolandırıcılık için imkanlar sunmaktadır. Müşteri arayan kişi otel rezervasyon memuru gibi davranarak, kişilerin kredi kart bilgilerini ele geçirmektedir.

İkinci rezervasyon şekli web sitesi üzerinden satışın tamamen otomatik, otel işletmesi envanter sistemine bağlanarak gerçekleştirilmesidir. Otel işletmesinin envanter üzerinden belirlenen tarih aralıklarında uygun olan odaların taraması ile başlamaktadır. Müşteri online rezervasyon sistemi üzerinden bilgilerini girerek oda ücret bilgilerine ulaşır. Rezervasyon işlemi gerçekleştikten sonra otel işletmesi otomatik sistemde oda ücretini kredi kartı ile tahsil etmekte, rezervasyon numarasını ekranda göstererek aynı bilgileri kişinin e-postasına da yollamaktadır. Bu sistemde rezervasyon ve satış tamamen kişilerden bağımsız olarak gerçekleşir. Otomatik sistemlere olan güvenin yüksek olmaması nedeniyle, müşteri teyit amaçlı otel işletmesi telefonunu arayarak işlemin gerçekleşip gerçekleşmediğini kontrol etmek isteyebilmektedir. Fakat alan adı ile yapılan dolandırıcılıklarda müşteri gerçek otelin web sitesinde bu işlemi gerçekleştirdiğini düşünmektedir.

Kısaca, müşteri üç farklı şekilde otel işletmeleri ile doğrudan rezervasyon ve satış işlemi gerçekleştirebilmektedir. Bu işlemlerin güvenilirliği tamamen müşterinin sorumluluğu altında gerçekleşmektedir. İlk iki işlem telefon görüşmesi ve form doldurma sonrası telefon görüşmesi yöntemlerinin canlı bir kişi ile gerçekleştirildiğinden, sistemin otomatik olarak gerçekleştirilmesinden daha fazla güvenilmektedir (Genç ve Erdoğan, 2013). Ancak, en fazla dolandırıcılığın gerçekleştiği yapı telefon ile gerçekleşmektedir. X ve Y kuşağı kişiler işlemlerini yaparken canlı olarak muhatap olacakları bir kişiyi tercih etmektedirler (Kuyucu, 2017; Kara, 2021). Üç farklı rezervasyon türü de dolandırıcılar için fırsatlar içermektedir.

Vurdum Duymazlık

Otel işletmelerinin çoğu sahte web sitesi dolandırıcılığının farkında olmasına rağmen durumu umursamamakta ve gerekli önlemleri almamaktadır. Bu nedenle, mağdur olan müşteriler dolandırıldıklarını ancak rezervasyonu iptal ettirmek istediğinde ya da otele giriş yaptıklarında fark etmektedir. Oltalamaya alet olan otel işletmesi ise yaşanan mağduriyet karşısında müşteriye çözüm üretmek yerine konuyu geçiştirmeye ve tüm sorumluluğu müşteriye yüklemeye çalışmaktadır. Çoğu zaman mağdurlar otel işletmesinde konu ile ilgili bir yetkili bile bulamamaktadır. Zaman zaman mağdurların otel işletmesi tarafından kaba davranışlara maruz kaldıkları da görülmektedir.

Otel işletmelerine yönelik oltalama saldırıları web sitelerinin kopyalanması ve e-posta yolu olmak üzere iki şekilde gerçekleşmektedir (Damar ve Gökşen, 2018). Otel işletmeleri pazarlama, yeni ürün duyurma, müşteri ilişkileri yönetimi sağlama, sadakat programları oluşturma ve diğer nedenler ile sıklıkla müşterilerine e-posta göndermektedir (Çalış vd., 2013; Yıldırım, 2016). Söz konusu e-postalar tamamen bilgi amaçlı gönderilirken, dolandırıcılar için kişilerin bilgilerini ve paralarını ele geçirmek amacına da hizmet etmektedir (Arslan, 2021). Ünlü marka otel işletmelerinin adları kullanılarak gerçekleştirilmiş e-posta oltalama saldırılarına iki örnek Loyaltylobby.com (2021) sitesinde yayınlanmaktadır. Dünya genelinde otel işletmesi sadakat programları içinde en ünlü ve aktif kullanımı olan Hilton Honors adı altında gerçekleştirilen Hilton sadakat programıdır (Akkuş ve Çakıcı, 2020). Bu örneklerde kişiye reddedilemeyecek puan ya da ücretsiz tatil teklif edilmektedir. Link ile gidilen web sitesi de sahte bir site olmakla birlikte otel işletmesinin bilgileri inanılamayacak şekilde bire bir aynıdır. Bu durum kişiyi kandırmak, yanıltmak ve aldatmak amacı ile yapılmaktadır. Bu cezbedici teklif karşılığında ise müşteriler bilgilerini linke tıklayarak gideceği web sitesi üzerinden kendi isteği ile vermiş olmaktadır.

İkinci ve en önemli oltalama şekli, otel işletmesi web sitesi alan (domain) adı üzerinde yapılan dolandırıcılıktır. Otel işletmesinin resmi olarak kullandığı alan adı üzerinde ufak değişiklikler ile yeni bir alan adı almak ve birebir web sitesini kopyalamak suretiyle oltalama gerçekleşmektedir (Haber7, 2020). Sahte otel alan adının Google arama motoruna ücretli reklam vererek görünürlüğü artırılmakta ve listelemede üst sıralamaya çıkması sağlanmaktadır. Bu ise, müşterinin arama yaptığı alan adına dikkat etmeden ilk çıkan sonucu tıklamasıyla, dolandırıcıların istediği siteye yönelmelerini sağlamaktadır. Ayrıca, web sitesinin alan adresine dikkat edilmediğinden, otel işletmesi ismi ve "Hızlı Rezervasyon için Arayın" ifadesinin kullanılması müşterileri tuzağa düşürmektedir. Web sitesine girildikten sonra ise müşteri birebir aynı web sitesiyle ama çok daha cazip

fiyatlar ile karşılaşmaktadır. Müşteriler sahte otelin cazip fiyatlarında ikna olarak rezervasyon yapmak istediğinde ise telefon numarası ile sahte çağrı merkezini aramaya yönlendirilmektedir. Dolandırıcılar tarafından rezervasyonun sorunsuz tamamlandığı imajı yaratılması için sahte onaylama e-postaları yollanmaktadır. Erken rezervasyonların sezondan en az altı ay önce gerçekleşmesi ve süreç içinde canlı bir kişi ile konuşulması gibi nedenlerle güven oluşturulmuş olmaktadır. Bu durumda müşteri otel işletmesinin kapısına gidinceye kadar durumdan haberdar olmayacaktır. Müşteri otele giriş yaptığında ise rezervasyonu olduğunu düşünen müşteri ile otel yönetimi karşı karşıya gelmektedir. Söz konusu durumda bazı oteller indirimli fiyat önererek bu durumu çözümlemeye çalışmakta, bazı oteller ise resmî web siteleri üzerinden oltalama sahtekârlığı ile ilgili bilgilendirmeler yapmaktadır. Örneğin, Adin Otel (2021) kendi web sitesi üzerinden resmî web sitesi adresini, telefon numaralarının ve oltalama ile ilgili durum hakkında bilgilendirme mesajı yayınlayarak müşterilerini uyarmıştır.

Web sitesi alan adı ile gerçekleştirilen dolandırıcılık süresi çok kısa olup, dolandırıcılar hemen hesapları kapatmaktadır. Bu ise haklarını mahkemelerde aramak isteyen müşterilerin muhatap bulamamalarına neden olmaktadır. Dolandırıcılar sezon başlamadan ve sezon başında yoğun bir şekilde ortaya çıkarken, dolandırıcılık eylemlerini gerçekleştirdikten hemen sonra alan adları ve web sitelerini iptal etmekte ve telefon numaralarını kapatmaktadır. 2021 yılında Webius tarafından yayınlanan sahte otel işletmesi listesinde bulunan otel işletmesi alan isimleri Almanya'da bulunan bir hosting firmasına aittir (Webius, 2021). Webius (2021) yer alan bilgilere göre tek bir firmanın 70'e yakın sahte otel işletmesi listesi bulundurmaktadır. Tablo 1'de bu sitelerden 10 adet sahte ve resmi otel alan adresleri örnek olarak verilmektedir. Sitelerin alan isimleri incelendiğinde tek bir harf değişikliği, küçük bir ekleme ya da yer değiştirme sureti ile aldatmacanın oluşturulduğu dikkat çekmektedir.

Tablo 1: Sahte web site ve resmî web site alan isimleri

SAHTE WEB SİTESİ	RESMİ WEB SİTESİ
lujobodrumresort.com	https://www.lujohotel.com/
miracleresortotel.com	https://www.miraclehotel.com/
maxroyals.com	https://www.maxxroyal.com/
maytermalsotel.com	https://maythermal.com/
adameveresort.com	https://www.adamevehotel.com/
dalyanresorts.com	https://www.dalyanresort.com/
royalasarlikbeachresort.com	https://www.royalasarlikbeach.com/
cangardenresorts.com	https://www.cangardenresort.com/
clubmarvyresorthotel.com	https://www.clubmarvy.com/
delphineresorts.com	https://www.delphinhotel.com/

Kaynak: Yazarlar tarafından Webius (2022) sahte otel işletmesi listesi ve otel işletmelerinin resmî web sitelerinden derlenmiştir.

Otel işletmelerinin web siteleri kopyalanmak ile kalmayıp dolandırıcı sitenin Google arama sonuçlarında ilk sıralarda çıkabilmesi için yüksek ücretler ödenerek reklamlar da verilmektedir. Turist çevresinden almış olduğu tavsiyeye göre otel ismi aratmakta ve genelde ilk çıkan sonucu açarak bilgileri incelemektedir. Karşılarına çıkan dolandırıcı siteler tasarım ve bilgi açısından gerçek web sitesinin birebir kopyası olduğundan şüphe uyandıracak bir durum da oluşmamaktadır. Hatta sayfalar açıldığında açılan pencereler ile yüksek indirimler sunulmakta ve böylece kişilerin ucuz tatil satın alma isteğine de cevap verilmiş olmaktadır. Müşterilerin yemek mollaları, akşam vakitleri gibi kısıtlı sürelerde rezervasyon yapma eğilimi ve fırsatı kaçırmama psikolojisi ile bilgilere çok dikkat etmeden ödeme gerçekleştirmesi otlama saldırılarının başarısını artırmaktadır.

Dijital Okuryazarlık

Oltalama saldırısına maruz kalan müşterilerin tuzağa düşmelerinde anlama, analiz etme ve bilgiyi bulma becerisinin yani dijital okuryazarlık düzeyinin yetersizliği önemli bir etki yaratmaktadır. Dijital okuryazarlık düzeyi yetersiz olan müşteri orijinal web sitesi ile sahte web sitesi arasındaki farkı ayırt edememekte, URL uzantısı, rezervasyon teyit formları, rezervasyon belgesi gibi özel araçların orijinalliğini sorgulayamamakta, e-posta adresleri ve URL isimlerinde yer alan yazım yanlışlarının farkına varamamaktadır. Dijital okuryazarlık düzeyi düşük müşteriler, kısa mesaj ya da e-posta gibi iletişim kanalları üzerinden sunulan tatil ve otel işletmesi

teklifleri içeriğinde yer alan tesis resimlerinin, kurumsal logo ve işaretlerin doğruluğunun sorgulanabileceği web sitelerini kullanma konusunda yeterli bilgiye sahip olmadığında geri dönüşü olmayan hatalar yapılmaktadır.

Söz konusu müşteriler, SMS, sosyal medya reklamı, internet sitesi ve e-posta içeriğinde resmi logoların bulunmasının söz konusu kanalların meşru olduğu anlamına gelmeyeceğini de bilmemektedir. E-ticaret faaliyetinde bulunan bir otel işletmesi ya da havayolu işletmesinin, bir seyahat acentasından daha ucuza bilet satma yetkisi olmadığına ilişkin bilgi eksikliği de oltalama saldırılarının gerçekleşmesinde etkili olmaktadır. Otel işletmesi isminin Google aranması sırasında sağ bölümde çıkan bilgiler ile sahte web sitesinde yer alan bilgilerin birbiri ile örtüşmeyeceği, sahte web sitelerinin ziyaretçileri bir iki sayfa ile karşılayacağı ve ilerleyen sayfalarda hata vereceği yönündeki bilgi eksiklikleri ise oltalama saldırılarının başarısını artırmaktadır. Yine bilinmeyen kaynaklardan gelen bağlantıların riskli olduğu, SMS, e-posta ya da sosyal medya mesajlarının özellikle çekiliş, hediye gibi vaatler içermesi durumunda dolandırıcılık riski taşıdığı göz ardı edilmektedir.

Web siteleri, logo, fotoğraf gibi bilgileri kopyalanarak dolandırıcılar tarafından kullanılan ve bu nedenle müşterilerin mağduriyetine ortak olan otel işletmeleri, söz konusu durumun farkına oldukça geç varmaktadır. Bu durumun en önemli nedeni ise gerek otel işletmesi yöneticileri gerek se iş görenlerin dijital okuryazarlık bilgisinin yeterli olmamasıdır. Google arama motoru üzerinden otel işletmesi isminin her gün aratılması gibi basit bir bilgi bile otel işletmesi adına açılmış sahte sitelerin farkına varılmasını sağlamaktadır. Oltalama saldırıların önlenmesi için tespit edilen izinsiz reklamları Google'a şikâyet etmek, otel işletmesi adına yasal olarak reklam yapan acentalara manuel olarak izin vermek, sahte web sitesinin kullandığı alan adlarını tespit ederek bildirmek ve tüm bunları tespit etmeye yarayan yazılımlar kullanmak gerekmektedir. Tüm işletme çalışanlarının dijital okuryazarlık eğitimi alması, otel işletmesi markası için profesyonel reklam çalışmalarının yapılması, dijital reklam dinamiklerinin iyi analiz edilmesi oltalama saldırılarının önlenmesinde kritik faktörler olarak anlaşılmaktadır.

Farkındalığın ve Yasal Düzenlemelerin Yeterli Olmaması

Otel işletmelerinden oltalama saldırıları müşterinin telefon ile aranarak tatil kazandığının söylenmesi; dolandırıcıların kendilerini otel işletmesi temsilcisi gibi tanıtıp müşteriyi kartından para çekildiğine ve paranın geri ödenebilmesi için telefonuna uygulama indirmesi gerektiğine ikna edilmesi ve sahte bir alan adı ile müşteriyi yanıltması şeklinde gerçekleşmektedir. Oltalama vakaları daha çok Antalya, Muğla, Didim, Bodrum, İzmir gibi popüler destinasyonlarda yer alan tanınmış otel isimleri kullanılarak gerçekleştirilmektedir. Oltalama saldırıları için çok sayıda paravan şirket kurulmaktadır. Özellikle yurt dışındaki sunuculardan yayın yaparak bu eylemler gerçekleştirilmektedir. Aynı isimde çok sayıda alan adı kullanılmaktadır. Sahte siteleri sosyal medya reklamları ve arama motorlarından duyurmak için çalıntı kredi kartları ile yüksek bütçeli çalışmalar yapmaktadırlar. Ödeme sırasında mail order, sanal pos gibi uygulamalar ile kredi kartı bilgilerini kopyalanmakta, ödeme sonrasında ise otel işletmesinin logosunun bulunduğu rezervasyon teyit formu gönderilmektedir. Dolandırıcılar, oltalama saldırıları konusunda son derece bilgili ve deneyimli uzman kişilerdir.

Oltalama saldırılarında kişilerin ucuza tatil yapma isteği ve telefon ile iletişim kuran kişilerin ikna edici tavırları sayesinde başarılı olunmaktadır. Gerçek bir otel işletmesi ya da seyahat acentası rezervasyon için kişiyi telefon aramasına yönlendirmeye çalışmamaktadır. Aksine telefon ile rezervasyon için ısrar edilmesi oltalama saldırısı olduğuna dair güçlü bir fikir vermesi gerekmektedir. Yine kısa mesaj ya da e-posta gibi iletişim kanalları üzerinden sunulan gerçek olamayacak kadar ucuz teklifler, sunulan teklifin geçerli olması için ödemenin peşin ve hemen yapılmasının istenmesi, online ödeme sırasında 3D ödeme yönteminin kullanılmaması, havale/eft ödemelerinde şirket hesabı yerine kişi hesaplarına ödeme yapılması müşterinin dolandırıldığını gösteren önemli bilgilerdir. Söz konusu unsurların bir araya gelmesi ve müşteri tarafından rezervasyon sonrasında hazırlanan mesafeli satış sözleşmesinde yer alan adres, unvan ve iletişim bilgilerinin ilgili web sitesi ile teyit edilmemesi oltalama saldırılarının başarısını artıran, müşteri farkındalığının düşük olması ile ilgili diğer etkenlerdir.

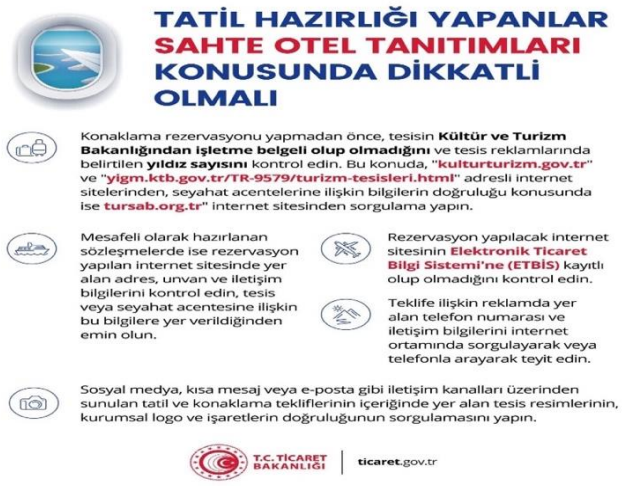
Müşteriler oltalama saldırıları sonucu mağdur olmaları nedeniyle karakol ve savcılık aracılığıyla suç duyurusunda bulunmakta, müşteri hakem heyetine mağduriyete konu olan otel işletmesini şikâyet etmekte ve avukat aracılığıyla Google'a başvurup sahte sitenin ilk sıralarda çıkmasını engellemeye çalışma gibi girişimlerde bulunmaktadır. Yine oltalama saldırısının diğer mağdur tarafı olan otel işletmeleri de gerçekleşen olaylar hakkında suç duyurusunda bulunarak hukuki süreci başlatmakta, Google'a sahte web sitesinin faaliyetlerinin durdurulması ile ilgili başvuru yapmakta ve resmî web sitelerinde müşteriyi sahte web sitesi konusunda uyarmaktadır. Gerek müşteri gerekse otel işletmeleri tarafından gerçekleştirilen girişimler, ilgili

suçun devlet tarafından meşrulaştırılmasını sağlamaktadır. Tarafların yasal süreci başlatması ile meşruluk kazanan oltalama saldırıları karşısında ilgili devlet kurumları yasal düzenlemeler gerçekleştirmektedir.

Yasal düzenlemeler ve oltalama saldırılarına karşı alınan önlemler yeterli gelmemekte, her yıl yüzlerce mağdur oluşmaktadır. Bir dolandırıcılık suçu olan oltalama saldırısı Türk Ceza Kanunun 157. ve 158. Maddelerinde düzenlenmiştir (EGM, 2021). Konu ile ilgili diğer bir devlet organı olan Ticaret Bakanlığı konuyu Müşteri Hakem Heyetleri Bilirkişilik Yönetmeliği kapsamında ele almaktadır (T.C. Resmî Gazete, 2020). Müşterilerin mağdur olmaması için Elektronik Ticaret Bilgi Sistemi (ETBİS) geliştiren Ticaret Bakanlığı, internet üzerinden ticaret yapan işletmelerin sorgulanmasına olanak tanımaktadır (E-Ticaret, 2021).

Konu ile ilişkili diğer bir devlet organı olan Kültür ve Turizm Bakanlığı müşterilerin dolandırılmamaları için ilgili otel işletmesini teyit edebilecekleri resmi internet sitesi üzerinden bir sistem oluşturmuştur (YİGM, 2021). Türkiye Seyahat Acentaları Birliği web sayfasından da otel işletmesi teklifi sunan acentanın gerçekliği kontrol edilebilmektedir (TURSAB, 2021). Ticaret Bakanlığı müşterinin tatil ürününü aldıktan sonra tesis ile ilgili bilgiyi "www.kulturturizm.gov.tr" ve "https://yigm.ktb.gov.tr/TR-9579/turizm-tesisleri.html" adresli internet sitelerinden, seyahat acenta bilgilerini ise "www.tursab.org.tr" internet sitesinden kontrol edilmesini önermektedir (TURSAB, 2021; E-Ticaret, 2021; YİGM, 2021). Ticaret Bakanlığı ayrıca twitter hesabı üzerinden de uyarılar yapmaktadır. Ticaret Bakanlığı müşterileri uyarmak için çeşitli sosyal medya kanallarından farkındalık ve uyarı afişleri yayınlamıştır. Şekil 1'de örnek afiş yer almaktadır.

Şekil 1: T.C. Ticaret Bakanlığı Kamu Bilgilendirme Duyurusu



Kaynak: T.C. Ticaret Bakanlığı (2021) Ticaret Bakanlığı Resmi Twitter Hesabı (https://twitter.com/ticaret/status/1406641048177233923?lang=en)

Sahte otel işletmesi siteleri ile yapılan sahtekarlığın ve aldatmanın ortaya çıkmasında en önemli görev mağdura düşmektedir. Yaşanan durumu yetkili mercilere şikâyet ederek, durumdan haberdar etmesi gerekmektedir. 2021 yılında, Turizmgüncel.com tarafından yayınlanan habere göre Aydın Didim ilçesinde lüks otel işletmelerinin kopya siteleri üzerinden gerçekleştirilen sahtekârlığın yaklaşık 300.000 TL olduğu tahmin edilmektedir (Turizmgüncel.com, 2021). Söz konusu olay mağdur olan tatilcilerin suç duyurusu ile ortaya çıkartılmıştır. Bir otel sitesi ve 30 ailenin karışması ile gerçekleşen olayın mağdurların otel işletmesine giriş yapmak istediklerinde ortaya çıktığı anlaşılmıştır. Sahte otel web siteleri örnek olayı oltalama eylemlerinin ne kadar önemli ve iyi yönetilmediği takdirde müşterileri maddi ve manevi zarara uğratacağını ortaya koymaktadır.

Tartışma ve Sonuç

Dolandırıcılık, internet kullanan her bireyin karşılaşma olasılığı olan en yaygın suçlardan birisidir. Bu araştırma ile otel web sitelerinin ve bilgilerinin kopyalanması ile turistlerin dolandırılması durumu incelenerek otel işletmelerine yönelik oltalama saldırılarının nedenleri ve alınacak önlemler ortaya konmaya çalışılmıştır. Araştırma kapsamında gerçekleştirilen örnek olay çalışması göstermektedir ki, konaklama sektöründe gerçekleşen dolandırıcılık vakaları da yaygınlaşmaya başlamıştır. Günümüz e-ticaret koşulları gereği internet ortamından uzak durmak olanaksızdır. Dolayısıyla internet ortamında gerçekleşen dolandırıcılık faaliyetleri hakkında bilgi sahibi olmak ve satın alma davranışını bilinçli bir biçimde gerçekleştirmek önem arz etmektedir.

Araştırma bulguları doğrultusunda müşterilerin farkındalık düzeyi, müşteri ev otel işletmesi yöneticilerinin dijital okuryazarlık seviyesi, işletmelerin olayı ciddiye alma düzeyi, dijital pazarlama konusundaki profesyonelliği, yasa ve yönetmeliklerin yeterlilik düzeyi gibi önemli konuların, otel işletmelerine yönelik oltalama saldırılarının başarısında kritik olduğu saptanmıştır. Dolandırıcılık konusunda sahip olduğu bilgi ve yetenekle oldukça profesyonel olan dolandırıcılar tarafından gerçekleşen oltalama saldırılarının önlenmesinde söz konusu unsurların iyi anlaşılması oldukça önemlidir. Çünkü turistik ürün yapısı gereği önceden deneyimlenememekte ve müşteri dolandırıldığını ancak otel işletmesine ulaştığında fark edebilmektedir. Aylar öncesinde ücretini ödediği ve büyük hevesler ile başladığı tatili, hayal kırıklığı ve mutsuzluk ile sonuçlanmaktadır. Dolandırıcılar, turistleri strese sokmakta ve otel işletmesi ile destinasyonun imajına uzun vadeli itibar zararı vermektedir. Dolandırıcılığı yapanlar için bunların hiçbir önemi olmamakla birlikte destinasyona ve turizm geneline verilen zarar oldukça büyüktür.

Dolandırıcılar kandırarak, aldatarak, doğru bilgilerin arasına yalan saklayarak turistin parasını almayı amaçlamaktadır. Bu amaç sadece turistlere zarar vermekle kalmaz aynı zamanda toplum genelinde güvensizlik oluşmasına neden olur. Fakat dolandırıcıların bu sonucu kesinlikle umursamadığı da ortadadır. Hâlbuki yerli ya da yabancı turistin bölgeye olan katma değeri sayesinde büyük bir ekonomi döngüsü yaşanmaktadır. Bir e-posta, sosyal medya reklamı ya da SMS üzerinden gönderilen cazip tatil teklifleri ile başlayan oltalama saldırıları birçok kişi ve kurumun mağduriyeti ile sonuçlanan küresel bir sorun haline gelmiştir. Bilgi ve iletişim teknolojileri müşterilere bilgiye kolay ve hızlı erişme olanağı sunarken, kötü niyetli girişimlere de zemin hazırlamıştır.

Bu araştırma kapsamında gerçekleştirilen örnek olay analizi sonucunda oltalama saldırılarının başarılı olmasının arkasında birçok neden olduğu anlaşılmıştır. Turistin zamanı ve harcanabilir geliri kısıtlıdır ve bu nedenle yoğun ve stresli günlük uğraşlardan uzaklaşacağı tatili ucuza mal etme psikolojisi ile hareket etmektedir. Bilgi arama ve seçenekleri değerlendirme aşamasında acele etmekte fırsatı kaçırmamak için ava giderken avlanmaktadır. Turistik ürün önceden deneyimlenmeye uygun bir ürün değildir. Bu nedenle müşteri satın aldığı tatilin gerçekte var olmadığını ancak tatile çıktığında fark edebilmektedir. Oltalama saldırıları hakkında yeterli bilgiye sahip olmayan müşteri kendini koruyamamaktadır. Teknoloji otel işletmelerine ücretin hemen tahsil edildiği doğrudan satış kanallarını kullanma olanağı sunarken, bu kanallar dolandırıcıların oltalama saldırıları için mükemmel alanlar haline gelmektedir. Otel işletmeleri ise oltalama saldırılarını ya ciddiye almamaktadır ya da konu hakkında yeterli bilgiye sahip değildir. Teknik bilgiye sahip profesyonel kişilerden oluşan dolandırıcılar, insan psikolojisini yönetme konusunda da yeteneklidir. Ayrıca, siber suçlar ile ilgili yasa, yönetmelik ve kanunların yeterli olmaması da oltalama saldırılarını teşvik etmektedir. Oltalama saldırılarına maruz kalan turist ve otel işletmelerinin ise yasal hakları konusunda yeterli bilgiye sahip olmaması oltalama saldırılarının artmasında kilit faktörlerden biri olarak dikkat çekmektedir. Oltalama saldırılarının psikolojik ve teknolojik altyapı kullanılarak gerçekleşmesi, her olayın farklı bir biçimde gerçekleşmesine ve sonuçlanmasına neden olmaktadır.

Oltalama saldırılarının başarılı olma nedenleri ve engellenmesi yönünde yapılacak olan çalışmalar müşteri, otel işletmeleri ve devlet olmak üzere üç paydaşa odaklanmalıdır. Akademik ve bilimsel araştırma yapan araştırmacılar tarafından tümdengelim ve tümevarım akıl yürütme yöntemleri kullanılarak oltalama konusunda detaylı araştırma sonuçları elde edilmelidir. İlerde yapılacak araştırmalarda oltalama saldırılarının başarısı ve turistlerin dijital okuryazarlık bilgisi; turistik tüketim davranışına etki eden psikolojik faktörler ve oltalama saldırıları; oltalama saldırıları ve otel işletmelerinin oltalama saldırıları konusunda sahip olduğu bilgi ve konuyu ciddiye alama düzeyleri ve yasal düzenlemelerin caydırıcılığı ile oltalama saldırılarının başarısı konuları incelemelidir. Bu konularda yapılacak araştırma sonuçları ile oltalama saldırıları hakkında daha fazla bilgi sahibi olunarak, farkındalığın artırılması sağlanabilir.

Bilimsel araştırmalar oltalama saldırılarının önüne geçebilmek için ihtiyaç olan bilgilerin tespitinde önemli rol oynarken; devlet tarafından müşteri bilincinin artırılması ve farkındalık için çalışmaların yürütülmesi gerekmektedir. Oltalama saldırılarının önlenmesinde müşteri ve otel işletmeleri kadar devlet organlarının da yükümlüğü bulunmaktadır. Mevcut yasa, yönetmelik ve uygulamalar özellikle uluslararası ticarette siber suçları önlemede yetersiz kalmaktadır. Yurtdışı menşeili bir oltalama saldırısını mevcut düzen ile önlemek oldukça zordur. Oltalama saldırıları her yıl giderek artmakta ve birçok kurumu zor durumda bırakmaktadır. Gerek turistlere gerekse otel işletmelerine maddi ve manevi zararlar vermekte, ülke imajını olumsuz yönde etkilemektedir.

Araştırma bulguları ve sonuçları çerçevesinde, oltalama saldırılarının önlenmesinde alınabilecek bazı çözüm önerileri belirlenmiştir. Birinci çözüm önerisi; müşteri herhangi bir otel rezervasyonu yapılmadan tesisin

Kültür ve Turizm Bakanlığı onaylı işletme belgesini kontrol etmelisidir (YİGM, 2021). İkincisi, Kültür ve Turizm Bakanlığı, Ticaret Bakanlığı ve E-Devlet iş birliği içinde otel işletmesi web sitesi doğrulama sistemi geliştirilmesi kısa vadede gerçekleşebilecek bir çözüm olabilir. Bu sistem ile kişi rezervasyon yapmadan önce doğrulamayı e-devlet üzerinden yaparak daha güvenilir ve emin bir rezervasyon gerçekleştirebilir. Üçüncüsü, otel web sitelerine otomatik kimlik doğrulama sisteminin entegre edilmesi olabilir. Bu sayede e-devlet onayına otomatik yönlendirilen web sitesi ile hızlı rezervasyon yapmak isteyen müşteri zaman kaybetmeden işlemi gerçekleştirebilir. Bu noktada, web sitesi güvenliği için devlet-sektör iş birliğine ihtiyaç duyulduğu anlaşılmaktadır. Teknik çözüm önerilerinin yanında müşterilerin dolandırıcılık konularında farkındalıklarını artırıcı eğitimlere ayrıca önem verilmelidir.

Müşteri için geliştirilecek oltalama dolandırıcılığı önleme ve farkındalık artırma seminerleri ve eğitimleri geliştirilmelidir. Turizm Bakanlığı, Ticaret Bakanlığı, Millî Eğitim Bakanlığı, Üniversiteler ve Sektör temsilcileri ile müşteri bilincinin artırılması ve önemlerin alınması konusunda ortak eğitim seferberliği başlatılmalıdır. Bu eğitim sürecinde müşteriye SMS, sosyal medya reklamı, internet sitesi ve e-postanın resmi logo içermesinin yeterli olmadığı, mesafeli olarak hazırlanan sözleşmelerde rezervasyon yapılan internet sitesinde yer alan adres, unvan ve iletişim bilgilerinin ve otel işletmesinin Elektronik Ticaret Bilgi Sistemi'ne (ETBİS) kayıtlı olup olmadığının kontrol edilmesinin önemi anlatılmalıdır. Yine, sosyal medya ya da e-posta benzeri mecralardan ulaşan otel tekliflerinin tehlikeli olabileceğine, rezervasyon işlemlerinin seyahat acentaları ya da resmi internet sitesi üzerinden gerçekleştirilmesinin önemine dikkat çekilmeli, müşteriler özellikle ucuz tatil ve otel tekliflerine karşı uyarılmalıdır. Bir otel ya da hava yolu işletmesinin, seyahat acentasından daha ucuza bilet satma yetkisinin olmadığı, yazım hataları içeren e-posta adresleri ve alan adlarının büyük olasılıkla sahte olacağı, web sitesi navigasyonu, rezervasyon sırasında web sitesinin telefon ile rezervasyona yönlendirmesi, mobil cihazlarda kimlik avı dolandırıcılığı ve kötü amaçlı yazılımlara karşı güvenlik uygulamaları, ödeme talimatları, peşin ödeme, toplu ödeme, şahıs hesabına ödeme yapılması, online ödemelerde sanal kart ya da 3D şifre kullanılması gibi daha teknik konularda da kapsamlı eğitimler tasarlanmalıdır. Oltalama saldırılarının azaltılmasında müşterinin bilinçli olması oldukça önemlidir.

Diğer yandan, müşteriye karşı olan sorumlulukları nedeniyle, otel işletmelerine de çok büyük bir sorumluluk düşmektedir. Oltalama saldırılarını engellemek için yapılacak adımların oltalama saldırısı gerçekleşmeden atılması önem arz etmektedir. Otel işletmesi oltalama saldırısını önlemek için Google marka başvurusunda bulunmalıdır. Başvurunun ardından tespit edilen sahte reklamlar Google şikâyet edilmelidir. Bu noktada sahte reklamları tespit eden yazılımlardan faydalanılmalıdır. Otel işletmesi adına reklam yapacak seyahat acentalarına manuel olarak izin verilmelidir. Farkına varılan durumlarda konu ivedilikle savcılığa bildirilmelidir. Bilgi Teknolojileri ve İletişim Kurumu aracılığıyla sahte sitelerin kapatılması sağlanmalıdır. Sahte web sitesine alan ismi veren hosting firmasına durum bildirilmelidir. Resmî web sitesi ve sosyal medya hesapları üzerinden basın bülteni yayınlanarak müşteriler uyarılmalıdır. Otel işletmesi çalışanlarına dijital okuryazarlık eğitimi verilmeli ve dijital pazarlama konusunda uzmanlaşılmalıdır. Oltalama saldırısına maruz kalmış müşterinin sorunu ciddiye alınmalı, kaba ve umursamaz davranışlardan kaçınılmalıdır. Otel işletmeleri teknoloji ile yeni ve mevcut müşterilerine ulaşabilmektedir. Fakat teknolojinin bilinçli kullanılması adına, teknolojik altyapıyı kuracak, yönetecek ve devam ettirecek bir birim de olmalıdır. Her işletmenin bu birimi oluşturma olanağı olmadığı dikkate alındığında, bu konularda uzmanlaşmış özel işletmelerden yardım alınması söz konusu olabilir. İşletmenin önemli işlevlerini yürüten departmanlar gibi teknoloji departmanlarının kurulması ise ideal olan çözümdür. Bu departmanlar işletmenin dijital dünyada varlığını koruyacak, yönetecek ve sürdürecek yapıyı sağlayacaklardır. Teknoloji geliştikçe ve yeni teknolojiyi kullanarak büyüyen kuşaklar yetişkin olduğunda oltalama gibi dolandırıcılıkları azaltmakta otel işletmelerinin, devletin ve eğitim kurumlarının aktif görev almaları gerekeceği göz ardı edilmemelidir.

Bu araştırma göstermektedir ki, otel işletmeciliği alanında oltalama saldırıları son zamanlarda yaygınlaşarak sayısız mağdur yaratmıştır. Bu durumun önlenmesi mümkün olmakla birlikte devlet, işletme ve müşteri üçgeninde ciddi önlemler alınması gerekmektedir. Tarafların birlikte hareket etmesi durumunda oltalama saldırılarına teşebbüs dahi edilemeyeceği ortadadır. Özellikle internet kullanım yaşının giderek küçüldüğü, çocukluk yaşlarına kadar indiği göz önüne alındığında, farkındalık oluşturacak eğitimlerine küçük yaşlarda başlaması faydalı olacaktır. Bu araştırmada siber güvenlik konularından sadece oltalama saldırıları ele alınarak otel web sitelerinin kopyalanması örnek olay çalışması kapsamında incelenmiştir. Fakat konu oldukça geniş kapsamlı olup, siber güvenlik konusunun bir bütün olarak ele alınmasının faydalı olacağı düşünülmektedir.

Kaynakça

Aboobucker, I., and Bao, Y. (2018). What Obstruct Customer Acceptance of Internet Banking? Security and Privacy, Risk, Trust and Website Usability and the Role of Moderators. *The Journal of High Technology Management Research*, *29*(1), 109-123.

Abraham, S. and Chengalur-Smith, I (2010). An Overview of Social Engineering Malware: Trends, Tactics, and Implications, *Technology in Society*, 32(3). 183-196

Acar, Y. (2021). Ülke turizmlerinin tanıtılması kapsamında kurumsal web sitede sunulan içeriklerin incelenmesi: Türkiye Turizm Tanıtım ve Geliştirme Ajansı (TGA) Örneği. *Erciyes Akademi*, *35*(2), 394-406.

Adin Otel (2021). *Adin otel işletmesi Resmi İnternet Sitesi*. https://www.adinhotel işletmesi.com/index.php?utm_source=google&utm_medium=cpc&utm_campaign=turkiye-branding&keyword=adinbeach&creative=558290464957&gclid=CjwKCAiAx8KQBhAGEiwAD3EiP62-WvGRh4K_n3zXEIgL5KsqjSIYHvjcvilFYcg1z0zMX0UMNh7qChoCDxIQAvD_BwE Erişim Tarihi: 10.02.2022.

Akan, F. Y. (2019). *Havacılık Sektöründe Bilgi Teknolojileri Uygulamaları ve Bilgi Güvenliği.* Yanımlanmamış Yüksek Lisans Tezi. İstanbul Bilgi Üniversitesi, İstanbul.

Akkuş, İ. ve Çakıcı, C. (2020). Turizm İşletmelerinde Sadakat Programları. *Avrasya Turizm Araştırmaları Dergisi*, *1*(1), 42-52.

Aldrich, R. (2013). Neuroscience, Education and the Evolution of the Human Brain. *HistoryoOf Education.* 42(3), 396-410.

Arslan, Y. (2021). Oltalama Saldırıları Farkındalık Tatbikatı Örneği. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 9(3), 348-358.

Ashton, C. F. (2020). The Fillip of the World Wide Web: Rewriting and Expanding History. *Collegian*, 27(6), 595-599.

APWG (2021). Phishing Activity Trends Report. https://apwg.org/trendsreports/ Erişim Tarihi: 10.02.2022.

Aymankuy, Y., ve Ceylan, U. (2013). Ailelerin Turistik Ürün Satın Alma Karar Sürecinde Çocukların Rolü (Yerli Turistler Üzerinde Bir Araştırma). *Elektronik Sosyal Bilimler Dergisi*, *12*(45), 105-122.

Baig, M. S., Ahmed, F., and Memon, A. M. (2021). Spear-Phishing campaigns: Link Vulnerability leads to phishing attacks, Spear-Phishing electronic/UAV communication-scam targeted. *4th International Conference on Computing & Information Sciences (ICCIS) IEEE*, Karachi, 29-30 Kasım 2021.

Bax, S., McGill, T., and Hobbs, V. (2021). Maladaptive Behaviour in Response to Email Phishing Threats: The Roles of Rewards and Response Costs. *Computers & Security*, 106 (102278), 1-15.

Brügger, N. (2009). Website History and the Website as an Object of Study. *New Media & Society*, *11*(1-2), 115-132.

Bozkır, A.S. and Aydos, M. (2019). Local Image Descriptor Based Phishing Web Page Recognition as an Open-Set Problem. *European Journal of Science and Technology*, Special Issue, 444-451.

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

Civelek, M. (2016). Korku Çekiciliğinin Tatil Pazarlamasında Kullanılmasına Yönelik Göstergebilimsel Analiz: Cinnetten Bir Köşe Örneği. *Ankara Hacı Bayram Veli Üniversitesi Turizm Fakültesi Dergisi*, *24*(1), 116-141.

Creswell, J. W. (2007). *Qualitative Inquiry and Research Design*. Thousand Oaks, Sage.

Creswell, J. W. ve Miller, D. L. (2000). Determining Validity in Qualitative Inquiry. *Theory into Practice*, 39(3), 124-130.

Çalış, K., Gazdağı, O. ve Yıldız, O. (2013). Reklam İçerikli Epostaların Metin Madenciliği Yöntemleri ile Otomatik Tespiti. *Bilişim Teknolojileri Dergisi*, *6*(1), 1-7.

Daengsi, T., Pornpongtechavanich, P., and Wuttidittachotti, P. (2021). Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. *Education and Information Technologies, 6*, 1-24.

Damar, M. ve Gökşen, Y. (2018). Akademik Yaşantıda Sanal Tehditler ve Vakalar Üzerine Bir Analiz. *Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 10(24), 330-350.

Demir, M., Demir, Ş. Ş., Ergen, F. D. E., ve Dalgıç, A. (2021). Covid-19 Sürecinde Müşterilerin Otel İşletmesi Seçimini Etkileyen Faktörler. *International Journal of Social Sciences and Education Research, 7*(1), 82-94.

Demir, Z. (2021). Havayolu Sektöründe Ödeme Sistemleri Yoluyla Yapılan Dolandırıcılık İşlemlerinin Sektöre Olan Etkisinin Değerlendirilmesi, Denetlenmesi ve Önlenmesine Yönelik Öneriler. *Marmara Üniversitesi Öneri Dergisi*, 16(55), 185-220.

EGM. (2021). Dolandırıcılık. https://www.egm.gov.tr/dolandiricilik. Erişim Tarihi: 18.2.2022.

Eğilmezgil, S. G., Yıldırım, H. M., Lütfi, A. ve Türkmen, S. (2021). Otel İşletmeleri Yöneticilerinin Bakış Açısından Dağıtım Kanallarında Yaşanan Çatışmalar: Antalya Bölgesi Örneği. *Ankara Hacı Bayram Veli Üniversitesi Turizm Fakültesi Dergisi*, 24(1), 1-19.

Emen, M. (2019). Turizm Pazarlaması ve Yabancı Turistlerin Seyahatlerini Etkileyen Etmenler: İstanbul Örneği. *Uluslararası Global Turizm Araştırmaları Dergisi*, 3(2), 66-82.

Eroğlu, E., Bozkır, A. S. and Aydos, M. (2019). Brand Recognition of Phishing Web Pages Via Global Image Descriptors. *European Journal of Science and Technology*, Special Issue, 436-443.

E-Ticaret. (2021). Kayıtlı Site Sorgula. https://www.eticaret.gov.tr/sirketsorgula. Erişim Tarihi: 18.2.2022

Foster, P. N. (2002). Using Case-Study Analysis in Technology Education Research. *Journal of Career and Technical Education*, 19(1), 32-46.

Fowdur, T. P. and Abdool Khader, R. (2018). An Anti-Web Phishing Application for Analyzing the Security of Websites. *Balkan Journal of Electrical & Computer Engineering*, 6(3), 146-152.

Ghafir, I. and Prenosil, V. (2016). Proposed Approach for Targeted Attacks Detection. *Advanced Computer and Communication Engineering Technology Proceedings*, 362, 73-80.

Genç, E. ve Erdoğan, E. (2013). Otel işletmesi İşletmelerinde İlişkisel Pazarlama Uygulamaları: Zonguldak, Karabük ve Bartın İllerinde Bir Araştırma. *Afyon Kocatepe Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 15(2), 195-216.

Grilli, M. D., McVeigh, K. S., Hakim, Z. M., Wank, A. A., Getz, S. J., Levin, B. E. and Wilson, R. C. (2021). Is this Phishing? Older Age is Associated With Greater Difficulty Discriminating between Safe and Malicious Emails. *The Journals of Gerontology:* Series B, 76(9), 1711-1715.

Grobler, T. and Louwrens, B. (2007). Digital Forensic Readiness as A Component Of Information Security Best Practice. *IFIP International Federation for Information Processing*, 232(9), 13-24.

Görgülü, V. ve Kosova, M. (2021). Elektronik Ağızdan Ağıza İletişim (Ewom), Web Sitesi İtibari ve Güvenilirliğinin, Otel işletmesi Rezervasyon Sitelerinden Rezervasyon Yapma Niyeti Üzerindeki Etkisinin İncelenmesi. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 23(3), 1071-1097.

Gummesson, E. (2017). *Case theory in business and management: Reinventing case study research*. Sage.

Haag, S., Siponen, M., and Liu, F. (2021). Protection Motivation Theory in Information Systems Security Research: A Review of the Past and a Road Map for the Future. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, 52(2), 25-67.

Haber7 (2020). Dolandiriciliga-Dikkat-Sahte-Tatil-Siteleri-Kredi-Kartlarini-Bosaltiyor. https://www.haber7.com/seyahat/haber/2970535-dolandiriciliga-dikkat-sahte-tatil-siteleri-kredi-kartlarini-bosaltiyor. Erişim Tarihi: 10.2 .2022.

Hodder, I. (2000). The Interpretation of Documents and Material Culture. *Handbook of Qualitative Research*, (Ed: N. K. Denzin and Y. S. Lincoln), Thousand Oaks: Sage.

Işılar, H. B. (2021). Havayolu Endüstrisinde Dijital Pazarlama Uygulamalarının Değerlendirilmesi. *Havacılık ve Uzay Çalışmaları Dergisi*, 1(2), 42-63.

John, A. M., Louisa, E. I. & Ngozi, N. (2019). Cyber Crime and Underdevelopment of Tourism Industry in Nigeria. *Enugu State University of Science and Technology (ESUT) Journal of Social Sciences (EJSS)*, 4(2), 354-6-363.

Kara, İ. (2021). Web Sitesi Tabanlı Oltalama Saldırılarının Adli Analizi. *Niğde Ömer Halisdemir Üniversitesi Mühendislik Bilimleri Dergisi*, 10(*1*2), 450-455.

Karimi, O. (2018). *İnsan Faktörünü İçeren Bilgi Güvenliği Çerçevesi İçin Kavramsal Bir Model Oluşturmak*. Yayımlanmamış Doktora Tezi. İstanbul Üniversitesi, İstanbul.

Kazim, D., Çavuşoğlu, S., & Demirağ, B. (2021) Covid-19'un Tüketici Davranışları Üzerindeki Etkisi: Yerli Turistler Üzerinde Bir Araştırma. *Süleyman Demirel Üniversitesi Vizyoner Dergisi*, 12(32), 1160-1175.

Kıycı, Ş., Aksoy, R. ve Koçoğlu, C. M. (2020). Turist Yenilikçiliğinin Yenilikçi Otel işletmesi Tercihi Üzerindeki Etkisi. *İnsan ve Toplum Bilimleri Araştırmaları Dergisi*, 9(1), 608-635.

Kulular İbrahim, M. A. (2019). Markanın Alan Adi Olarak Kullanılması: Türkiye, ABD ve Avustralya Örnekleri. *Bilişim Hukuku Dergisi*, 1(1), 85-112.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., and Nunge, E. (2007). Protecting People From Phishing: The Design and Evaluation of an Embedded Training Email System. *SIGCHI Conference on Human Factors in Computing Systems*, San Jose, CA, 28 Nisan-3 Mayıs 2007.

Kuyucu, M. (2017). Y Kuşağı ve Teknoloji: Y Kuşağının İletişim Teknolojilerini Kullanım Alışkanlıkları. *Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi*, 5(2), 845-872.

Lazarević, J. (2017). Domain Name as a Function of Identity and Public Relations of Companies Operating on the Internet. *CM: Communication and Media*, 12(39), 83-98.

Liao, Z. and Shi, X. (2017). Web Functionality, Web Content, Information Security, and Online Tourism Service Continuance. *Journal of Retailing and Consumer Services*, 39, 258-263.

Loyaltylobby.com (2021). Otel İşletmesi Eposta Oltalama Örneği. https://loyaltylobby.com/2021/01/21/scam-emails-getting-more-professional-hilton-honors-20000-points-offer Erişim Tarihi: 18.10.2021.

Mehraj, H., Jayadevappa, D., Haleem, S. L. A., Parveen, R., Madduri, A., Ayyagari, M. R., & Dhabliya, D. (2021). Protection Motivation Theory Using Multi-Factor Authentication for Providing Security over Social Networking Sites. *Pattern Recognition Letters*, 152, 218-224.

Mitnick, K. D. ve Simon, W. L. (2002). *The Art of Deception: Controlling The Human Element of Security*, Wiley Publishing, Indianapolis.

Mohd Zaharon, N. F., Mohd Ali, M., and Hasnan, S. (2021). Factors Affecting Awareness of Phishing Among Generation Y. *Asia-Pacific Management Accounting Journal*, 16*(*2), 410-444.

Mou, J., Cohen, J. F., Bhattacherjee, A., and Kim, J. (2022). A Test of Protection Motivation Theory in the Information Security Literature: A Meta-Analytic Structural Equation Modeling Approach. *Journal of the Association for Information Systems, 23*(1), 196-236.

Mouton F., Leenen L., Malan M.M. and Venter H.S. (2014). Towards an Ontological Model Defining the Social Engineering Domain. *11th Human Choice and Computers International Conference,* Turku, Finland 27-28 Eylül 2014.

Nedelea, A. and Bălan, A. (2010). E-Tourism and Tourism Services Consumer Protection. *Amfiteatru Economic*, XII*(*28), 492-503.

Okul, T., Şimşek, G., Hafçı, B., ve Barış, Z. (2018). Konaklama işletmesi yöneticilerinde bilgi güvenliği farkındalığı: Kuşadası'ndaki beş yıldızlı oteller örneği. *Uluslararası Türk Dünyası Turizm Araştırmaları Dergisi,* 3(2), 189-201.

Ongun, U., Kervankıran, İ. ve Çuhadar, M. (2021). Kültür ve Kırsal Turizm Destinasyonlarına Yönelik Çevrimiçi Yorumlarının İncelenmesi: Şirince Köyü Örneği. *Türk Turizm Araştırmaları Dergisi*, 5(1), 219-235.

Oguama, L. (2021). Domain Name Theft – Cybersquatting: What It Means for Trademarks. *SSRN*, https://Ssrn.Com/Abstract=3837629. Erişim Tarihi: 15.01.2022.

Packard, N. (2020). Three Kinds of Demand Pull for The ARPANET into The Internet. *Cogent Social Sciences*, 6(1), 1-21.

Pesen, M. M. (2015). Bilgi Güvenliği Nedir ve Nasıl Sınıflandırılır?) https://www.sibergah.com/genel/bilgi-guvenligi-nedir-ve-nasil-siniflandirilir/. Erişim Tarihi: 3.6.2021.

Pilatin, A. ve Dilek, Ö. (2021). Müşterilerin Online Alışveriş Alışkanlıklarının Demografik Özelikler Bakımından İncelenmesi Doğu Karadeniz Şehirleri Üzerinde Bir Araştırma. *Aksaray Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 13(1), 11-28.

Plumley, G. (2010). *Website Design And Development: 100 Questions To Ask Before Building A Websit*e. John Wiley & Sons., Indianapolis.

Rasulovich, Z. N., Nuralievich, M. A., Ugli, B. U. B., Nizomovich, M. O., Utkirovich, K. J and Dusmurod, Q. (2019). Information Security Issues for Travel Companies. 2019 International Conference on Information Science and Communications Technologies (ICISCT), Karachi, Pakistan 9-10 Mart 2019.

Salloum, S., Gaber, T., Vadera, S., and Shaalan, K. (2021). Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey. *Procedia Computer Science*, 189, 19-28.

Sankhwar, S., Pandey, D., Khan, R. A., and Mohanty, S. N. (2021). An Anti-Phishing Enterprise Environ Model Using Feed-Forward Backpropagation And Levenberg-Marquardt Method. *Security and Privacy*, 4(1), 1-15.

Sezgin, M., & Yurtlu, M. (2021). Dijital Pazarlama Yöneticilerinin Bakış Açısıyla En Uygun Otel Seçimi: Analitik Hiyerarşi Prosesi (AHP) ve PROMETHEE Yaklaşımı. *Türk Turizm Araştırmaları Dergisi*, 5(3), 1756-1784.

Shahbaznezhad, H., Kolini, F., and Rashidirad, M. (2021). Employees' behavior in phishing attacks: what individual, organizational, and technological factors matter?. *Journal of Computer Information Systems*, 61(6), e132, 539-550.

Shabani, N. (2016). *Study of Cyber Securıty in Hospıtality Industry Threats and Countermeasures: Case Study in Reno, Nevada.* Yayımlanmamış Yüksek Lisans Tezi. University of South Florida, Florida.

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

Şenocak, K. (2009). Tescilli markanın aynısının veya benzerinin alan adı (Domain name) olarak kullanılması suretiyle marka hakkının ihlali. *Banka ve Ticaret Hukuku Dergisi*, 25(3), 87-141.

T.C. Ticaret Bakanlığı. (2021). Ticaret Bakanlığından Sahte Internet Siteleri Üzerinden Otel Rezervasyonu Uyarısı. https://twitter.com/ticaret/status/1406641048177233923?lang=en. Erişim Tarihi: 18.2.2022

T.C. Resmi Gazete. Müşteri Hakem Heyetleri Bilirkişilik Yönetmeliği. 09.7.2020. Sayı:31180, Başbakanlık Basımevi, Ankara.

Turizmgüncel.com (2021). Sahte Otel İşletmesi Rezervasyonu ile Sadece Bir Otel İşletmesinde 300 Bin Liralık Vurgun. https://www.turizmguncel.com/haber/sahte-otel işletmesi-rezervasyonu-ile-sadece-bir-otel işletmeside-300-bin-liralik-vurgun Erişim Tarihi: 18.01.2022.

TURSAB. (2021). Üye Acentalar. https://www.tursab.org.tr/acenta-arama. Erişim Tarihi: 15.09. 2021.

Türeli, N. Ş., Davras, G. M. ve Dolmacı, N. (2015). Turizm Sektöründe Kişisel Bilgilerin Mahremiyeti. *International Journal of Human Science*, 12(1), 236-254.

Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2018). Detecting Malicious Domain Names Using Deep Learning Approaches At Scale. *Journal Of Intelligent & Fuzzy Systems*, *34*(3), 1355-1367.

Visconti, R. M. (2020). *Domain Name and Website Valuation. In The Valuation of Digital Intangibles*. Palgrave Macmillan, Cham.

Vishva, E. S., and Aju, D. (2022). Phisher Fighter: Website Phishing Detection System Based on URL and Term Frequency-Inverse Document Frequency Values. *Journal of Cyber Security and Mobility*, 11(1), 83-104.

Vladimirov, A., Michajlowski, A. and Gavrilenko, V. (2010). *Assessing Information Security: Strategies, Tactics, Logic and Framework*. IT Governance Publishing, Londra.

Vrhovec, S. and Mihelič, A. (2021). Redefining Threat Appraisals of Organizational Insiders and Exploring the Moderating Role of Fear in Cyberattack Protection Motivation. *Computers & Security*, 106, 102309.

Wang, Q., Li, L., Jiang, B., Lu, Z., Liu, J. and Jian, S. (2020, June). Malicious Domain Detection Based On K-Means and Smote. *International Conference on Computational Science* Bildiri Kitabı, Springer Yayınları, 468-481.

Webius (20212). Sahte Otel İşletmesi Listesi. https://webiusdigital.com/sahte-otel işletmesi-sitesi-nasil-mucadele-edebilirsiniz. Erişim Tarihi: 18.10.2021.

Whitman M.E. and Mattord H. J. (2012). *Principles of Information Security*. Cengage Learning, Boston.

Yağcı, K., Akçay, S. and Efendi, M. (2020). The Importance of Information Security in Travel Enterprises: Kuşadası Case. *Journal of Tourism and Gastronomy Studies*, 8(1), 569-583.

Yıldırım, Y. (2016). Müşterinin Satın Alma Karar Sürecinde Bilgi Kaynakları ve Güvenirlikleri: Referans Grubu Olarak Yakın Çevrenin Etkisinin İncelenmesi. *Akademik Yaklaşımlar Dergisi*, 7(1), 214-231.

YİGM. (2021). Turizm Tesisleri. https://yigm.ktb.gov.tr/TR-9579/turizm-tesisleri.htm. Erişim Tarihi: 11. 10. 2021.

Yin, R. K. (2011). *Applications of case study research*. sage.

Yuan Sun, J. C., Jou Yu, S., Lin, S. S. J. and Shyong Tseng, S. (2016). The Mediating Effect of Anti-Phishing Self-Efficacy Between College Students' Internet Self-Efficacy and Anti-Phishing Behavior and Gender Difference. *Computers in Human Behavior*, 59, 249-257.

Zhang, C., Fathollahi-Fard, A. M., Li, J., Tian, G., & Zhang, T. (2021). Disassembly sequence planning for intelligent manufacturing using social engineering optimizer. *Symmetry*, 13(4), 663.