BÖLÜM 7

DİJİTAL PAZARLAMA UYGULAMALARINDA HİLE

DİJİTAL PAZARLAMA UYGULAMALARINDA HİLE

Dr. Öğr. Üyesi Zuhal AKGÜN
Yozgat Bozok Üniversitesi Yozgat MYO
Orcid ID: 0000-0002-5737-7920

Öğr. Gör. Dr. Pınar HACIHASANOĞLU
Yozgat Bozok Üniversitesi Yozgat MYO
Orcid ID: 0000-0002-4595-5156

Giriş

Geçtiğimiz birkaç yıl içinde muazzam düzeye ulaşan teknolojik gelişmeler, iletişim zorluklarını aşmaya yardımcı olmaktadır. Olumlu bir ilişki ortamının tam kalbinde yükselen teknoloji, işletmelere çok kültürlü bir ortamda yaşamak ve küreselleşme eğilimlerini takip etme fırsatı da sunmaktadır. İşletmenin "yıldız" paydaşları olan müşteriler ile ilişki yaratma, geliştirme ve sürdürme süreçlerinde temel soru, farklı kültürel geçmişlere sahip, ışık hızında işlemler arayan aynı zamanda değerli bilgiler toplamaya ve iletişim halinde olmaya çalışan müşterilere nasıl etkili ve verimli bir şekilde hitap edileceğidir. Müşteri ilişkileri yönetimi açısından en iyi teklifi sunan pazarlama araçları çevrimiçi olanlardır. İnternet'in en büyük avantajı, geniş, sürekli artan bir pazarda büyük bir giriş için nispeten ucuz bir bilet olması ve aynı zamanda izleyiciye ulaşmak için kullanılabilecek çeşitli multimedya enstrümanları sunmasıdır (Carmen ve Nicole, 2010: 737).

İnternet, kullanıcı sayılarının artmaya devam ettiği göz önüne alındığında, klasik pazarlamaya göre çok daha fazla kullanıcıya ulaşabilen pazarlama faaliyetlerinin uygulanması açısından işletmeler için oldukça önemlidir (Hudák vd., 2017: 346).

Dijital pazarlama, internet ve teknolojik gelişmelerin işletme ve tüketicilere çeşitli fırsatlar sunan bir pazarlama disiplini olarak, yeni nesil alışveriş kültürünün şekillenmesini sağlamaktadır. Farklı teknolojik ve dijital platformlar kullanılarak pazarlama faaliyetleri yürütülmektedir. Hız, esneklik ve özellikle zaman ve mekândan bağımsız yapılan pazarlama faaliyetleri hem tüketiciler hem de işletmeler için önemli avantajlar sunmaktadır. Ancak sanal dünyanın karanlık yüzü son yıllarda kötü niyetli kullanıcıların profesyonel çalışma alanı haline gelmiştir. Güvenlik zafiyeti bulmak suretiyle pek çok şekilde, bireysel tüketicileri ve işletmeleri çeşitli dijital yöntemler ile aldatma ve hileli uygulamalar ile dolandırma eylemlerinin sayısı giderek artmaktadır. Bu tarz uygulamalar karşısında kamuoyunun farkındalığının artması da oldukça önem kazanmaktadır.

Bu çalışmada dijital pazarlama stratejilerinden olan, arama motoru pazarlaması, mobil pazarlama, elektronik posta pazarlaması ve sosyal medya pazarlaması alanlarında yapılan aldatıcı ve hileli pazarlama uygulamalarına yer verilmektedir.

Arama Motoru Pazarlaması

Bilgi patlamasının yaşandığı internet çağında arama motoru insanların vazgeçilmez internet araçları haline gelmiştir (Hui vd. 2012: 930). Günümüzde internetin muazzam içeriği, bir konu hakkındaki bilgileri bulmayı zorlaştırmaktadır. Bu nedenle bilgiye ulaşmaya yardımcı olan yöntemler özellikle önemli hale gelmektedir. Bu nedenle arama motoru, bilgi aramak için herkesin hayatının ayrılmaz bir parçası haline gelmektedir (Patil Swati vd., 2013: 10). Arama motoru, anahtar sözcüklerle belgelerde ve dosyalarda arama yapan ve bu anahtar sözcükleri içeren sonuçların listesini çıkaran, internet üzerinden kullanılabilen bir web yazılım programı veya web tabanlı komut dosyasıdır. Bugün, internette her biri kendi tekniklerine ve uzmanlıklarına sahip çok sayıda farklı arama motoru bulunmaktadır (Jain, 2013: 99). Arama motorları, büyük miktarda bilgiye artırılmış ve rahat erişim sağlamakta, bilgi arama ve erişim sürecinde insan aracılara olan ihtiyacı

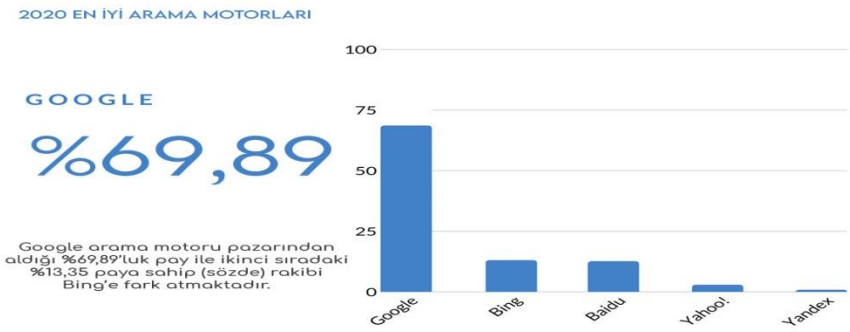
ortadan kaldırarak bilgi erişim süresinde göz ardı edilemeyecek bir azalma sağlamaktadırlar (Onaifo ve Rasmussen, 2012: 87).

Arama motorları; (1) araştırmacının bilgi alabileceği evreni oluşturan bir dizi web sayfasını bir araya toplamakta (kavramsal olarak), (2) bu evrendeki sayfaları, içeriklerini yakalamaya çalışan bir tarzda temsil etmekte, (3) araştırmacıların konular yayınlamasına izin vermekte ve onlar için bu evrendeki en alakalı sayfaları bulmaya çalışan bilgi alma algoritmaları kullanmaktadır (Gordon ve Pathak, 1999: 142-143).

Arama motorlarının geldiği son durum aşağıdaki gibi sıralanmaktadır (Ranga ve Ranga, 2014: 24):

- Arama motoru pazar payının % 65-70'i Google'a aittir.
- Çevrimiçi deneyimlerin % 93'ü bir arama motorunun sonucu olmaktadır.
- Pazarlama Grafikleri, müşterilerin % 61'inin arama motorundan geldiğini göstermektedir.
- Ayda dünya çapında 100 milyardan fazla arama yapılmaktadır.
- İnternet kullanıcılarının % 82'sinden fazlası arama motoru kullanmaktadır.

Şekil 1. Dünya'daki En İyi Arama Motoru



Kaynak: Ilgar, 2020.

Veriler 2020 yılına ait dünyadaki en çok kullanılan arama motorlarını göstermektedir. Şekilde en çok kullanılan arama motorunun % 69,89'la Google olduğu, onu % 13,35' le Bing ve diğerlerinin takip ettiği görülmektedir.

Kullanıcıların ihtiyaçlarını karşılamak için arama motorunun kullanıcı sorgusuyla eşleşen en alakalı bilgileri bulması ve filtrelemesi bu bilgileri kullanıcıya göstermesi gerekmektedir. Google gibi büyük arama motoru, sayfanın kalitesini ölçmek için sayfa sıralamasına güvenmektedir. Daha yüksek sayfa sıralama değeri, web sitesinin çok popüler olduğunu göstermekte ve arama motoru sonuçlarında daha yüksek bir sıralama elde etmek için web sitesi tasarımcıları tarafından birçok web sitesi tanıtım tekniği kullanılmaktadır. Web sitesi tasarımcıları arama motorunun doğal listelemesinde web sitesini tanıtmak için, arama motoru iyileştiricileri sonuçlarını analiz etmekte ve buna göre arama motoru optimizasyonu tekniklerini kullanılmaktadırlar (Patil Swati vd., 2013: 10).

Arama motorları, World Wide Web'deki web sitelerini indekslemekte ve veri tabanlarında binlerce web sayfasını depolamaktadır. Kullanıcı tarafından yazılan "anahtar kelimeler" olarak bilinen kelimelere dayalı bir web sitesi listesi sunmaktadırlar. Web sitesi bu listede ne kadar yüksekse,

birinin onu ziyaret etme şansı da o kadar yüksek olmaktadır (Kumar, 2013: 123).

Arama motorları çevrimiçi dünyada önemli bir konuma sahiptir ve web sitelerine gelen tüm ziyaretçilerin yarısından fazlası başka bir web sayfasından doğrudan bağlantı yerine bir arama motorundan ulaşmaktadır. Aramaların artan önemi ile birlikte, arama motorları, imajlarını oluşturmak için interneti kullanan firmalar ile hedef müşterileri arasında daha büyük roller oynamaktadır (Dou vd. 2010: 262).

Arama motoru pazarlaması, pazarlamacıların ve web yöneticilerinin, arama motorlarının sonuç sayfalarında (Google, Bing, AlltheWeb, Altavista vb.) web sayfası listelerinin uygun bir konumda görünmesini sağlamak için bir dizi teknik kullandıkları bir çevrimiçi pazarlama biçimidir. Temel strateji, şirketin web sayfalarının uygun anahtar kelimeler içermesini ve web sitesinin sayfa hiyerarşisinin mantıksal olarak düzenlenmesini sağlayarak arama motorları için web sayfalarını optimize etmektir (Paraskevas vd. 2011: 200). Firmaların arama motorlarına reklam yerleştirerek tüketicileri hedeflemelerine olanak sağlayan arama motoru pazarlamacılığı, etkili bir kitle edinme stratejisi olduğunu kanıtlamıştır (Boughton, 2004: 29).

Arama motoru pazarlama teknikleri aşağıdaki gibi sıralanmaktadır;

1. Arama Motoru Optimizasyonu Tekniği: Bir web sitesinin arama motorundaki görünürlüğünü artırmaya yönelik bir tekniktir (Jain, 2013: 99). Arama motoru optimizasyonu, web sitelerinin yapısını, içeriğini ve programlamasını belirli arama terimlerine göre ayarlayarak bir web sitesinin yapısal listelerde sıralamasını iyileştirmeye çalışmaktadır. Bu optimizasyon, yüksek çaba ve masrafın yanı sıra teknik kısıtlamalar nedeniyle genellikle birkaç anahtar kelimeyle sınırlı olmaktadır (Olbrich ve Schultz, 2008: 5).

2. Tıklama Başına Ödeme Reklamcılığı Tekniği: Tıklama başına ödeme reklamcılığı tekniği, bir web sitesinin çeşitli motorlarda seviyesini yükseltmek için çok iyi bilinen bir yöntemdir. Gelişmekte olan tüm şirketler, web sitelerinde reklam alanı satmaktadır. Bir şirket, tıklama başına ödeme

reklamcılığı tekniğini kullanarak, ürünleri ve hizmetleri için müşteriler veya tüketiciler oluşturmaktadır (Ranga ve Ranga, 2014: 25). Arama motoru reklamlarında geleneksel reklamcılığın (bir reklam yerleştirirken maliyetlerin ortaya çıktığı) aksine, gösterimler için değil, yapılan tıklamalar için ödeme yapılır (Mladenow vd., 2015: 110).

3. Arama Motorlarına Ücretli Katılım Tekniği: Bu teknikte, arama motoru sağlayıcılarına, web sitelerini arama sonuçlarında tanımlanan anahtar kelimelere göre listelemeleri için ödeme yapılmaktadır. Artık bir web sitesinin kesin arama terimiyle ilişkilendirilmesi kolaylaşmıştır. Bu teknik kapsamında, düzenli ve otomatik olarak kataloglanan bir web sayfası için yıllık abonelik şeklinde ücretler alınmaktadır (Ranga ve Ranga, 2014: 25).

Arama motoru pazarlaması, bir tür internet pazarlamacılığıdır. Optimizasyon ve reklam yoluyla arama motoru sonuç sayfalarında görünürlüğünü artırarak web sitelerinin tanıtımını içermektedir. Tüm bunlar, arama motoru için optimize edilmiş web sitesi tasarımı, ücretli reklamcılık, yüksek kaliteli pazarlamanın bir karışımı kullanılarak yapılmaktadır. Diğer bir deyişle, arama motoru pazarlaması, arama motorunun sonuç sayfalarında görünen reklamları satın almaya vurgu yapmaktadır (Ranga ve Ranga, 2014: 24).

Web üzerinden ürün ve hizmetler sunan firmalar, potansiyel müşterileri zaten çevrimiçi olduklarından, internet reklamcılığından açıkça kazanç elde etmektedir. Web tabanlı olmayan şirketler, görünürlüğü artırmak ve markayı tanıtmak için çevrimiçi pazarlamayı seçebilmektedir. Arama motoru pazarlaması, şirketlerin bir hedef kitleden elde ettikleri yatırım getirilerini yakından takip etmelerini sağlamaktadır (Boughton, 2004: 29). Şirketlerin arama motoru pazarlamacılığına yaptığı harcamalar, diğer çevrimiçi reklamcılık araçlarına yapılan harcamalardan daha hızlı artmakta ve analistler, arama motoru pazarlamacılığı harcamalarının, e-ticaret faaliyetleri için kilit büyüme sektörü olan çevrimiçi reklam

pastasından aslan payını yakında alınacağını tahmin etmektedirler (Dou vd. 2010: 262).

Arama Motoru Pazarlamasında Hile

İşletmeler, müşterilerin dikkatini çekmek için mücadele ederken, sonuçların arama motoru sorguları listesinde en iyi sıralama konumunu ve dolayısıyla görünürlüğünü artırmayı istemektedir. Arama motoru optimizasyonu yoluyla doğal arama sonuçlarını iyileştirme olasılığına ek olarak, arama motoru reklamları ile müşteriye hızlı ve hedefli bir şekilde hitap etmeyi başarmaktadır (Mladenow vd., 2015: 110). Arama motorunun işletmelere ve müşterilerine sunduğu bu inanılmaz imkânlar hilekârların bu sisteme dâhil olmasını kaçınılmaz kılmaktadır. Dolayısıyla hilekârlar dijital ortamın sağladığı sanallığı kullanarak haksız kazanç elde etmek için birçok yöntemi kullanmaktadırlar.

Arama motoru pazarlamasını da içine alan ve arama motorları aracılığıyla yapılan yaygın hile türleri aşağıda verilmiştir:

Arama Motoru Optimizasyonu Hilesi: Arama motoru optimizasyonu teriminin yaygın olarak kullanılmasıyla, kendi adını taşıyan birçok "SEO Uzmanı" ortaya çıkarak, gerçekçi olmayan vaatlerde bulunmakta ve garantili sıralamalar sunmaktadır. SEO hilelerine karşı en iyi savunma şekli konu hakkında daha fazla bilgi sahibi olmaktır (https://www.purelybranded.com/notes/t...., Erişim Tarihi: 30.05.2021).

Çevrimiçi hileciler, reklamcılardan çalmaya, rakiplere zarar vermeye veya başka bir şekilde sistemde dürüst olmayan bir şekilde oyun oynamaya çalışmaktadırlar. Reklamla ilgili hileleri incelemek, pazarlamacıların, yöneticilerin ve teknoloji uzmanlarının potansiyel güvenlik açıklarını ve bunlarla savaşmak için kullanılan yöntemleri anlamalarına yardımcı olmaktadır. Çevrimiçi reklamcılıkta denenen yaygın hile türlerinden bazıları şunlardır (A Manager's Guide to Harnessing Technology, 2010):

Zenginleştirici tıklama hilesi: Site operatörlerinin reklam geliri elde etmek için sahte reklam tıklamaları oluşturmasıdır.

Zenginleştirilmiş gösterim hilesi: Site operatörlerinin sitelerinin reklam kazançlarını artırmak için yanlış sayfa görüntülemeleri (ve dolayısıyla reklam gösterimleri) oluşturmasıdır.

Tüketen tıklama hilesi: Rakibin reklam bütçesini tüketmek için Web'deki reklamlarına tıklamaktır.

Tüketen gösterim hilesi: Bir rakibin reklam bütçesini tüketmek için sahte gösterimler oluşturmaktır.

Sıralamaya dayalı gösterim hilesi: Reklam sıralamasının tıklama performansına dayandığı sitelerde, dolandırıcılar, rakip reklamlara bağlı anahtar kelimeleri tekrar tekrar arayarak rakip reklamların göründüğü sayfalara erişmektedir. Amaç, tıklamalar olmadan gösterimler oluşturmaktır. Bu süreç, bir rakibin reklamlarının performans sıralamasını (kalite puanını) muhtemelen reklamları sıralama sonuçlarından düşürerek ve hilecilerin daha önce rakipleri tarafından işgal edilen reklam alanları için daha sonra daha az teklif vermesine olanak tanımaktadır.

Kovma hilesi: Rakibin bir reklam ağından yasaklanacağını veya arama motoru listelerinde cezalandırılacağını umarak, rakiple ilişkili görünen sahte tıklamalar veya gösterimler oluşturarak bir rakibi çerçevelemeye çalışmaktır.

Link hilesi (spam dizini oluşturma veya bağlantı çiftliği olarak da bilinir): Bir sayfanın doğal aramadaki sonuçlarını artırmak umuduyla, hepsi bir sayfaya bağlanan bir dizi sahte Web sitesi oluşturmak.

Anahtar kelime doldurma hilesi: Normalde Web sitesini ziyaret etmeyecek kullanıcıları cezbetmek veya daha değerli içeriğe dayalı reklamları çekmek umuduyla, bir Web sitesini alakasız anahtar kelimelerle (bazen bir Web sitesinin arka planıyla aynı renkteki yazı tiplerinde gizlenir) doldurmaktır.

Yaygın hilecilik durumu, reklam verenlerin yatırım getirisini düşürmekte ve çevrimiçi reklamcılık pazarını çökertmektedir. Bu nedenle Google ve rakipleri, dolandırıcıları ortaya çıkarmak ve kovuşturmak için özenle çalışmaktadır (A Manager's Guide to Harnessing Technology, 2010).

Bir diğer arama motoru hilesi olan bireyin kişisel verilerini (adları, doğum tarihleri, sosyal güvenlik bilgileri, banka hesap numaraları, kredi kartı bilgileri, şifreleri ve diğer verileri) elde etmeyi amaçlayan "kimlik avı" dır. Kimlik avı, çevrimiçi web sitesi arama motorları aracılığıyla gerçekleşmektedir. Burada kişi, web sitesini ziyaret etmeye ikna eden teklifler veya mesajlarla karşılaşmaktadır. Arama işlemi yasal olabilmekte, fakat web sitesi aslında sahte ve yalnızca kişinin kişisel bilgilerini çalmak için hazırlanmaktadır. Arama motoru kimlik avı şemaları farklı biçimde olabilmektedir. Arama motoru kimlik avının bazı yaygın örnekleri şunlardır:

Ücretsiz/İndirim Teklifleri: Burada, web sitesi yüksek indirimli fiyatlarla ürünler veya web sitesinin arkasındaki kuruluşların gerçekte sahip olmadığı ve göndermeyecekleri ücretsiz ürünler sunmaktadır. Var olmayan "ürünleri" elde etmek için kişinin gizli bilgilerini vermesi gerekmektedir.

İş Teklifleri: Kişinin sosyal güvenlik numarasını girmesini gerektiren sahte iş teklifleri sunulmaktadır. Bu teklifler, çevrimiçi iş aramalarıyla bağlantılı olarak ortaya çıkmaktadır.

Acil Durumlar: Bazı web siteleri, acil veya zorunlu durumlar nedeniyle tüketiciyi bilgi vermesi için korkutmaya çalışmaktadır. Bu duruma örnek olarak, kişinin bilgisayarında virüs olduğunu belirten bir web sitesinden gelen uyarı mesajı alması verilebilir (https://www.legalmatch.com/law-library/arti..., Erişim tarihi: 05.06.2021).

Mobil Pazarlama

Geçtiğimiz on yıl boyunca, "mobil" tanımı, cep telefonunu tanımlamakla birlikte, taşınabilir bilgi işlem cihazlarını (tabletler ve akıllı hoparlörler) ve mobil hizmetleri (mobil uygulamalar ve sanal asistanları)

daha geniş kapsayacak şekilde hızla gelişmektedir. Mobil telefonlar, pazarlamacıların müşterilerle etkileşim biçimini yeniden şekillendirmekte ve yeni pazarlama fırsatları yaratmaktadır. Ayrıca, mobil pazarlamanın iş potansiyeli önümüzdeki 5 yıl içinde 183 milyar doları aşacağı (BusinessWire 2019) ve dünya nüfusunun yarısından fazlasının en az bir mobil cihaza sahip olacağı (Statista 2019) tahmin edilmektedir (Tong vd., 2019: 64).

Günümüzde mobil telefon, gençlerin de yaşamları dâhil olmak üzere çoğu tüketicinin hayatının merkezinde yer almaktadır. Birçok tüketicinin onsuz yapamayacağı, her zaman yanlarında taşıdığı ve gittikleri hemen hemen her yerde kontrol ettikleri bir cihazdır. Tüketiciler için cep telefonu sadece arkadaşlar ve aile ile bağlantıda kalmak için kullanılan kişisel bir cihaz değil, aynı zamanda kişiliklerinin ve bireyselliklerinin bir uzantısıdır. Pazarlamacılar için cep telefonlarının yaygın olarak benimsenmesi, tüketicilere her zaman, her yerde ulaşmak ve hizmet vermek için büyük bir pazarlama fırsatı anlamına gelmektedir (Persaud ve Azhar, 2012: 418)

Mobil pazarlama, bir firma ile müşterileri arasında bir mobil ortam, cihaz veya teknoloji kullanarak bir teklifin iki yönlü veya çok yönlü iletişimi ve tanıtımı olarak tanımlanmaktadır (Hofacker vd., 2016: 25). Ayrıca mobil pazarlama, müşterilere malları, hizmetleri ve fikirleri tanıtan, böylece tüm paydaşlar için değer yaratan, zamana ve yere duyarlı, kişiselleştirilmiş bilgiler sağlamak için etkileşimli kablosuz medya kullanmak olarak tanımlanmaktadır (Haghirian vd., 2005: 2).

Mobil Pazarlama Derneği (MMA, 2008) ise mobil pazarlamayı; kuruluşların herhangi bir mobil cihaz veya ağ aracılığıyla hedef kitleleriyle etkileşimli ve ilgili bir şekilde iletişim kurmasını sağlayan bir dizi uygulama olarak tanımlamaktadır (Smutkupt vd., 2010: 127).

Kuruluşlar, hedef kitleleriyle arasındaki bu etkileşimi çeşitli mobil pazarlama teknikleri kullanarak yapmaktadır. En çok kullanılan mobil pazarlama teknikleri:

Bunlar SMS Yoluyla Mobil Pazarlama, MMS Yoluyla Mobil Pazarlama, Oyun İçi Mobil Pazarlama, Mobil İnternet Üzerinden Pazarlama, Bluetooth Aracılığıyla Mobil Pazarlama, Konum Tabanlı Hizmetler (LBS-Location Based Services) ve Mobil Viral Pazarlama gibi yöntemler kullanılmaktadır.

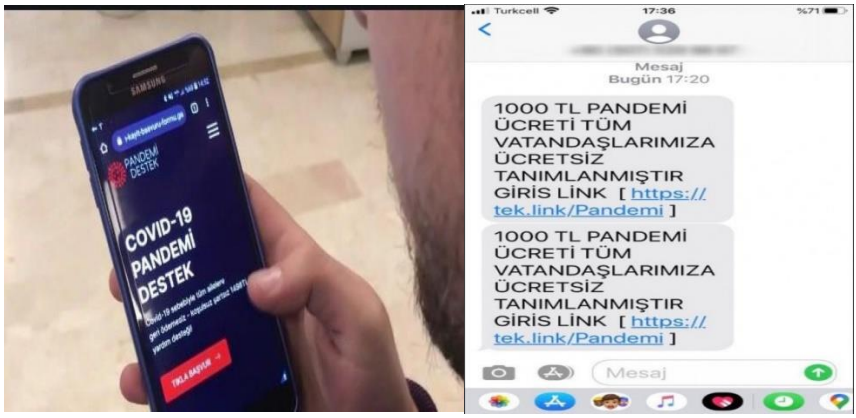
Mobil Pazarlamada Hile

Mobil pazarlama, işletmeler için harika fırsatlar sunmaktadır. Mobil cihazlarla desteklenen pazarlama faaliyetleri, şirketlerin tüketicileriyle zaman veya konum engeli olmaksızın doğrudan iletişim kurmasına olanak tanımaktadır (Haghirian vd., 2005:1). Mobil e-ticaret, tüm perakende e-ticaret satışlarının yarısından fazlasını oluşturmaktadır. 2021 yılına kadar % 14 daha büyümesi beklenmektedir ve bu durum mobil cihazları hilecilik girişimleri için ana hedef haline getirmektedir (Benari, 2019).

Hileler, bireylerin, firmaların, endüstrilerin ve ekonomilerin hayatta kalmasını tehdit eden küresel ekonomik bir tehdit durumundadır (Akomea-Frimpong vd., 2019: 300). Hileciler, çalışma yöntemlerini sürekli olarak değiştirmekte ve yeni teknolojilere uyum sağlamaktadır. Kişilerin kendilerini güvende tutması ve hilecilerin kişisel bilgilerden kâr elde etmek için telefonları ve interneti nasıl kullanabileceğini bilmesi önemlidir. Hilenin verdiği zararları daha iyi tanımak için mobil pazarlamada yer alan hile türleri aşağıdaki gibi sıralanabilir:

Kimlik avı hilesi: Hileciler, güvenilen bir şirket veya kuruluştan (telefon şirketi, banka veya bir devlet kurumu) geliyormuş gibi mesajlar göndermektedir. Bu mesajlar SMS mesajları, e-posta veya sosyal medya aracılığıyla gönderilebilmektedir. Kimlik avı mesajlarında genellikle bir bağlantının tıklanması ve kişisel bilgilerin girilmesi istenmektedir.

Şekil 2. Covid-19 Pandemi Desteği Adı Altında Mobil Kullanıcılara Yönelik Hile Örneği



Kaynak: https://www.yenidonem.com.tr/haber/burs....., Erişim tarihi: 04.06.2021.

Cevapsız arama hilesi: Bu hilekârlar, telefonu kapatmadan önce cep telefonuna çok kısa bir arama yapmaktadırlar. Hilekârlar, yüksek bir ücret karşılığında para alabilmeleri için cevapsız numarayı geri aramanızı istemektedirler. Kişiyi telefonda ne kadar uzun süre tutabilirlerse, o kadar çok para kazanabilmektedirler. Numara tanınmıyorsa, uluslararası bir numaraysa veya telefon numarası 190 ile başlıyorsa (ücretli bir hizmeti tanımlar), bunun bir cevapsız arama hilesi olma olasılığı bulunmaktadır.

Sahte çevrimiçi alışveriş hilesi: Çevrimiçi alışveriş hilesi, gerçek çevrimiçi mağazalar gibi davranan hilekârları ifade etmektedir. Bu genellikle gerçek alışverişe çok benzeyen sahte bir web sitesiyle (örneğin, "Telstra.com.au"daki büyük "I" yerine "i" kullanılması) veya mal teslim etmeyen bir web sitesi kurarak yapılmaktadır. Bu çevrimiçi alışveriş dolandırıcılıklarının çoğu para almayı amaçlarken, diğerleri kişisel bilgileri ulaşmak için kullanmaktadır. Ürünlerin inanılmaz derecede düşük fiyatlarla reklamını yapan mağazalardan uzak durarak sahte çevrimiçi alışveriş sitelerinden kaçınılabilir (örneğin, en yeni IPhone'u 100 $'a satmak). Çevrimiçi ödeme yaparken, güvenli web siteleri aranmalıdır. Bunların URL

çubuğunda kapalı bir asma kilit sembolü vardır ve "https" ile başlamaktadır (http://accan.org.au/talki., Erişim tarihi: 03.06.2021).

İndirme hilesi: Dolandırıcıların çeşitli hile yaklaşımlarıyla uygulamaların indirilme sayısını manipüle ettiği mobil uygulama pazarlarında yaygın bir tehdit olmaktadır. Satın alınan sahte indirmeler, tavsiye ve arama algoritmalarını yanlış yönlendirebilmekte ve ayrıca uygulama pazarlarında kötü kullanıcı deneyimine yol açabilmektedir. Datavisor' deki yakın tarihli bir rapor, mobil pazarlamada % 10'a yakın indirme ve yüklemelerin sahte olduğunu ve bunun 2018'de uygulama pazarlamacıları için 300 milyon dolara kadar kayba yol açtığını iddia etmektedir. Uygulama pazarındaki sahte indirmeler, tavsiye sistemini yanlış yönlendirerek düşük kaliteli öneri sonuçlarına sebep olmakta ve hatta tüm uygulama pazarı ekosistemini rahatsız etmektedir (Dou vd., 2019: 671).

Mobil reklam hilesi: Mobil reklamcılık teknolojisinden yararlanarak reklamcıları, yayıncıları veya tedarik ortaklarını dolandırma girişimidir. Dolandırıcıların amacı, reklam bütçelerinden çalmaktır. Mobil reklam dolandırıcılığı, sahte gösterimler, tıklama spam'ları veya sahte yüklemeler gibi çeşitli şekillerde olabilir. Örneğin, sahte izlenimlerden yararlanmaya çalışan dolandırıcı yayıncılar, reklamları tek bir piksele sığdırabilmekte veya hiç gerçekleşmemiş görünümler veya gösterimler oluşturmak için bir reklamı kasıtlı olarak görünüm dışına hizalayabilmektedir (https://www.adjust.com/glossary/mobile-ad-fraud/, Erişim tarihi: 03.06.2021).

Elektronik Posta (E-Posta) Pazarlaması

Elektronik posta ile pazarlama, ticari amaçla veya para kazanma niyetiyle mesajların bir hedef kitleye iletilmesi için elektronik postayı kullanan, doğrudan bir pazarlama biçimidir. En geniş anlamıyla, işletmenin mevcut müşterileri ile ilişkisini geliştirmek, müşteri sadakatini sağlamak, yeni müşteriler kazanmak ve diğer firmaların müşterilerine gönderdiği e-posta mesajlarına reklam eklemek amacıyla yapılan pazarlama faaliyetleri,

e-posta pazarlaması kapsamında yer almaktadır (Fariborzi ve Zahedifard, 2012: 232).

E-posta pazarlaması, işletmelerin internet kullanımı yoluyla potansiyel ve mevcut müşterilerini bilgilendirmek için kullandığı, web'in en popüler unsuru ve yatırımın kârlılığı bakış açısıyla, doğrudan pazarlamanın internet üzerindeki cephaneliğinin en etkili araçlarından biridir (Carmen ve Pop Nicolae, 2010: 738).

E-posta pazarlaması, elektronik pazarlamanın bir parçası olarak, site trafiğini ve satış desteğini artırmak için kullanılan, ticari ve ticari olmayan mesajların, e-posta adreslerinin ayrıntılı bir listesine hedeflenmiş olarak gönderilmesi olarak tanımlanmaktadır. Kayıtlı müşterilere düzenli olarak gönderilen, genellikle HTML formatındaki e-postalardır. Modern, ucuz ve popüler bir pazarlama aracıdır. E-posta ile pazarlama markayı inşa etmede, müşterilerle ilişkileri geliştirmede, yeni bağlantılar kurmada ve satış promosyon açısından en etkili pazarlama faaliyetlerinden biri olarak kabul edilmektedir (Hudák vd., 2017: 343). E-posta pazarlaması bir takım avantaj ve dezavantajlara sahiptir (Tablo 1).

Tablo 1. E-Posta Pazarlamasının Avantaj ve Dezavantajları

E-posta Pazarlamasının Avantajları	**E-posta Pazarlamasının Dezavantajı**
Yatırım getirisinin yüksekliği	E-postaların teslim edilememesi
Anlamlı, özelleştirilebilir ve müşteri profilleri ile tutarlı mesajlar	E-posta yanıtının bozulması
Ölçülebilirlik	Mailin renk, yazı kalitesinin düşük olması
Kolay ve otomatik kullanım	Aşırı e-posta yüklenmesi
Hızlı ve etkili işlemler	Güven sorunu

Kaynak: Fariborzi ve Zahedifard, 2012: 233.

Elektronik Posta Pazarlamasında Hile

İnternet kullanımının önemli ölçüde artmasıyla birlikte, insanlar kişisel bilgilerini giderek daha fazla çevrimiçi paylaşmaktadır. Sonuç olarak, muazzam miktarda kişisel bilgi ve finansal işlem siber suçlulara karşı savunmasız hale gelmektedir (Alkhalil vd., 2021: 1).

E-posta genellikle diğer iletişim biçimlerine (örneğin mektuplar, telefon görüşmeleri, toplantılar vb.) göre daha hızlı bir alternatiftir ve kullanıcılar e-postaları ne zaman kullanacaklarına ve yanıtlayacaklarına kendileri karar verebilirler. Ancak, e-posta kullanmanın, spam e-posta ("istenmeyen ticari e-posta" olarak da bilinir), kimlik avı (Phishing-Oltalama) ve kimlik sahtekârlığı gibi dezavantajları bulunmaktadır.

Spam yani istenmeyen e-posta gönderme, elektronik mesajlaşma sistemlerinin ayrım gözetmeksizin istenmeyen toplu mesajlar göndermek için kötüye kullanılmasıdır (Hoonakker vd., 2009: 2-3). 1990'ların ortalarında internetin halka açılmasıyla e-postadaki spam bir sorun olmaya başlamıştır. Takip eden yıllarda katlanarak büyümüş ve dünyadaki tüm e-postaların yaklaşık % 80 ila % 85'ini oluşturacak boyuta ulaşmıştır (Kanich vd., 2008).

Kimlik sahtekârlığı, uygulamada en sık karşılaşılan aldatma faaliyetlerinden biridir. Bilişim sistemleri aracılığıyla dolandırıcılık eylemleri içinde yer alan bu sahtekârlık biçimi, failin bir kişiye ait e-posta hesabının şifrelerini ele geçirerek, bu kişinin yakınlarına kendisini profil sahibi gibi tanıtıp belli bir menfaat istemesiyle gerçekleşmektedir (Dülger, 2015: 616).

Kimlik avı, suçluların kullanıcıları aldatmasına ve önemli verileri çalmasına olanak tanıyan oldukça etkili bir siber suç biçimine bir örnektir. İnternet'teki en yaygın sahtekârlık faaliyeti örneklerinden biri olarak kimlik avı saldırıları, hassas bilgiler, kimlik hırsızlığı, şirketler ve devlet sırları dâhil olmak üzere kurbanları için ciddi kayıplara yol açmaktadır (Alkhalil vd., 2021: 1). Kimlik avı, kullanıcıları kandırmak için çevrimiçi aldatma yoluyla bireylerden kişisel ve hassas bilgiler elde etme girişimidir. Sistem güvenliğini tehlikeye atmak için teknik uzmanlık kullanmak yerine, “anlamsal saldırı”

olarak tanımlanan kimlik avı, kullanıcıları kullanıcı adları ve parolalar, hesap ayrıntıları gibi özel bilgileri ifşa etmeye ikna etmek amacıyla sosyal mühendislik tekniklerini kullanmaktadır (Harrison vd., 2016: 265). Gartner Inc. (2006) kimlik avı saldırıları hakkında 5.000 çevrimiçi yetişkin ile yaptığı araştırmada 2004'te 57 milyon ABD'li yetişkin, 2006'da yaklaşık 109 milyon ABD'li yetişkinin kimlik avı e-posta saldırılarına maruz kaldığını belirlemiştir (Hoonakker vd., 2009: 3).

Oltalama yoluyla yapılan e-posta dolandırıcılığı, rastgele kullanıcı hesaplarına e-mail göndermek şeklinde yapılan bir çevrimiçi saldırı olmakla birlikte, gönderilen e-postalar, kişilerin devamlı temas halinde olduğu banka, internet sitesi, e-posta veya internet hizmeti sağlayıcısı vb. kuruluşlardan gönderilmiş gibi gösterilmektedir. Bununla birlikte kullanıcının e-posta kotasının dolduğu iletisiyle hesapların güncellenmesi gerektiği belirtilerek bir internet bağlantısı (link) adresi verilmesi şeklinde de yapılmaktadır. Yönlendirilen sayfa sahte veya değiştirilmiş bir web sitesi olmaktadır. Kişiler bu siteye yönlendirildiklerinde istenen bilgileri sunarak dolandırıcıların taleplerini yerine getirmiş olmaktadır. Saldırganlar genellikle hesap numarası, şifre, kredi kartı numarası, internet bankacılığına ait kişisel bilgileri talep etmektedir. Benzer şekilde e- posta ile yarışma ilanları ve ödüllere yönelik ileti gönderilerek kişinin bilgileri istenebilmektedir (https://bim.aku.edu.tr/phishing-oltalama-nedir/, Erişim Tarihi: 25.05.2021). Kimlik avı dolandırıcılığının temel amaçları şöyle sıralanmaktadır (https://www.kaspersky.com/resou.., Erişim Tarihi: 25.05.2021) ;

- Cihaza kötü amaçlı yazılım bulaştırmak.
- Para veya kişisel hesap bilgilerini almak için özel kimlik bilgilerini çalmak.
- Çevrimiçi hesapların kontrolünü ele geçirmek.
- Kişiyi gönüllü olarak para veya değerli eşya göndermeye ikna etmek.

İnternet veya telefon kullanan herkes, her yaş grubu kimlik avı dolandırıcılarının hedefi olabilmektedir. Kişisel bilgi hırsızlığı ile çevrimiçi dolandırıcılığın yaygın hale gelmesi, kimlik avına karşı önlemler almayı gerektirmektedir. Aldatıcı şekilde güvenilir görünen hatta kullanıcıya özel kişiselleştirilmiş e-postalara karşı dikkatli olmak, kimlik avı e-postalarını tespit etme konusunda uyanık olmak çok önemlidir. Gelen kutunuzda (spam olarak otomatik olarak filtrelenmemiş) bir ileti ile karşılaşıldığında, bir kimlik avı saldırısının kurbanı olmaktan kaçınmak için kullanılabilecek stratejiler şöyle özetlenebilir (https://www.kaspersky.com/resource-cen.., Erişim Tarihi: 25.05.2021):

- *Şüphelendiğiniz e-postayı açmadan silmek:* Çoğu virüs, bir eki açtığınızda veya bir e-posta içindeki bir bağlantıyı tıkladığınızda etkinleşmektedir. Ancak bazen yalnızca şüpheli görünen bir e-posta açarak virüs kapmak mümkün olmaktadır. Bu nedenle şüpheli görünen maillerin açılmadan silinmesi önerilmektedir.
- *Göndereni manuel olarak engellemek*: E-posta istemciniz manuel olarak bir blok oluşturmanıza izin veriyorsa bunun yapılması ve gönderenin engellenenler listesine eklenmesi önerilmektedir.
- *Fazladan bir güvenlik hattı kullanmak*: Spam klasörünün parçası olmayan meşru görünümlü bir e-postaya rastlama ve bu durumda yapılmaması gereken bir şey yapma ihtimalinin hep var olması nedeniyle, e-posta kutusunu izlemeye yardımcı bir virüsten korunma yazılımı kullanılması önerilmektedir.

Sosyal Medya Pazarlaması

Sosyal medya, kullanıcılar arasında sosyal etkileşimi teşvik eden ve onlara çevrimiçi bilgi havuzunu birlikte oluşturmaya, bulmaya, paylaşmaya ve değerlendirmeye izin veren bir çevrimiçi hizmetler koleksiyonudur (Chua ve Banerjee, 2013: 239). Bireysel ve profesyonel anlamda, sosyal medya kullanıcılarının sayısının giderek arttığı (Huberman vd., 2008: 2) ve sosyal medya platformlarının (Facebook, LinkedIn ve Twitter vb.), birbirlerini takip

etmek ve ticari işlemlere katılmak için bu ağları kullanan pek çok üyeye ev sahipliği yaptığı görülmektedir (Kleinberg, 2008: 66). Her tür sosyal medya, kişinin kendisini ve ürünlerini, ilgilenebilecek dinamik topluluklara ve bireylere sunma fırsatı sunmaktadır (Roberts ve Kraynak, 2008: 149).

Sosyal medya, günümüz modern işletmeleri için yaygın kullanılan, hızlı ve dinamik bir iletişim aracıdır (Xiong vd., 2018: 623). Sosyal medyanın gelişimi, geleneksel medyanın nispeten daha statik bilgi yayma kanallarını dinamik bir yapıya dönüştürmekte, işletmelerin tüketicilerle ilişkilerinde, ürünleri tanıtmak ve tüketici sorularını yanıtlamak suretiyle çift yönlü bir iletişim süreci geliştirilmektedir (Hanna vd., 2011: 271; Shin vd., 2015: 215). Sosyal medyanın; (1) sosyal sermaye, (2) müşterilerin açıklanmış tercihleri (3) sosyal pazarlama ve (4) sosyal kurumsal ağ gibi kanallar ile işletmenin finansal, operasyonel ve kurumsal sosyal performansını etkilediği belirlemiştir (Paniagua ve Sapena, 2014: 719).

Sosyal medya pazarlaması, işletmelerin ürünlerini tanıtmak için sosyal medya kanallarını kullanarak hedeflenen müşterilere kolayca ulaşabildiği yeni bir trend ve hızla büyüyen bir yoldur. Bu tür bir pazarlama, internet tabanlı tanıtım (e-posta bültenleri ve online reklam) stratejilerini tamamlayan çevrimiçi pazarlama etkinliklerinin bir alt kümesi olarak düşünülmektedir. Sosyal medya başarılı bir etkileşim ve iki yönlü bir alışveriş taahhüt etmektedir. Daha fazla satışa dönüşebilecek uzun vadeli ilişkiler kurmaya odaklanan bu güç, sosyal ağlar yoluyla geleneksel pazarlamanın doğasını değiştirmektedir. Her bir ağı izlemek, yorumları ve soruları yanıtlamak, müşterinin değerli gördüğü ürün bilgilerini göndermekle başlayan önemli bir zaman yatırımıdır (Barefoot ve Szabo 2010: 13; Nadaraja ve Yazdanifard, 2013: 2-6).

Sosyal medya pazarlaması, markaların müşterilerle, müşterilerin markalarla ve belki de en önemlisi Web 2.0' dan önce imkânsız olan müşterilerin birbirleriyle konuştuğu çok yönlü diyaloglardan oluşmaktadır. Kullanıcı tarafından oluşturulan ve kullanıcı katılımına bağlı sosyallik, sosyal

medya pazarlamasının gerçekleştirilebilmesi için temel gereksinimlerdendir. Çevrimiçi bir topluluktaki içerik ve bağlantıların çoğu marka tarafından değil, kullanıcılar tarafından oluşturulmaktadır (Awareness, 2008). Bireylerin kendi mal veya hizmetlerini çevrimiçi sosyal kanallar aracılığıyla sunarak, geniş bir toplulukta geleneksel reklam ile mümkün olmayan bir iletişim kurmalarına ve o topluluğu dinlemelerine olanak tanıyan bir süreçtir (Weinberg, 2009: 3).

Sosyal medya, teknik terimleri kullanarak ürünler, markalar, hizmetler ve sorunlar hakkında birbirlerini eğitmek isteyen tüketiciler tarafından oluşturulan içeriklerin, "yayınlamasına", "etiketlemesine", "bloglanmasına" olanak tanıyan çeşitli uygulamalar içermektedir. Bu yayılan ve kullanılan çevrimiçi bilgiler, yeni tür bir kaynak konumuna gelmektedir (Xiang ve Gretzel, 2010: 180). Nielsen BuzzMetrics araştırmasına göre, ürün ve hizmetlerle ilgili olarak tüketicilerin %60'ından fazlası, Red Bridge Marketing'e (2008) göre küresel tüketicilerin %78'i diğer tüketicilerin yorumlarına ve önerilerine inanmakta ve güvenmektedir (Akar ve Topçu, 2011: 42). Cone Inc. (2008), araştırmasına göre ise sosyal medya kullanıcılarının %93'ü satın aldıkları markaların sosyal medyada yer alması gerektiğine inandıklarını belirtmiştir. Bu doğrultuda pazarlamacıların sosyal medyaya giderek daha fazla ilgi duymaya başladığı ortaya konmuştur. Ayrıca katılımcıların %85' i işletmelerin müşterileriyle sosyal medya aracılığıyla etkileşime girmesi gerektiği görüşünü paylaşmış, %56'sı bir sosyal medya ortamında kendileriyle etkileşime girebildiklerinde hem işletme ile daha güçlü bir bağlantı kurabildiklerini hem de işletmeden daha iyi hizmet aldıklarını ifade etmiştir (Cone Inc., 2008). Pazarlama halkla ilişkilerinin yeni ve en iyi arkadaşı olan sosyal medya, pazarlamacıları hedef kitleleriyle buluşturacak *günün aracı* haline gelmektedir. Bir sosyal ağda yer almak isteyen işletmeler çabalarını, ilginç bir içerik oluşturmaya, bir topluluğu teşvik etmeye ve müşterileriyle daha doğrudan, rahat ve kişisel bir etkileşim kurmaya odaklamalıdır. Sosyal medyanın iletişime getirdiği değişimi

tüketiciler benimsenmekte ve takdir etmektedir (Papasolomou ve Melanthiou, 2012: 325).

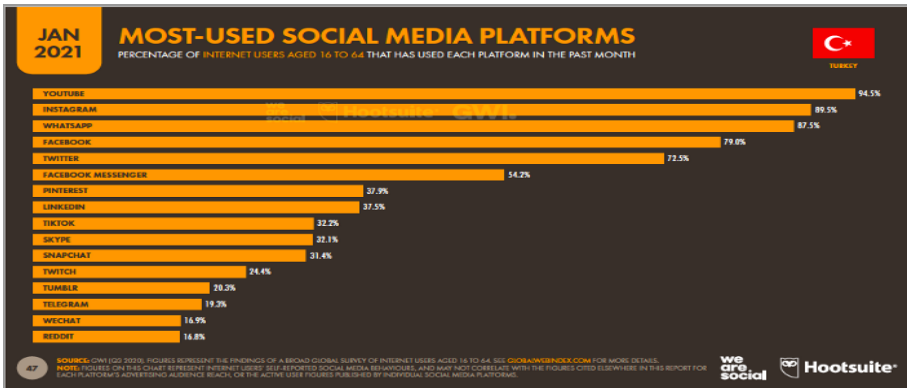
Sosyal medya platformlarını kullanan tüketiciler, markalar ve ürünler (mal veya hizmet) hakkında çevrimiçi bilgiler sunabilmekte bunları düzenleyebilmekte ve paylaşabilmektedir. Ayrıca, sundukları bilgileri yönlendiren çevrimiçi topluluklar ve ağlar da oluşturabilmektedir. Tüketicilerin bu aktarımı işletmenin verdiği mesajdan daha güvenilir olarak algılanabilmektedir. Bu nedenle, akran görüşü satın alma davranışı üzerinde büyük bir etki haline gelmektedir.

Sosyal Medya Pazarlamasında Hile

Sosyal medya pek çok açıdan bireylerin kullanım alanında yer almaktadır. Haber, eğlence, alışveriş, sohbet, ticaret, iş ağı kurma veya katılma gibi çeşitli amaçlarla gündelik hayatın vazgeçilmez bir iletişim unsuru haline gelmektedir. Wİ-Fi' nin temel fizyolojik ihtiyaçlar arasına girdiği günümüz dijitalleşme çağında bireylerin tüm kararlarında internet ve sosyal medya platformlarında yapılan yorumların, beğenilerin, takipleşmelerin ilk araştırma birimi haline geldiği görülmektedir.

We Are Social ve Hootsuit verilerine göre, Türkiye'de nüfusun %77,7'si aktif olarak internet kullanırken, nüfusun yaklaşık %70,8'i sosyal medyada yer almaktadır. Facebook, Twitter, Instagram ve Youtube gibi sosyal medya platformları 2021 yılı raporlarında en çok kullanılan siteler olarak öne çıkmaktadır. Türkiye'de 60 milyon sosyal medya kullanıcısının 16-64 yaş aralığında olduğu, en fazla kullanılan sosyal medya platformları listesinde zirvede Youtube yer aldığı görülmektedir. Instagram ve Whatsapp ilk üçte yer alırken dünyada birinci sırada yer alan Facebook, Türkiye'de 4. sırada bulunmaktadır (https://wearesocial.com/digit.., Erişim Tarihi: 27. 05. 2021).

Şekil 3. Türkiye 'De Kullanılan Sosyal Medya Platformları



Kaynak: https://wearesocial.com/digital-2021 , Erişim Tarihi: 27.05.2021

Bu veriler giderek büyüyen sosyal medya toplulukları olduğunu göstermektedir. Ancak sosyal medyanın popülerliğinin artması beraberinde bazı riskleri de getirmektedir. Bu sanal gücün içinde her daim doğru amaçlar edinen hesapların veya uygulamaların olduğunu düşünmek pek de mümkün olmamaktadır. Sosyal medyada mal veya hizmet sunan bireysel veya işletme hesaplarının sayısı her geçen gün artmaktadır. Ancak kötü niyetli kullanıcılar bu popüler dijital kültürü hile, sahtekârlık ve kullanıcıları çeşitli yöntemler kullanarak aldatma amaçlarıyla kullanmaya başlamaktadır.

Sosyal medya pazarlaması, markasını, mal veya hizmetlerini tanıtmak için sosyal medyayı kullanan işletmeler için güven, gizlilik ve veri güvenliği sorunlarını da beraberinde getirmektedir. Hile ve sahtekârlık karşısında önlem alması gereken ilk merciinin işletme olduğundan hareketle işletmelerin bu konuların farkında olması ve kişisel veri toplama, kullanma ve bakımıyla ilgili sorumluluklarını üstlenerek riskleri en aza indirmek için uygun önlemleri almaları gerekmektedir (Nadaraja ve Yazdanifard, 2013: 6). Güven, özellikle de işlemsel güvenlik ve mahremiyetin benzersiz boyutları (Hoffman vd., 1999: 133), sosyal medya pazarlamacılarına müşteri sadakati oluşturmada kritik bir rol atfetmektedir. Ratnasingham, araştırmasında çevrimiçi kredi kartı dolandırıcılığı korkusunun, müşterilerin daha kapsamlı online alışveriş yapmasının önündeki ana engellerden biri olduğunu

göstermiştir (Nadaraja ve Yazdanifard, 2013: 6). Genel olarak online alışverişte ürünü hissedemez, koklayamaz veya dokunamazsınız. Bu nedenle güvenlikle yakından ilgili olan güven, çevrimiçi satın alma sürecinde çok önemli bir faktördür (Steinman ve Hawkins, 2010). Güvene yönelik algılar potansiyel müşterilerin internet üzerinden iş yapmasını engellemektedir. İnternette güveni geliştirmekte, marka güveni ön plana çıkmaktadır ve belirsizliği azaltmaktadır. İnternetin dürüst olmayan ve güvenilmez bir pazar olduğu yönündeki algıların üstesinden gelmekte güvenin tutumsal bir bileşeni olan sadakatin ve marka güveninin, bazı dezavantajların üstesinden gelmeye yardımcı olabileceği düşünülmektedir. Bu amaçla markaların güven oluşturmaya yönelik bir araç olarak "üçüncü taraf onayı" uygulamasına yöneldiği görülmektedir (Gommans vd., 2001: 50). Facebook ve Twitter gibi sosyal medya platformları genellikle kişisel verilerle ilgili olarak tüketici verilerini ve üçüncü taraf davranışlarını yöneten kendi gizlilik politikalarına sahiptir. Kendi bloglarını veya diğer sosyal medya platformlarını yöneten şirketler, şirketin veri toplama, kullanma ve depolama uygulamalarını ve üçüncü tarafların gizlilik ve veri güvenliği ile ilgili sorumluluklarını açıklayan kapsamlı politikaları da sürdürmektedir (Steinman ve Hawkins, 2010: 4-8). Mahremiyet endişeleri sosyal medya pazarlaması için bir halkla ilişkiler fiyaskosuna neden olarak marka imajı erozyonuna yol açmaktadır (Advertising Age, 2000).

Yeni tip koronavirüsle birlikte tüketicilerin online alışverişe yöneldiği ve bu süreçte sosyal medya platformlarındaki satışlarda hilekâr ve aldatıcı uygulamaların yarı yarıya arttığı görülmektedir (https://www.aa.com.tr/tr/t.., Erişim Tarihi: 30.05.2021).

Günlük hayatımızın bir parçası haline gelen sosyal medya ile çevrimiçi gizlilik ve güvenlik sorunu, gün geçtikçe büyük bir sorun haline gelmektedir. Sosyal medyanın pek çok kullanım alanının olması, riskleri de beraberinde getirmektedir. Sosyalleşmek, etkileşim kurmak yanında, para kazanmak için bağışık bir yer haline gelen sosyal medyada hileli satışlar ve sahtekârlık kapsamlı bir şekilde artmaktadır. Sosyal medya dolandırıcılığı farklı pek çok

yöntemle yapılmakla beraber, örneğin; "Usame Bin Ladin'in ölüm görüntülerinin yer aldığı videoyu gördünüz mü? İzlemek için Flash oynatıcınızın versiyonunu yükseltin" gibi bir başlıkla sahte hesaptan yapılan bir öneri cümlesi yöntemiyle, bu görüntüleri izlemeye meraklı hedef kitlenin uygulama güncellemesi yapması istenerek bu güncelleme yapıldığı takdirde bilgisayara virüs bulaştırmak ve tüm şifreleri ele geçirmek hedeflenmektedir(https://tusbeyinli.com/2014/09/son-yillarin-10-buyuk-dijita.., Erişim Tarihi: 25.05.2021).

Sosyal medya platformlarında yaygın olarak kullanılan aldatma ve dolandırıcılık senaryoları şöyle sıralanmaktadır (Woodburn, 2020);

Sahte ürün: Facebook veya diğer sosyal medya hesabından orijinal ürünleri düşük bir fiyatla satma vaadi sunup daha sonra sahte bir ürün satmak. Gerçeği ile ayırt edilmesi zor ürünleri uygun fiyatlarla sahte sosyal medya hesaplarından satışa sunup, ödemenin bir bölümünü aldıktan sonra iletişimi kapatması (Şekil 4) ya da ödemesini aldığı halde ürünlerini göndermeyip kişileri engellemek ya da eksik, yanlış, hatalı ürün göndermek.

Şekil 4. Sahte Ürüne İlişkin Hile Örneği



Kaynak: https://www.hurriyet.com.tr/ekono....., Erişim tarihi: 01.06.2021.

Acil durum bildirimi: Facebook Messenger veya direkt mesaj üzerinden hesabınızda ekli olan birisinin (aile üyesi, arkadaş, tanıdık) acil olarak mali yardım talebinde bulunduğu izlenimi vererek para istemek ya da gönderilen linke ilk tıklayanın hediye kazanma fırsatı olduğunu söylemek.

Piyango/Çekiliş hilesi: Bir piyangonun veya çekilişin kazananları arasında olduğunuz gibi mali kazanç ya da hediye vaatleri ile kişisel bilgiler veya giriş ücreti isteyen bir web sitesine yönlendirmek (Şekil 5).

Şekil 5. Çekiliş Yöntemine İlişkin Hile Örneği



Kaynak: https://www.milliyet.com.tr/gu..., Erişim tarihi: 01.06.2021.

Ünlü dolandırıcılığı: Bir ünlünün sahte fotoğraflarının büyük miktarlarda nakit veya lüks eşyalarla yayınlanarak, bilgilerini verene ve / veya bir giriş ücreti ödeyene bu hediyeyi kazanma şansı vaat etmek.

İş Fırsatı sunma hilesi: Yanıltıcı veya sahte iş ilanlarını vererek kişisel bilgiler veya para talep etmek.

Sahte Influencer sponsorluğu: Reklam teklifi sunan gerçek bir marka gibi davranarak takipçi sayısı yükselişte olan Instagram kullanıcılarını banka bilgilerini almak için kandırmaya çalışmak.

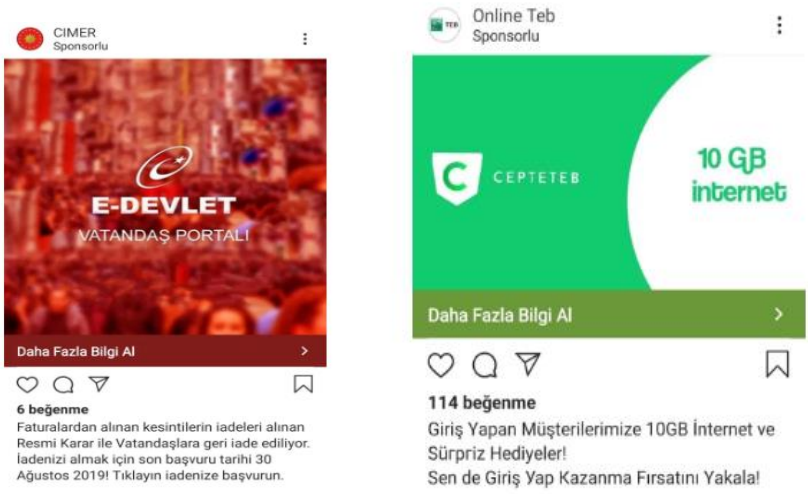
Erişim jetonu hırsızlığı: Gerçek bir uygulamadan geliyormuş gibi bir bağlantı paylaşılarak ve sosyal medya hesabınıza veya sayfanıza erişim isteğinde bulunmak.

Romantik dolandırıcılık (kedi balıkçılığı): Sahte fotoğraflar ile başkalarını cezbetmek. Genellikle uçuş veya vize parası alma umuduyla internet üzerinden ilişkiler kurmak için tanımadıkları insanlara romantik mesajlar atmak.

Sosyal medyada sponsorlu reklam dolandırıcılığı: İnternet reklamcılığı 1994 yılında Hot Wire dergisinin web sitesinde AT&T şirketinin ilk banner reklamıyla gündeme gelmiştir (Zeff ve Aronson, 1997: 17). İnternet reklamcılığının dijitalleşme yolculuğunun en önemli durağı olan sosyal medya, iki yönlü etkileşime izin veren bir işlevin yerine getirilmesine yardımcı olmuş (Zarrella, 2009: 1) ve bugün farklı ilgi alanlarına sahip kişilere reklam gösterilmesini mümkün kılan bir internet reklam ortamına dönüşmüştür. Sosyal medya kullanıcıları, bir reklam gönderisine tıklamanın ötesinde beğenme, paylaşma veya yorum gibi reklam yayınlarıyla etkileşime girmektedir. Bu nedenle sosyal medya, bir internet reklam platformu olmaktan çok kişiselleştirilmiş reklam ortamı olarak adlandırılmaktadır. Günümüzde işletmeler, felsefelerini iletmek ve potansiyel müşterilere ulaşmak için sosyal medya pazarlamasını kullanmakta ve reklam kampanyalarını koordine etmektedir (Jang vd., 2013: 7493). Facebook, Twitter, Linkedin ve Instagram gibi reklam verebileceğiniz en popüler sosyal medya araçları arasında Instagram, olağanüstü e-ticaret alanına dönüşerek, e-ticaret konusunda yüksek gelir elde etmeye vesile olan ve reklamcılık açısından en cazibeli ve en çok kullanılan platform haline dönüşmüştür. Instagram reklamcılığı iki şekilde yapılmaktadır. Bunlar, sponsorlu (ücretli) gönderiler ve Influencer (etkileyici) adı verilen çok sayıda takipçisi olan kullanıcılarla ya da ünlülerle işbirliği (sponsorluk) şeklinde olmaktadır. Instagram'da reklamı yapılan gönderiler analiz edildiğinde, büyük ölçekli işletmelerin etkileyicilerle işbirliği yaptığı, düşük bütçeli küçük ölçekli işletmelerin (küçük şirketler veya mağazalar) sponsorlu reklamı kullanmayı tercih ettiği görülmektedir (Çetintürk ve Poyraz, 2019: 143). Ancak yalnızca gerçek amaçlarla sponsorlu reklamcılık faaliyetleri yürütülmemektedir. Sponsorlu reklamlar yoluyla aldatma adına son günlerde karşımıza bankalar,

Cimer, e-devlet gibi önemli kurumların reklamlarının da çıktığı görülmektedir. Profesyonel olarak hazırlanan görseller görünüşte hiçbir şüphe uyandırmasa da bu reklamlar ve sayfalar yanıltıcı niyetinde bulunan sayfalar olabilmektedir (Şekil 6).

Şekil 6. Sponsorlu Reklamlara Yönelik Hile Örneği



Kaynak: Avcı, 2019.

Bu sayfalarda "Daha fazla bilgi al" butonuna tıklandığında kredi kartı bilgisi istenmekte, hatta bu süreçte oldukça profesyonel sistemler kullanılarak telefonunuza kısa mesaj gönderilip kod bile istenmektedir. Kişi ödeme yapmak için bu bilgilerin istenmediğini bilse bile oldukça güvenilir görünen bu uygulama ile dolandırılması söz konusu olmaktadır. Bu tarz reklamların gerçek olup olmadığını anlamak için birkaç noktada dikkatli olmak gerekmektedir (Avcı, 2019);

- Özellikle paylaşımın görsel kalite, bütünlüğüne ve içeriğine dikkat edilmelidir.
- "Daha fazla bilgi al" butonuna tıkladıktan sonra (buton yazıları değişebilir) üstte bulunan linki kontrol edilmelidir.

- Kredi kartı bilgileri istediğinde asıl kurum ile iletişime geçip bilgi alınmalıdır.
- Son olarak böyle bir sahtekârlık faaliyeti ile karşılaşıldığında mutlaka şikâyet edilmesi gerektiği de unutulmamalıdır. Reklam veya paylaşım hangi kurum veya kuruluş adına yapılıyorsa onaylanmış sayfalarını yorum kısmına etiketleyerek yapılabilmektedir (Şekil 7).

Şekil 7. Şikâyet Örneği



Kaynak: Avcı, 2019.

2020'nin ilk altı ayında insanların sosyal medyada başlayan sahtekârlık ve dolandırıcılık faaliyetlerinde 117 milyon dolar gibi rekor yükseklikte para kaybettikleri belirlenmiştir. Teslimat yapmayan online satıcılarla, aşk dolandırıcıları ve sahte mali yardım teklifleri için para isteyenlerle, salgın nedeniyle hibe ve diğer mali yardımlar sunuyormuş gibi görünen ancak gerçekte para, kişisel bilgi veya her ikisini de almaya çalışan sosyal medya sahtekârlarıyla karşılaşmıştır (https://www.consumer.ftc.gov/blog.., Erişim tarihi: 01.06.2021).

Sosyal medyada maruz kalacağınız sahtekârlıklara karşı alınacak önlemlerin başında size arkadaşlık isteği gönderen ya da mesaj ile ulaşan kişilerin gerçekten sizin arkadaşınız ya da tanıdığınız olduğunu doğrulamak

gelmektedir. Bankacılık ve finansal bilgilerinizi verirken dikkatli olmak gerekmektedir. Kopyalanması zor olan şifrelerin oluşturulması ve hatta virüs, solucan, Truva atı virüslerine ve diğer tehditlere karşı korumak için bilgisayarınıza, akıllı telefonunuza ve tabletinize sıkı bir kötü amaçlı yazılımdan koruma çözümü yüklemekte bir çözüm olarak sunulmaktadır (https://www.kaspersky.com/resource-ce.., Erişim tarihi: 25.05.2021).

Dijital Pazarlama Hilelerinden Korunma

Tüketicilerin dijital pazarlamada karşı karşıya kaldığı sayısız hileden korunmaları için aşağıda verilen önlemleri göz önünde bulundurmaları gerekir (American Bankers Association, 2016):

- Bilgisayarların ve mobil cihazların güncel tutulması (en son güvenlik yazılımına, web tarayıcısına ve işletim sistemine sahip olmak virüslere, kötü amaçlı yazılımlara ve diğer çevrimiçi tehditlere karşı en iyi savunmadır),
- Güçlü parolalar belirlenmesi (güçlü bir parola en az sekiz karakter uzunluğundadır, büyük ve küçük harfler, sayılar ve özel karakterlerin bir karışımını içerir),
- Kimlik avı hilelerine dikkat edilmesi (kullanıcıları özel hesap veya giriş bilgilerini ifşa etmeleri için sahte e-postalar ve web siteleri kullanılmaktadır. Bu nedenle aşina olunmayan kaynaklardan gelen bağlantılara, eklere veya açılır ekranlara tıklanmaması),
- Kişisel bilgilerin paylaşılmaması (bilgisayar korsanları, parolaları bulmak ve parola sıfırlama araçlarında bu güvenlik sorularını yanıtlamak için sosyal medya profillerini kullanabilir. Gizlilik ayarlarının kilitlenip, doğum günleri, adresler, anne kızlık soyadı gibi şeyleri paylaşmaktan kaçınılması),
- İnternet bağlantısının güvenli hale getirilmesi (ev kablosuz ağının her zaman bir parola ile korunması, herkese açık Wi-Fi ağlarına

bağlanırken, bu ağ üzerinden hangi bilgilerin gönderildiğine dikkatli edilmesi),

- Güvenli çevrimiçi alışveriş yapılması (çevrimiçi alışveriş yapmadan önce, web sitesinin güvenli teknoloji kullandığından emin olunması, ödeme ekranındayken web adresinin https ile başladığının doğrulanması, ayrıca sayfada küçük bir kilitli asma kilit simgesinin görünüp görünmediğinin kontrol edilmesi),
- Sitenin gizlilik politikalarının okunması (uzun ve karmaşık olsa da, gizlilik politikalarının sitenin topladığı kişisel bilgileri nasıl koruduğunu söylemesi).

Firmaların ise dijital pazarlamada karşılaştıkları hilelerden korunmaları için aşağıda verilen hususları göz önünde bulundurmaları gerekmektedir (Bross, 2021):

- Kibarca referans istenmesi ve bunların takip edilmesi (çalışılacak firma hakkında referanslar istenmesi),
- Düzenli raporlar istenmesi (dijital pazarlama ajansından yaptıkları işle ilgili haftalık düzenli raporlar göndermesinin gerekmesi),
- Araştırma, araştırma, araştırma (en iyi olduklarına dair sözlerine inanılmaması, onlarla iletişime geçmeden önce araştırılması, birkaç hızlı Google aramasıyla, firmanın köklü mü yoksa dolandırıcı mı olduğu hakkında iyi bir fikir edinilmesi),
- İş geçmişini doğrulamak için Linkedin'in kullanılması (çok fazla referansı olmayan yeni bir firmanın, o firmanın bireysel ekip üyelerinin, çalışma geçmişini her zaman Linkedin üzerinden araştırılması),
- Sezgiye güvenilmesi (dolandırıldım hissi varsa buna inanılması, bir firmayla çalışmayı taahhüt etmeden önce, işlerin sarpa sarması ihtimaline karşı bir "acil çıkış stratejisi" olduğundan emin olunması).

Sonuç

Dijital teknolojilerde yaşanan gelişmeler birçok yeniliği ve değişimi de beraberinde getirmektedir. Bu teknolojilerin iş hayatında, kişilerin günlük yaşamında ve daha birçok alanda yoğun şekilde kullanıldığı göz ardı edilemez bir gerçektir. Dolayısıyla bu gelişmeler dijitalleşme kavramını da hayatın merkezine yerleştirmektedir. Zaman, mekân ve hız gibi daha birçok imkân sağlayan dijitalleşme, işletmelerin ve tüketicilerin öncelikleri arasında yerini almaktadır. Dijitalleşmenin sağladığı yararlar göz önünde bulundurulduğunda işletmelerin tüketicilerine ulaşması ve tüketicilerinde işletmelerden haberdar olabilmesi için dijital pazarlama kanalları yoğun bir şekilde kullanılmaktadır. Dijital pazarlama, bu dijital araçlar yoluyla yapılan her türlü pazarlama faaliyetini içine alan geniş bir kavram olarak ortaya çıkmaktadır.

Çalışmada dijital pazarlama türlerinden olan mobil pazarlama, arama motoru pazarlaması, e-posta pazarlaması ve sosyal medya pazarlaması kapsamlı bir şekilde ele alınmış, bu dijital pazarlama kanallarından işletmelere ve tüketicilere ulaşarak yapılan hile girişimleri ve hile türleri ayrıntılı şekilde açıklanmaya çalışılmıştır.

Dijital dünyada hilenin verdiği zararların bilincinde olup, devam eden yaygın dijital pazarlama hilelerinin ne kadar farkında olunursa, hilekârların tuzağına düşme olasılığı da o oranda azalmaktadır. Kullanılan dijital pazarlama hizmetlerinin iyi tanınması ve gerekli önlemlerin alınması ile tüketici ve firmaların zararlarının da en aza ineceği anlamına gelmektedir.

Kaynakça

A Manager's Guide to Harnessing Technology (2010). https://open.lib.umn.edu/informationsystems/chapter/14-9-search-engines-ad-networks-and-fraud/, Erişim Tarihi: 30.05.2021.

Advertising Age. (2000). Crisis RX for Double Click, https://adage.com/article/viewpoint/crisis-rx-doubleclick/59249 , Erişim Tarihi: 25.05.2021.

Akar, E. ve Topçu, B. (2011). "An Examination of the Factors Influencing Consumers' Attitudes Toward Social Media Marketing", *Journal of Internet Commerce*, 10 (1), 35-67.

Akomea-Frimpong, I., Andoh, C., Akomea-Frimpong, A. ve Dwomoh-Okudzeto, Y. (2019). "Control Of Fraud On Mobile Money Services In Ghana: An Exploratory Study", *Journal of Money Laundering Control*, 22(2), 300-317.

Alkhalil, Z., Hewage, C., Nawaf, L. and Khan, I. (2021). "Phishing Attacks: Recent Comprehensive Study and a New Anatomy", *Frontiers in Computer Science*, 3, 1-23.

American Bankers Association (2016). *Seven Tips to Avoid Online Fraud,* https://www.centralbank.net/personal/security/security-news/seven-tips-to-avoid-online-fraud/, Erişim Tarihi: 25.06.2021).

Avcı, U. (2019). Yeni Nesil Sosyal Medya Dolandırıcılığı, https://blog.avciufuk.com/yeni-nesil-sosyal-medya-dolandiriciligi.html, Erişim Tarihi: 27.05.2021.

Awareness (2008). Social Media Marketing: Integrating Social Media in Your Marketing Mix. http://www.awarenessnetworks.com/resources/Integrating-SocialMedia.pdf , Erişim Tarihi: 25.05.2021.

Barefoot, D. and J. Szabo. (2010). *Friends With Benefits: A Social Media-Marketing Handbook.* San Francisco: No Starch Press.

Benari, N. (2019). 9 Common Types of Mobile Fraud, https://blog.securedtouch.com/most-common-types-of-mobile-fraud, Erişim Tarihi: 30.05.2021.

Boughton, S. B. (2004). "Search Engine Marketing", *Perspectives in Business*, 29-33.

Bross, C. (2021). Avoid These Digital Marketing Scams, https://www.evereffect.com/blog/avoid-these-digital-marketing-scams/, Erişim Tarihi: 25.06.2021

Carmen, P. and Pop Nicolae Al. (2010). "Email Marketing Campaigns: The Easiest Path From Organizations To Consumers - An Exploratory Assessmen", *Annals of Faculty of Economics*, 1(1), 737-742.

Chua, A. Y. K. and Banerjee, S. (2013). "Customer Knowledge Management Via Social Media: The Case Of Starbucks", *Journal of Knowledge Management*, 17(2), 237-249.

Cone Inc. (2008). Cone Finds That Americans Expect Companies to Have A Presence in Social Media. https://www.conecomm.com/news-blog/cone-finds-that-americans-expect-companies-to-have-a-presence-in-social-media , Erişim Tarihi: 25.05.2021.

Çetintürk, N. and Poyraz, E. (2019). *Sponsored Ads in Instagram as a Marketplace and the Concept of Social Affiliation: Differing Outlook of Contemporary Advertising,* Differing Outlook of Contemporary Advertising Peter Lang, 139-158.

Dou, W., Lim, K.H., Su, C., Zhou, N. and Cui, N. (2010). "Brand Positioning Strategy Using Search Engine Marketing", *MIS Quarterly*, 34(2) , 261-279.

Dou, Y., Li, W., Liu, Z., Dong, Z., Luo, J. and Yu, P. S. (2019). *Uncovering Download Fraud Activities in Mobile App Markets,* International Conference on Advances in Social Networks Analysis and Mining, 671-678.

Fariborzi, E. and Zahedifard M. (2012). "E-mail Marketing: Advantages, Disadvantages and Improving Techniques", *International Journal of e-Education, e-Business, e-Management and e-Learning,* 2 (3), 232-236.

Gartner (2006). Number of Phishing E-Mails Sent to U.S. Adults Nearly Doubles in Just Two Years, http://www.gartner.com/it/page.jsp?id=498245 , Erişim Tarihi: 25.05.2021.

Gommans, M., Krishnan, K.S. and Scheffold, K.B. (2001). "From Brand Loyalty to E-Loyalty: A Conceptual Framework", *Journal of Economic and Social Research,* 3(1), 43-58.

Gordon, M. and Pathak, P. (1999). "Finding Information on the World Wide Web: The Retrieval Effectiveness of Search Engines", *Information Processing and Management*, 35, 141-180.

Haghirian, P., Madlberger, M. and Tanuskova, A. (2005). "Increasing Advertising Value of Mobile Marketing - An Empirical Study of Antecedents", *Proceedings of the 38th Hawaii International Conference on System Sciences*, 1-10.

Hanna, R., Rohm, A. and Crittenden, V. L. (2011). "We're All Connected: The Power of the Social Media Ecosystem", *Business Horizons*, 54(3), 265-273.

Harrison, B., Svetieva, E. and Vishwanath, A. (2016). "Individual Processing of Phishing Emails: How Attention and Elaboration Protect Against Phishing". *Online Information Review,* 40(2), 265-281.

Hofacker, C. F., Ruyter K., Lurie, N. H., Manchanda, P. and Donaldson, J.(2016). "Gamification and Mobile Marketing Effectiveness", J*ournal of Interactive Marketing*, 34, 25-36.

Hoffman, D., Novak, T. and Peralta, M. (1999). "Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web", *Information Society*, 15 (2). 129-140.

Hoonakker, P., Carayon, P. and Bornø, N. (2009*). Spamming, Spoofing and Phishing E-Mail Security: A Survey Among End-Users,* 17th World Congress on Ergonomics.

http://accan.org.au/talking-telco/your-digital-safety/avoiding-phone-and-internet-scams, Erişim tarihi: 03.06.2021.

https://tusbeyinli.com/2014/09/son-yillarin-10-buyuk-dijital-dolandiricilik-girisimi.html

https://wearesocial.com/digital-2021

https://www.aa.com.tr/tr/turkiye/pandemi-doneminde-sosyal-medya-uzerinden-dolandiricilik-artti/2101469

https://www.adjust.com/glossary/mobile-ad-fraud/, Erişim Tarihi: 02.06.2021.

https://www.consumer.ftc.gov/blog/2020/10/scams-start-social-media

https://www.hurriyet.com.tr/ekonomi/instagramda-dolandiricilarin-oltasina-takilmayin-40800255

https://www.kaspersky.com/resource-center/preemptive-safety/facebook

https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips

https://www.legalmatch.com/law-library/article/search-engine-phishing.html, Erişim Tarihi: 30.05.2021.

https://www.milliyet.com.tr/gundem/dolandiricilarin-tuzagina-dusmeyin-6339828

https://www.purelybranded.com/notes/top-10-seo-scams-and-how-to-avoid-getting-burned/, Erişim Tarihi: 30.05.2021.

https://www.yenidonem.com.tr/haber/bursa-da-dev-pandemi-vurgunu-mesaj-gonderip-tuzaga-dusurmusler-101380.html, Erişim Tarihi: 04.06.2021.

Huberman, B. A., Romero, D. M. and Wu, F. (2008). "Social Networks That Matter: Twitter Under The Microscope", *First Monday*, 14, 1-5.

Hudák, M., Kianičková, E. and Madleňák, R. (2017). "The Importance of E-Mail Marketing In E-Commerce", *Procedia Engineering,* 192, 342-347.

Hui, Z, Shigang, Q., Jinhua, L. and Jianli, C. (2012). *Study on Website Search Engine Optimization,* International Conference on Computer Science and Service System, 930-933.

Ilgar, G. (2020), Dünyadaki 10 En İyi Arama Motoru 2020, https://seowpclub.com/dunyadaki-10-en-iyi-arama-motoru-2020/, Erişim Tarihi: 30.05.2021.

Jain, A. (2013). "The Role and Importance of Search Engine and Search Engine Optimization", *IJETTCS,* 2(3), 99-102.

Jang, H. J., Sim, J., Lee, Y. and Kwon, O. (2013)."Deep Sentiment Analysis: Mining the Causality Between Personality-Value-Attitude for Analyzing Business Ads in Social Media", *Expert Systems with Applications*, 40(18), 7492-7503.

Kanich, K. C., Levchenko, K., Enright, B., Voelker, G. M. and Paxson, V. (2008). *Spamalytics: An Empirical Analysis of Spam Marketing Conversion*. 15th ACM Conference On Computer And Communications Security.

Kleinberg, J. (2008). "The Convergence of Social and Technological Networks", *Communications Of The ACM*, 51(11), 66-72.

Kumar, A. (2013). "International Journal of Emerging Technology and Advanced Engineering", *International Journal of Emerging Technology and Advanced Engineering,* 3(3), 123-128.

Mladenow, A., Novak, N. M. and Strauss, C. (2015). "Online Ad-fraud in Search Engine Advertising Campaigns Prevention, Detection and Damage Limitation", *Information and Communication Technology*, 109-118.

Nadaraja, R. and Yazdanifard, R. (2013). "Social Media Marketing: Advantages And Disadvantages", *Center of Southern New Hempshire University*, 1-10.

Olbrich, R. and Schultz, C. D. (2008). "Search Engine Marketing and Click Fraud", *Department of Business Administration and Economics*, 11, 1-44.

Onaifo, D. and Rasmussen, D. (2012). "Increasing Libraries' Content Findability on the Web With Search Engine Optimization", *Emerald*, 31(1), 87-108.

Paniagua, J. and Sapena, J. (2014). "Business Performance and Social Media: Love or Hate?" , *Business Horizons*, 57(6), 719- 728.

Papasolomou, I. and Melanthiou, Y. (2012). "Social Media: Marketing Public Relations' New Best Friend", *Journal of Promotion Management*, 18(3), 319-328.

Paraskevas, A., Katsogridakis, I. , Law, R., and Buhalis, D. (2011). "Search Engine Marketing: Transforming Search Engines into Hotel Distribution Channels", *Cornell Hospitality Quarterly*, 52(2), 200-208.

Patil Swati, P., Pawar, B.V. and Patil Ajay, S. (2013). "Search Engine Optimization: A Study", *Research Journal of Computer and Information Technology Sciences*, 1(1), 10-13.

Persaud, A. and Azhar, I. (2012). "Innovative Mobile Marketing Via Smartphones, Are Consumers Ready?", *Marketing Intelligence & Planning*, 30(4), 418-443.

Ranga, M. and Ranga, S. (2014). "Search Engine Marketing-A Study of Marketing in Digital Age", *International Journal of Management and Social Sciences Research (IJMSSR)*, 3(6), 24-26.

Roberts, R. R. and J. Kraynak. (2008). *Walk Like A Giant, Sell Like A Madman*. Hoboken, NJ: Wiley.

Shin, W., Pang, A. and Kim, H. J. (2015). "Building Relationships through Integrated Online Media", *Journal of Business and Technical Communication*, 29 (2), 184-220.

Smutkupt, P., Krairit, D. and Esichaikul, V. (2010)." Mobile Marketing: Implications for Marketing Strategies", *Mobile Marketing Association*, 5(2), 126-139.

Steinman, M. L. and Hawkins, M. (2010). "When Marketing Through Social Media, Legal Risks Can Go Viral", *Intellectual Property & Technology Law Journal,* 22(8), 1-9.

Tong, S., Luo, X. and Xu, B. (2019). "Personalized Mobile Marketing Strategies", *Journal of The Academy Of Marketing Science,* 48, 64–78.

Weinberg, T. (2009). *The New Community Rules: Marketing on The Social Web.* Sebastopol, CA: O'Reilly Media Inc.

Woodburn, B. (2020). Facebook Marketplace Scams: An Overview, https://www.redpoints.com/blog/facebook-marketplace-scams-an-overview/?nab=0&utm_referrer=https%3A%2F%2Fwww.google.com%2Fhttps%3A%2F%2Fwww.facebook.com%2Fbusiness%2Flearn%2Flessons%2Fhow-spot-avoid-scams, Erişim Tarihi: 15.04.2021.

Xiang, Z. and U. Gretzel. (2010). "Role of Social Media in Online Travel Information Search", *Tourism Management*, 31,179-188.

Xiong, F., Chapple, L. and Yin, H. (2018). "The Use of Social Media to Detect Corporate Fraud: A Case Study Approach", *Business Horizons*, 61(4), 623-633.

Zarrella, D. (2009). *The Social Media Marketing Book.* O'Reilly Media, Inc.

Zeff, R. L. and Aronson, B. (1997). *Advertising on The Internet,* New York: Wiley Computer Publishing.