PAPER DETAILS

TITLE: AKADEMIK YASANTIDA SANAL TEHDITLER VE VAKALAR ÜZERINE BIR ANALIZ - AN ANALYSIS THROUGH CASES AND CYBER THREATS IN ACADEMIC LIFE

AUTHORS: Muhammet DAMAR,Yilmaz GÖKSEN

PAGES: 330-350

ORIGINAL PDF URL: https://dergipark.org.tr/tr/download/article-file/498548

Mehmet Akif Ersoy Üniversitesi
Sosyal Bilimler Enstitüsü Dergisi
ISSN: 1309-1387
Cilt: 10 Sayı: 24 2018 Haziran (s. 330-350)

AKADEMİK YAŞANTIDA SANAL TEHDİTLER VE VAKALAR ÜZERİNE BİR ANALİZ[1]

AN ANALYSIS THROUGH CASES AND CYBER THREATS IN ACADEMIC LIFE

Muhammet DAMAR[2], Yılmaz GÖKŞEN[3]

Öz

İnternet, insan hayatını kolaylaştıran çok sayıda uygulama ve hizmet barındırmasının yanında, kötü niyetli kullanımlar ve barındırdığı tuzaklar nedeniyle kullanıcılar için tehdit oluşturabilmektedir. Çalışma bu bağlamda akademik dünyada gerçekleşebilecek olası saldırıları merkeze alarak, internet üzerinden gerçekleşen dolandırıcılık yöntemlerini kavramsal olarak ele almaktadır. Akademik yaşamdaki deneyimler örnek olaylar ile ortaya konulmakta ve akademik yayıncılıktaki mevcut siber tehditler gözden geçirilmektedir. Önemli sanal tehditlerden ve saldırı yöntemlerinden oltalama yöntemi, kapsamlı bir şekilde analiz edilmektedir. Makalede, oltalama yöntemi vakalar üzerinden tartışılmakta ve bu süreçlerden korunma yöntemleri, eksiklikleri, yapılabilecekler, sunduğu öneriler değerlendirilmektedir. İlaveten akademik camia için büyük tehlike arz eden avcı dergiler üzerinde kapsamlı olarak durulmaktadır. Çalışma akademik yayıncılıktaki mevcut siber tehditler üzerinde genel bir farkındalık oluşturmayı hedeflemektedir.

Anahtar Kelimeler: Bilgi Güvenliği, Oltalama, Akademik, Yayın, Dolandırıcılık, Avcı Dergiler

Abstract

Despite hosting a large number of applications and services that facilitate human life, the Internet also poses a threat to users due to malicious use and scam. In this context, the study focuses on possible attacks to the academic world and conceptually deals with fraud methods on the internet. Real-World Experiences on the issue in academic life are presented by case studies and the current cyber threats to academic publishing are examined. The method of phishing, which is among important virtual threats and methods of attack, is analyzed in a comprehensive manner. In the article, the method of phishing is discussed using case study and the methods of protection, deficiencies, and possible measures

[1] Bu çalışma International Conference on Quality in Higher Education (ICQH 2017) Konferansında sözlü bildiri olarak sunulmuştur.
[2] Öğretim Görevlisi, Muhammet Damar, Dokuz Eylül Üniversitesi Bilgi İşlem Daire Başkanlığı, muhammet.damar@deu.edu.tr
[3] Prof. Dr., Dokuz Eylül Üniversitesi İİBF Yönetim Bilişim Sistemleri Bölümü, yilmaz.goksen@deu.edu.tr

Makale Türü: Derleme
Başvuru Tarihi: 28.01.2018
Yayına Kabul Tarihi: 29.06.2018
DOI: 10.20875/makusobed.384988

are evaluated. Study lays emphasis especially on predatory journals, which pose a great danger to the academic community. The aim of this study is to raise a general awareness of the current cyber threats in academic publishing.

Keywords: Information Security, Phishing, Academic, Publication, Fraud, Predatory Journal

1. GİRİŞ

Bilişim dünyasının gelişimi, insanlığın işlerini kolaylaştırmanın yanında, insanlığa zarar vermek isteyen bireylerin suç işlemesi için de imkanlar sağlamaktadır(Akyazı vd.,2008,s.31). Dünya'da milyonlarca kredi kartı bilgisinin çalındığı saldırıların, basit olta e-postalar ile gelen yazılımlar aracılığı ile başladığı gözden kaçırılmamalıdır. Bilgi güvenliği yönetiminde hedef, güvenliğin zamanla kurum kültürü haline dönüşmesidir. Kurum içindeki art niyetli veya bilinçsiz personelin, deneyimli bilişim suçlusundan daha riskli olabileceği unutulmamalı ve güvenlik yönetiminin başarısı için istekli, bilinçli ve bilgili bir personel yapısı hedeflenmesi gerektiği ifade edilmektedir(Eminağaoğlu ve Gökşen,2009,s.13).

Kötü amaçlı yazılımlar, birçok programlama veya betik dil ile yazılabilmekte veya dosyalar içinde taşınabilmektedirler. Virüsler, trojenler, kötü amaçlı e-postalar, klavye dinleme sistemleri, tarayıcı soyma en genel kötü amaçlı yazılımlardır(Elmas vd.,2011,s.137). Bunların yanında son dönemde hızla artan aldatma ve dolandırmaya dönük oltalama saldırıları söz konusudur. Jakobsson ve Meyers(2007) oltalamayı, hedef web sitesine tamamen benzeyen gayrimeşru web sitesi aracılığıyla kullanıcının hassas bilgilerini (kişisel kimlik numarası, şifre, kredi kartı numarası gibi) elde etmeyi amaçlayan bir eylem olarak tanımlamaktadır. İngiltere Kart Birliği Organizasyonu raporuna göre İngiltere'de kredi kartlarındaki dolandırıcılık kayıpları 2013 yılının Ocak ve Haziran ayları arasında 216.1 milyon £ iken, 2014 yılının aynı döneminde 247.6 milyon £ olarak gerçekleşmiş, % 15'lik artış göstermiştir(The UK Card Association,2015,s.15). Oltalama, 2013 yılında dünya çapında 1.6 milyar $ üzerinde bir kayıp oluşturan önemli bir suç türüdür(RSA, 2013). Bu durumdan en çok etkilenen ülke % 51 ile Çin, % 44 ile Peru ve Türkiye olmuştur. ABD oltalama için en çok hosting alanını barındıran ülke olmayı sürdürmektedir. Gene aynı çalışmalarında oltalama ile baş etme yöntemlerini; hukuksal çözümler, eğitim, teknik çözüm (kara liste ve sezgisel yaklaşım) şeklinde sınıflandırırken, literatüre göre oltalamayı engelleyici yöntemleri; kara liste ve beyaz liste bazlı yaklaşım, anlık koruma yaklaşımı, karar destek araçları, topluluk derecelendirmesine dayalı yaklaşım, akıllı sezgisel tabanlı sınıflandırma yöntemleri olarak sınıflandırmıştır(Mohammad vd., 2015,s.6-19). He vd. (2011:12018), oltalama saldırısı her yıl önemli ölçüde artmakta ve kullanıcıların elektronik ticarete olan güveninin kaybetmesine neden olan en büyük tehdit olarak ifade edilmektedir.

Son dönemde siber saldırılar ile bilim dünyası farklı konu başlıkları ile karşılaşmaktadır. Gün geçtikçe, araştırmacılar e-posta kutularına yeni ve şüpheli e-postalar alırlar(Katz,2017,s.641). Birçoğu bu tür e-postalar hakkında yeterli bilgiye sahip değildir ve siber saldırıların kurbanı olmaktadır(Dadkhah vd.,2017,s.27; Clemons vd., 2017,s.236). Bu saldırılar çoğunlukla oltalama yöntemi ile avcı dergiler veya avcı yayın evleri tarafından gerçekleşmektedir. Bu tür avcı dergiler veya yayın evleri düşük maliyetli ve açık erişimli çevrimiçi yayıncılık hareketinin kolaylığından faydalanmaktadır(Noga-Styron vd.,2017,s.174). Uluslararası standartlara sahip sahte birliktelikleri ve etki faktörlerinin yanıltıcı

iddialarını kullanarak araştırmacıları özellikle de deneyimsiz bilim insanlar tuzağa düşürülmektedir(Beninger vd.,2016,s.). Bunun yanında araştırmacılar hızlı yükselmek ve kriterleri hızla sağlayabilmek için bilerek ve isteyerek de bu dergilere yayınlarını gönderebilmekte, ücretleri karşılığında yayın sahibi olabilmektedir. Kanada'da (Pyne, 2017, s.13), Sırbıstan'da (Djuric, 2015, s.183) ve Endonezya'da (Wiratningsih, 2018, s.21) bilim dünyası ve akademik yaşantıda gerçekleşen bu yöndeki olaylar tehlikeyi daha net ortaya koymaktadır. Pek çok bilim adamı, akademisyen ve araştırmacı kendini alanında ispatlama ve tanıtmak, aldığı ücreti artırmak veya yükselmek için yayın yapma baskısı altında kalabilmektedir. Son dönemlerde bu baskıdan faydalanmak isteyen ve bundan faydalanmak isteyen avcı dergiler olarak ifade edebileceğimiz sahte yayın evleri ve dergileri ortaya çıkmıştır. Birçok araştırmacı bu dergiler tarafından mağdur edilmiştir. Sahte veya avcı dergilerin yazarları, genel olarak özgeçmişlerini ve kariyer fırsatlarını geliştirmek için bu dergilerin tuzağına düşmektedir (Pamukçu Günaydın ve Doğan, 2015,s.94).

Genelde bu tür dergiler araştırmacıları tuzak olta e-postalar ve oltalama yöntemi aracılığı ile kandırmakta veya dolandırmaktadır. Araştırmacılar, konferans ve kongreler sonrasında, yayın çalışmalarının değer taşıdığını belirten, övgü dolu sözler içeren, oltalama amaçlı, bir davet yazısı ile ücret karşılığında çalışmalarının yayın yapılmasına dönük e-posta almaktadır. Genel olarak bu teklifler avcı-yırtıcı dergiler olarak adlandırılan dergilerden gelmektedir. Araştırmacıların sonrasında mağduriyetleri ile son bulacak bu çalışmalara dikkat etmeleri gerekir. Dadkhah ve Bianciardi (2016, s.1)'e göre, avcı dergiler, bilimsel yayınlar için iyi bilinen bir konudur ve bu dergiler kurmaca bir yapı ile "öde ve yayınlat" modelinde çalışmaktadır. Bunun yanında avcı yayıncılar dünya çapında araştırma kültürünü baltalamakta ve yok etmektedir. Bu durumdan bazı kötü niyetli araştırmacılar akademik kariyerlerinde hızla yükselebilmek veya kolayca yayın yapabilmek için bu dergilerde yayın yapabilmekte ve durumdan faydalanmaktadır(Beall, 2015,s.476; Xia vd.,2015,s.1406-1407; Masten ve Ashcraft,2017,s.1). Avcı yayıncılar, bilim insanlarına, bilime, bilimin iletişimine ve aktarımına zarar vermektedir (Beall, 2016, s.3). Kullanıcıların tehlikeden korunabilmesi, siber saldırılar veya siber ortamda karşılaşabilecekleri tehlikeler konusunda farkındalık oluşturma ile mümkün olabilir. Araştırma bu gereksinimi ve Türkçe literatürde bu yönde eksikliği görerek, akademik camiadaki siber suçları, oltalama yöntemini ve avcı dergileri merkeze alarak literatür çerçevesinde bilişim suçları kavramını ortaya koymaktadır. Gerçek vakalar aracılığı ile sürecin gerçekleşme şeklini ve korunma yöntemlerini, sunduğu öneriler ışığında ifade etmektedir. Bir oltalama saldırısından kurtulmanın en iyi yolu, yemin bir oltanın ucunda olduğunun farkında olmak ve yemden uzak durmaktır. Çalışmada amaçlanan akademik camiada bu yönde olası gerçekleşebilecek siber suçlar konusunda bilinç düzeyini ve farkındalığı artırmaktır. Çalışmada bu bağlamda sırasıyla kavramsal olarak, suç ve siber suç kavramı, bilgi güvenliği ve sosyal mühendislik, bilişim suçları, oltalama yöntemi ile avcı-sömürgeci ya da yağmacı yayıncılar ele alınmış, örnek olaylar (internet üzerinden domain ücreti dolandırıcılığı ve oltalama yöntemiyle yayın hırsızlığı) çerçevesinde gerçekleşmiş senaryolar üzerinden olaylar değerlendirilmiştir.

2. LİTERATÜR ÇERÇEVESİNDE BİLİŞİM SUÇLARI

2.1 Suç ve siber suç kavramı

Suçların ve cezaların kanuniliği ilkesi, birey hak ve özgürlüklerinin korunmasının güvencesi olarak ifade edilmektedir. Suç ve suçlara karşı uygulanacak yaptırımlar bu ilke ile belirlenerek kişi hürriyetinin sınırları çizilmektedir(Eşitli,2013,s.226). İnternetin tüm dünya üzerinde yaygınlaşmasıyla, bu ortamda bir takım hukuka aykırı eylemler oluşmaktadır. İnternet suçu adı verilen, siber uzayda gerçekleşen söz konusu eylemin hukuk tarafından tanımlanması ve ceza hukukunun ilkeleri ile belirlenmesi zorunluluğu ortaya çıkmaktadır(Yıldız,2007,s.616). Herhangi bir suçun, elektronik ortam içinde işlenmesi ve eylemin hukuka aykırı olarak tanımlanması ile oluşan suç, siber suç olarak ifade edilmektedir. Siber suçlar; devlet ve kamu düzenine, mal varlığına ve kişilere karşı işlenen olmak üzere üçe ayrılır(Balcıoğlu,2014,s.66-67).

2.2 Bilgi güvenliği ve sosyal mühendislik

Bilgi güvenliği açısından güvenlik altyapısının ve politikalarının doğru belirlenmesi, korunacak bilginin analiz edilmesi ve yönetimin fonksiyonlarının eksiksiz gerçekleşmesi gerekir. Siber saldırıların elektronik ortamda tanımadığımız kötü niyetli kişilerden gelebileceği gibi, arkadaş grupları veya tanıdık kişilerden de gelebilir. Bu tür durumlar sosyal mühendislik alanında incelenmektedir(Canbek ve Sağıroğlu,2006,s.169-172). Sosyal mühendislik yöntemleri, davranışlardaki önyargılar üzerine inşa edilir. Önyargılar insanın sistem açıkları olarak ifade edilebilir. Sosyal mühendislik yöntemleri ile hareket eden dolandırıcılar, kişi ve kurumlara ait bilgi ve sistemleri çeşitli yollarla, haksız çıkar elde etmek amacıyla ele geçirmektedir. Dolandırıcılığın yaşam döngüsü; ayak izini takip et, güven yarat, manipüle et, hedefi terk et şeklinde ifade edilmektedir(Türkiye Bankalar Birliği,2015,s.5).

2.3 Bilişim suçları

Devletler bilişim suçuyla mücadele için hukuk sitemleri içinde düzenlemeler yapmakta, özel ve ceza muhakemesi hukuk kuralları ile siber suçları önlemeye çalışmaktadır. Devletlerin kendi içinde aldığı önlemler etkili görünse de çoğu zaman etkisiz kalabilmekte ve bazı suçlar uluslararası bir ağ içinde gerçekleşebilmektedir. Siber suçlarda, çok az sayıda ülkenin mevzuatında düzenlemelerin yer alması, siber suçlular için büyük bir avantaj ortaya çıkarmaktadır(Özbek,2017,s.75). Bilişim üzerindeki bilgisini, gizli verilere ulaşmak veya ağlar üzerinde zarar verici işler yapmak için kullanan kişilere, internet bilgi hırsızı veya korsanı denir. İnternette bilişim suçunun gerçekleşebilmesi için ilk olarak kullanıcıların bilgisayarına bir takım casus yazılımların kurulması gerektiği ifade edilmektedir ve hiçbir casus program kendi kendine bilgisayar sistemlerine kurulamamaktadır(Türkiye Bankalar Birliği,2015,s.13). Aşağıda Tablo 1 üzerinde ülkemizde 2003-2012 yılları arasında yapılan siber suç sayıları gösterilmektedir.

Tablo 1. 2003-2012 Yılları Arası Siber Suç Sayıları(**Taşçı ve Can,2015,s.236**)

Yıllar	KKSD	BK	BSD	İAD	Diğer	Toplam
2003	80	15	X	X	X	95
2004	146	22	16	X	X	184
2005	195	9	91	X	X	295
2006	122	98	4	X	X	224
2007	594	642	416	X	91	1.743
2008	830	1.177	560	X	157	2.742
2009	1.511	550	353	412	45	2.871
2010	1.131	151	972	71	28	2.353
2011	1.772	141	1.738	111	31	3.793
2012	1.724	264	3.669	278	783	6.718

KKSD: Kredi Kartı Sahteciliği ve Dolandırıcılığı
BK: Banka Dolandırıcılığı
BSD: Bilişim Suçları ve Dolandırıcılığı
İAD: İnternet Aracılığıyla Dolandırıcılık
X: Kayıtlı Veri Yok

Bilişim suçları, bilişim ihlali, bilgisayar kullanılarak işlenen suç, bilgisayarın kötü niyetli kullanımı gibi kullanımlara sahiptir. Bilgin vd. (2013, s.91), bilişim suçlarını teknoloji kullanımı ile, kanun dışı kişisel ya da kurumsal bilgisayar ve sistemde zarar verici etki bırakmak olarak tanımlamaktadır. Bilişim suçlarının işlenmesinde kullanılan başlıca yöntemler; çöpe dalma, gizli dinleme, veri aldatmacası, truva atı, sistem tarama, süper darbe, salam tekniği, sistemin kırılıp içeri girilmesi, gizli kapılar, ağ solucanları, bilgisayar virüsleri, mantık bombaları, spam e-posta, oltalama, web sayfası hırsızlığı, hukuka aykırı içerik sunma, şeklinde ifade edilebilir. İnternet üzerinde en yaygın görülen dolandırıcılık yöntemleri ise, sosyal ağ dolandırıcılığı, bahis dolandırıcılıkları, kriz vurguncuları, büyük kazanç vaadi oltalama gibi yöntemleridir. Aşağıda internet ve internet üzerinden dolandırıcılık yöntemlerinden oltalama yöntemi üzerinde detaylı bir şekilde durulacaktır.

2.4 Oltalama yöntemi

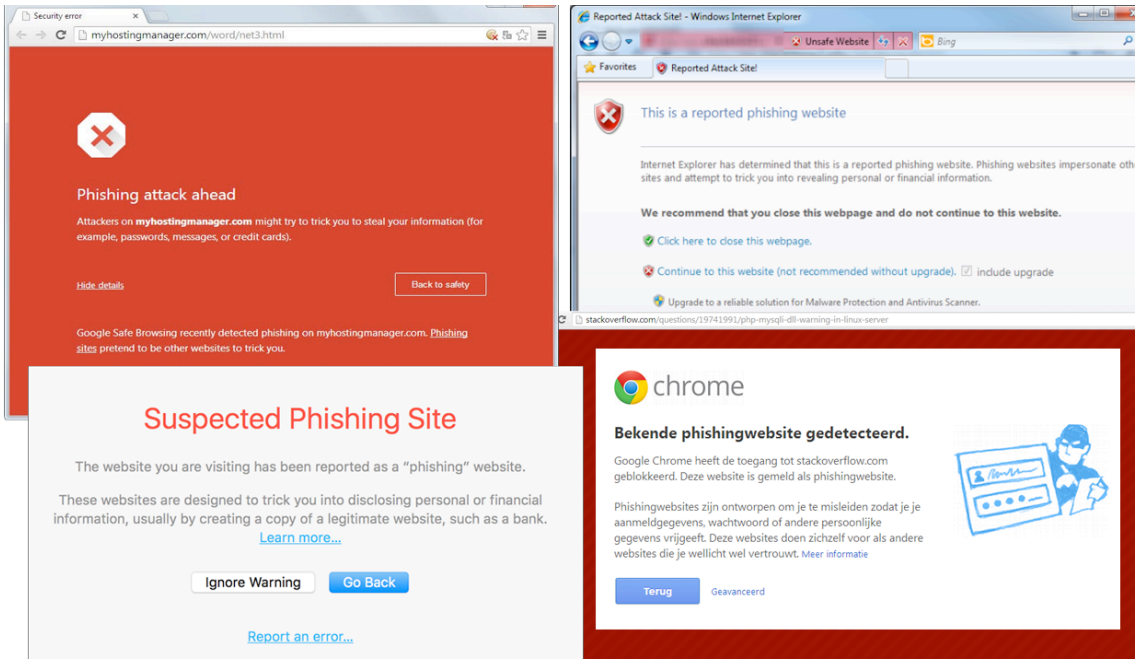
Oltalama yöntemi, bilgi hırsızlığı adı verilen, içinde sosyal mühendislik yöntemlerini barındıran, kullanıcıların e-posta gibi araçlar ile tuzağa düşürüldüğü, kredi kartı bilgilerini, kişisel bilgilerini, paralarını, bilgisayar sistemlerini ve sistemlerinde barındırdıkları verilerinin elde edilmesi olarak ifade edilebilir. Rao ve Ali(2015,s.147)'e göre oltalama, çevrimiçi kullanıcıların hassas bilgilerini izlemek ve çalmak için bir web sitesi sahteciliğidir ve saldırgan, sms, sesli posta, web sitesi ve kötü amaçlı yazılım gibi sosyal mühendislik teknikleriyle kullanıcıyı kandırır. Patil ve Devale(2016,s.198-199) oltalama

saldırılarını; kötü amaçlı yazılımlara dayalı oltalama, sistem yeniden yapılandırma, sunucu dosyalarına sızma, veri hırsızlığı, kişiyi sahte web sitesi ile tuzağa düşürme, içeriğe entegre kodlar ile oltalama, arama motorları yoluyla oltalama, telefonla oltalama, kötü amaçlı yazılım ile oltalama olarak sınıflandırmışlardır.

Oltalama bir dolandırıcılık yöntemidir. Aburrous vd.(2010) oltalama göstergelerini; domain kimliği ve url, şifreleme ve güvenlik, java script ve kaynak kod, içerik ve sayfa sitili, web adres çubuğu ve insan algısı olarak altı başlık ile çalışmalarında açıklamışlardır. Khonji vd.(2013,s.2095), oltalama algılaması için yöntemleri kullanıcı bilinci oluşturmak ve yazılımsal algılama (kara listeler, sezgisel yaklaşımlar, görsel benzerlik yöntemi, makine öğrenmesi) olarak iki ana başlık altında sınıflandırmışlardır. Bunun yanında Singh vd. (2015,s.63) olta amaçlı web sitelerinin; IP bazlı site ismi olabilir, @ simgesini içeren url adrese sahip olabilir, domainde (-) simgesi bulundurabilir, çok uzun url'ye sahip olabilir, https protokolü olmayabilir, alt alan ve çoklu alt alanlara sahip olabilir, çapa(anchor) kullanabilir, url talep edebilir, sunucu farklı bir yerde bulunabilir, yönlendirme sayfasına sahip olabilir, bağlantıyı gizlemek için mouseover'ı kullanabilir, açılır pencere özelliğine sahip olabilir, genç domainin yaşı, yeni dns kayıtları, anormal url gibi özelliklere sahip olabileceğini ifade etmişlerdir.

Hong (2012,s.75-76) insanların neden oltalama saldırısına düştükleri konusunda; kişilerin yeni teknolojilere ilgisi ve merakıyla bir ilişki bulmuş ve bu tür kişilerin oltalamaya daha kolay düştüklerini ifade etmiştir. Dhamija vd. (2006,s.589-590) katılımcılardan çeşitli web sitelerini meşru veya sahte olarak tanımlamalarını istedikleri çalışmalarında; iyi oltama sitelerinin katılımcıların % 90'ı aldattığını tespit etmişlerdir. Çoğu tarayıcının da herhangi bir ipucu vermediğini çalışmalarında görmüşlerdir. Deneyimli kullanıcıların bile oltalama konusunda problem yaşadığını görmüşlerdir. Aşağıda bazı browserların oltalamaya karşı verdikleri uyarıların ekran görüntüsü verilmiştir (Şekil 1). Modern web tarayıcıları, bilinçli güvenlik kararları vermelerinde kullanıcılara yardımcı olacak araçları sağlar. Örneğin, URL çubuğu ve SSL asma kilidi içindeki görsel göstergeler, kullanıcıların web sitelerinin meşruluğunu değerlendirmesine olanak tanıyacak şekilde tasarlanmıştır. Maalesef bu göstergeler, oltalamayı önlemeye karşı kısmen başarılı olmuştur (Alsharnouby vd., 2015). Kumar (2017), her ne kadar browserlar olası oltalama sitelerine uyarı verse de bazen hataya düştüklerini, browser adres bölümünde gerçekte olmaması gereken bir adresin gösterilebileceğini ve kullanıcının bunu adres çubuğu üzerinden ayırt edemeyeceğini göstermiştir.

Şekil 1. İnternet Explorer, Safari, Chrome ve Firefox Tarayıcıları İçin Oltalama Uyarıları



Bu bağlamda internet üzerinden ödeme şekillerimizin güvenli olmasına dikkat etmemiz önerilebilir. İnternette yapılan ödeme şekilleri, kredi kartı, e-posta order, sanal kredi kartı, kullan at kredi kartı, EFT, havale, kapıda ödeme, paypal, elektronik para şeklinde sınıflandırılmaktadır (Sanal Pos ve Ödeme Şekilleri,2017).

3. YÖNTEM

Kullanıcıların tehlikeden korunabilmesi, siber saldırılar veya siber ortamda karşılaşabilecekleri tehlikeler konusunda farkındalık oluşturma ile mümkün olabilir. Araştırma bu bağlamda, akademik camiadaki siber suçları, oltalama yöntemini ve avcı dergileri merkeze alarak literatür çerçevesinde bilişim suçları kavramını yaşanmış örnek olaylar ile ortaya koymaktadır. Literatürde değinilen konular, suç ve siber suç kavramı, bilgi güvenliği ve sosyal mühendislik, bilişim suçları ve oltalama yöntemi şeklindedir. Bu kurgudaki amaç okuyucuya konu hakkında tam bir kavramsal çerçeve sunabilmektir.

Basit bir e-posta ile başlayan oltalama saldırılarında kullanıcıların kişisel bilgileri, banka hesap bilgileri ve paraları gidebilmektedir. Bu noktada akademik camiada kullanılan olta yöntemleri üzerinde kapsamlı bir şekilde durulmaktadır. Akademik yaşantıda araştırmacılar, katıldıkları kongreler sonrasında veya yayınlanan bir makaleleri sonrasında olta e-postalar alabilmektedir. Çalışmada örnek vaka seçimlerinde bu tür e-postalar kullanılmıştır. Gerçek vakalar üzerinde durularak okuyucu üzerinde yaşanılacak bir oltalama saldırısı için farkındalık oluşturmak amaçlanmıştır. Oltalama sürecinin gerçekleşimi tam olarak ifade edebilmek için kredi kartlarını almak için kullanılan site alt yapıları ve ekran görüntüleri, site sahiplerinin bulundukları coğrafya ve olası siber suç için kanun karşısında hak arama durumları değerlendirilmiştir. Çalışmada tüm bunlara ek olarak, son yıllarda akademik yaşantıda karşımıza sıklıkla çıkmaya başlayan avcı dergiler veya avcı yayın evleri tarafından gerçekleştirilen yayın

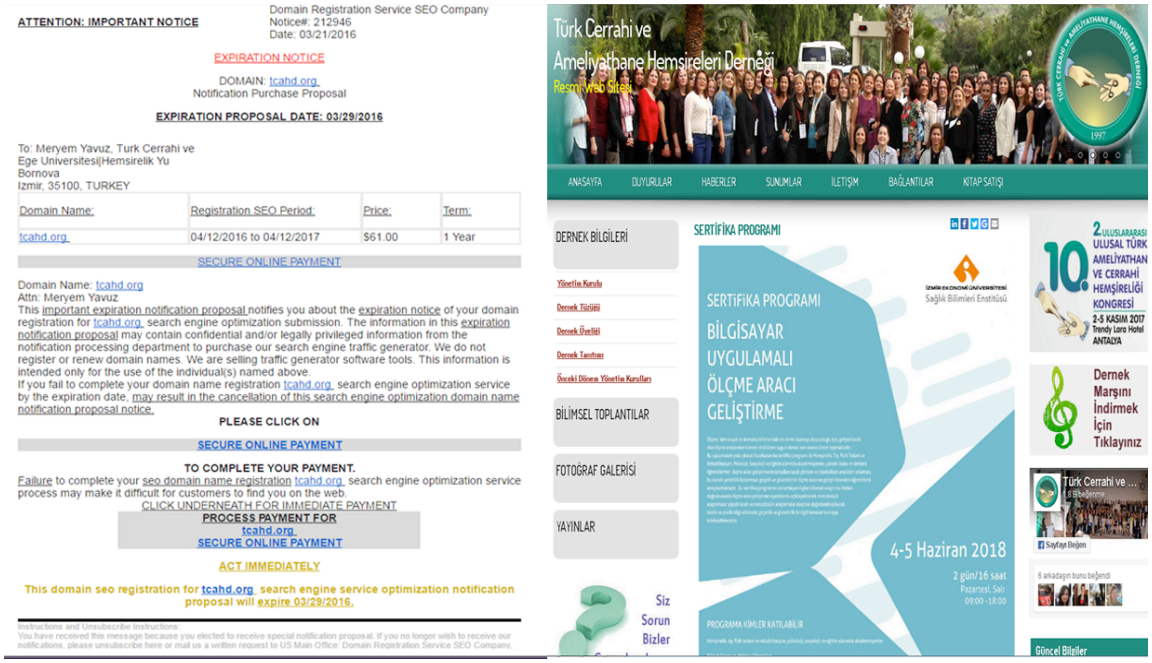
dolandırıcılığı üzerinde durulmaktadır. Çalışma akademik yaşantıda olası av durumlarını engelleyebilmek, araştırmacıların dolandırıcı yayın evlerinden korunabilmeleri için olası yöntemler literatür çerçevesinde ortaya konulmuştur.

4. BULGULAR VE DEĞERLENDİRME

4.1 Örnek olay 1: İnternet üzerinden domain ücreti dolandırıcılığı

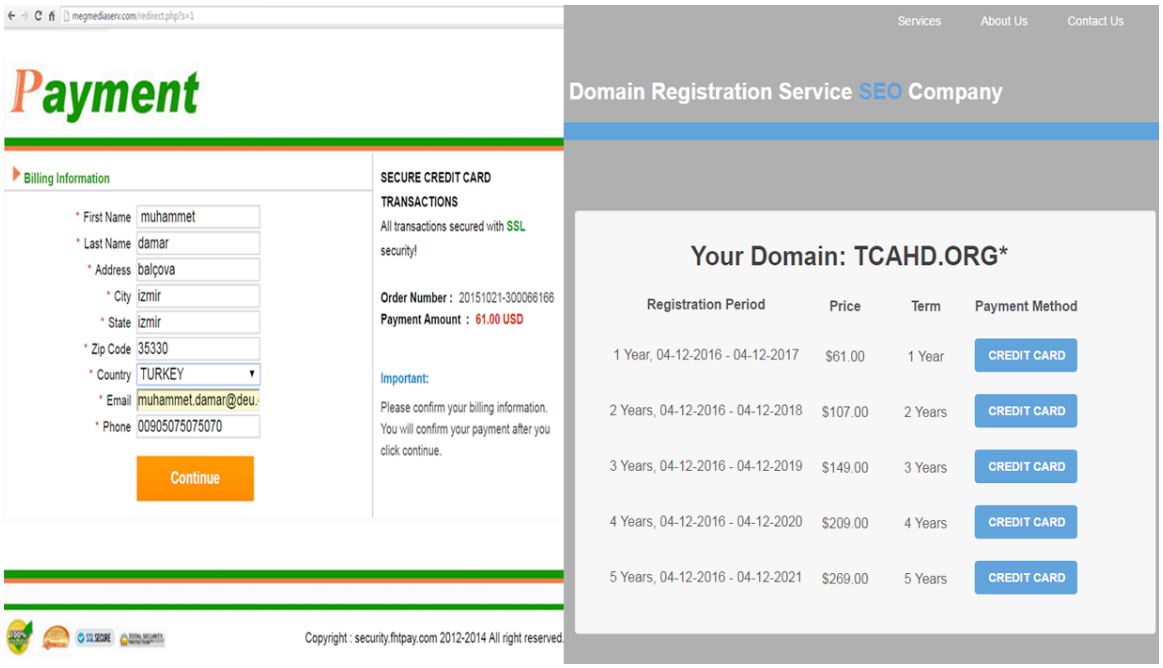
İnternet siteleri domain olarak ifade edilen bir isim üzerinde faaliyetlerini sürdürmektedirler. Bu isim hakkı için belli süre aralıklarıyla ücret ödemek zorundadırlar. Burada incelenen vaka bu bağlamda kullanıcıların paravan bir site ile avlanmasına-oltalanmasına dönüktür. Olayı gerçekleştiren kişiler, Papua Yeni Gine'nin kuzeyinde Palau ada ülkesi üzerinden alınmış bir başka domain sitesi üzerinden oluşturdukları site aracılığı ile kullanıcı kredi kart bilgilerini avlamayı hedeflemektedir. Aşağıda Şekil 2 üzerinde oltalama için kullanılan e-posta ve site görüntüsü paylaşılmaktadır. İlgili site ismi, akademik camiada etkin bir şekilde faaliyet gösteren bir dernek sitesidir. Burada yaşanılan olay oltalama amaçlı akademik camiada karşılaşılabilecek farklı bir vakaya örnek teşkil etmektedir.

Şekil 2. Oltalama İçin Kullanılan E-posta ve Site Ekran Görüntüsü



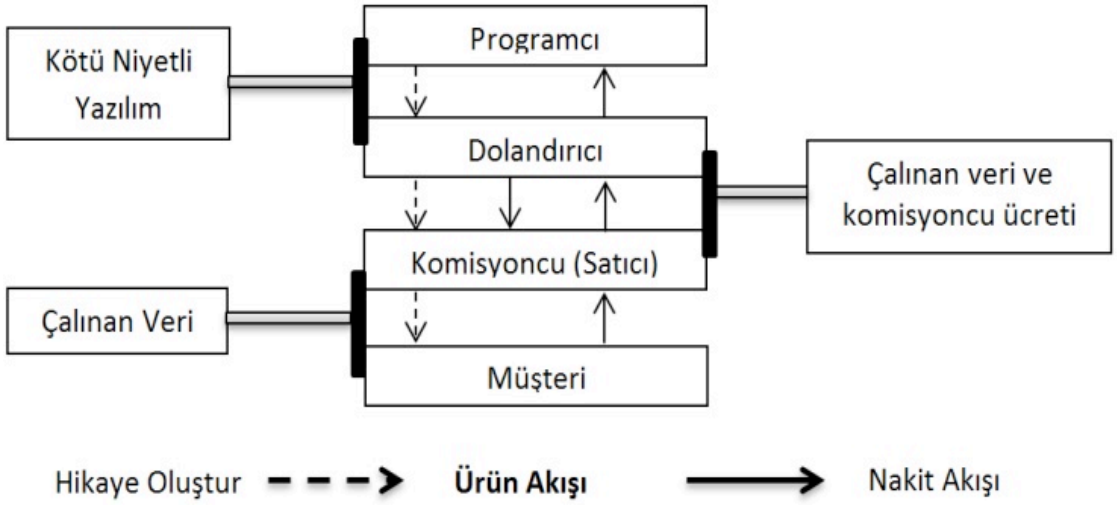
Gelen e-posta aracılığı ile önce ilgili ülke üzerinden alınmış bir domain ismi ve bu siteden yönlendirilen kredi kartı bilgilerini avlama sitesine yönlendirmektedir. Oltalama için gönderilen e-postalar, kullanıcıların domain kaydı için vermiş oldukları e-postalarına gelmektedir. Kullanıcılar kendi üzerine kayıtlı bu şekilde bir web sitesi olduğu için süreçten şüphelenmeden oluşturulan paravan site üzerinden kredi kartıyla ödeme yaparlar ve oltaya yakalanırlar. Aşağıda Şekil 3 üzerinde oluşturulan web sitesi görüntüsü ve kredi kartı bilgilerinin kopyalandığı site görüntüsü paylaşılmaktadır.

Şekil 3. İlgili Sitenin Oltalama İçin Kullandığı Web Ara Yüzleri



Dolandırıcılık sırasında kişinin kredi kartı bilgileri alınarak kişinin banka hesabına sızılmakta ve hesaptaki parasına sahip olunmaktadır. Hesaptan paranın çekilmesi sırasında çeşitli yöntemler uygulanabilir. Bu sitede olduğu gibi Palau gibi ada ülkeleri ve kanunlarında bu suçun karşılığı olmadığı ülkeler seçilebilir. Bu sayede aldatılan kullanıcıların yasa karşısında haklarını aramaları imkansız hale gelmekte, mağdurun parasını rahatlıkla hesaplarına aktarabilmektedir. Aslında bu durum, Dünya çapında bu tür suçlar ile mücadele etmenin gereğini ortaya koymaktadır. Bunun yanında suçlular, elde ettikleri kredi kartı bilgileri ile sahte kredi kartı hazırlayarak ATM ya da alışveriş merkezlerinden harcama yapabilmektedir. Konradt vd.(2016,s.41) bir oltalama saldırısının gelir akışını, şekil üzerinde ifade etmiştir (Şekil 4).

Şekil 4. Bir Oltalama Saldırısının Gelir Akışı (Konradt vd., 2016, s.41)

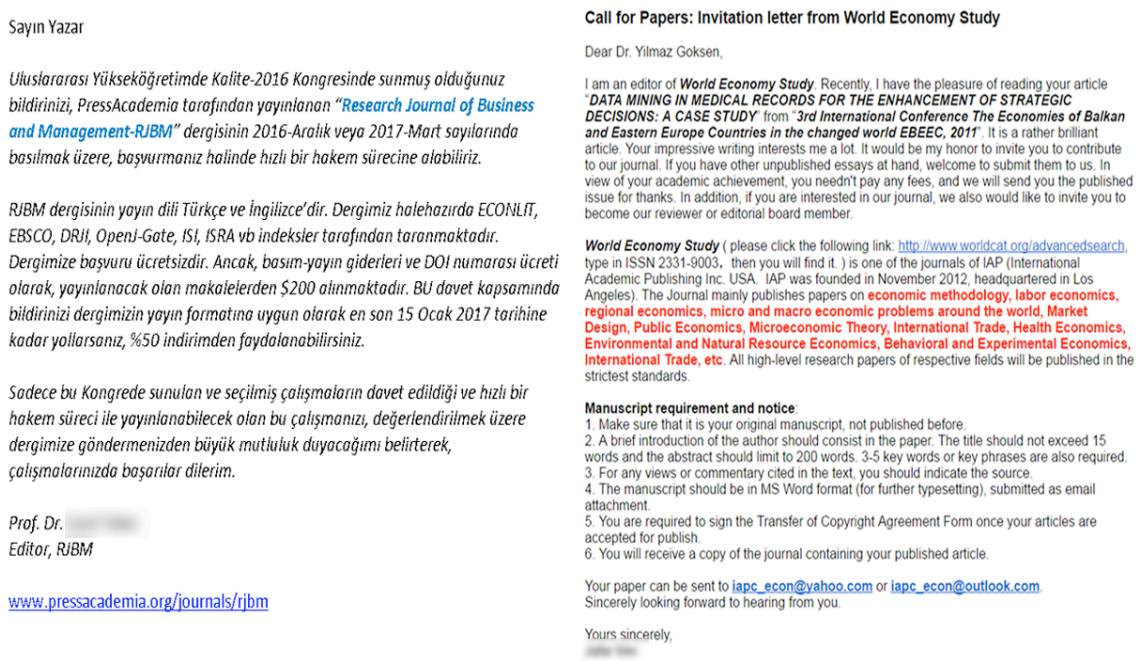


4.2 Örnek olay 2: Oltalama yöntemiyle yayın hırsızlığı

Oltalama yönteminde sosyal mühendislik yetenekleri önemli bir yer tutmaktadır. Dolandırıcılığın gerçekleşebilmesi için kullanıcıların aldatılması gerekmektedir. Tabi bunun için uygun ortamın hazırlanması gereklidir. Oltaya takılacak yem oltalamak istenen hedefe göre değişiklik göstermektedir. Son zamanlarda dolandırıcıların bir başka hedefi ise akademik camiadaki öğretim üyeleri ve yayınlarıdır. Bu bağlamda ikinci örnek olayda, yayın ve ücret hırsızlığını hedefleyen ve basit bir olta e-postası ile başlayan durum değerlendirilmektedir.

Korsanlar kullandıkları araştırmacı veya akademisyen e-posta adreslerini bulmak için çeşitli yöntemler kullanabilmektedir. Aslında en temel yöntem çeşitli özel yazılımlar aracılığı ile web siteleri üzerindeki (akademik cv, kongre-sempozyum web siteleri, dergi web siteleri gibi.) kişi e-postaları toplamaktır. Tüm bunların yanında korsanlar sahte konferans/sempozyum/kongre düzenleyebilir, katılımları daha fazla sağlayabilmek için olta e-postalar aracılığı ile (Şekil 5) araştırmacıları tuzağa düşürebilir. Korsanlar araştırmacıları kolaylıkla tuzağa düşürebilmek için e-posta satışı sağlayan kişilerden veya akademisyenler için sosyal paylaşım ortamı sağlayan çeşitli amaçlardaki partalların yöneticilerinden e-posta adresleri satın alabilmektedir. Konferanslar gerçekleştiren şirketler, sayısız konferansa sponsorluk yaparak değerli yazar bilgileri listeleri üretebilmekte bu bilgiler ise sosyal mühendislik ve oltalama için korsanlara çok kıymetli bilgiler sunmaktadır. Bu şirketlerin bazıları, gizliliğin ihlali anlamına gelen spam e-postaları için yazarın e-posta adreslerini satabilmektedir (Dadkhah vd, 2016, s.417).

Şekil 5. Yayın Hırsızlığı İçin Yem Olarak Gönderilen İki Örnek E-posta



Sayın Yazar

*Uluslararası Yükseköğretimde Kalite-2016 Kongresinde sunmuş olduğunuz bildirinizi, PressAcademia tarafından yayınlanan "**Research Journal of Business and Management-RJBM**" dergisinin 2016-Aralık veya 2017-Mart sayılarında basılmak üzere, başvurmanız halinde hızlı bir hakem sürecine alabiliriz.*

RJBM dergisinin yayın dili Türkçe ve İngilizce'dir. Dergimiz halehazırda ECONLIT, EBSCO, DRJI, Open J-Gate, ISI, ISRA vb indeksler tarafından taranmaktadır. Dergimize başvuru ücretsizdir. Ancak, basım-yayın giderleri ve DOI numarası ücreti olarak, yayınlanacak olan makalelerden $200 alınmaktadır. BU davet kapsamında bildirinizi dergimizin yayın formatına uygun olarak en son 15 Ocak 2017 tarihine kadar yollarsanız, %50 indirimden faydalanabilirsiniz.

Sadece bu Kongrede sunulan ve seçilmiş çalışmaların davet edildiği ve hızlı bir hakem süreci ile yayınlanabilecek olan bu çalışmanızı, değerlendirilmek üzere dergimize göndermenizden büyük mutluluk duyacağımı belirterek, çalışmalarınızda başarılar dilerim.

Prof. Dr.
Editor, RJBM

www.pressacademia.org/journals/rjbm

Call for Papers: Invitation letter from World Economy Study

Dear Dr. Yilmaz Goksen,

I am an editor of ***World Economy Study***. Recently, I have the pleasure of reading your article "***DATA MINING IN MEDICAL RECORDS FOR THE ENHANCEMENT OF STRATEGIC DECISIONS: A CASE STUDY***" from "***3rd International Conference The Economies of Balkan and Eastern Europe Countries in the changed world EBEEC, 2011***". It is a rather brilliant article. Your impressive writing interests me a lot. It would be my honor to invite you to contribute to our journal. If you have other unpublished essays at hand, welcome to submit them to us. In view of your academic achievement, you needn't pay any fees, and we will send you the published issue for thanks. In addition, if you are interested in our journal, we also would like to invite you to become our reviewer or editorial board member.

World Economy Study (please click the following link: http://www.worldcat.org/advancedsearch, type in ISSN 2331-9003，then you will find it.) is one of the journals of IAP (International Academic Publishing Inc. USA. IAP was founded in November 2012, headquartered in Los Angeles). The Journal mainly publishes papers on **economic methodology, labor economics, regional economics, micro and macro economic problems around the world, Market Design, Public Economics, Microeconomic Theory, International Trade, Health Economics, Environmental and Natural Resource Economics, Behavioral and Experimental Economics, International Trade, etc**. All high-level research papers of respective fields will be published in the strictest standards.

Manuscript requirement and notice:
1. Make sure that it is your original manuscript, not published before.
2. A brief introduction of the author should consist in the paper. The title should not exceed 15 words and the abstract should limit to 200 words. 3-5 key words or key phrases are also required.
3. For any views or commentary cited in the text, you should indicate the source.
4. The manuscript should be in MS Word format (for further typesetting), submitted as email attachment.
5. You are required to sign the Transfer of Copyright Agreement Form once your articles are accepted for publish.
6. You will receive a copy of the journal containing your published article.

Your paper can be sent to iapc_econ@yahoo.com or iapc_econ@outlook.com.
Sincerely looking forward to hearing from you.

Yours sincerely,

Bilindiği üzere akademik yaşantıda en değerli unsur fikirdir. Siber korsanlar, kongre sitelerinde yayınlanmış olan tam veya özet bildirilerden toparladıkları e-posta hesapları, Şekil 5 üzerinde gösterilen e-postalara benzer e-postalar hazırlayarak, kullanıcıları oltaya düşürmektedir. Gerçek bir dergi

editöründen gelen bir e-posta gibi hazırlanan e-postalara kullanıcıların yayınlarını göndermeden önce dergi ve editörün gerçekliğini sorgulamaları gerekmektedir. Gelen e-postadaki linkler bu bağlamda sorgulama için referans olarak kullanılmamalıdır. Bilindiği üzere aldatma için kullanıcılar, indeksli dergilerin tıpa tıp benzerini yapabilirler. Bununla beraber kullanıcıdan dergide yayın yapabilmesi için ücret talep edebilirler ve bu esnada kredi kartı bilgilerini kopyalayıp kötü amaçlı kullanabilirler. Öğretim üyelerinin bu hususta kendi bildikleri siteler üzerinden dergi, editör sorgulamaları yapmaları önerilebilir.

5. AVCI, SÖMÜRGECİ YA DA YAĞMACI YAYINCILAR

Tez, araştırma makalesi, kongre veya seminerlere katılan araştırmacıların başına gelen veya gelebilecek olaylardan birisi bazı yayıncılardan gelen şüpheli ve yem niteliğindeki e-postalardır. Bu e-postalar Dünya'nın herhangi bir yerinden size gelebilir ve sizin araştırmanızı ücretli bir şekilde taahhüt ettikleri ortamda yayınlayacaklarını ifade edebilir. Hatta bu e-postalarda, size özel indirim, çalışmanızı çok beğendik, yayın için süper fırsat gibi sizi daha kolay kandırmaya dönük ifadeleri barınabilir. Bu tür oltalama e-postaları bazı karakteristik unsurlara sahiptir. Bu unsurlar; zayıf grafiksel özelliklere ve metin içi hatalara sahiptirler. E-postaların aceleci bir havası vardır(maksimum 4 ile 6 iş günü gibi), dergi ismi vurgulanır, dergiye ve sunulan imkana önemli havası verilir, yayın maliyeti düşük tutulur (Ibba, vd., 2017, s.506).

Genelde bu tarz yayıncılar veya şirketler internette taratıldığında, bu durumu yaşayan ve benzer mesajları almış birçok kişi ve bundan mağdur olmuş kurbanların haberleri ile karşılaşılmaktadır. Bu tür mesajlar genelde akademik yayınlara ücretsiz erişim sağlayan açık erişimli platformlarından gelmektedir. Açık erişimli platformların sayısı gittikçe artmaktadır. Bunlar arasından hangileri şüpheli, hangileri güvenilir, bunu anlamak oldukça zordur. Dadkhah ve Bianciardi (2016, s.2-3) bu bağlamda avcı dergilerin değerlendirebilmek için bir tablo oluşturmuşlardır (Tablo 2). Dergilerin avcı olup olmadığı 4 boyut altında toplanan 14 kriterden alınan puanların toplam kriter sayısı olan 14'e bölünmesi ile oluşur. Eğer bir dergi bu kriterlere göre değerlendirildiğinde 0.22 puan üzerinde bir puan alırsa avcı dergi olarak nitelendirilmekte, 0.22'den küçük 0'a eşit olmayan bir değer aldıysa şüpheli ve avcı dergi uygulamalarını kullanmakta, eğer 0 puana sahipse dergi avcı dergi değildir.

Tablo 2. Avcı Dergileri Değerlendirme Kriterleri (Dadkhah ve Bianciardi, 2016, s.2)

Kriter Grubu	**Kriterler**	**Ölçüler**	**Ağırlık Puanı**
Editör Bölümü	Editörün e-posta adresi	Resmi e-posta	0
		Genel e-posta adresi	1
		Bulunmuyor	2
	Editörlerin üyelikleri	Tam üyelik	0
		Sadece ülke ismi	1
		Bulunmuyor	2
		Editörler belirli bir ülkeden	2
	Editör sayısı	5'ten az	2
		5-7 arası	1
		7'den fazla	0
Değerlendirme süreci ve yayınlama	Değerlendirme zamanı	1 haftadan az	2
		1 aydan az	1
		1 aydan fazla	0
	Açık olmayan değerlendirme süreci	Evet	1
		Hayır	0
	Her sayıdaki makale sayısı	20 sayfadan az	0
		20 sayfadan fazla	1
	Kuşkulu özel sayılar	Evet	1
		Hayır	0
Duyuru	Derginin tam adresinin yayınlanması	Evet	0
		Hayır	1
	Sahte metrik ve dizin kullanımı	Evet	1
		Hayır	0
	Makaleleri almak için dergi spam e-posta gönderir	Evet	1
		Hayır	0
Açık erişim politikaları ve sorumlulukları	Hızlı değerlendirme ücreti	Evet	1
		Hayır	0
	Yükleme ücreti	Evet	1
		Hayır	0
	Yayınlama ücreti	Evet	1
		Hayır	0
	Yazar ve okuyucular için ücret talebi	Evet	1
		Hayır	0

Colorado Denver Üniversitesi kütüphanesinde görev yapan Jeffrey Beall, bu noktada şüpheli olan ve yayıncılığı kötü amaçlı çalışmaları avcı-yırtıcı dergileri adlandırmış ve oluşturmuş olduğu kriterlere göre yüzlerce avcı dergiyi içine alan bir liste hazırlamıştır (Bakınız: https://beallslist.weebly.com). Burada amaç, dürüst olmayan yayıncılık uygulamaları konusunda farkındalık oluşturmaktır (Xia vd., 2015, s.1406-1407). Fakat internette potansiyel şüphelileri, avcı yayıncılar dediğimiz bu tarz firmaları içeren listeler mevcuttur (Enago, 2014a). Avcı dergiler için tek bir site hizmet vermemektedir. Bu alanda farklı siteler de hizmet vermekte, hatta bazı üniversite kütüphane sayfalarında (Jeffrey Beall veya diğer listeleri referans alarak), konu hakkında bilgilendirme yapılmakta, araştırmacılar için bu noktada farkındalık oluşturmaktadır (Bakınız: https://jefferson.libguides.com/, https://predatoryjournals.com/journals/,https://guides.library.yale.edu/c.php?g=296124&p=1973764,http://libguides.wits.ac.za/Scholarly_Research_Resources/Predatory_Publishers gibi). Avcı yayıncılar Dünya'nın bazı bölgelerinde diğer bölgelere oranla daha başarılı olmuştur. Bu bölgelerde avcı yayıncıların başarılı olmasının nedeni, akademik değerlendirme ve yükseltme kriterlerinin yayın sayısı üzerine kurulmasıdır. Bu durum, hızlı, kolay ve daha az emekle yayıncılık sunan avcı dergiler için mükemmel bir ortam oluşturduğu ifade edilmektedir (Beall, 2016, s.3).

Şekil 6. Sahte - Yağmacı Dergilerin Listesini Gösteren Bir Site Görünümü (Erişim: https://sites.google.com/site/fakeresearchjournalpublishers/home)

Bunun yanında Tom Spears; toprak, kanser tedavisi ve mars hakkında yazdığı hiçbir akademik değeri olmayan bir araştırma makalesi yazar ve bunu yayınlatmak ister. Hazırladığı bu sahte makaleyi 18 yayıncıya göndermekte ve 8 tanesi bunu yayınlamayı kabul etmektedir. Bu tür yayıncılar, etik olarak, bir hakem kontrol sürecinden dergileri geçirmemektedir. Kısacası gelen makaleler ücret karşılığında yayınlanmakta ve akademik değer önemsenmemekte bir uzman görüşünden geçmemektedir. Spears'ın makalesini yayınlamayı kabul eden yayıncılardan her biri yayın ücreti olarak 1000 ile 5000 Amerikan doları arasında bir meblağ talep etmişlerdir. Bir başka örnekte ise John Bohannon bir bilim dergisi olan Science ile beraber bir çalışmaya imza atmıştır. Kanserle savaş konusunda Spears'ınkinden daha az saçma ama tamamen sahte olan bir makale hazırlar ve 340 adet yayıncıya gönderir. Yayıncıların %60'ı

makaleyi yayınlamayı kabul eder ve bunlar avcı dergilerdir. Yayıncıların IP adreslerine bakıldığında büyük çoğunluğunun Hindistan ve Nijerya'dan olduğu görülmüştür(Enago, 2014b). Tüm bu örnek olaylardan ve durumlardan çıkarabileceğimiz önemli sonuçlardan birisi de makale yazdıktan sonra yayın yapacağımız derginin de özenle seçilmesinin gereğidir.

5.1 Yasal dayanaklar

Kullanıcılar, sanal ortamda oltaya geldiklerinde, neler yapabilir veya yasal olarak hakkını nasıl arayabilir, bu başlık altında ilgili kanunun maddeleriyle açıklanmaktadır. Siber suçlar Türkiye'nin iç mevzuatında ilk defa, 1991 yılında 765 sayılı Türk Ceza Kanunu'nda, 3756 sayılı kanunla (525/a, b, c ve d maddeleri) eklenen bilişim alanında suçlar bölümüyle girmiştir. 2004 yılında çıkarılan 5237 sayılı yeni Türk Ceza Kanunu'nda siber suçlar, siber suçların güncel gelişimi göz önüne alınarak oldukça ayrıntılı şekilde açıklanmaktadır. 5237 sayılı Türk Ceza Kanunu'nda bilişim alanında suçlar; hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçu, bilişim sisteminin isleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçu, bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu, banka veya kredi kartlarının kötüye kullanılması suçu olarak ifade edilmiştir. Bunun yanında özel hayata ve hayatın gizli alanına karsı suçlar bölümündeki siber suçlar; kişisel verilerin kaydedilmesi, kişisel verileri hukuka aykırı olarak verilmesi veya ele geçirilmesi, verilerin yok edilmemesi suçları olarak ifade edilmiştir(Taşçı ve Can,2015,s.232-233).

Bilişim suçlarını ilgilendiren diğer bir kanun 5271 sayılı Ceza Muhakemesi Kanunu'dur. Ceza Muhakemesi Kanunu'nun "bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma" başlıklı 134. maddesinde dijital delillerin toplanması ve muhafaza edilmesi usulüne ilişkin hükümler bulunmaktadır. Siber suçlar ile mücadele amaçlı bir diğer kanun 5651 sayılı internet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanundur. İlgili kanun bazı yönetmelikler ile düzenlenmiştir. Kanun içerik ve içerik sağlayıcıların rol ve sorumluluklarını belirlemektedir(Hekim ve Başıbüyük, 2013,s.151-152).

5.2 Süreçten nasıl kaçınılabilir

Oltalama yönteminden elbette anti virüs uygulamaları sayesinde sistemleriniz korunmaktadır. Bunun yanında, bankacılık işlemlerinde ya da internetten ödeme işlemlerinde şifre korunması ve güçlü şifrelerin kullanılması gerektiği söylenebilir. Güvenlik önlemleri, korsanların işlerini zorlaştırmaktadır. Ancak unutulmamalıdır ki, tam olarak güvenli sistem yoktur. Suç girişiminde bulunanlar hedeflerine ulaşabilmek için sosyal mühendislik uygulamakta ve onları avlamak için yol yöntem aramaktadırlar. Bu bağlamda yukarıdaki iki örnek oltalama yönteminden kaçınabilmek için; whois sorgulama, ip sorgulama, dns sorgulaması, arama motorlarından faydalanma yöntemleri ile veri toplama aşamasında elde edilen verilerin birleştirilerek oltalama yönteminden kaçınılabilir. Bunun yanında bilişim suçu ile karşılaşıldığında; emniyet müdürlüklerine suçu şikayet edebilir, deliller ile en yakın Cumhuriyet Başsavcılığına müracaat edilebilir. Şikayetçi olunan konuda emniyet müdürlükleri internet servis sağlayıcının yurt dışında bulunması durumunda bile, konunun takibini yapabilmektedir.

Tüm bunların yanında, kredi kartı bilgilerinin verilmesi veya oltaya gelmenin öncesinde, araştırmacıların, herhangi bir dergiye bir yayın göndermeden önce, iletişim bilgilerini, ilgili derginin web site adresini, yayın kurulunu ve üyelerini, derginin üyeliklerini, telif hakkı ücretlerini, hakem

değerlendirme süreçlerini, varsa etki faktörünü kontrol etmeleri en uygun olanıdır. Ayrıca, derginin Açık Erişim Dergisi olması durumunda ilgili dizini (www.doaj.org) veya Açık Erişim Akademik Yayıncılar Derneği (www.oaspa.org) üyesi olup olmadığını kontrol etmek de gereklidir(Grzybowski vd., 2017, s.610).

6. SONUÇ

Çalışmada, akademik camiada gerçekleşen siber suçlar ve ilgili örnekler çerçevesinde detaylı olarak bilgi sunulmaktadır. Bu suçlar akademik camiada daha çok ve daha hızlı yayın yapma arzusu ile özellikle genç ve hırslı araştırmacılar tarafından bilinçli olarak işlenmek ile birlikte, çoğu zaman korsanların oltasına gelen bilinçsiz kullanıcılar tarafından işlendiği ifade edilebilir. Korsanların sayısı kadar son dönemde onların kullanmış oldukları taktikler de çeşitlenmiş ve sayısal olarak artmıştır. Siber suçlar konusunda bilgisi olmayan ve basit bir e-posta ile oltaya gelen kullanıcılar, bazen uzun süre emek sarf ettikleri yayınlarını niteliksiz bir dergide yayınlayarak değerini düşürebilmekte, emeklerini heba edebilmektedir. Siber suçlular siber suçlar için fırsatlar sunan akademik dünyanın mevcut durumu hakkında mükemmel bir bakış açısına sahip olduklarını unutulmaması gerekmektedir. Çalışma bu konuda akademik yaşantıda karşılaşılan veya karşılaşılabilecek oltalama olayları merkeze alarak konuyu detaylı olarak ortaya koymayı hedeflemiştir. Oltalama yöntemi çok eski bir teknik olsa da avcı dergiler, avcı yayıncılar kavramı literatürde çok yeni ve özellikle 2014 ve sonrasında literatüre kazanılmış kavramdır. Türkçe literatür bu konuda çok zengin değildir. Çalışma bu nedenle konuyu kapsamlı bir şekilde ele almıştır.

7. ÖNERİLER

İnternet, yapısal olarak kötü amaçlı kullanımlara açıktır. Kullanıcıların internet kullanımlarında, sistem güvenliğini tehlikeye düşürecek, başkalarının kullanım haklarını engelleyecek davranışlardan kaçınmaları gerekmektedir. Aşağıda bu kapsamda sırasıyla, kurum ve kuruluşlar için öneriler, küresel ölçekte öneriler ve örnek olaylar doğrultusunda öneriler ve gelecek çalışmalar için öneriler olmak üzere dört başlık altında oltalama saldırısından kaçınılması için detay bir şekilde öneriler sunulmaktadır.

7.1 Kurum ve kuruluşlar için öneriler

Bu bağlamda, internet kullanımıyla ilgili kurum ve kuruluşların da almaları gereken bir takım önlemler söz konusudur. Bunları şöyle sıralayabiliriz; birinci olarak, kurumların internet üzerinden güvenli bir şekilde çalışabilmeleri için güçlü bir güvenlik politikası oluşturmaları, ikinci olarak; kurumlar personel için internet kullanımı ile ilgili etik ilkeleri belirlemelidir(Sanal Pos ve Ödeme Şekilleri,2017). Bunun yanında spam olan ve oltalama için en önemli araç olarak e-postalar konusunda en önemli araç olarak ifade edilebilecek e-postalara karşı, kurumların önlemler alması gerektiği ifade edilebilir. Kim vd.(2011,s.700) spam engelleme yöntemlerini; dizin bazlı filtreleme, kural tabanlı filtreleme, içerik tabanlı filtreleme, işbirlikçi filtreleme, sosyal ağ üzerinden spam sınıflandırması, alan adı doğrulama, link yapısı analizi olarak sınıflandırmışlardır. Bu yöntemleri kurumların kullanması önerilebilir. Kullanıcılar oltalama yöntemiyle avlanılmamak için, bilmedikleri kaynaklardan gelen e-postaları açmamaları; şifre, banka kartı, kişisel bilgi vb. bilgileri bilmedikleri sayfalara kesinlikle paylaşmamaları önerilebilir.

İnternet üzerinden tanımadığınız tüm e-postalara şüpheyle yaklaşmanız önerilir. Dernek veya diğer kurumlara örnek olay değerlendirildiğinde, tr uzantılı domain almaları önerilebilir. Aynı zamanda süreçte domain satın alınmasından, domain sürdürülmesi süreçlerinde muhakkak whois sorgusu yapılması, bu şekilde gelen e-postalara karşı daha dikkatli olmaları önerilmektedir.

Bunun yanında Türkiye'de, internet ortamında hak ve özgürlüklerin tam anlamıyla güvence altına alınmadığı düşünüldüğünde konuyla ilgili mevzuatlarda düzenleme yapılmalı ve yeni yasalar çıkarılmalıdır(Ercan,2009,s.7). Kamu kurumları için bir diğer öneri ise, Nevşehir Hacı Bektaşi Veli Üniversitesi Bilgi İşlem Daire Başkanlığı(NHBVÜ-BİD.,2013) ve Erzurum Emniyet Müdürlüğü'nün(Erzurum Emniyet Müdürlüğü,2013) yapmış olduğu gibi oltalama konusunda, kurum geneli bilgilendirmeler yapmalarıdır. Bunun yanında, bilişim hukukunun gelişmesi için akademik alanda yüksek lisans veya doktora seviyesinde günün ihtiyaçlarına cevap verecek bilişim uzmanlarının yetişmesi için programlar açılabilir. Kurumsal firmalarda veya kamu kurumlarında bilgi işlem yetkilileri tarafından bilgi güvenliği zafiyetleri veya bu tür oltalama yöntemlerinden kullanıcıları koruyabilmek için bilgi güvenliği politikası yürütmesi gerektiği ifade edilebilir.

7.2 Küresel ölçekte öneriler

Siber suçlar ulusal sınırlar içerisinde kalmamaktadır. Bunlarla mücadele edilebilmesi dünya çapında elbirliğiyle etkin bir mücadele yürütmesi halinde anlamlı olabilmektedir. Bu sorunu aşmak adına adım atan ilk bağlayıcı uluslararası metin Avrupa Siber Suçlar Sözleşmesi'dir. Sözleşme siber suçlularla mücadele için önemli bir enstrümandır. Sözleşme gereği, siber suçlarla etkin mücadele için üye devletlere 7/24 hizmet verebilen irtibat noktaları kurma yükümlülüğü getirilmiştir. Türkiye için bu nokta Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı'dır(Özbek, 2015,s.86-88). Yasal mevzuatlardaki boşluklar küresel ölçekte bir çözüme kavuşturulmalı, suçluların yasaların sağladığı boşluklardan faydalanmasının önüne geçilmelidir.

Aşağıda, konuyla ilgilenen araştırmacıların veya kurumların bilgi işlem sorumlularının takip etmesinin faydalı olacağı düşünülen, küresel ölçekte siber suçlara karşı korunma konusunda halkı eğitmeye çalışan bazı uluslararası gruplar ve kuruluşlar bulunmaktadır(Kim vd.,2011:701):

- Siber Yurttaşlık Ortaklığı (http://www.cybercitizenship.org)
- Siber Melekler (http://www.cyberangels.org)
- GetNetWise (http://www.getnetwise.org)
- İnternet Güvenliği Koalisyonu (http://www.ikeepsafe.org)
- Scambusters.org (http://www.scambusters.org)
- Kimlik Hırsızlığı Araştırma Merkezi (http://www.idtheftcenter.org)
- ABD Ulusal Siber Güvenlik Birliği(NCSA) (http://www.staysafeonline.org)

7.3 Örnek olaylar doğrultusunda öneriler

Yukarıdaki iki örnek olayda gerçekleşen oltalama hedef odaklı bir saldırıdır. Bu tür saldırılardan korumanın ilk adımı, hedef olunabileceğinin farkında olmaktır. Sonuçta, siz ve sizin kurumunuz muhtemel hassas bilgilere sahip olabilir ya da başka kuruma erişim için paravan olarak kullanılabilmektedir. Siber saldırganlar sizin hakkınızda ne kadar bilgiye sahipse, oltalama için, size özgü

ve sizinle ilgili hedef odaklı olta e-postası hazırlaması o kadar kolay olacaktır (Sans Institute,2013,s.3).

Avcı dergiler, yazarların ve akademik kurumların önemli etik problemleri arasında yer almaktır. Bu noktada, yazarlara, kurumlara, editörlere ve yayıncılara özetle akademik ortamdaki tüm paydaşlara önemli sorumluluklar düşmektedir. Akademik ortamdaki meşru ve kurallara uygun yayın girişimlerini desteklemek ve avcı dergilerin yayınlarına engel olmak ve fakülte veya enstitüler araştırmacıların burada yayın yapmasını engellemek ile yükümlüdür(Ferris ve Winker, 2017, s.283). Tüm bunların yanında özellikle Türkiye için doçentlik jürilerinde araştırmacıların dosyalarının bu tür dergilerde yayınlananlar puanlama dışında bırakılabilir, YÖK, ÜAK veya üniversitelerin kendi etik komisyonları dönemsel avcı dergi listelerini açıklayarak, araştırmacıların bu dergilere kaynak oluşturmalarını engelleyebilir ve yayın sayısından çok, yayın niteliğini referans alan, atama ve yükseltme kriterleri getirilebilir.

Araştırmacıların oltaya düşmemeleri için yapabilecekleri; bir metin eşleştirme yazılımı yardımı ile sitedeki metnin başka sitelerden alınıp alınmadığına bakmaları, dergi ile bağlantılı hakem, editör vb. araştırmacıların gerçekten dergi ile ilişkisi olup olmadığı araştırabilir. İnternette açık erişimli potansiyel sahte yayıncıları içeren kara listeleri kontrol edebilirler(Enago, 2016). Etki faktörlerine çok fazla itibar etmemeleri, dergiler hakkında detaylı araştırma yapmaları önerilebilir. Yayıncıların çalışmalarını hazırladıktan sonra isin bittiğini düşünmemeli, yem e-postalara dikkat etmeleri gerektiğini ve yayıncı seçimini özenle yapmaları önerilebilir. Bunun yanın doçentlik jürilerinde, jüri üyelerinin bu tür açık erişimli dergilerin kara listelerindeki dergiler hususunda dikkatli olmaları, üniversitelerin personelleri için bu tür listeler hususunda uyarmaları öneri olarak getirilebilecek diğer hususlardır (https://guides.library.yale.edu/c.php?g=296124&p=1973764 gibi).

Park vd. (2018,s.52)'e göre kimlik avı ve kaçırma olaylarının önlenmesi için, akademisyenler ve akademisyenler, farkındalığı arttırmalı ve olası koruyucu ve koruyucu yöntemlerle ilgili bilgileri yükseltmesi gerekmektedir. Bu noktada akademik camianın bilinçlenmesi gerekmektedir. Bunun yanında bu durumu kötü amaçlı, hızlı yükselmek ve daha çok teşvik almak için kullanan kullanıcıların eğilimlerini engelleyebilmek için önlem alınması gerekmektedir. Bu noktada üniversitelerin bilimsel etik ve yayın komisyonları görev alabileceği gibi Yüksek Öğretim Kurumu (YÖK) ve Üniversitelerarası Kurul Başkanlığı (ÜAK) gibi kurumların daha aktif görev alması gerektiği ifade edilebilir. Bunun yanında tüm bu süreçlerin taraflarca sistematik şekilde analiz edilerek, yayın sayısından çok, yayınların atıf değerleri ve niteliğini ön plana alacak atama yükseltme kriterlerinin ve yöntemlerin ortaya konması önerilebilir. Aksi takdirde, gerek avcı dergiler sayısı gerekse bu dergilerde yayın yapan araştırmacıların sayısı artacak, akademisyenler kişisel bilgilerini, kredi kartı bilgilerini kaybetmeye devam edecek, siber suçluların ve suçların sayısı artabileceği gibi avcı dergi ve yayıncıların sayısı her geçen gün artmaya devam edeceği ve akademik yaşama ciddi zararlar vermeye devam edeceği düşünülmektedir.

Eğer oltaya gelindi ve kredi kartı bilgileri kaptırıldı ise, hemen kredi kart şifresi değiştirilmeli ve banka çağrı merkezi aranarak bilgi verilmelidir. Oltaya gelmemek için; tanımadığınız kişi ya da kurumlardan gönderilen e-postaları açmamalı, e-posta içindeki linkleri tıklamamalı ve e-postayla gelen dosyalar bilgisayara yüklenmemelidir. Bunun yanında, bankacılık şifresi herhangi bir yere yazılmamalı, bilgisayar ve tarayıcıya kayıt edilmemeli ve kimseyle paylaşılmamalıdır. Sadece güvenliğinden emin olunan bilgisayarlardan işlem yapılmalıdır. Güvenliğinden şüphelenilen bilgisayarlarda internet

bankacılığı gibi riskli işlemler yapılmamalı, arama motorlarından ve güvensiz sitelerden işlem yapılmamalı, sanal post ve sanal klavye kullanımına ve lisanslı anti virüs yazılımlarının kullanılmasına dikkat edilmelidir. İnternet üzerinde alış veriş yapılırken, internet sitelerinin güvenli olduğunu gösteren sertifikalar kontrol edilmelidir. Güvenlik duvarı kullanılmalı ve bu tür uygulamalar bilgisayarlarda aktif tutulmalıdır. İnternet gezgini tarafından indirilen dosyaların sık sık temizlenmesi gerekir. Kullanıcıların internet çıkışında kullandıkları cihazlara güçlü şifre koymaları gerekmektedir(Türkiye Bankalar Birliği,2015,s.40-41). Genelde oltalama amaçlı gelen e-postalar, e-posta sunucuları tarafından spam e-posta olarak algılanmaktadır. Spam e-postalar ile mücadele için sunucu ve kullanıcı tarafında alınması gereken çeşitli önlemler söz konusudur. İnternet tabanlı veya outlook benzeri e-posta okuyucularda önemsiz posta klasörü ayarlamalar yapılmalıdır(Şahinaslan vd.,2009).

7.4 Gelecek çalışmalar için öneriler

Oltalama yöntemi sosyal mühendislik çerçevesinde gerçekleşen karşı tarafı kandırmaya ve aldatmaya yönelik saldırılar olarak ifade edilebilir. Bunun yanında avcı dergiler veya avcı yayıncılar kavramının son yıllarda akademi dünyası için bir tehdit olarak ortaya çıktığı ifade edilebilir. Oltalama yönteminin kavramsal olarak değerlendirildiği çalışmalar Türkçe literatürde bulunmasına rağmen bu noktada yöntemlerin ve suçlardan kaçınmanın detaylı bir şekilde ele alındığı çalışmalara rastlanmamıştır. Bunun yanında uluslararası literatürde avcı dergi ve avcı yayıncılara yönelik son yıllarda pek çok çalışmanın yapılmasına rağmen Türkçe literatürde bu noktada önemli boşluklar görülmektedir. Araştırmacılar bu noktadaki boşlukları değerlendirmeleri, farklı konu ve araştırma soruları ile, bilimsel yayın kalitesinin artması, nitelikli Türkçe literatüre sahip olunması ve akademik camiada farkındalık oluşturulabilmesi için çalışmalar gerçekleştirmeleri ve paylaşmaları önerilebilir.

KAYNAKÇA

Aburrous, M., Hossain, M. A., Dahal, K. ve Thabtah, F. (2010a). Predicting Phishing Websites Using Classification Mining Techniques. *Inseventh İnternational Conference On Information Technology*; 2010 (s.176–181). Las Vegas, Nevada,USA: IEEE.

Akyazı, E., Dilmen, N.E. ve Kara, T. (2008). Türkiye Bilişim Derneği, 2. *İstanbul Bilişim Kongresi* 3-4 Haziran 2008, s.31-39.

Alsharnouby, M., Alaca, F. ve Chiasson, S. (2015). Why Phishing Still Works: User Strategies For Combating Phishing Attacks. *Int. J. Human-Computer Studies*, *82*(2015), 69-82.

Balcıoğlu, İ.(2014). İnternet Kullanımı ve Getirip Götürdükleri, *Somuncubaba İlim Kültür ve Edebiyat Dergisi*, (160), 64-67.

Beall J. (2015). Predatory Journals and The Breakdown of Research Cultures. *Information Development*, *31*(5), 473-476.

Beall J. (2016). Essential Information About Predatory Publishers and Journals. *International Higher Education, 86*, 2-3.

Beall's List. (2017). Potential, Possible, or Probable Predatory Scholarly OpenAccess Publishers. Erişim 09.12.2017, https://beallslist.weebly.com.

Beninger, P.G., Beall, J., ve Shumway, S.E. (2016). Debasing The Currency of Science: The Growing Menace of Predatory Open Access Journals. *Journal of Shellfish Research*, *35*(1),1-5.

Bilgin, U.E., Doğan, C.E., Koçak, A. ve Aktaş, E.Ö.(2013). Bilişim Teknolojisi İle Bankada İşlenen Bir Dolandırıcılık Suçu. *E-Journal of New World Sciences Academy*, *8*(3), 91-95.

Canbek, G. ve Sağıroğlu, Ş.(2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. *Politeknik Dergisi*, *9*(3), 165-174.

Clemons, M., M.D.E Silva, Joy, A.A., Cobey, K.D., Mazzarello, S., Stober, C. ve Hutton, B. (2017). Predatory Invitations from Journals: More Than Just a Nuisance?. *The Oncologist*, *2017*(22), 236-240.

Dadkhah M., Maliszewski T. ve Jazi M.D. (2016). Characteristics of Hijacked Journals and Predatory Publishers: Our Observations in the Academic World. *Trends in Pharmacological Sciences*, *37*(6), 415-418.

Dadkhah M. ve Bianciardi G. (2016). Ranking Predatory Journals: Solve the Problem Instead of Removing It!. *Advanced Pharmaceutical Bulletin*, *6*(1),1-4.

Dadkhah, M., Borchardti G. ve Maliszewski, T. (2017). Fraud in Academic Publishing: Researchers Under Cyber-Attacks. *The American Journal of Medicine*, *130*(1),27-30.

Djuric, D. (2015). Penetrating the Omerta of Predatory Publishing: The Romanian Connection. *Science and Engineering Ethics*, *21*(1), 183-202.

Dhamija, R., Tygar, J.D. ve Hearst, M.A.(2006). Why Phishing Works. *Conference on Human Factors in Computing Systems (CHI 2006), 22-27 Nisan, Quebec/ Canada*. *s*.581-590.

Elmas, Ç., Orman, A. ve Dener, M.(2011). İnternette Bilgi Güvenilirliğini Artıracak Bir Uygulama Geliştirilmesi. *e-Journal of New World Sciences Academy Engineering Sciences*, *6*(1), 135-147.

Eminağaoğlu, M. ve Gökşen, Y.(2009). Bilgi Güvenliği Nedir, Ne Değildir, Türkiye' de Bilgi Güvenliği Sorunları ve Çözüm Önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 11*(4), 1-15.

Enago. (2016). Sahte Dergiler Nasıl Tespit Edilebilir?, Erişim 09.12.2017, https://www.enago.com.tr/blog/sahte-dergiler-nasil-tespit-edilebilir/.

Enago. (2014a). Bir Yayıncıdan Çalışmanızı Ücretsiz Yayınlama Teklifi Gelirse Ne Yaparsınız?, Erişim 09.12.2017, https://www.enago.com.tr/blog/bir-yayincidan-calismanizi-ucretsiz-yayinlama-teklifi-gelirse-ne-yaparsiniz/.

Enago. (2014b). Bilimsel Dergiler Neden Sahte Makale Yayınlar?, Erişim 09.12.2017, https://www.enago.com.tr/blog/bilimsel-dergiler-neden-sahte-makale-yayinlar/.

Ercan, C.(2009). İnternet Kullanımında Etik Kaygılar ve Etik Kaygıların Giderilmesi Yönünde Organizasyonların Sorumlulukları. *Mevzuat Dergisi*, *11*(141), 1-11.

Erzurum Emniyet Müdürlüğü.(2013). İnternetteki Sahtekarlık ve Dolandırıcılıklar. Erişim: 12.05.2017, http://www.erzurum.pol.tr/Duyurular/Sayfalar/Internetteki-Sahtekarliklar-ve-Dolandiriciliklar-21102014.aspx.

Eşitli, A.E.(2013). Suçların ve Cezaların Kanuniliği İlkesi. *Türkiye Barolar Birliği Dergisi*, *2013*(104), 225-246.

Ferris, L.E. ve Winker, M.A. (2017).Ethical Issues in Publishing in Predatory Journals. *Biochemia Medica, 27*(2), 279-84.

Grzybowski, A., Patryn, R. ve Sak, J. (2017). Predatory Journals and Dishonesty in Science. *Clinics in Dermatology, 35*(2017), 607-611.

He, M., Horng S., Fan, P., Khan, K.M., Run, R., Lai, J., Chen, R. ve Sutanto, A.(2011). An Efficient Phishing Webpage Detector. *Expert Systems with Applications*.*38*(2011), 12018–12027.

Hekim, H. ve Başıbüyük, O.(2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları, *Uluslararası Güvenlik ve Terörizm Dergisi*, *4*(2),135-158.

Hong,J.(2012).The Current State of Phishing Attacks. *Communications of the ACM*, *55*(1), 74-81.

Ibba S., Pani F.E., Stockton J.G., Barabino G., Marchesi M. ve Tigano D. (2017). Incidence of Predatory Journals in Computer Science Literature. *Library Review*, *66*(6/7), 505-52.

Jakobsson, M. ve Myers, S.A.(2007). Phishing and countermeasures: Understanding the increasing problem of identity theft. *Introduction to Phishing* (Eds.). (ss.1–2). NewYork: John Wiley & Sons Inc.

Jeffrey Beall.(2017). Predatory Publishing. Erişim 09.12.2017, https://jefferson.libguides.com/c.php?g=250298&p=1666257.

Katz, A. (2017). The Predatory Journal Issue: Part II. *Oncology Nursing Forum*, *44*(6), 641-642.

Khonji, M., Iraqi, Y. ve Jones, A.(2013). Phishing Detection: A Literature Survey. *IEEE Communications Surveys & Tutorials, Fourth Quarter*, *15*(4), 2091-2121.

Kim, W., Jeong R.O. , Kim, C. ve So, J.(2011). The Dark Side of the Internet: Attacks, Costs and Responses". *Information Systems*, *36*(2011), 675-705.

Konradt, C., Schilling A. ve Werners, B.(2016). Phishing: An Economic Analysis of Cybercrime Perpetrators. *Computers & Security*. *58*(2016), 39-46

Kumar, M. (2017). Unicode and Phishing Attack. Erişim 12.05.2017 tarihinde, http://thehackernews.com/2017/04/unicode-Punycode-phishing-attack.html?m=1.

Masten, Y. ve Ashcraft, A. (2017). Due Diligence in the Open-Access Explosion Era: Choosing A Reputable Journal for Publication. *FEMS Microbiology Letters*, *364*(21), 1-7.

Mohammad, M.R., Thabtah, F. ve McCluskey, L.(2015). Tutorial and Critical Analysis of Phishing Websites Methods. *Computer Science Review*, *17*(2015), 1-24.

NHBVÜ-BİD.(2013). E-Posta ile Dolandırma Yöntemleri ve Alınacak Tedbirler, Erişim 12.05.2017, https://bidb.nevsehir.edu.tr/tr/5734.

Noga-Styron K.E., Olivero, J.M. ve Britto, S.(2017). Predatory Journals in the Criminal Justices Sciences: Getting our Cite on the Target. *Journal of Criminal Justice Education*, *28*(2), 174-191.

Özbek, M.(2015).The Impacts of European Cybercrime Convention on Turkish Criminal Law. Erişim12.05.2017,http://www.goksusafiisik.av.tr/Articletter/2015_Summer/GSI_Articletter_2015_Summer_Article6.pdf.

Pamukçu Günaydın G. ve Doğan N.Ö. (2015). A Growing Threat for Academicians: Fake and Predatory Journals. *The Journal of Academic Emergency Medicine*, (14), 94-96.

Park S.S., Lee E.Y.Y. ve Suh J.H. (2018). Arbitral Action and Preventive Methods Against Predatory Journal Practice. *Science Editing*, *5*(1),49-52.

Patil, P. ve Devale, R.P.(2016). A Literature Survey of Phishing Attack Technique. *International Journal*

of Advanced Research in Computer and Communication Engineering, *5*(4), 2091-2121.

Predatory Journals. (2017). List of Predatory Journals. Erişim:09.12.2017, https://predatoryjournals.com/journals/

Pyne, D. (2017). The Rewards of Predatory Publications at a Small Business School. *Journal of Scholarly Publishing, 48*(3), 137-160.

Rao, S.R. ve Ali, T.S.(2015). PhishShield: A Desktop Application to Detect Phishing Webpages through Heuristic Approach. *Procedia Computer Science, 54*(2015), 147-156.

RSA.(2013). 2013 A Year in Review, Erişim 12.05.2017, https://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-012014.pdf.

Sanal Pos ve Ödeme Şekilleri,(2017). Sanal Pos. Erişim 12.05.2017, https://201111604033k.wordpress.com/sanal-pos-ve-odeme-sekilleri/.

Sans Institute (2013). Hedef Odaklı Oltalama Saldırıları (Phishing Spear). Erişim 12.05.2017, https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201307_tr.pdf.

Şahinaslan, Ö., Borandağ, E., Can, E. ve Şahinaslan, E.(2009). Posta Sunucularında Spam Önleme Teknikleri. *Akademik Bilişim 2009*,11-13Şubat 2009 Harran Üniversitesi, Şanlıurfa-Turkey.

Singh, P., Maravi, P.S.Y. ve Sharma, S. (2015). Phishing Websites Detection Through Supervised Learning Networks. *2015 International Conference on Computing and Communications Technologies*. 26-27 Feb. 2015. Chennai, India. s.61-65.

Taşçı, U. ve Can, A.(2015). Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014, *Fırat Üniversitesi Sosyal Bilimler Dergisi*, *25*(2), 229-248.

The UK Card Association. (2015). Annual Report 2015. Erişim 12.05.2017, http://www.theukcardsassociation.org.uk/wm_documents/UK%20Cards%20Annual%20Report%202015%20FINAL.pdf.

Türkiye Bankalar Birliği. (2015). Dolandırıcılık Eylemleri ve Korunma Yöntemleri. Erişim: 12.05.2017, https://www.tbb.org.tr/Content/Upload/Dokuman/7328/TBB-Dolandiricilik-Eylemleri-ve-Korunma-Yontemleri.html.

Wiratningsih, R.(2018). Library Clinic Services in Avoiding Transaction in the Predatory Journal. *Library Management*, *39*(1/2), 21-30.

Xia J., Harmon J.L., Connolly K.G., Donnelly R.M., Anderson M.R. ve Howard H.A. (2015). Who Publishes in "Predatory" Journals?. *Journal of the Association for Information Science And Technology*, *66*(7), 1406-1417.

Yıldız S.(2007). Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi, *Selçuk Üniversitesi sosyal Bilimler Enstitüsü Dergisi*, (17), 609-623.