

İnternette Ödeme ve Güvenlik

Gülnur Eti İçli, Bora Aslan

Kırklareli Üniversitesi, Lüleburgaz Meslek Yüksekokulu
gulnuricli@yahoo.com, bora.aslan@kirkklareli.edu.tr

Özet: İnternet üzerinden alışveriş yapan tüketici sayısı gün geçtikçe artmaktadır. Fakat internet üzerindeki güvenlik riskleri tüketicilerin online alışverişe uzak kalmasına neden olmaktadır. Bu çalışmada, tüketicilerin güvenli bir alışveriş için dikkat etmeleri gereken noktalar üzerinde durulmaktadır.

Abstract:The number of the consumers shopping on internet is increasing day by day. Though, because of the security risk in shopping online the consumers are staying away. In this study, we are looking for the answer of the questions related with what should the consumers do for a secure on line shopping.

Anahtar Kelimeler: E-ticaret, güvenlik, internette ödeme.

1. Giriş

Elektronik ticaret günümüzde iş yapmanın yeni yolu olan internet üzerinden gerçekleştirilmektedir. Elektronik ticaret genel olarak düşünüldüğünde pek çok kişiyi, firmayı, üreticiyi, satıcıyı, kamu kurumunu, sivil toplum kuruluşunu içine alır. Yani elektronik ticarete; örneğin tüketiciler-satıcılar, üretici firmalar-devlet, ya da üretici firmalar-satıcılar bir taraf oluşturabilir.

Firma ile tüketici arasındaki elektronik ticaretin gelişmesinde; tüketicinin alışveriş için hiç beklemezsizin istediği zaman uygun fiyatlarla ve karşılaştırmalar yaparak ürün ve hizmet satın alması, gerektiğinde kendine özel ürünler sipariş etmek suretiyle kişiselleştirilmiş hizmetten yararlanması, her şeyin kendi kontrolünde olması ve bunu eğlenceli, rahat bir şekilde gerçekleştirebilmesi gibi kriterler ön plana çıkmaktadır. İnternet üzerinden alışveriş; tüketiciye sadece ürün ve hizmet değil bununla birlikte katma değer sunulmasıyla, güven oluşturulmasıyla ve daha fazla bilgiyi sunmak üzere web sitelerinin etkin tasarlanmasıyla daha da artacaktır.

E-tüketicinin seçim yaparak satın alım kararını vermesi kazanmış olduğu güvene, edindiği bilgilere ve oluşturulan bilince bağlıdır. Çünkü

e-tüketiciler de seçimleri sırasında tıpkı geleneksel yollarla satın alım kararını veren tüketiciler gibi - belki de elektronik ticaretin doğası gereği daha fazla - risk algılamaktadır. Risk algısı; tüketicilerin satın alım kararını vermesinde, değiştirmesinde ya da ertelemesinde rol oynayan önemli bir etmendir ve tüketicilerin satın alım kararının sonucu ile ilgili güvensizlik ve belirsizlik yaşamaları halidir. Satın alınacak ürün karmaşık ve fiyatı yüksek bir ürünse, ürün özellikleri belirsiz ise, ürünün markası yoksa ve satan kişi tanınmıyorsa, gerekli güvenlik önlemleri alınmamışsa bu durum e-tüketicinin güvensizliğini ve dolayısıyla riskini daha da artırır. Risk algılayan kişi de çeşitli firmaların kendisine en iyi olanakları sunan iyi tasarlanmış web sitelerini karşılaştırmak suretiyle bilgi arayacak yani risk algısını azaltmaya çalışacak bir davranış içine girecektir. Tüketicinin algıladığı riski çeşitli risk azaltıcı metotlarla en aza indirebilen ya da ortadan kaldırmayı başarabilen yani e-tüketici üzerinde güven oluşturmayı başarabilen firmalar tüketicinin karar vermesini kolaylaştırmakta, e-tüketicinin ürün ya da hizmeti satın almasını sağlamaktadır.

Tüketicilerin elektronik ortamdaki alımlarda kişisel risk - kredi kartı bilgilerinin kaybolmasından doğan bireysel zarar - ve özel hayat riski - mahremiyetin kaybedilmesi - önemli rol

oynamaktadır [1]. Kişisel risk olarak ifade edilen risk, kredi kartı bilgilerinin çalınması olasılığının yarattığı güvensizliği ifade etmektedir, yani güvenlik riskidir. Tüketiciler internet ortamında alışverişte herhangi bir şeyi satın almaya karar verdiğinde ürün bedelini genelde kredi kartıyla ödemektedir. İnternette alışveriş yapan tüketiciler bir ürün ya da hizmeti satın almak istediklerinde birtakım ödeme bilgilerini internet ortamında vermek durumundadırlar ki bu durum güvenlik sorununu doğurmaya ve tüketicilerin algıladıkları kişisel riski (güvenlik ile ilgili riski) arttırmaktadır.

İnternette alışverişte ekranda gözüken sipariş formuna kişiye ait kredi kartı numarası, kart sahibinin adı, son kullanma tarihi gibi bir takım bilgilerin girilmesi gerekmektedir. Ayrıca bunların yanında kişinin mesleği, toplam geliri, medeni durumu v.b birtakım sorularla da karşılaşmak mümkün olabilmektedir. Bu sorulara alınacak yanıtlar ileride bazı firmalarca kişinin kendisine ait olan, özel hayatı ile ilgili birtakım bilgilerin kişinin haberi olmaksızın değişik yerlerde kullanılması sonucu doğabilmektedir ki bu da özel hayat riski olarak ifade edilmektedir.

Kişisel risk olarak ifade edilen ve genellikle internette satın alımda güvenlik sorunu olarak ortaya çıkan risk aslında mağazadan yapılan alışverişlerde de karşılaşılan bir risktir. Örneğin; bir lokantada yenilen yemeğin bedelini ödemek üzere garsona kredi kartının teslim edilmesi ile internette bir mal satın alınması halinde kredi kartı bilgilerinin verilmesi arasında üstlenilen risk açısından fark bulunmamaktadır. Dolayısıyla aslında kişisel riskin sadece internette alımlarda değil her zaman karşılaşılabileceğimiz bir risk tipi olduğunu söylemek mümkündür. Kısaca ödemenin kredi kartı ile yapılması halinde karşılaşılan güvenlik riski sadece internette yapılan alışverişlerde değil kredi kartının kullanıldığı tüm alanlarda mevcuttur. Bu nedenle de hem gerçek dünyada hem de sanal ortamda güvenliğe dikkat etmek kaçınılmazdır.

2. Güvenlik Riskleri

İnternet milyonlarca bilgisayarı içine alan ağ sistemidir. Her bilgisayarda depolanan bilgi özel önlemler alınmadığı takdirde potansiyel olarak diğer bilgisayarların erişimine açıktır. Bu nedenle güvenlik önlemleri kaçınılmazdır. Güvenlik, bilginin doğruluğunu kanıtlayan ve bilginin bütünlük ve gizliliğini garanti eden bilgisayar programları ve mekanizmalardan oluşan prosedürler setidir [2]. Sanal mağazaları etkileyen güvenlik riskleri şunlardır [3] [4]:

- Sitenin Gizlice Dinlenmesi (Snopping Attacks): Bir kişinin web sitesine girerek müşteri bilgilerini örneğin kredi kartı numarasını ele geçirebilir. Bu riski minimize etmenin yolu bilgilerin iletilmesi sırasında şifrelenmesidir. Müşterinin kendisini güvende hissetmesi için SSL (Secure Sockets Lock) ve SET (Secure Electronic Transactions) gibi güvenlik yazılımlarını kullanmak suretiyle bilgiler şifrelenmekte ve risk en aza indirilmektedir. Aslında bu risk ile karşılaşma olasılığı diğer risklere bakıldığında daha azdır fakat internette alışverişte tüketicilerin en fazla korktukları tehlikelerin başında gelmektedir. Ayrıca yapılan çalışmalar kadınların erkeklere göre bu riski daha fazla algıladıklarını göstermektedir[1].
- Web Sitesini Kırmak (Web Site Break-Ins): Yetkili olmayan kişilerin ana sisteme girişi engellenememesinden ötürü sanal mağazaların web siteleri yetkisiz kişilere karşı korunamamaktadır. Sistemden sorumlu olan kişilerin ihmali sonucu sisteme birçok izinsiz giriş meydana gelir. Bunun önüne geçebilmek için güvenlik duvarı (firewall) ve virüs koruma programları kullanılarak şüpheli dosyalar ve yetkisiz kişilerin sisteme girişleri ve olası zararlarının önüne geçmek mümkündür.
- Güvenlik Eksikliği (Security Leaks): Sistemle ilgili ayrıntılı bilgisi olan kişilerin gizli bilgileri sistem dışındaki kişilere aktarması

şeklinde gerçekleşir. Gizli bilgilerin web sitesinde görülmemesi gerekirken görülebilmesi olarak ta ifade edilmektedir. İnternet üzerinde oluşan bu güvenlik açıklarının birçoğu insan hatasından kaynaklanmaktadır.

- Kasıtlı Olmayan Veri Kayıpları (Accidental Data Loss): Donanımla ilgili sorunlar ya da elektrik kesilmesi, sel gibi doğal felaketlerden dolayı sistemin zarar görmesidir. Bu riskten korunmak için bilgilerin yedeklenmesi gerekmektedir.
- Hizmeti Engelleyen Saldırıları (Denial of Service Attacks): Web sitesine çok sayıda ziyaretçi girmiş izlenimi verilerek sisteme çok yüklemeye yapılır ve site çöker, hizmet veremez. 1999'da Kosovo krizi sırasında NATO ve diğer organizasyonların sitelerine karşı bu tür hizmeti engelleyen saldırılar yapılmıştır.
- Değişirme ve Bütünlüğü Bozma (Unauthorized Modification and Integrity Attacks): Yetkisiz bir kişinin web sitesine girip fiyatları ve ürün bilgilerini değiştirmesi, müşterinin de bu doğru olmayan bilgilerle satın alımını gerçekleştirmesi şeklinde gerçekleşen bir saldırdır.

Yukarıda sözü edilen güvenlik risklerinin hepsi sanal mağazaları etkilemekle birlikte tüketicilerce en fazla bilinen ve en önemli güvenlik riski olarak belirtilen risk, kişilerin kredi kartı bilgilerinin çalınması ile ilgili olmaktadır. Yapılan araştırmalar da tüketicilerin sanal ortamdan alışverişini ancak kredi kartı numaraları ve kişisel bilgileri güvence altına alınır ve bu web sitesinde belirtilirse yapabileceklerini ortaya koymaktadır; bu nedenle firmalar web sitelerini oluştururken bu noktayı göz önüne almaları güvenlik önlemlerinin alındığına dair mesajların tüketicilere gösterilmesi gerekmektedir [6]. Yine başka bir araştırma sanal alışverişin en az tatmin olunan yönünün hala güvenlik olduğunu göstermektedir, buna göre tüketicilerin finansal güvenlik ve kişisel bilgilerin güvenliği ile ilgili algıladıkları risk, satıcının ünü (tanınan ve güvenilir bir firma olması) ve ne kadar iyi gü-

venlik teknolojileri kullandığıyla yakından ilişkilidir; bu nedenle sanal ortamda faaliyet gösteren firmaların ileri şifreleme teknolojilerini kullanmaları ve bunun hakkında müşterilerini bilgilendirmeleri gerekmektedir [7].

3. Güvenlik Önlemleri

İnternet üzerinde kredi kartı numaralarının güvenli bir şekilde iletilmesi ve yetkisiz herhangi bir kişinin bu bilgileri ele geçirmemesi için sitenin güvenlik yazılımları (SET, SSL gibi) kullanılması gerekmektedir. Pek çok firma ödeme sistemleriyle ilgili bu güvenlik sorununu aşmak için söz konusu yazılımları kullanmaktadır. Bu yazılımların kullanılması internet üzerinden işlem yapan bütün tarafların özel bir kodlama sistemi ile tanımlanması temeline dayanmaktadır.

Kredi kartı ile yapılan alışverişte taraflar; müşteri, satıcı (sanal ortamdaki satıcı ve onun web sitesi) ve bankalardır. Elektronik ödeme, tüketici, satıcı firma ve banka (finansal kurum) arasında bir protokol olarak düşünülmelidir [2].

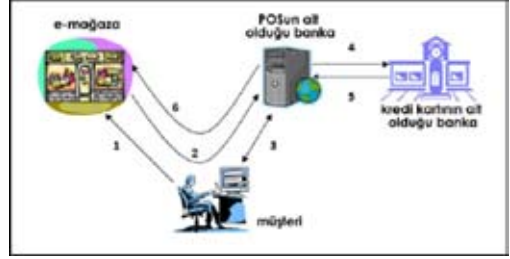
İnternet ortamında alışverişte kredi kartı fiziksel olarak kullanılmamakta, kredi kartı numarası internet üzerinden verilmektedir. Kredi kartı numarasının üçüncü şahısların eline geçme riski tüketicileri korkutmaktadır. Siber ödeme, elektronik para sistemi, SET (secure electronic transaction) ve SSL (secure sockets layer) gibi elektronik ödeme sistemleri içinde en çok kullanılan sistem SSL 'dir [2]. İnternette hizmet veren firmalar kredi kartı bilgilerinin güvenliği ve gizliliğini sağlamak için SSL (secure sockets layer) ve SET (secure electronic transaction) gibi güvenlik yazılımları kullanmaktadırlar. SET'in (Security Electronic Transactions) 'Güvenilir İşlemler Protokolü'; SSL'e göre daha güvenli olduğu belirtilmektedir. Güvenlik konusunda uluslararası bir standart getirmek amacıyla ilk önce Master Card, Visa Card, IBM, Microsoft, Netscape, Terica Systems ve Verisign' in katılımıyla geliştirilmiştir. SET protokolünün geliştirilmesi

internet üzerinden yapılacak işlemlerin şifrelenmesi yoluyla güvenlik sağlamak amacıyla yöneliktir. SSL ve SET ile kredi kartı numaraları güvenli bir şekilde (şifreli olarak) satıcı işletmeye iletilmekte ve bilgilerin başka bir kimse tarafından okunmasına olanak tanınmamıştır. SET güvenlik protokolünde; bilgilerin gizliliğini, kredi kartı kullanıcısının kartın gerçek sahibi olduğunu ve sitesinden alışveriş yapılan firmanın banka ile anlaşmalı bir firma olduğunu garantilemektedir. SET'te kartın kullanıcısının kredi kartının gerçek kullanıcısı olup olmadığı sorgulanırken SSL'de ise sorgulanmamaktadır.

Temel olarak e-mağaza ile e-müşteri arasında gelişen alışveriş süreci Şekil 1'deki gibi olmaktadır. Müşteri satın alacağı ürünün web sitesine bir internet tarayıcı (Internet Explorer, Firefox, Opera, Safari gibi) aracılığı ile bağlanır. Almak istediği ürünü alışveriş sepetine ekler ve sitenin ödeme sayfasına ulaşır. Bu sayfa müşterinin kredi kartı bilgilerinin alındığı özel ve güvenli bir alandır. Müşteri kredi kartı bilgilerini sisteme girer ve siteye iletir (1). Bu esnada bilgiler iletilirken e-mağaza ile müşteri arasında başka kimsenin anlamayacağı SSL şifrelemesi kullanılır. Kredi kartı bilgileri e-mağazanın POS sisteminin ait olduğu bankaya iletilir (2). Bu bölümde de SSL şifreleme kullanılarak POS banka, e-mağaza ve müşteri arasındaki bilgiler şifrelenir (3). Daha sonra POS banka ile müşterinin kredi kartının sahibi olan banka arasında veri transferi gerçekleştirilir ve kartın bilgileri kontrol edilip, onaylanır (4,5). Burada da büyük güvenlik önlemleri kullanılır. Son olarak POS banka ve e-mağaza arasında yine güvenli bir bağlantı kurularak kredi kartının onaylanıp ödemenin işleme alındığı ile ilgili bilgiler iletilir (6). Böylelikle müşteri elektronik alışverişini tamamlamış olur.

Müşteri, sanal ortamdaki firma ve banka arasındaki veri transferi sırasında bilgilerin şifrelenerek aktarılması esasına dayanan güvenlik önlemleri sayesinde bilgilerin başka kişilerin

eline geçmesi durumunda bu bilgilerin çözülerek kullanılmasının önüne geçilmiş olmaktadır. Güvenlik yazılımlarıyla bilgiyi gönderen bilgisayar ile alan bilgisayar arasında güvenli bir veri iletişimi sağlanmış ve kredi kartı numarası, isim, adres vb. bilgiler güvenli olarak iletilmiş olmaktadır.



Şekil 1 İnternet üzerinden alışverişte ödeme süreci

İnternette alışveriş yapmak, günlük yaşamda alışveriş yapmaktan daha güvenlidir. Fakat bunun için müşterilerin alması gereken bir çok önlem vardır. Eğer bu önlemler tam anlamıyla sağlanırsa güvenli bir alışveriş ortamı oluşturulur. Özellikle dikkat edilmesi gereken önlemler aşağıdaki gibidir:

- Müşteri öncelikli olarak kendi bilgisayarını korumak zorundadır. Günümüzde bilgisayarlar ve dolayısı ile içerisindeki bilgiler bir çok tehdit ile karşı karşıyadır. Bunların en önemlileri bilgisayar virüsleri, kötü amaçlı ajan yazılımlar ve bilgisayar korsanlarıdır. Bilgisayar virüslerinden korunmak için güncel bir anti-virüs programı kullanılmalıdır. Kötü amaçlı ajan yazılımlar için yine güncel anti-ajan yazılımları müşterinin bilgisayarında bulunmalıdır. Bilgisayar korsanlarının bilgisayarlardaki bilgilere ulaşamaması için ise güçlü bir güvenlik duvarı yazılımı kullanılmalıdır. Bu yazılımlar sayesinde bilgisayarın yerel güvenliği sağlanmış olur.
- İnternette alışveriş için kullanılacak olan internet tarayıcı güncel olmak zorundadır. İnternet tarayıcı geliştiren şirketler, internetteki tehditler ve yazılımdaki açıkları gi-

dermek için yeni yamalar veya versiyonlar yayınlamaktadır. Bazı tarayıcılar kendilerini otomatik olarak güncellemektedir bazı tarayıcılar ise bu işlemi kullanıcıya bırakmaktadırlar. Güncel bir tarayıcı sayesinde daha güvenli şekilde internet ortamında gezilebilir ve alışveriş yapılabilir. Düzenli olarak, kullanılan tarayıcının yeni versiyonlarını veya yamalarını, üreticinin web sitesinden takip etmek güvenli bir alışveriş için önemlidir.

- Alışveriş yapılan e-mağazanın tanınması önemlidir. Bilinmeyen bir mağaza tehlikeli olabilir. Bunun için e-mağazanın iletişim bilgileri, güvenlik sertifikası, dijital imza ve gizlilik politikası gibi bilgiler e-mağazayı tanımak için gerekli bilgilerdir. Bu bilgiler internet tarayıcılar aracılığı ile görülebilir. Örneğin Internet Explorer 7 tarayıcısında bir e-mağazanın ödeme kısmına gelindiğinde adres çubuğu bölümündeki kilit işaretine tıklanılarak sitenin sertifikaları, sertifika için başvuran ve veren şirketi, sertifikanın geçerlilik süresi gibi bilgiler görülebilir (Şekil 2).



Sertifika Bilgisi

Bu sertifika, aşağıdaki amaçlarla verilmektedir

- Uzak bir bilgisayarın kimliğini elde eder

* Ayrıntı için sertifika düzenleyicinin açıklamasına bakın.

Verilen:

Veren:

Geçerlilik 25.09.2008 - 25.09.2010

Şekil 2 İnternet Explorer için güvenlik sertifikası

Başka bir tarayıcı olan Firefox 3 yazılımında ise durum çubuğundaki asma kilide çift tıklanıldığında veya adres satırının başındaki yeşil bölmeye tıklanıldığında sitenin güvenlik sertifikası ile ilgili bilgiler görülebilir (Şekil 3).

Bu sertifika şu amaçlar için doğrulandı:

SSL Sunucusu Onay Belgesi	
Onaylanan	
Genel İsimler (CN)	
Kurumlar	
Kurumsal Birimler	
Seri Numarası	68:2D:CD:90:7B:74:1E:AE:07:40
Düzenleyen	
Genel İsimler (CN)	
Kurumlar	
Kurumsal Birimler	
Geçerlilik	
Yayımlama tarihi	25.09.2008
Bitiş tarihi	25.09.2010
Parmak izleri	
SHA1 Parmak izi	6A:6C:6F:9B:B4:2C:69:80:28:56:95:5E
MD5 Parmak izi	5C:C7:22:24:24:A2:8F:8F:F1:17:6C:8D

Şekil 3 Firefox 3 için güvenlik sertifikası

- Genellikle e-mağazalar kullanıcılarını müşterilerini sistemlerine üye yapmak isterler. Böylelikle onlara daha rahat ulaşarak ürünlerini, kampanyalarını tanıtabilirler. Bu üyelik işlemleri içerisinde belirlenecek olan şifre ve kullanıcı adları güçlü olmalıdır. Mümkünse harf ve rakam karışımı, tahmin etmesi mümkün olmayan uzun şifreler tanımlanmalıdır.
- Alışveriş yapılan sitenin veri iletiminde güvenliği sağlamak amacıyla geliştirilmiş SSL, SET gibi bir teknolojiyi kullandığından emin olmak gerekmektedir. Firmalar genellikle SSL güvenlik yazılımını kullandıklarını sitelerinin belirli yerlerinde belirtmektedirler. SSL sayesinde e-mağaza ile müşteri arasında bir şifreleme sistemi kurulur. Bu sayede müşterinin bilgisayarından gönderilen kredi kartı bilgileri gibi çok önemli bilgiler e-mağazaya şifreli olarak iletilirler. Böylelikle önemli bilgilerin sızması önlenmiş olur. Bunun yanında müşterilerin kullandığı tarayıcılar da SSL gibi teknolojileri basit resim ve ikonlar ile tarayıcı yazılımın görünür bir yerinde belirtmektedirler.



Şekil 4 Adres çubuğu ve durum çubuğundaki güvenlik simgesi

Örneğin bir çok popüler tarayıcı (Internet Explorer, Firefox gibi) Şekil 4'te olduğu gibi sayfanın adres çubuğunda veya durum çubuğunda asma kilit simgesi ile sayfanın güvenli olduğunu belirtmektedir.

- Kredi kartı ile bilgilerin girileceği sayfadaki internet adresinin sona eklenen "s" harfi ile "https (hyper text transfer protocol secure)" ye dönüşmesi kullanılan sitede SSL'in çalıştığını göstermektedir. Özellikle alışveriş tamamlanıp ödeme işlemi bölümüne gelindiğinde, bu dönüşüme dikkat edilmesi gerekir. Kredi kartı bilgileri sadece bu sayfada verilmelidir. Popüler internet tarayıcıların güncel versiyonları ise adres çubuğu bölümünü yeşil renkli olarak göstererek sitenin ve yapılan alışverişin güvenli olduğuna işaret etmektedir. Bunların yanı sıra alışveriş yaparken bu sitenin güvenli bir site olup olmadığını Secure Side Index'ten taramakta mümkündür.
- İnternet servis sağlayıcıların kablo ağının güvenli yerlerden geçmesi ve buradaki kabloların fiber optik kablolar olması daha güvenilirdir. Genelde bütün servis sağlayıcılar hem güvenlik hem de hız nedeniyle fiber optik kabloları tercih ederler.
- Tanınmış ve iyi bilinen firmaların web sitelerinden alışveriş yapmayı tercih etmek gerekmektedir. Bu firmalar müşteri memnuniyeti konusunda daha duyarlı davranmakta ve gerekli tedbirleri almaktadırlar. Firmaya güven ve sitenin genel görünümü -açık renklerde tasarlanmış bir site koyu renklerde tasarlanmış olandan daha güvenli algılanmaktadır- riski azaltmaktadır [5].
- Tanınmamış firmaların e-mağazalarından alışveriş yapılacak ise yukarıdaki işlemlere dikkat edilmelidir. Gerekirse sitenin güvenlik bilgilerini içeren sertifikaya bakılmalıdır. Tarayıcının durum çubuğunda veya adres çubuğunda kilit işareti yok ise bu siteden alışveriş yapılmamalıdır.
- Alışveriş yapılan sitede güvenlik ile ilgili birtakım sorunlar yaşandığında anında

başvurulacak bir isim, mail adresi, telefon numarası v.b bilgilerin olup olmadığına bakmak uygun olacaktır. Bir çok güvenli ve büyük e-mağaza müşterileri ile online sohbet ortamı sağlamaktadır. Elektrik veya internet kesintisi gibi durumlar kullanıcılar için tedirginlik uyandırmaktadır. Bu gibi durumlarda sitedeki müşteri ilişkileri ile iletişime geçmek gerekir.

- Sitelerin tüketicilerden birtakım bilgileri isterken bu bilgilerin başkalarıyla paylaşılıp paylaşılmayacağı hakkında tüketiciyi bilgilendirmeleri gerekmektedir. Yani firmanın gizlilik politikası olup olmadığına dikkat etmek gerekmektedir. Bir çok alışveriş sitesinin ana sayfalarında gizlilik politikası başlığı mevcuttur. Eğer bu konuda bir bilgi yetersizliği söz konusuysa o zaman bilgilerin verilmemesi gerekmektedir.
- Bankalar tarafından internette alışveriş için çıkarılan sanal kartlar tüketicilerin güvenlik sorunlarını yenmeleri için kullanıma sunulmuştur. Yüksek limitli kredi kartları yerine bu kartların tercih edilmesi uygun olacaktır. Bu kartların limitini yapılacak harcamaya göre oluşturmak mümkün olduğu için en azından bilgiler üçüncü bir kişinin eline geçse bile harcanabilir limit sınırlı olduğu için büyük bir kayıp meydana gelmeyecektir.

Eğer bu güvenlik önlemleri sağlanabilirse sorunsuz ve güvenli bir alışveriş yapılabilir.

4. Sonuç

İnternette alışverişin önündeki en önemli engel olarak güvenlik gösterilmektedir. Tüketicilerin algıladıkları güvenlik riskinin minimuma indirilmesi gerekmektedir. Bunun yapılabilmesi için de tüketicinin bu konularda bilgilendirilmesi kaçınılmazdır. Tüketiciler bilmedikleri konularda daha fazla güvensizlik yaşarlar ve daha fazla temkinli hareket ederler. Konu hakkında bilgi sahibi olmak ve nasıl hareket edileceğini bilmek tüketicilerin bu riskini azaltacak-

tır. Tüketicilerin bilgilendirilmesi için hem firmalara hem devlete hem de tüketici dernekleri gibi birtakım derneklere önemli görevler düşmektedir. Çeşitli iletişim araçları kullanılarak tüketicilere bilinçli alışverişin yolları hakkında bilgiler verilmesi, eğitici programların yapılması, gazete ve dergilerde güvenli alışveriş için izlenmesi gereken yollar hakkında haberlere ve köşe yazılarına daha fazla yer verilmesi, tüketicilerin dilek ve şikayetlerini değerlendirme ve kısa sürede çözüme konusunda ilgili birimlerin işbirliği içinde çalışmaları ve tüketicinin yasalarla korunması internette alışveriş, ödeme ve güvenlik konularında algılanan riski azaltmada ve dolayısıyla internette alışveriş oranını arttırmada son derece etkili olacaktır.

Kaynaklar

[1] Peterson, R. A., ' Electronic Marketing and The Consumer ', Safe Publications, 1997.

[2] Raja, J., Senthil velmurugan M., ' E-payments: Problems and Prospects ', Journal of Internet Banking and Commerce, Vol 13, Isu 1, April 2008.

[3] Carroll, J., Broadhead, R., ' Selling Online ', McMillan, Canada, 1999.

[4] Özmen, Ş., ' E-ticaret ', İstanbul Bilgi Üniv. Yayınları, Ocak 2003.

[5] Peppers, D., Rogers, M., 'The Future of Marketing', Prentice Hall, 2002.

[6] Salisbury, D., Pearson, R. A., Pearson, A. W., Miller, D.W., ' Perceived Security and World Wide Web Purchase Intention ', Industrial Management and Data Systems , 101/4, 2001,.

[7] Shergill, S., G., Chen, Z., ' Web-Based Shopping: Consumers' Attitudes Towards Online Shopping In New Zealand ', Journal of Electronic Commerce Research, Vol:6, Isu 2, May 2005.