İNTERNET BANKACILIĞI VE TARAFLARIN YÜKÜMLÜLÜKLERİ

Yrd. Doç. Dr. Abdurrahman SAVAŞ*

ÖZET

İnternet günlük hayatımızın vazgeçilmezleri arasında yer almaktadır. Pek çok diğer işlem gibi internet bankacılığı da çoğu kimse için önemlidir. Ev ve ofis bankacılığı, telefon bankacılığı, mobil bankacılık ve internet bankacılığı elektronik bankacılık uygulamalarının en önemlilerindendir. İnternet bankacılığı bankacılık işlemlerinin internet üzerinden yapılmasıdır. İnternet bankacılığı, hem bankalar hem de müşteriler açısından avantajlara sahip olduğu kadar sakıncalar da barındırmaktadır. Güvenlik internet bankacılığının en önemli problemidir.

ANAHTAR KELİMELER: *Elektronik Bankacılık, İnternet Bankacılığı, Güvenlik, Şifre, Kötü Amaçlı Yazılımlar*

INTERNET BANKING AND OBLIGATIONS OF PARTIES

ABSTRACT

The Internet is an integral part of our daily lives. Like other transactions, internet banking is very important for many people. Home and Office banking, telephone banking, mobile banking and internet banking are some of the electronic banking kinds. Internet banking is making banking transactions via internet. Internet banking has some adventages and disadventages both of banks and consumers. Security is the leading problem in internet banking.

KEYWORDS: *Electronic Banking, İnternet Banking, Security, Password, Malwares*

GİRİŞ

Son yıllarda teknoloji baş döndürücü bir hızla gelişmektedir. Şüphesiz bu gelişmelerin de en başında internet ve buna bağlı teknoloji gelmektedir. 1960'lardan itibaren ABD'de sadece askeri alanda kullanılmaya başlanan bilgisayarlar arasındaki iletişim, 1990'lardan itibaren sivil hayatta da kullanılmaya başlanmıştır. Birbirine bağlı bilgisayarlardan oluşan ağların (network) yine birbirlerine bağlanması ile oluşan global bir ağ ortaya çıkmış ve buna da internet adı verilmiştir.

İnternetin ortaya çıkışı ile birlikte pek çok işletme pek çok farklı şekilde faaliyetlerini internet ortamına taşımaya başlamıştır[1]. Bunun da bir sonucu olarak ticari faaliyetlerin de önemli bir kısmı internet ortamında icra edilmeye başlanmıştır. Pazarlama, reklam, bilgilendirme gibi aşamalardan başlayan bu faaliyetler bir süre sonra hukuki işlemlerin ve hatta tarafların borçlarını ifasının da internet ortamında yapıldığı bir düzeye çıkmıştır. Bununla beraber bankacılık uygulamaları da internet ortamından yapılmaya başlanmıştır.

Bankacılık uygulamalarının internet ortamında yapılmaya başlanmasından önce pek çok bankacılık uygulaması, çeşitli isimler altında, müşterilerin bankaya gitmeden hizmet alabilmelerini ve işlemlerini halledebilmelerini sağlamaya çalışmaktaydı. Elektronik bankacılık adı verilen bu uygulamalar çeşitli görünümler ve isimler altında uygulana gelmekteydi. İnternet bankacılığı ise bu yöndeki son nokta olmuştur. Gerçi internet teknolojisinin de temelinde elektronik altyapı olduğu için aslında internet bankacılığı da elektronik bankacılık başlığı altında incelenebilir. Ancak hem işlem hacmi, hem kendisine özgü yapısı ve işleyişi hem de tarafların yükümlülükleri ve sorumlulukları açısından arz ettiği önem ve farklılık, ayrı bir başlık altında incelenmesini gerektirmektedir.

Bu çalışmada öncelikle elektronik bankacılık uygulamaları ile internet bankacılığı uygulamaları ayrı ayrı başlıklar halinde incelenmiştir. Daha sonra da internet bankacılığında tarafların yükümlülüklerine

---

* Selçuk Üniversitesi Hukuk Fakültesi Öğretim Üyesi.

1 Adel M. Aladwani, Online banking a field study of drivers, development challenges, and expectations, International Journal of Information Management 21 (2001), s. 213.

değinilmiştir. En sonda da bu yükümlülüklerin ihlali durumunda doğabilecek sorumluluklar üzerinde durulmuştur

I- ELEKTRONİK BANKACILIK

A- Genel Olarak

Bankalar gelişen iletişim teknolojisinin bir sonucu olarak pek çok hizmeti, müşterilerinin bankaya gitmelerine gerek bırakmadan onların ayağına götürmeyi ve bu şekilde ticari faaliyetlerini artırmayı hedeflemişlerdir. Bunun sonucunda pek çok farklı uygulama ortaya çıkmıştır. Bütün bu faaliyetleri kapsayacak şekilde elektronik bankacılık şu şekilde tanımlanabilir. Bankacılık maliyetlerinin düşürülmesi, hizmet ağının genişletilmesi, rekabet üstünlüğünün kazanılması amacıyla bankacılık faaliyetlerinin elektronik iletişim araçları vasıtası ile yapılmasıdır[2]. Uygulamada elektronik bankacılık denilince belki akla ilk önce ATM bankacılığı gelmektedir. Ancak Elektronik bankacılık bu kadarla sınırlı değildir. Ev ya da ofis bankacılığı, telefon bankacılığı, televizyon bankacılığı, mobil bankacılık ve nihayet internet bankacılığı elektronik bankacılık türleri arasında sayılabilir[3]. Konunun daha iyi

2 Gup, Benton E., Elektronic Banking, The Future of Banking, (editor: Gup, Benton E.) Londra 2003, 131; Yıldırım, Kadir, Elektronik Bankacılık-Avrupa Birliği Ve Türkiye Uygulamaları, Yayınlanmamış Yüksek Lisans Tezi, İstanbul 2006, S. 44; Biçer, Murat, İnternet Bankacılığı Ve İnternet Bankacılığında Müşteri Eğitimi, Yayınlanmamış Yüksek Lisans Tezi, Ankara 2006, S. 47; Özcan; Zeynep Özge, Türkiye'de Elektronik Bankacılık: İnternet Bankacılığı Üzerine Bir Çalışma, Yayınlanmamış Yüksek Lisans Tezi, Sakarya 2007, 54; Wu, Jun, Factors that influence the adoption of internet banking by South Africans in the Ethekweni metropolitan region, Durban Güney Afrika, Tarih yok, s, 20.

3 Gup, 131; Shah, Mahmood/Clarke, Steve, E-banking management issues, solutions, and strategies, Newyork 2009, s. 2; Aktan, Bora/Teker, Edip/Ersoy, Pervin, Changing Face of Banks and the Evaluation of Internet Banking in Turkey, Journal of Internet Banking and Commerce, April 2009, vol. 14, no.1, s, 2-3; Durer, Salih/Özsözgün çalışkan, Arzu/Akbaş, Halil Emre, Gündoğdu, Ceren Erdin, İnternet Bankacılığını Kullanma Kararını Etkileyen Faktörler. Türk Banka Müşterileri Üzerine Bir Araştırma, MÜİİBFD, Yıl: 2009, C. XXVI, Sayı :1, s. 135; Wu, 20; Schaechter, Andra, Issues in Electronic Banking: An Overwiev, International Money Fund, 2002, s. 3..

anlaşılması için elektronik bankacılık uygulamalarına kısaca göz atmakta fayda vardır[4].

B- Ev ya da Ofis Bankacılığı

Ev ve ofis bankacılığı; özellikle gerçek kişilerin kişisel bilgisayar, kablolu ve dijital televizyon, özel görüntü ekranı (videotex) ya da telefon kullanarak, haberleşme ortamları üzerinden bankaların veri bankası tabanlarına erişmeleri, kendi hesapları üzerinde istedikleri işlemleri yapmaları ve bankaların sunduğu açık bilgi kaynaklarını ücretli veya ücretsiz kullanmaları uygulamalarının tümüdür[5]. Diğer bir ifade ile ev (veya ofis) bankacılığı müşterilerin bankaya gitmeden bulundukları yer ile banka arasında doğrudan bir elektronik iletişim hattının olmasına bağlı olarak bankacılık işlemlerini yapabilmelerini ifade etmektedir[6]. Kişilerin ev ya da ofislerinden bankanın bilgisayarına, bilgisayar, videotext, televizyon veya başka bir elektronik araç ile bağlanmaları önemli değildir. Bu açıdan bakıldığında ev bankacılığının müşterinin kullandığı elektronik araç, bu aracın bankaya bağlanmasını sağlayan iletişim hattı ve bankanın bilgisayar sistemi olarak üç ana temel üzerine kurulduğunu söyleyebiliriz[7].

C- Telefon Bankacılığı

Telefon bankacılığı, banka müşterilerinin; fatura ödeme, fon transferi, hesap kontrolü, bilgi alma ve kredi başvurusu yapabilme gibi çeşitli bankacılık işlemlerini banka şubelerine gitmeden, sabit veya mobil

---

4 Aslında elektronik bankacılık uygulaması 1870 li yıllara kadar uzanmaktadır. Western Union Telegraph Company 1871 yılında ülke çapında uygulanmak üzere talimatla para transfer uygulaması başlatmıştır. 1918 yılında telgraf kullanılmaya başlanmış, 1960'larda üzerine veri kaydedilebilen plastik kart teknolojisi keşfedilmiş ve bankalar da bu teknolojiyi ilk önce kullana sektör olmuşlardır. 1970'lerde ise çipli ödeme sistemleri geliştirilmiştir. 2000'lerde de internet bankacılığı başlamıştır. Kz. Gup, 132; Shah/Clarke, 10. Genel olarak e-banking olarak ifade edilen diğer elektronik bankacılık uygulamaları için bkz. Shah/Clarke, 30-52

5 Yıldırım, 97.

6 Yılmaz, Süleyman, Hukukî Açıdan Internet Bankacılığı, Yayınlanmamış Doktora Tezi, Ankara 2007, S. 19.

7 Yıldırım, 97.

bir telefon kullanarak, herhangi bir yerden günün yirmi dört saati yapabilmelerini sağlayan bankacılık türüdür[8]. Bu sistemde müşteri bir telefon hattından bankayı aramakta ve tuşları[9] kullanmak suretiyle bankacılık işlemlerini gerçekleştirmektedir[10]. Telefon bankacılığını diğer geleneksel kanallardan ayıran en önemli özellik, tamamen mekanik bir sisteme dayalı olması ve müşterilerin karşı taraftan canlı bir müşteri temsilcisiyle irtibat kurmadan telefonun tuşlarıyla işlem gerçekleştirebilmesidir[11]. Bazı telefon bankacılığı sistemlerinde telefon tuşları yerine doğrudan müşterinin sesini ve verdiği cevapları tanıyabilen bilgisayarlar kullanılmaktadır. Ancak ses tanıma sistemi ile çalışan bu bilgisayarların hata oranları oldukça yüksektir[12]. Telefon bankacılığı ile hesap işlemleri, transferler, yatırımlar, döviz işlemleri, kredi kartı işlemleri, hisse senedi ve bilgi güncelleme işlemleri yapılabilmektedir[13].

D- Televizyon Bankacılığı

Televizyon bankacılığı, bankalar tarafından hazırlanmış olan bir kanala, dijital televizyon hattı aracılığı ile bağlanılarak ve televizyonun tuşları ile komut vererek bankacılık işlemlerinin gerçekleştirilmesidir. Bu işlemde komutlar bankaya telefon hattı aracılığı ile ulaştırılmaktadır. Tüm bunları televizyona bağlanan ve adına STB bağlayıcı üst kutu denen dijital sinyalleri analog haline dönüştüren bir elektronik alet sağlamaktadır[14]. Bu işlemler banka ile müşteri arasındaki sözleşme

---

8 Yıldırım, 94.

9 Bu aramanın tuşlu telefon kullanılmak suretiyle yapılması gerekmektedir. Daha doğru bir ifade ile ton göndermeli olarak bu işlemin yapılması gerekmektedir. Bilindiği gibi telefon tuşlarına her basılmada farklı bir ton sesi duyulmaktadır. Bu farklı tonlar, farklı elektronik komutlara ayarlanmakta ve bankanın bilgisayarına bu surette talimat verilmektedir. Eski teknolojide çevirmeli telefon olarak bilinen ve tuşlu telefonlarla da gerçekleştirilebilen pulse olarak da ifade edilen gönderme şekli ise vuruşlu olarak çalışır. Bu sistem ile bilgisayarı kontrol etmek mümkün değildir.

10 Yılmaz, 21.

11 Biçer, 91.

12 Özcan, 69.

13 Özcan, 70.

14 Biçer, 90.

hükümlerine göre yapılmaktadır[15]. Buna göre müşteriye bir kullanıcı (müşteri) numarası ve bir de şifre verilmektedir. Bu yönüyle dijital TV, alternatif elektronik bankacılığın yeni bir kolu haline gelmektedir. Bu bankaların internet şubelerini kullanan müşterileri herhangi bir ek işlem yapmadan internet şubesi hesap bilgilerini ve şifrelerini kullanarak dijital TV bankacılığı hizmetlerini kullanabilmektedirler[16].

E- Mobil Bankacılık

Cep telefonu teknolojisi kullanılmak suretiyle global erişim imkanı sağlayan wap protokolünün ve GSM operatörlerinin sunmuş olduğu diğer hizmetlerin kullanılması ile bankacılık işlemlerinin gerçekleştirilmesidir[17]. Mobil bankacılık üç değişik şekilde gerçekleştirilmektedir. Bunlardan ilki kısa mesaj servisi (SMS) yoluyla müşterilerin bilgilendirilmesi, ikinci yol WAP destekleyen cep telefonları yoluyla internet üzerinden işlemlerin yapılması, üçüncü ve son yol ise palmtop (avuç içi) adı verilen bilgisayarlar ile internet üzerinden işlemlerin yapılmasıdır[18].

SMS bankacılığı, bazı bankacılık hizmetlerinin kısa mesaj uygulamaları ile gerçekleştirilmesini ifade etmektedir. Bu hizmetler genel olarak bakiye bildirimi, kur bildirimi, hesap hareketlerinde uyarı, kredi kartı son ödeme tarihi, hesap kesim tarihi, borç tutarı, kredi kartı limit azalması durumunda uyarı, kredi kartı borç ödeme günü geciktiğinde uyarı vadeye bağlı tüm ürünlerin hesaba dönüşünde uyarı, verilmiş emirlerin gerçekleşmemesi durumunda uyarı, banka kartı ile para çekildiğinde uyarı kredi kartı ile nakit avans çekildiğinde uyarı şeklinde ifade edilebilir[19].

Diğer bir tür olan wap bankacılığı ise wap teknolojisi temeline dayalı olarak internet üzerinden bankacılık işlemlerinin yapılmasıdır. Kablosuz Uygulama Protokolü (Wireless Application Protocol) ifadesinin İngilizce kısaltması olan WAP ile günlük döviz kuru, repo oranları, yatırım fonu fiyatları, altın fiyatları, mevduat faiz oranları,

---

15 Yılmaz, 21;

16 Biçer, 91.

17 Biçer, 88; Yılmaz, 22; Yıldırım, 96-97, Özcan, 72.

18 Shah/Clarke, 33; Özcan, 72.

19 Biçer, 89; Özcan, 72, Yıldırım, 96.

hazine bonosu faiz oranları, hesap bakiyeleri ve kredi karı borcu görüntüleme şeklinde bankacılık hizmetleri yapılabilmektedir[20].

Diğer mobil bankacılık türü olan PDA bankacılığı, cep bilgisayarlarından bankanın internet bankacılığı servisine ulaşarak bankacılık işlemlerinin yapılmasını sağlayan teknolojidir[21]. PDA ile doğrudan internete bağlanılabilmesi ve bu sistemlerin WAP teknolojisine sahip cep telefonlarından daha gelişmiş özelliklere sahip olması, WAP bankacılığına kıyasla bankacılık konusunda daha fazla hizmetin sunulabilmesine olanak tanımaktadır[22]. Avuç içi bilgisayarların pahalı oluşu sebebiyle, avuç içi bilgisayar bankacılığı çok gelişmemiştir[23].

F- Kabin (Kiosk) Bankacılığı

Kiosk bankacılığı ATM bankacılığının biraz daha gelişmiş türünü oluşturmaktadır. ATM bankacılığı 1939 da Amerika'da nakit para verme makinası ile başlamış, altı ay sonra hizmetten kalkmış ve 1967 de bu günkü anlamda ANM bankacılığı hizmet vermeye başlamıştır[24].

Kiosk, müşteri ilişkilerinin interaktif bir şekilde yürütülmesini sağlayan bir bilgi merkezi seklindeki bilgisayarlara verilen genel sistemdir[25]. Kabinler, bankaların ATM makineleri görünümünde tasarlanmış olup, alışveriş merkezlerinde, açık hava ortamlarda, sinemalarda ve her türlü genel ortamda kabin içinde veya serbest olarak kurulabilmektedir. Bankalar kabin aracılığıyla, alternatif bankacılık, online işlemler, her türlü kart bazlı hizmetler ve bilgilendirme amaçlı hizmetleri vermektedir[26]. Kiosk aracılığıyla, kamusal internet erişimi, alternatif bankacılık, online işlemler, bilet, rezervasyon işlemleri, hizmet tanıtımları, bilgi görüntüleme, şehir ve bina rehberleri, turistik bilgiler,

20 Shah/Clarke, 37; Özcan, 73.Yılmaz, 23.

21 Biçer, 90; Özcan, 73-74.

22 Biçer, 90.

23 Yılmaz, 23.

24 King, Brett, Bank 2.0, Singapore 2010, s. 231.

25 Özcan, 74; Yılmaz, 24.

26 Yılmaz, 24.

insan kaynakları, promosyon, kredi izleme ve her tür kart bazlı hizmetler verilebilmektedir[27].

II- İNTERNET BANKACILIĞI

A) Genel Olarak

İnternet, birden fazla haberleşme ağının birlikte meydana getirdikleri, metin, resim, müzik, grafik ve buna benzer dosyalar ile bilgisayar programlarının ve dijital ortamda depolanabilen her türlü verinin paylaşıldığı ve bilgisayarlar aracılığı ile karşılıklı olarak iletildiği, bilgisayarlar arasında kurulmuş bir ağlar ağıdır. Bu ağlar arasındaki ilişkiler IP (internet protokolü) kullanılmak suretiyle bilgisayarlar arasında gerçekleşir. Bilgisayarlar arasında sağlanan bu hızlı ve sonsuz olarak nitelenebilen ilişki sayesinde bilgiye kolay, hızlı ve aynı zamanda da çok ucuz bir şekilde ulaşılabilmektedir.

İnternet bankacılığı da internetin tanımına paralel olarak müşterilerin bankaya gitmesine gerek olmaksızın her türlü bankacılık işlemlerini bulundukları yerden internet ortamından bankaya bağlanarak yapmalarını ifade eden sistemin genel adıdır[28]. İnternet bankacılığında para çekme dışında tüm bankacılık uygulamaları yapılabilmektedir[29].

İnternet bankacılığı, elektronik ticaret faaliyetlerinin belki de en yaygın olanıdır. İnternet bankacılığının kolay ve ucuz olması yaygınlaşması sonucunu doğurmuş, bu yaygınlaşma da pek çok problemi beraberinde getirmiştir. Bu problemlerin hukuki görünümleri ve sorumluluğun tespiti de internet bankacılığındaki en önemli konular arasında yer almaktadır. Bu sebeple öncelikle internet bankacılığının yaygınlaşmasına sebep olan yararları üzerinde kısaca durmak gerekir. Bununla beraber bu yaygınlaşmanın getirdiği sakıncalara da kısaca değinilmelidir.

---

27 Özcan, 74; Ayrıca bkz. King, 240 vd..

28 Aladwani, 214, Yılmaz, 30; Durer/Çalışkan/Akbaş/Gündoğdu, 136; Wu, 21.

29 Durer/Çalışkan/Akbaş/Gündoğdu, 136.

B) İnternet Bankacılığının Yarar ve Sakıncaları

1- İnternet Bankacılığının Yararları

İnternet bankacılığı her şeyden önce kullanıcılara zaman kazandırmaktadır[30]. Hem banka şubesine ulaşmada hem de banka şubesinde işlemlerin yapılması için beklenen zaman açısından müşterilerce tercih edilmektedir. Mesai saati kavramının olmaması ve 365 gün 24 saat işlem yapılabilmesi de zaman açısından sağladığı diğer bir yarardır[31].

İnternet bankacılığının sağlamış olduğu diğer bir yarar da komisyon ücretlerinin neredeyse sıfır veya sıfıra yakın olmasıdır[32].

Müşterilerin çok sık aralıklarla bilgilendirilmesi de internet bankacılığının yararları arasında sayılabilir[33].

Müşterilerin hesaplarına bizzat kendilerinin girmesi, işlemlerin bizzat kendilerince yapılması ve her aşamada onaylarla kontrolünün sağlanmasının yanı sıra işlem yapmadan da durum kontrolleri ile hesap hareketleri izlenebilmektedir[34]. Böylece istenmeyen bir hareketliliğin en kısa sürede farkına varılabilmekte ve müdahale edilebilmektedir[35].

İnternet bankacılığının müşteriler kadar bankalar açısından da sağladığı yararlar bulunmaktadır. Kuruluş sebebi para kazanmak olan bankalar açısından en başta düşük maliyetli işlemler sağlamasıdır[36]. Banka şubesinden yapılan işlemlere göre, internet bankacılığı % 99

---

30 Yılmaz, 37; Shah/Clarke, 259; Biçer, 66; Yıldırım, 23; Özcan, 119; Wu, 24, Azouzı, Dhekra, The Adoption of Electronic Banking in Tunisia: An Exploratory Study, Journal of Internet Banking and Commerce, December 2009, vol. 14, no.3, s. 5 vd.

31 Shah/Clarke, 259; Yılmaz, 37; Özcan, 121; Durer/Çalışkan/Akbaş/Gündoğdu, 137; Azouzi 5.

32 Wu, 26; Yılmaz, 37-38.

33 Yılmaz, 38.

34 Shah/Clarke, 260; Azouzi, 5.

35 Yılmaz, 39; Yıldırım, 22.

36 Wu, 25; Durer/Çalışkan/Akbaş/Gündoğdu, 136.

tasarruf sağlamaktadır[37]. Bankanın kendi müşterilerine karşı sunmuş olduğu hizmetin kalitesi ve diğer imkanlar artarak müşterileri ile arasındaki bağlantılar daha da pekişmektedir. İnternet bankacılığının yaygınlaşması da bankalara müşteri sayısı açısından avantaj sağlamaktadır. Her yerden ve her zaman bankacılık işlemlerinin yapılabilmesi, bu işlemlerin sürekliliği ve kolaylığı müşteri sayısının artması sonucunu doğurmaktadır[38].

İnternet bankacılığının IP temelli olması ve bu işlemlerin bankaların log kayıtlarında tutulması, müşterilerin işlem zamanı, işlem türü, işlem sıklığı, işlem hataları ve bir çok konudaki eğilim ve beklentilerinin tespit edilmesine imkan tanımaktadır. Bu da bankaların kendilerini geliştirmeleri konusunda yarar sağlamaktadır. İnternet bankacılığı belli bir mali ve kültürel birikim temeline bağlı olarak kullanılmaktadır. Bunun sonucu olarak da internet bankacılığı hizmeti sunan bankalar yüksek gelirli müşterilerin yanında kültür ve eğitim seviyesi yüksek olan ve daha problemsiz müşteriler elde etmektedirler[39]. Ayrıca internet bankacılığı, bankaya müşterilerine karşı teknolojiyi kullanmanın getirdiği yüksek bir imaj sağlamaktadır[40]. Müşteri kitlesi artan bankaların gelirleri de buna bağlı olarak artmaktadır[41]. İnternet bankacılığı sayesinde iş yükü azalan bankalar daha başka alanlarda efor sarf etmekte ve müşterileri ile daha fazla ilgilenebilmektedirler[42].

---

37 Yuan, Xina/Lee, Hyung Seok/ Kim, Sang Yong, Present and Future of Internet Banking in China, Journal of Internet Banking and Commerce, April 2010, vol. 15, no.1, s. 3; Özcan, 119; Yılmaz, 39;

38 Durer/Çalışkan/Akbaş/Gündoğdu , 137; Shah/Clarke, 257; Yılmaz, 40; Özcan, 119.

39 Shah/Clarke, 260; Karş. Yuan/Lee/Kim, 6, 8, Bu konuda ayrıntılı bilgi için bkz. Riquelme, Hernan E., Internet Banking Customer Satisfaction and Online Service Attributes, Journal of Internet Banking and Commerce, August 2009, vol. 14, no.2, s. 2 vd.

40 Durer/Çalışkan/Akbaş/Gündoğdu , 137; Shah/Clarke, 261.

41 Shah/Clarke, 261; Durer/Çalışkan/Akbaş/Gündoğdu, 137.

42 Shah/Clarke, 262; Durer/Çalışkan/Akbaş/Gündoğdu, 137.

2- İnternet Bankacılığının Sakıncaları

İnternet bankacılığının yaygınlaşması ile birlikte çok farklı sebeplere dayanan sakıncalar da ortaya çıkmıştır. Bu sakıncalar müşteriler için olduğu kadar bankalar için de söz konusu olmaktadır. Bu sakıncalardan ilki işlem yapan kişinin kimliğinin tespitindeki zorluklardır.

Müşteriler açısından ilk sakınca, bir bilgisayar ve internet bağlantısına ihtiyaç göstermesidir[43]. Bilgisayar fiyatlarının yüksekliği, bağlantı ücretlerinin ve/veya şartlarının ağırlığı internet bankacılığının önündeki ilk engeldir[44]. Bu sebeple toplumda kendilerini teknoloji özürlü olarak tanıtan kimseler internet bankacılığından yararlanamamaktadırlar.

Güvenlik problemi hem bankalar hem de müşteriler açısından önemli riskler oluşturmaktadır. Bu da internet bankacılığının belki de en önemli sakıncalarından birisini oluşturmaktadır[45].

Müşteriler açısından oluşan ve son zamanlarda oldukça sık rastlanan diğer bir sakınca da girilen web adresinin gerçekte girilen bankaya ait olup olmadığının tespitidir[46]. Özellikle elektronik posta adresine gelen ve sanki müşterisi olunan bankadan gelmiş gibi bir görüntü arz eden maillerdeki linklere tıklanması ile aslında gerçek olmayan banka sitesine yönlendirme yapılmaktadır. Gerek dizayn ve gerekse alan adı benzerliği gibi sebeplerle müşteri giriş bilgilerini girmekte ve bu bilgiler sistem tarafından elde edilmiş olmaktadır. Gerçek banka sitesi olmadığı için hesabına ulaşamayan müşteri sayfadan ayrılmakta, problemi anlayıncaya kadar veya tekrar giriş yapıncaya kadar hesaplar boşaltılmaktadır. Müşteriler, bilgisayarlarını her türlü internet erişimi için kullanmaktadırlar. Bunun sonucu olarak mail, usb bellek, hatta ziyaret edilen bir siteden dahi bilgisayarlarına Truva atı adı verilen ve çok küçük boyutlardaki yazılımlar bulaşabilmektedir. Bu sayede de

---

43 Wu, 24; Durer/Çalışkan/Akbaş/Gündoğdu, 138.

44 Yılmaz, 42; Shah/Clarke, 264.

45 Azouzı, 5 vd.

46 Turan, Mehmet, http://www.olympos.net/belgeler/guvenlik/alternatif-bankacilik-yontemleri-ve-karsi-karsiya-kaldiklari-sorunlar-5336.html; Yılmaz, 42.

üçüncü kişiler yapılan her türlü işlemi uzaktan takip edebilmekte, bu kişilerin hesap bilgilerine ulaşabilmektedirler.[47]

Bankaların işlemlerini internet ortamına taşımaları ve müşterilerin de bankaya gitmeden işlemlerini online yapmaları, banka ile müşterilerin arasındaki ilişkileri azaltmaktadır[48].

İnternet bankacılığındaki en önemli problemlerden birisi de işlem yapan kişinin kimliğini tespitte yaşanan sıkıntıdır[49]. Bunun aşılması için bankalar müşterilerine kullanıcı adı, müşteri numarası, parola, şifre, güvenlik kodu gibi isimlerde kendilerini tanıtmalarına yarayacak bilgiler vermektedirler. Müşteriler de kimseyle paylaşmamaları gereken bu bilgileri sisteme girerek kendilerini tanıtmaktadırlar. Bu parolaların kolay tahmin edilebilir olması, bir yere yazılması, birisine söylenmesi gibi sebeplerle müşteriler mağduriyet yaşamaktadırlar. Pek çok zaman da bilgisayardaki casus yazılımlar sebebiyle bu bilgiler kötü niyetli kişilerce öğrenilmekte ve hesaplar boşaltılmaktadır[50].

Müşterilerin işlem yapabilmelerinin ön şartı internet bağlantısının mevcut olmasıdır. Bazen ne banka ne de müşterilerin kusuru olmaksızın kesintiler ve yavaşlamalar oluşabilmektedir. Bu da internet bankacılığı kullanan kişiyi mağdur edebilmektedir.

A- İNTERNET BANKACILIĞINDA TARAFLARIN GÖREV VE SORUMLULUKLARI

1- GENEL OLARAK

İnternet bankacılığının sorunsuz işleyebilmesi için hem bankalara hem de müşterilere düşen görevler bulunmaktadır. Bu görevlerin yerine getirilmesi konusunda gösterilecek en küçük bir duyarsızlık ya da ihmal telafisi zor zararların ortaya çıkmasına sebep olabilmektedir. Bu görevler

---

47 Yılmaz, 43; Shah/Clarke , 111; Turan, http://www.olympos.net/belgeler/guvenlik/alternatif-bankacilik-yontemleri-ve-karsi-karsiya-kaldiklari-sorunlar-5336.html, Schaechter, 23; Bu konuda geniş bilgi için bkz. Canbek, Gürol/Sağıroğlu, Şeref, Casusu Yazılımlar ve Korunma Yöntemleri, Ankara 2006, 171 vd.

48 Shah/Clarke, 114.

49 Yılmaz, 45.

50 Lininger, Rachael/ Vines, Russell Dean, Phishing Cutting the Identity Theft Line, 106 vd.

çoğunlukla taraflar arasındaki sözleşmeden kaynaklanmaktadır[51]. Bu sözleşmeler içerisinde yer alan ve ortaya çıkan uyuşmazlıklarda bankaların dayanak noktalarından birini oluşturan genel işlem şartı niteliğindeki maddeler ve bunların geçerliliği konusundaki tartışmalar konumuz dışında kalmaktadır. Ancak gerek sözleşme serbestisi ve gerekse internet ortamının yapısından kaynaklanan bazı yükümlülükler taraflara dağıtılmaktadır. Bu yükümlülüklerin bir kısmına ait olan en önemli özellik de zamanla değişebilir nitelikte olmasıdır. Bu sebeple internet ortamının ve özelliklerinin taraflarca yakından takip edilmesi ve üzerlerine düşen yeni yükümlülükleri buralardan tespit edip yerine getirmeleri beklenmelidir.

Bu başlık altında tarafların yerine getirmekle yükümlü oldukları ve pek çoğu sözleşmeden kaynaklan görevlerin neler olduğuna kısaca göz atılmıştır.

2- TARAFLARIN GÖREVLERİ

a) BANKANIN GÖREVLERİ

Banka, anonim şirket şeklinde örgütlenmiş tüzel kişi tacirdir. İnternet bankacılığı hizmeti sunan bankalar bu hizmeti müşterilerine kolaylık olması için yapmalarının yanında kendi işlem hacimlerini artırmak ve daha fazla gelir elde etmek için yapmaktadırlar. Bunun için de sadece bu hizmeti uygulamaya koymak yeterli olmayıp bunun gerektiği gibi işlemesi ve hedeflediği amaca ulaşması için gerekli diğer tüm görevlerin de yerine getirilmesi gerekmektedir.

Bankalar güven kurumu olarak faaliyet göstermektedirler. Bu sebeple her şeyden önce internet bankacılığı işlemlerinin güvenilir bir şekilde yapılabilmesi için tüm altyapının güvenliğinin sağlanması gerekir.

Bu güvenlik hem dijital ve hem de matbu diğer evrak açısından sağlanmalıdır. İnternet ortamında yapılan bankacılık işlemlerinde bankalar sistemlerini SSL adı verilen bir güvenlik sistemi ile

---

[51] Bu konuda ayrıntılı bilgi için bkz. Yılmaz, 51 vd; http://hukukcu.com/modules/smartsection/item.php? itemid=116

korumaktadırlar[52]. Bu SSL protokolü kriptolu bir güvenlik protokolüdür[53]. Bu protokol son zamanlarda SSL/TLS olarak uygulanmakta ve elektronik ticaret yapan web siteleri ile özellikle internet bankacılığında kullanılmaktadır[54].Bankalar bu güvenlik sistemini kurmalı, devamlı işler bir durumda bulundurmalı ve gerektiğinde daha üst versiyonları ile değiştirmelidir.

Bankaların, özellikle müşterilerine ait dijital ve matbu dokümanları saklamak şeklinde beliren ilk görevlerinin ardından ikinci görevleri, internet bankacılığı kullanmak suretiyle bu saklanan verilere ulaşmaya çalışan kişinin, gerçekten hesap sahibi ya da yetkili erişimci olup olmadığının tespitidir. Bu amaçla bankalar kullanıcılara password, kullanıcı adı, giriş kodu, parola, şifre gibi isimlerle, kendilerini sisteme tanıtmalarına yarayacak bilgiler vermektedirler. Bu bilgiler başkaları ile paylaşılmaması gereken veriler olup sadece kişiye özeldir. Bu bilgilerin sisteme girilmesi durumunda banka başka kişide olmaması gereken bu bilgileri doğru giren kişinin kimliğini tespit etmiş olmaktadır. Bankalar özellikle kişilere ait olan ve sisteme giriş izni veren bu verileri de farklı katmanlarda ve ayrı ayrı saklamalıdır. Banka personelinin dahi bu verilere ulaşması mümkün olmamalıdır.

Bu amaçla bankaların müşterilerine tanımladıkları kullanıcı adları ile şifreler, işlem parolaları, tek kullanımlık şifreler, smart kartlar, mobil imzalar zaman, IP veya ISS kısıtlamalarına yönelik ek önlemler bu amaçla getirilmiş önlemlerden bazılarıdır. Bankalar bu önlemlerin kullanıcı adı ve şifresi olarak bilinenlerden başka bir ya da birkaç tanesinin aynı anda kullanılmasına imkan tanıyarak sistemi daha güvenli hale getirmeye çalışmaktadırlar. Ancak şunu unutmamak gerekir ki dijital teknoloji ve dolayısıyla internet baş döndürücü bir hızla gelişmekte, takip etmek neredeyse imkansız hale gelmektedir. Buna bağlı olarak da

---

52 Mannan, Muhammad, Security and Usability: The Gap in Real-World Online Banking, http://www.ccsl.carleton.ca/paper-archive/mannan-nspw07.pdf, s,3.

53 Oppliger, Rolf, SSL and TLS: Theory and Practice, Narwood, USA 2009, 82.

54 Alain Hiltgen/ Thorsten Kramp/ Thomas Weigold, Secure Internet Banking Authentication, IEEE Security and Privacy, vol. 4, no. 2, s. 24, Oppliger, 227.

internet dolandırıcılığı veya sahtekarlığı olarak isimlendirilebilecek uygulamalar da hızla artmaktadır. Bir güven kurumu olan bankaların da aynı zamanda bir tüzel kişi tacir olarak basiretli bir şekilde hareket etmesi, bu gelişmeleri takip etmesi, ortaya çıkan dolandırıcılık yöntemlerinden etkilenmemek için gerekli her türlü önlemi almaları gerekmektedir. İşlemlerini internet ortamına taşıyarak daha fazla müşteri kitlesine ulaşmak ve dolayısıyla daha fazla kar elde etmek isteyen bankaların buna paralel olarak gerekli teknolojik ve yazılımsal önlemleri almaları da gerekmektedir. Bu konuda internet bankacılığı ile ilgili doğrudan bir düzenleme bulunmamakla beraber aynı mantık içerisinde geliştirilen ve çoğunlukla aynı sistem üzerinden çalışan kredi kartlarında da benzer bir düzenleme bulunmaktadır. Buna göre 5464 sayılı Banka Kartları ve Kredi Kartları Kanununun kartı çıkaran kuruluşların yükümlülüklerini düzenleyen 8. maddesinde **"***Kart çıkaran kuruluşlar, kartların kullanılması bir kod numarası, şifre ya da kimliği belirleyici başka bir yöntemin kullanılmasını gerektiriyorsa, bu tür bilgilerin gizli kalması amacıyla gerekli önlemleri almak ve harcama ve alacak belgesinin müşteri nüshası üzerinde ve yazışmalarda kart numarasının açıkça yer almasını engellemekle yükümlüdür."* denmektedir**.** Bu hükmün kıyasen uygulanması da bankaların görevlerini açıklamak açısından önemlidir.

Bankaların açıklanan konumları gereği belirtilen güvenlik tedbirlerini re'sen almaları ve bu konuda gerekli internet güvenliği bilgisi ve tecrübesi olmayan kişilerin bir talebinin olmasını beklememeleri gerektiğini düşünmekteyiz[55]. Müşteriden herhangi bir talep gelmemesine rağmen müşterilerine yeni faiz kampanyaları hakkında bilgi veren bankaların güvenlik sistemlerindeki değişiklik veya gelişmeleri doğrudan müşteriye ulaştırmaları gerekir. Bankaların bu bilgilendirme servisini doğrudan devreye sokması, müşteri açıkça bu güvenlik tedbirini

[55] Nitekim banka ile her hangi bir şekilde müşteri olarak bağlantısı olan kişilerin cep telefonlarına her gün en az birkaç kere bankaların yeni kampanyalarının, faiz oranlarının, anlaşmalı firmalarla olan uygulamalarının duyurulmasına yönelik kısa mesajların geldiği bilinen bir gerçektir. Bu mesajların gelmesinde müşterilerin herhangi bir talebi ve isteğinin olmamasına rağmen mesajların yollanmasında titizlik gösteren bankanın, sistem güvenliğine yönelik tedbirleri almada daha dikkatli davranması gerekir.

kullanmak istemediğini ifade etmişse o takdirde kullanımdan kaldırması gerektiğini düşünmekteyiz.

Bankaların üzerine düşen diğer önemli bir görev de müşterilerin bilgilendirilmesidir. Küçük tasarruf hesapları açıp bankaların yaygın para çekme ağından yararlanmak isteyen kişiler tüketici sıfatı ile bankalarla işlemler yapmaktadırlar. Bu sebeple her şeyden önce tüketicilerin aydınlatılmasına yönelik yükümlülük ilk planda karşımıza çıkmaktadır[56].

Banka ile müşteriler arasındaki hukuki ilişki bir sözleşme ilişkisidir. Dolayısıyla taraflara sözleşmeden bazı yükümlülükler doğmaktadır. Tüketicinin aydınlatılmasına yönelik yükümlülük esasında sözleşmeden doğan genel bir yükümlülüktür. Bu yükümlülük en etkin bir şekilde yerine getirilmelidir.

Bankalar, sayfalarına giren müşterilerine hizmetleri hakkında bilgiler vermekte ve genel anlamda reklam yapmaktadırlar. Bu işlevi kusursuz bir şekilde yerine getiren bankalar, internet bankacılığı kullanan müşterilerini aydınlatma konusunda da aynı hassasiyeti göstermelidirler. Bu da hem internet bankacılığının yapılmasına ve işleyişine hem de taşıdığı risklere yönelik olmalıdır. Ayrıca bu bilgilendirme bir kereye mahsus olmamalı ve müşterinin sayfayı her ziyaretinde, gerektiğinde güncellenerek ve bunun da müşteriler tarafından fark edilmesi sağlanarak yapılmalıdır[57].

Daha önce de ifade edildiği gibi internet bankacılığı IP temeline dayanmaktadır. IP, kişilerin internete çıkış yapabilmeleri için kendilerine bu hizmeti sunan İSS tarafından atanan nümerik bir adrestir[58]. Bu adres (numara) sabit olabileceği gibi değişken de olabilir[59]. Statik ve dinamik

---

56 Memiş, http://hukukcu.com/modules/smartsection/item.php?itemid=116.

57 Memiş, http://hukukcu.com/modules/smartsection/item.php?itemid=116

58 Yatlı, Binnur, Elektronik Ticarette Vergilendirme, İstanbul 2003, s. 48.

59 Statik ve dinamik IP olarak isimlendirilen bu sabit ve değişken IP numaraları İSS sağlayıcı tarafından alınan hizmetin şartlarına göre atanabilmektedir. İSS ile yapılan sözleşme gereği sabir bir IP tahsis edilmesi gerekiyorsa internete her bağlantı yapılışında İSS, kendisinden IP numarası isteyen bilgisayar (kullanıcısına) aynı IP numarasını verecektir. Eğer her seferinde aynı IP adresi verilmesine ilişkin bir sözleşme yoksa bu sefer İSS, o andaIP havuzunda boş olan bir IP numarasını kullanıcıya tahsis eder. Bunu da tarih, saat ve saniye olarak kaydeder. Eğer IP havuzu o

IP numaralarından herhangi birisi ile devamlı sisteme giriş yapan kullanıcının giriş yaptığı bu numaralar log kayıtları olarak kaydedilir. Bu da bankaların önemli görevleri arasında yer alır. Bankaların log kayıtları incelendiğinde hangi IP adresinden ne zaman sisteme log on olunduğu (giriş yapıldığı), hangi işlemlerin gerçekleştirildiğinin kaydedildiği görülecektir. Bankalar bu numaraları devamlı takip etmeli eğer devamlı aynı numaralı IP adrsinden sisteme giriş gerçekleştirilmesine rağmen bu sefer başka bir (havuza ait) IP adresinden giriş gerçekleştirilmişse banka bu durumu hemen tetkik etmelidir. Her seferinde baka başka IP numaralarından sisteme giriş yapan tabiri caiz ise gezgin bir müşteri söz konusu ise banka, IP değişikliğine bağlı herhangi bir kilitleme yapmamalıdır[60].

Son zamanlarda bankaların bankacılık işlemlerinin yapılabilmesi için tek kullanımlık şifre uygulamasına geçtiği bilinmektedir. Bu yöntem kötü niyetli kişilerin hesaplara sızmalarını büyük ölçüde engellemiştir. Ancak tamamen yok edememiştir. Çünkü yaşanan bazı olaylarda kötü niyetli kişiler, müşterilerin bankadaki kayıtlı telefon numaralarına ait GSM operatörlerine müracaat ederek, kendilerini kart sahibiymiş gibi tanıtmakta ve kart/telefonlarını kaybettiklerini söyleyerek yenisini çıkartmaktadırlar. Maalesef bunu da sahte belgelere dayanarak, nüfus idaresinden aldıkları soğuk damgalı nüfus cüzdanları ile yapmaktadırlar. Yeni Sim kartını alan kişiler hesabı boşaltmakta ve bu işlemi de bankanın bu yeni karta yolladığı tek kullanımlık şifreyi girerek yapmaktadırlar. Dolayısıyla bankalar tek kullanımlık şifre uygulaması ile rehavete kapılmamalı, bunun yanında başka sistemleri de devreye sokmalıdırlar.

Yine müşterilerin hesap hareketleri belli istatistikler dahilinde takip edilmeli ve müşterinin o zamana kadar yaptığı işlemlerden farklı ve olağan dışı bir işlemi olduğunda banka bu durumu fark etmelidir. Örneğin hiç gece işlem yapmayan veya hafta sonlarından başka zaman sisteme girmeyen, ya da hiç havale yapmamış olmasına rağmen bu sefer

bölgedeki kullanıcılardan daha fazla IP numarasına sahipse, aboneye karşı herhangi bir taahhüdü olmamasına rağmen aynı IP numarasını atayabilir. Ancak ister aynı IP olsun isterse her seferinde farklı IP numarası olsun bütün numaralar belli bir aralığın içerisinde olan ve baş kısmı tamamen aynı olan IP numaraları olacaktır.

60 Memiş, http://hukukcu.com/modules/smartsection/item.php?itemid=116.

yüklü miktarda havale yapan veya çok kısa aralıklarla ve çok sayıda havale işlemi gerçekleştiren bir müşteri işlemi hemen algılanmalı ve gerekli güvenlik tedbiri hemen uygulamaya konulmalıdır. Burada sayılan hususlar, sınırlı sayıda değildir. Bankaların ekonomik gücü ve İnternet bankacılığını başlatan ve idare eden taraf olmaları sebebiyle dikkat edilmesi gereken hususlar ve alınması gereken önlemler bankaca tespit edilmelidir. Teknolojik şartlardaki değişmelere paralel olarak bankalar da bu tedbirleri geliştirmeli ve değiştirmelidir. Bu konuda hem bilgi hem ekonomik bakımdan hem de tecrübe bakımından daha zayıf olan müşterilerden bunu beklemek hakkaniyete uygun düşmez.

Bankaların müşteriler ile yaptıkları sözleşmelerin şartlarında sonradan değişiklik yapma hakkını saklı tuttukları görülmektedir. Bu hakkın müşteri aleyhine ve haksız olarak kullanılması, konumuzu aşan bir problemdir. Ancak gerek işleyiş ve gerekse teknolojik gelişmeler müşteriler ile sözleşme yapan bankaların, bu sözleşme şartlarındaki değişikleri, online olarak yapacakları yeni ek sözleşmelerle değiştirmeleri veya boşlukları doldurmaları da mümkündür. Bankalar clickwrap veya browswrap sözleşme olarak isimlendirilen ve kabul ediyorum (ya da bu anlama gelen başka bir ibare) butonunun tıklanması suretiyle kurulan elektronik sözleşmeler de akdedebilmektedirler.

Bu anlamda internetten gerçekleşen mesafeli sözleşmelerdeki aydınlatma yükümlülüğünün teyidi işleminin de internetten yapılabilmesine imkan tanıyan Tüketicinin Korunması Hakkında Kanunun 9/A maddesi bu konuya açıklık getirmektedir. Yapılması şekil şartına bağlı olmayan sözleşmelerin internet ortamında yapılması ve bankacılık işlemleri gibi B2C olarak isimlendirilen İşletmeden Tüketiciye elektronik ticaret kapsamındaki uygulamalar kapsamında Click-Wrap sözleşme veya Web-Wrap sözleşme olarak isimlendirilen bu sözleşmelerin de genel hükümler çerçevesinde kuruluş ve geçerlilik şartları ile genel işlem şartlarına ilişkin istisnalar saklı olmak üzere geçerliliğinden kuşku duymamak gerekir[61].

---

[61] Grossman, Mark, Technology law : what every business (and business-minded person) needs to know, Maryland ABD 2009, 57 vd.; Landy, Gene K., The IT Digital Legal Companion A Comprehe Business Guide to Software, IT, Internet, Media and IP Law, Boston ABD, 419 vd.

b) MÜŞTERİLERİN GÖREVLERİ

Sadece bankalar değil aynı zamanda bankaların müşterileri de İnternet ortamının nimetlerinden yararlanmak amacıyla internet bankacılığını tercih etmektedirler. Çünkü bu sayede hem bankaya giderek zaman kaybına engel olmakta hem de daha hızlı, kolay ve ucuz bir şekilde işlemlerini yapabilmektedirler. Bankaların internet bankacılığından çok az masraf alması veya hiç almaması, fatura ödeme, harç ödeme, cep telefonlarına kontör yükleme gibi hizmetleri de sunmaları müşterilerin internet bankacılığına olan rağbetini artırmaktadır. Bununla beraber kullanıcı bilgisayarlarının güvenliği de sistem güvenliğinin yanında önemli bir problem olarak ortaya çıkmaktadır.

Hizmetlerini elektronik ortama taşıyarak daha fazla gelir elde etmeyi amaçlayan bankaların görevlerinin ve sorumluluklarının artmasına paralel olarak internet bankacılığı kullanıcılarının da ek yükümlülükler altına girmesi hakkaniyet gereğidir. Öncelikle kullanıcılar, bilgisayarlarının güvenliğini sağlamak zorundadırlar[62]. Bu yükümlülüklerin başında zararlı yazılımlardan korunmak gelmektedir.

aa) Zararlı Yazılımlardan Korunmak

aaa) Genel Olarak

Bilgisayarlara dışarıdan gönderilen, değişik program ve uygulama dosyalarına gizlenmiş virüs ve trojanlar (Truva atı, zararlı program barındıran veya yükleyen programdır) gibi zararlı yazılımların kullanıcı adı ve şifresi gibi bilgileri tespit ederek kendilerini üreten/kullanan kişilere yolladıkları, bulundukları bilgisayarları dışarıdan müdahalelere açık hale getirdikleri, dolayısıyla kişisel bilgilerin üçüncü kişilerce öğrenilmesine sebep oldukları bilinmektedir[63]. Müşterilerin internet bankacılığı işlemlerini yaparken gizli kalması gereken bilgilerinin kötüniyetli üçüncü kişilerce öğrenilmesine hizmet eden bu yöntemler çok çeşitlidir. Bunların ilk akla geleni ve en yaygını zararlı yazılımlardır.

bbb) Trojan (Truva atı)

Truva atları meşru yazılım görüntüsündeki zararlı yazılımlardır[64]. Bu yazılım bilgisayarın içerisine yararlı bir programa bohçalanarak

---

62 Yılmaz, 152.

63 Canbek/Sağıroğlu, 172.

64 Packard, Ashley, Digital Media Law, ABD 2010, s. 72.

sokulabileceği gibi, bu yazılımların yararlı olduklarına kullanıcıların ikna edilmeleri ile de çalıştırılabilir[65]. Diğer bir yol da bilgisayarlar için yararlı yazılımları oluşturup bunlara trojanları gömerek çok ucuz fiyatlarla (veya bedava) bunları dağıtmaktır[66]. Bu yazılımlar, bilgisayarların başkalarının erişimine açılması, bilgilerin doğrudan gönderilmesi, tarayıcının bir siteye yönlendirilmesi, ekran hareketlerinin okunarak bir merkeze yollanması, başka bir yazılımın bilgisayara yüklenmesinin ön basamağını oluşturması gibi pek çok farklı amaçla kullanılabilmektedir[67].

ccc) Casus Yazılımlar (Spyware)

Casus yazılım, kullanıcılara ait önemli bilgilerin ve kullanıcıların bilgisayarda yaptıkları işlemlerin, kullanıcıların bilgisi olmadan toplanması ve bunların kötü niyetli kişilere gönderilmesini sağlayan yazılım olarak tanımlanır[68]. Bu yazılımlar virüsler gibi kopyalanarak kendilerini çoğaltmazlar. Sadece bilgisayara yerleşerek buradaki gizli bilgilerin dışarıya çıkarılmasına hizmet ederler.

ddd) Klavye Dinleme Sistemleri (Koylogger)

1980'lerden beri kullanılan bu programlar, klavye hareketlerini takip ederek okumakta ve böylece tuşlanan, yazılan kullanıcı adı ve şifre gibi bilgileri çözerek dışarı çıkarmaktadırlar[69].

eee) Phishing

1995'lerde America Onlinekullanıcılarının hesaplarının ele geçirilmesi ile Amerika'da başlayan[70] Phishing, internet bankacılığı hizmeti alan müşteriye bilinen sembol ve formatlar içerisinde yanıltıcı bir elektronik posta gönderilerek burada verilen linkler aracılığı ile banka müşterilerinden, kullanıcı adı, şifre, kart bilgileri, kart şifreleri, internet şubesi şifreleri ve diğer kişisel bilgilerinin alındığı bir hırsızlık

---

65 Canbek/Sağıroğlu, 181.

66 Salomon, David, Foundations of Computer Security, ABD 2006, 116.

67 Salomon, 114-124; Canbek/Sağıroğlu, 180- 182.

68 Salomon, 211; Canbek/Sağıroğlu, 182.

69 Canbek/Sağıroğlu, 185-186, Salomon, 220.

70 James, Lance, Phishing Exposed, ABD 2006, s. 10

yöntemidir[71]. Kullanıcı bu elektronik postanın bankasından geldiği inancı ile verilen linkleri tıklayarak bankanın web sayfasına benzer sayfalara yönlen(diril)mekte ve orada şifre ve diğer kişisel bilgilerini girerek sisteme girmeye çalışmaktadır. Böylece bu işlemler sonucu, kullanıcının şifre ve diğer bilgileri üçüncü kişilerin eline geçebilmektedir[72]. 2006 yılında 109 milyon Amerikalıya bu amaçlı mail gönderilmiştir[73].

fff) Zararlı Yazılımlardan Korunma Yöntemleri

Yukarıda kısaca ve belirgin örneklerle bahsedilen zararlı yazılımlardan korunmanın en temel yöntemi bilgisayara ve bilgisayardaki bilgilere zarar veren zararlı yazılımlara karşı üretilen antivirüs anti spyware türü programların kullanılmasıdır. Ancak uygulamada bilgisayarın çalışmasını yavaşlattığı için, küçük de olsa bir lisans ücreti ödeme zorunluluğu içerdiği için çoğunlukla tercih edilmemektedir. Bunun yerine kullanıcılar antivirüs yazılımlarını internetten ücretsiz olarak indirme yolunu daha çok tercih etmektedirler. Ayrıca arkadaşlar arasında paylaşım yöntemi ile de bu yazılımlar elde edilmeye çalışılmaktadır. Ancak yukarıda da belirtildiği gibi kişilerin bilgisayarlarını koruyacaklarına inanarak elde ettikleri bu yazılımlar içerisinde de zararlı yazılımlar gömülü olabilmektedir. Kullanıcıların, bilgisayarlarına yapılan saldırının kaynağının korumak için kurdukları programlar olabileceği akıllarının ucundan bile geçmemektedir.

Bu tür programların internetten indirilmek suretiyle elde edilmesi, güncel olmamaları, güncellenememeleri bilgisayarın korunmasını zorlaştırmaktadır. Bu sebeple kullanıcılar öncelikle bu yazılımları lisanslı olarak edinerek bilgisayarlarının güvenliğini sağlamalıdırlar.

Burada üzerinde durulması gereken önemli bir husus da bu yazılımların her zaman işe yaramaması ve bunun sorumluluğunun da her zaman kullanıcıya ait olmamasıdır. Bilindiği gibi insan sağlığını tehdit eden en önemli etkenlerden birisi de virüslerdir. Neredeyse her yıl dünyanın bir köşesinde bir virüs ortaya çıkmakta ve yayılarak dünyayı

---

71 James, 10, Memiş, http://hukukcu.com/modules/smartsection/item.php?itemid=116; Lininger/Vines, 1 vd; OECD, Onlıne Identıty Theft, OECD 2009, s, 23; Packard, 73; Alain/Thorsten/Thomas, 24.

72 Canbek/Sağıroğlu , 198; Memiş, http://hukukcu.com/modules/smartsection/item.php ?itemid=116, ; OECD, 23.

73 Packard, 73.

tehdit etmektedir. Buna karşı da hemen dünyadaki gelişmiş ülkeler antivirüs ilaçlar hazırlamakta, bir süre sonra başarıya ulaşılarak etkin ilaç bulunmakta ve üretilerek dağıtılmaktadır. Bu arada virüsün ortaya çıkıp antivirüs ilacın üretilmesine kadar pek çok kişi bu virüsten etkilenmektedir. Yukarıda bahsedilen zararlı yazılımlar ve bunlardan korunmak için üretilen antivirüs veya antispyware ya da antitrojan türü yazılımların tam ve etkin koruma sağlayabilmesi için saldırıyı tanıması gerekir. Bu da o koruyucu programın veritabanında daha önceden kendisine tanıtılan zararlı programlar arasında adının veya türünün olmasına bağlıdır. O güne kadar hiç bilinmeyen, duyulmayan, karşılaşılmamış bir zararlı yazılıma karşı en güncel antivirüs yazılımlar bile etki etmemektedir çünkü tanımamaktadır. Dolayısıyla müşterilerin kendilerine düşen, antivirüs yazılımlarını resmi yollardan elde etmeleri, sürekli güncel tutmaları yükümlülüklerini yerine getirmeleri de her zaman işe yaramamaktadır.

Zararlı yazılımların bilgisayara yüklenmesinin en basit yollarından birisi internet siteleridir. Bu yazılımların en çok pornografik içerikli sitelerle çocuklar için hazırlanan oyun içerikli sitelere yerleştirildikleri bilinmektedir. Bu sebeple internet bankacılığı yapılan bilgisayarın, sadece kullanan kişiye özgü olması ve başkalarının erişimine açık olmaması gerekmektedir. Başkalarına ait olan ve farklı sunucular (serverler) üzerinden internete giren bilgisayarlardan banka hesaplarına erişim yapmaya çalışmaları, bu bilgisayarlarda bulunan ve kişinin klavyeden girdiği bilgileri kişiden habersiz bilgisayarda saklayan zararlı yazılımlar ile kullanıcı adı ve şifrelerinin ele geçirilmesi sonucunu doğurabilmektedir. Bu sebeple üniversite, kütüphane, kafe, işyeri gibi çok kullanıcılı bilgisayarlardan internet bankacılığı yapmak büyük riskler taşımaktadır.

bb) Kullanıcı Adı ve Şifrelerini Doğru Oluşturmak ve Korumak

Şifreli ve kriptolu bir kilidin aşılabilmesi için bir password'e ihtiyaç vardır. Antik çağlardan beri kullanıla gelen ve kişilerin teşhis edilmesinde kullanılan password yöntemi bilgisayar teknolojisinde

sadece oluşturan kişinin bilmesi gereken bir bilgiyi ifade etmektedir[74]. Bu sebeple internet bankacılığı kullanıcılarının sisteme giriş yapmaları ve işlem yapabilmeleri için, kendilerinin tanıtılmasına yarayacak, kendileri tarafından oluşturulmuş ve sadece kendilerinin bilmesi gereken kullanıcı adı ve şifre gibi belirleyici anahtar kelimeler verilmektedir[75].

Bu kelimeler oluşturulurken kullanıcılar karmaşık passwordlerin çekiciliği karşısında bunların hatırlanması ve yazılmasındaki zorluk arasındaki ikilemde kalmaktadırlar. Bunun sonucu olarak da kullanılan şifre kelimeler, kısalmakta, bir yere yazılmakta daha hatırlanabilir olanlara dönüşmektedir[76].

Bu sebeple kullanıcıların şifre oluştururken bunların başkaları tarafından tahmin edilebilir şifreler olmamalarına özen göstermeleri gerekir. Bu sebeple doğum yeri, doğum tarihi, telefon numarası, araç plakası, hayvan adı, kardeş veya eş ya da çocuk adı gibi kelimeler şifre olarak oluşturulmamalıdır[77].

Şifrelerin kırılamaması için zor olmaları çok önemlidir. Bunun sağlanması için ilk akla gelen unsur uzunluktur. Bunun yanında farklı karakter türlerinden oluşan bir dizin de seçilebilir. Yani "$1fre" gibi harf, rakam, özel işaret ve şekillerden oluşan bir kombinasyon kullanılabilir. Büyük harf küçük harf duyarlılığı da önemli bir faktördür. Ancak ilk tahmin edilecek büyük harf denemesinin ilk harf olacağı unutulmamalı ve "şiFRe" oluştururken buna dikkat edilmelidir[78]. Bilinen ve hatırlaması kolay bir bilginin de zorlaştırılarak şifre yapılması bir çözüm olabilir. "doğum günüm bir ocaktır" veya "adım @bdurr@hm@andır"gibi bir ifade de zor bir şifre oluşturabilir[79].

---

74 Dube, Roger, Hardware-based Computer Security Techniques to Defeat Hackers From Biometrics to Quantum Cryptography, New Jersey 2008, 5-6.

75 Şifre ile yapılan işlemin aşamaları için bkz. Alain/Thorsten/Thomas, 27 vd.

76 Dube, 6.

77 Bradley, Tony/ Carvey, Harlan, Essential Computer Security, Rockland ABD 2006, s, 33.

78 Bradley/Carvey, 33.

79 Bradley/Carvey, 34-35.

Şifrelerin oluşturulması kadar korunması da oldukça önemli bir faktördür. Bu sebeple şifreler başkaları ile paylaşılmamalı ve bir yere özellikle de işlemin yapıldığı bilgisayara yazılmamalıdır[80].

İnternet bankacılığının nimetlerinden istifade eden banka müşterilerinin de basiretli bir internet kullanıcısı gibi hareket etmeleri ve yukarıda belirtilen güvenlik tedbirlerini almaları gerekmektedir.

3- TARAFLARIN SORUMLULUKLARI

a) BANKANIN SORUMLULUĞU

Bankalar bir güven kurumudur[81]. Bu özellikleri pek çok Yargıtay kararında vurgulanmaktadır[82]. Bankaların müşterilerinin kullandığı internet bankacılığı hizmetinin gerektiği gibi işleyebilmesi için gerekli olan altyapıyı kurmaları ve çalışır vaziyette bulundurmaları her şeyden önce aralarındaki sözleşme hükümlerine dayanmaktadır[83]. Bankalar yukarıda kısaca açıkladığımız ve zamanla gelişip değişebilen yükümlülüklerini yerine getirmezlerse BK. m. 96 ve devamına göre sözleşmenin hiç veya gereği gibi ifa edilmemesi sebebiyle sorumlu olacaklardır.

Bir güven kurumu olan bankaların aynı zamanda tüzel kişi tacir olmaları sebebiyle basiretli bir tacir gibi davranmaları ve bundan doğan objektif özen yükümlülüğü çerçevesinde hareket etmeleri de gerekmektedir. Müşterileri ile girişmiş oldukları sözleşme ilişkisi çerçevesinde objektif özen yükümünün bir sonucu olarak kast ve ağır ihmallerinin yanı sıra hafif ihmallerinden dahi sorumlu olmaları gerekmektedir. Bankaların yürütmüş oldukları faaliyetler de göz önünde bulundurulduğunda bankaların sorumluluklarını daraltan veya kaldıran sözleşme şartlarının BK. m. 99 ve TKHK'nun Sözleşmedeki Haksız Şartlar başlığını taşıyan 6. maddesi gereği geçersiz sayılması gerektiği

---

80 Yılmaz, 151-152.

81 Bu konuda bakınız Battal, Ahmet, Güven Kurumu Nitelendirmesi Işığında Bankaların Hukuki Sorumluluğu, Ankara 2001; s. 1.vd.

82 Yargıtay 11. HD. E. 2005/4748 ve K. 2006/7341; Yargıtay 11. HD E:2007/12559 K:2009/1362.

83 Yılmaz, 126.

kanaatindeyiz[84]. Bunların banka ile başlangıçta yapılan müşteri sözleşmesi içerisinde olması ile daha sonra internette web-wrap sözleşme şeklinde ekrana çıkan ve evet, kabul ediyorum gibi butonları tıklamadığınız sürece işleme devam etmenize imkân tanımayan sözleşmelerde olması arasında fark bulunmamaktadır.

Bankaların sorumluluklarının temeline baktığımızda bunun objektif özen yükümüne dayandığını görmekteyiz. Bunun sonucu olarak da hafif kusurlarından dahi sorumludurlar[85]. Ancak uygulamada, bazı bankalar aleyhine açılan davalarda bu sorumluluk sanki objektif sorumlulukmuş gibi ifadeler kullanılmaktadır. Objektif sorumluluk ile objektif özen yükümlülüğüne dayanan sorumluluk karıştırılmamalıdır. Bankaların sorumluluğu objektif sorumluluk değildir. Ağırlaştırılmış bir kusur sorumluluğudur. Objektif sorumluluk ise kusura dayanmayan sorumluluk olup sebep sorumluluğu olarak da anılır. Dolayısıyla bankalar hafif ihmalleri dahi olmayan bir internet bankacılığı dolandırıcılığından sorumlu değildirler.

Bankalar tüzel kişi tacir olarak personel çalıştırmaktadırlar. Bu personelin bankaya ait bir işlem yaparken müşterilerine zarar vermesi durumunda banka müşterisine karşı BK. m. 100 hükmüne göre sorumlu olacaktır. Bankanın sözleşme ilişkisi içerisinde olduğu müşterilerine karşı personelinin vermiş olduğu zararın kusura dayanıp dayanmaması ise önemli değildir. Banka bu durumda kusursuz sorumluluk esasına göre sorumlu olacaktır. Bu sorumluluk türünde ise kurtuluş beyyinesi getirme imkanı tanınmamıştır[86].

b) MÜŞTERİLERİN SORUMLULUĞU

Müşteriler internet bankacılığının nimetlerinden yararlanmak amacıyla bankalarla sözleşmeler imzalamakta veya imzalanan sözleşmelere eklenen madde veya hükümlerle internet bankacılığını kullanmak istediklerini beyan etmektedirler. Bu sözleşme hükümlerine de yukarıda müşterilerin görevleri kısmında açıklanan hususlar yazılmakta

---

84 Memiş, http://hukukcu.com/modules/smartsection/item.php?itemid=116, ; Yılmaz, 144-145.

85 Yılmaz, 140.

86 Oğuzman, Kemal/Öz, Turgut, Borçlar Hukuku, Genel Hükümler, İstanbul 2005, s. 380.

ve müşteri bunları okuduğunu beyan ederek imzalamaktadır. Ancak uygulamada çok uzun olan ve küçük harflerle yazılmış olan bu sözleşme hükümlerinin çoğunlukla okunmadan imzalandığı görülmektedir. Böyle bile olsa bu hükümler müşteriyi bilgilendirmeye ve ona yükümlülüklerini açıklamaya yönelik bir karakter de taşımaktadır. Bu sebeple belirtilen hükümlerin çok uzun olduğu ve okunmadan imzalandığı gerekçesiyle haksız şart olarak kabul edilerek geçersiz sayılması mümkün değildir. Buna benzer düzenlemelerin internet bankacılığı işlemi sırasında tıklama ile yapılmasında da aynı sonuç benimsenmelidir. Buna göre müşteriler kendi rızaları ve istekleri ile imzaladıkları bu sözleşmeler ile kullanmaya başladıkları internet bankacılığının gereklerine uygun davranmak zorundadırlar. Bu amaçla kendilerinden beklenen her türlü tedbiri almaları hakkaniyet gereğidir ve kendilerinden beklenen her türlü dikkat ve özeni göstermek zorundadırlar. Bu sebeple bilgisayarlarına başkalarının ulaşmasına imkan tanıyan her türlü gerçek ve sanal saldırıyı önleyici tedbirleri almaları, bunu sağlayamamaları durumunda ise bunun sonuçlarına katlanmaları gerekmektedir. Bu sebeple kullanıcılar da kast ve ağır ihmal gibi hafif ihmallerinden de sorumludurlar. Bilgilerini kötü niyetli olmadıklarını düşündükleri kişilere vermeleri veya bir yerlere yazmaları ve bu suretle üçüncü kişilere bilginin geçmesi ağır ihmale, bilgisayarlarına istekleri dışında gelen virüs, trojan gibi zararlı yazılımlar sebebiyle bilgilerinin üçüncü kişilerin eline geçmesi hafif ihmale örnek verilebilir. Ancak hangi ihmal türü olursa olsun kullanıcının sorumluluğunun doğacağı açıktır.

Bununla beraber bilgisayarlarda kullanılan sanal klavye gibi uygulamaların da yeterli olmadığı ve girilen şifreleri gizlemeye yetmediği bilinmektedir. Buna paralel olarak antivirüs sektörü de öncelikli olarak virüsün ortaya çıkmasından sonra devreye girmektedir. Önce virüs veya trojan olarak ifade edilen zararlı yazılımlar üretilmekte, daha sonra bunların ve zararlarının farkına varan antivirüs yazılım firmaları antivirüs üretmektedirler. Tabiidir ki bu arada güncel ve lisanslı yazılım kullansalar bile bazı kişilerin bilgisayarları veya verileri zarar görebilmektedir. Böyle bir durumda ise kullanıcının bir kusuru olduğundan bahsedilemez.

Almanya'da, Alman Yüksek Mahkemesinin "dialer" kararı olarak bilinen bir kararında, müşterilerin bilgisayarlarının internete bağlanmalarını sağlayan çevirmeli ağ bağlantısı gerçekleştirme

programlarının, istem dışı olarak bilgisayarlarına girmiş olan dialer adlı programlarla sağlanması durumunda, bunların temizlenmesi için müşterilerin ek yazılım bulundurmalarının kendilerinden beklenemeyeceğini belirtmiştir. Hem kararın verildiği ve olayın gerçekleştiği zamanın internet kullanıcı profili, hem de şimdiki anti-malware yazılımların daha etkin olması sebebiyle müşterilerin daha dikkatli olması gerektiği kanaatindeyiz. Yani kanaatimizce ortalama internet kullanıcısı ölçütü kararın verildiği zamana göre daha ileridir. E-Devlet uygulamalarının başladığı ve anti-malware yazılımların 15-20 TL fiyatla satıldığı bir dönemde müşterilerin bu yazılımları elde ederek internet bankacılığı işlemlerini yapmaları beklenmelidir.

SONUÇ

İnternet hayatımızın her aşamasına girmiştir. İnsan hayatını büyük ölçüde kolaylaştıran internet sayesinde pek çok ticari faaliyet de internet ortamına taşınmıştır. Bankacılık işlemleri de bu değişimden nasbini almış ve internet bankacılığı ortaya çıkmıştır. İnternet bankacılığı online bankacılık ve elektronik bankacılık kavramları ile eş anlamlı olarak da kullanılabilmektedir. Ancak İnternet bankacılığı, Ev ve ofis bankacılığı, ATM bankacılığı gibi elektronik bankacılık türlerinden birisidir.

İnternet bankacılığının hem bankalar hem de müşteriler açısından yararları ve sakıncaları mevcuttur. Yer ve zaman sınırlaması ile karılaşmaksızın işlem yapabilmek, işlem maliyetlerinin çok düşük olması, bankaya gitmek zorunda olmamak müşteriler açısından sayılabilecek başlıca yararlardır. Bankalar da işlem maliyetlerinin azalması ve başka alanlara yatırım yapmaları, daha kültürlü ve problemsiz müşterilerle muhatap olmamaları, ve kolay işlem sebebiyle müşteri sayılarının artması gibi açılardan internet bankacılığından yararlanmaktadırlar.

Kimlik tespiti, kimlik hırsızlığı, bilgisayar ve internet erişimin zorunluluğu, bankalarla müşteriler arasındaki yüz yüze iletişim eksikliği ve kötü amaçlı yazılımlarla banka hesaplarının boşaltılması ve faillere ulaşılamaması, internet bankacılığının başlıca sakıncaları arasında yer almaktadır.

İnternet bankacılığında bankalar tecrübeli elemanlar çalıştırarak, internet güvenliğini artırarak, tek kullanımlık şifre uygulamasına geçerek internet bankacılığının risklerini minimuma indirmeye çalışmalıdırlar.

Müşteriler de anti malware yazılımlar kullanmak suretiyle virüs, trojan, spyware gibi kötü amaçlı yazılımlara karşı tedbir almalıdırlar. Umuma açık yerlerden hesaplarına girmemeli, hesap hareketlerini sık sık kontrol etmeli ve kendilerine tahsis edilen kullanıcı adı ve şifreleri başkaları ile paylaşmamalıdırlar.

Tarafların üzerlerine düşen yükümlülükleri yerine getirmeleri durumunda internet bankacılığı hem daha kolay ve yaygın hem de daha güvenli hale gelecektir.

KAYNAKÇA

Adel M. Aladwani, Online banking A Field Study of Drivers, Development Challenges, And Expectations, International Journal of Information Management 21 (2001).

Aktan, Bora/Teker, Edip/Ersoy, Pervin, Changing Face of Banks and the Evaluation of Internet Banking in Turkey, Journal of Internet Banking and Commerce, April 2009, vol. 14, no.1,

Alain Hiltgen/ Thorsten Kramp/ Thomas Weigold, Secure Internet Banking Authentication, IEEE Security and Privacy, vol. 4, no. 2, s. 24-32.

Azouzı, Dhekra, The Adoption of Electronic Banking in Tunisia: An Exploratory Study, Journal of Internet Banking and Commerce, December 2009, vol. 14, no.3

Battal, Ahmet, Güven Kurumu Nitelendirmesi Işığında Bankaların Hukuki Sorumluluğu, Ankara 2001.

Biçer, Murat, İnternet Bankacılığı Ve İnternet Bankacılığında Müşteri Eğitimi, Yayınlanmamış Yüksek Lisans Tezi, Ankara 2006,

Bradley, Tony/ Carvey, Harlan, Essential Computer Security, Rockland ABD 2006

Canbek, Gürol/Sağıroğlu, Şeref, Casusu Yazılımlar ve Korunma Yöntemleri, Ankara 2006

Dube, Roger, Hardware-based Computer Security Techniques to Defeat Hackers From Biometrics to Quantum Cryptography, New Jersey 2008.

Durer, Salih/Özsözgün çalışkan, Arzu/Akbaş, Halil Emre, Gündoğdu, Ceren Erdin, İnternet Bankacılığını Kullanma Kararını

Etkileyen Faktörler. Türk Banka Müşterileri Üzerine Bir Araştırma, MÜİİBFD, Yıl: 2009, C. XXVI, Sayı :1.

Grossman, Mark, Technology law : What Every Business (and business-minded person) Needs To Know, Maryland ABD 2009.

Gup, Benton E., Elektronic Banking, The Future of Banking, (editor: Gup, Benton E.) Londra 2003.

James, Lance, Phishing Exposed, ABD 2006.

King, Brett, Bank 2.0, Singapore 2010.

Landy, Gene K., The IT Digital Legal Companion A Comprehe Business Guide to Software, IT, Internet, Media and IP Law, Boston ABD.

Lininger, Rachael/ Vines, Russell Dean, Phishing Cutting the Identity Theft Line.

Mannan, Muhammad, Security and Usability: The Gap in Real-World Online Banking, http://www.ccsl.carleton.ca/paper-archive/mannan-nspw07.pdf.

Memiş, Tekin, Elektronik Bankacılıkta Bankanın Yükümlülük Ve Sorumlulukları
http://hukukcu.com/modules/smartsection/item.php?itemid=116.

OECD, Onlıne Identıty Theft, OECD 2009.

Oğuzman, Kemal/Öz, Turgut, Borçlar Hukuku, Genel Hükümler, İstanbul 2005.

Oppliger, Rolf, SSL and TLS: Theory and Practice, Narwood, USA 2009.

Özcan; Zeynep Özge, Türkiye'de Elektronik Bankacılık: İnternet Bankacılığı Üzerine Bir Çalışma, Yayınlanmamış Yüksek Lisans Tezi, Sakarya 2007.

Packard, Ashley, Digital Media Law, ABD 2010.

Riquelme, Hernan E., Internet Banking Customer Satisfaction and Online Service Attributes, Journal of Internet Banking and Commerce, August 2009, vol. 14, no.2.

Salomon, David, Foundations of Computer Security, ABD 2006.

Schaechter, Andra, Issues in Electronic Banking: An Overwiev, International Money Fund, 2002.

Shah, Mahmood/Clarke, Steve, E-banking Management Issues,Ssolutions, and Strategies, Newyork 2009.

Turan, Mehmet, http://www.olympos.net/belgeler/guvenlik/ alternatif-bankacilik- yontemleri-ve-karsi-karsiya-kaldiklari-sorunlar-5336.html.

Wu, Jun, Factors That Influence The Adoption of Internet Banking By South Africans In The Ethekweni Metropolitan Region, Durban Güney Afrika, Tarih yok,

Yaltı, Binnur, Elektronik Ticarette Vergilendirme, İstanbul 2003.

Yıldırım, Kadir, Elektronik Bankacılık-Avrupa Birliği Ve Türkiye Uygulamaları, Yayınlanmamış Yüksek Lisans Tezi, İstanbul 2006.

Yılmaz, Süleyman, Hukukî Açıdan Internet Bankacılığı, Yayınlanmamış Doktora Tezi, Ankara 2007.

Yuan, Xina/Lee, Hyung Seok/ Kim, Sang Yong, Present and Future of Internet Banking in China, Journal of Internet Banking and Commerce, April 2010, vol. 15, no.1.