İNTERNET BANKACILIĞI KULLANIMINDA GÜVENLİK UNSURLARININ BİLİNİLİRLİĞİ (ANKET UYGULAMASINA DAYALI SPSS ÇÖZÜMLEMESİ)

Salih BARIŞIK[1]
Halime TEMEL[2]

ÖZET

İnternetin insan yaşamına sağladığı kolaylıklar internet kullanımının yaygınlaşmasını hızlandırmaktadır. Bu yaygınlaşmanın bankacılık sektöründe de yaşanmasına rağmen, internet bankacılığı kullanımı artışıyla birlikte internet bankacılığına yönelik saldırılarla dolandırıcılık yapılabilmektedir. Dolandırılıcılık haberleri internet bankacılığına güven sorununu ortaya çıkarmıştır. İnternet bankacılığı güvenlik unsurlarının bilinilirliğinin internet bankacılığı kullanımında etkin olduğu düşünülmektedir. Bu amaçla güvenlik unsurlarının bilinilirliği ve kullanılırlığını tespit etmeye yönelik pilot bir uygulama yapmak amaçlanmıştır. Uygulama ile internet bankacılığına güven duyup duyulmadığı, internet bankacılığı kullanımında en çok yapılan işlemler ve internet bankacılığı kullanımında güvenlik unsurlarının bilinirliğini ve kullanımı tespit edilmeye çalışılmıştır. Çalışmada, Zonguldak Karaelmas Üniversitesi İktisadi ve İdari Bilimler Fakültesi öğrencileri ve öğretim elemanları örneklem seçilmiştir. İnternet bankacılığının ve güvenilirliğinin bilinilirliğinin öğrenciler ve öğretim üyeleri arasında farklı olduğu, bu farklılığın kullanımı etkilediği gözlenmiştir. Bankaların internet bankacılığını yaygınlaştırabilmek için internet bankacılığı hizmetlerinin yanı sıra internet bankacılığı güvenlik sistemlerini tanıtması gerekmektedir

Anahtar Kelimeler: İnternet Bankacılığı, Güvenlik Unsurları, Güvenlik**.**

ABSTRACT

The facilities provided by the internet bring about its wide usage. Banking sector is one of the leading sectors in which internet-provided-services are used extensively. However, the cases of internet fraud is also spreading as a result of this wide-spread usage. This situation causes a trust problem in the internet banking sector. The knowledge of internet security is an important element in convincing people to use internet banking effectively. The aim of this study is to determine the level of internet-banking-users' knowledge of internet security, most frequently used internet banking services and seriousness of the trust problem in using internet banking. The faculty and the students of the Zonguldak Karaelmas University, Faculty of

[1] Doç.Dr., Zonguldak Karaelmas Üniversitesi İİBF İktisat Bölümü, sbarisik@yahoo.com
[2] Arş.Gör. Zonguldak Karaelmas Üniversitesi İİBF İşletme Bölümü, halimetemel@yahoo.com

Economics and Administrative Sciences constitute the sample of this study. The results indicate that the knowledge in internet security differs between the students and the faculty, and this difference affects the use of internet banking. This result suggests that in order to increase the volume of internet banking, banks need to introduce not only their internet banking services but also the security systems which increase the trustworthiness of internet banking.
Keywords: Internet Banking, Security Elements, Security.

1. Giriş

Bilgi, iletişim teknolojileri ve internet'in gelişimi ile bilgisayar kullanımı hızla artmaktadır. İnternet kullanımının yaygınlaşmasına bir diğer katkı da müşteri memnuniyetini arttırmayı amaçlayan işyerleri, kafeler ve oteller gibi internet ulaşımını hizmet kapsamına dahil edilen işyerlerinden gelmektedir. Bilgi ve iletişim teknolojilerinin en kolay ve hızlı uygulandığı alan finansal hizmetler sektörüdür. Bu sektörde geçmişte ofis içi bankacılık işlemlerinin gerçekleştirilmesinde kullanılan bilgisayarlar günümüzde bazı bankacılık hizmetlerinin otomasyonunda kullanılmaktadır (Sevinç, 2001). Bu gelişmeler 1990'lı yıllardan itibaren internet bankacılığın gelişmesine ve yaygınlaşmasına neden olmuştur. İnternet bankacılığının ilk hizmete sunulduğu dönemde kullanıcıların sisteme duydukları güvenlik endişesi, kişisel bilgisayara sahip olmanın maliyeti ve böyle bir hizmeti kurmanın bankalara yükledikleri maliyet internet bankacılığının yaygınlaşmasında bir engel teşkil etmiştir.

Diğer taraftan kişisel bilgisayarların fiyatlarının reel olarak düşmesi ve yaygınlaşması potansiyel internet bankacılığı kullanıcı sayısını arttırmıştır. İnternet bankacılığı kullanıcı sayısının artması ile bankaların bu hizmetleri sunmadaki müşteri başına maliyetlerinde düşüşler meydana gelmiştir. Özellikle müşteri başına maliyetlerdeki düşüşler bankaları internet bankalığı uygulamalarını artırmaya yöneltmektedir. 1990'lardan günümüze kadar yaşanan süreçte toplum internet bankacılığının sunduğu hizmetleri tanıdıkça ve sisteme olan güveni artıkça kullanımında artışlar olduğu gözlenmektedir. Sisteme olan güvenin sağlanabilmesinin yolunun da güvenlik ağlarının bilinilirliğinde yattığı gözden kaçmamalıdır. Bankalar internet bankacılığıyla sunulan hizmetlerin yanı sıra hizmetin güvenliğini sağlayan sistemleri de tanıtması gerektiği ortaya çıkmaktadır.

Yukarıda sayılan açıklamalar ışığında anket sistemine dayanan pilot bir uygulama ile bankacılık hizmetlerinden yararlanmada internet bankacılığının ve güvenilirliğinin bilinilirliğine açıklama getirebilmek için bu çalışma yapılmıştır. Çalışma elde edilen bulgular teori ile kıyaslanmaktadır.

2. İnternet Bankacılığı Güvenlik Sistemleri Ve Kullanıcı Önlemleri

Bankacılık hizmetlerinin internet üzerinden sunulması şeklinde tanımlanabilen internet bankacılığı, yeni hesap açılmasından para transferlerine (EFT, Havale, Swift vb), kredi kartı ve bireysel kredi başvurularına, elektronik fatura ve vergi ödemelerine kadar birçok işlemi kapsamakta ve dünyanın her yerinden 24 saat sunum

yapmaktadır (TBB, 2007). İnternet bankacılığı aynı zamanda, hızlı ve kesintisiz işlem, şubeye gitmeden, sıra beklemeden kolay bankacılık işlemleri, görerek ve seçerek işlem yapabilme, işlemler hakkında detaylı rapor ve bilgi alabilme, çok çeşitli bankacılık hizmetlerini görme, çok daha ucuza işlem maliyeti gibi faydalar sağlamaktadır (TBB, 2007). İnternetten yararlanmada kullanılan projelerin birebir benzerlerinin online bankacılık hizmetlerinde kullanılması bireysel bankacılık hizmetlerinden yararlanma kolaylığı sağlanmaktadır. Bu kolaylıklarla birlikte bu hizmetlerden yararlanma bedelinin olmaması ve bankalar tarafından kullanımın teşvik ediliyor olması internet bankacılığının yaygınlaşmasına katkı yapan bir başka faktördür.

Bu avantajların yanı sıra, güvenlikle ilgili endişeler, İnternet bankacılığının gelişmesini yavaşlatan temel nedenler arasında gösterilmektedir. Deutsche Bank, güvenlik endişeleri ile İnternet bankacılığından faydalanma arasında negatif bir korelasyon tespit etmiştir. Böylece, internet bankacılığının kullanımında etkili olan en önemli faktörün internet bankacılığı hizmetlerinin tanınılırlığı ve güvenlik unsurlarının bilinirliği olduğu söylenebilir. Tüm Avrupa ülkelerinde internet bankacılığına güvenlik endişesi ve internet bankacılığı kullanımı arasındaki negatif ilişkiye geçmişte yaşanan kötü tecrübelerin etkili olduğu gözlenmiştir. En sık rastlanan kötü tecrübeler arasında kişisel bilgilerin kötüye kullanılması ve kredi kartı dolandırıcılıkları olduğu belirtilmiştir (Active, 2006: 26). Bu tür olumsuzluklardan kaçınabilmede oluşturulabilecek güvenlik sistemlerini açıklamak gerekir.

Güvenlik Duvarları (Firewall): Güvenlik duvarı ağı ile internet arasına engel koyan donanım veya yazılım parçasıdır. Dışarıdakilerin ağa ve sisteme erişimini ve gizli bilgilere ulaşmasını veya kötü amaçlı eylemler gerçekleştirmesini engellemektedir. Ayrıca kullanıcıların güvenilmeyen siteleri ziyaret ederken zararlı kodlara maruz kalmamak için gezinme etkinliklerini kısıtlamak yoluyla sistemler korunabilmektedir. Bankalar bilgisayar sistemlerini güvenlik altına almak için harcamalar yapmakta ve güvenlik politikaları geliştirmektedirler. Bankaların internet bankacılığı güvenliğinin sağlanması açısından banka networkunun hangi şartlarda dış sistemlere açılıp açılmayacağını detaylı olarak düzenlemektedir. Bu amaçla kullanılan araçlardan biri "firewall"lardır. (Microsoft, 2006).

Firewall'lar yalnızca sistem güvenliğine adanmış bilgisayarlardır. Firewall'lar şirket sisteminin dış dünyaya bağlandığı noktaya yerleştirilirler. Burada şirket sistemine dışarıdan gelen her bağlanma talebi firewall'lar tarafından daha önceden belirlenen güvenlik politikaları kullanılarak değerlendirilir ve yetkisiz bağlanma girişimleri önlenmiş olur. Bankanın içinden gelebilecek tehditlerin de bilgisayar sistemlerine dışarıdan gelebilecek tehdit ve saldırılar kadar,

hatta daha fazla önemsenmesi ve bu saldırılar için hazırlıklı olunması gerekmektedir. (Microsoft, 2006).

İşletim Sistemi Güvenlik Güncellemeleri: İşletim sistemi güvenlik güncellemeleri, üretici yazılım firma tarafından yapılan güvenlik ve sistem geliştirmeleridir. Bu güncellemeler sürekli bilgisayara yüklenmelidir. Üretici web siteleri, yazılım güncellemeleri ve yamalar ile ilgili bilgiler için temel kaynak olmalıdır (Dayıoğlu, 2001: 3).

Anti-Virüsler: Bilgisayar Virüsleri, bilgisayarın çalışmasını engelleyecek, verileri kaydedecek, bozacak veya silecek ya da kendilerini internet üzerinden diğer bilgisayarlara yayarak bilgisayarın yavaşlaması gibi sorunlara neden olacak şekilde tasarlanmış yazılım programlarıdır (Microsoft, 2005). Temel virüsler, yeterli bilgisi olmayan bilgisayar kullanıcıları tarafından farkında olmadan paylaşılır veya gönderilir. Daha karmaşık olan virüsler, bir e-posta paylaşma uygulaması gibi diğer yazılımları denetleyerek kendilerini otomatik olarak çoğaltabilir ve diğer bilgisayarlara gönderebilir. Truva atı adı verilen belirli virüsler (adlarını efsanevi Truva Atı'ndan alırlar), faydalı bir program gibi görünerek kullanıcıların aldanıp onları karşıdan yüklemelerine yol açabilir. Bazı Truva atları, beklenen işlemleri yerine getiriyor gibi görünürken bir yandan da sisteme veya ağa bağlı diğer bilgisayarlara zarar verebilir (Microsoft, 2005).

AntiSpyware: Spyware kavramından önce adware kavramını açıklamak gerekir. Adware programlama masraflarını telafi etmek için programcıların, yazdıkları programa ekledikleri reklamlardır. Masum görünen bu reklam bannerları, kullanıcıların sörf alışkanlıklarını kayıt etmenin yanında, kullanıcıların fark etmeyeceği şekilde Internet bağlantısını kullanarak zararlı birçok programcının da sisteme girmesine neden olmaktadır. Bu işleme spyware adı verilmektedir (Akça, 2005).

Elektronik İmza: Elektronik imza, 5070 sayılı Elektronik İmza Kanunu'nda; başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri şeklinde tanımlar. Elektronik imza; bir bilginin üçüncü tarafların erişimine kapalı bir ortamda, bilgi bütünlüğü bozulmadan ve tarafların kimlikleri doğrulanarak iletildiğini elektronik veya benzeri araçlarla garanti eden harf, karakter veya sembollerden oluşur. (Forsnet, 2007) Bu yöntemin amacı göndericinin kimliğini kesin olarak belirlemektir. (Can ve Bozkurt, 1994: 107).

SSL Protokolü: İnternet erişim programları tarafından kullanılan SSL (Secure Socket Layer) ve 128 bit şifreleme programları sayesinde bilgisayar ile banka arasındaki bilgi transferinde gerekli olan güvenlik düzeyi sağlanmaya çalışılmaktadır

(Çelik, 2002: 8-9). SSL hem gizli anahtarlar ve hem de ortak anahtar teknolojilerini kullanan güvenlik protokolüdür. SSL, veri şifreleme, sunucu ve tarayıcı doğrulama ve ileti bütünlüğü güvenlik tekniklerinin tamamını sağlamaktadır (Ertaş, 2000: 17). Birçok internet sitesi kredi kartı işlemleri için SSL protokolünü uygulamaktadır. Veri iletiminde kullanılan şifreleme yönteminin etkinliği kullanılan anahtarın uzunluğu ile doğru orantılıdır. Örneğin, 128 bit üzerinden yapılan bir şifrenin çözülebilmesi minimum 1 Milyon dolarlık bir yatırım ve yıllarca sürecek zaman demektir (Walther-Levine, 2001:235).

PKI (Public Key İnfrastruce): Açık anahtar altyapısı**,** asimetrik çift anahtardan oluşan şifreleme olarak adlandırılmıştır. Sayısal imzaya asimetrik şifrelemede imzanın doğruluğunu kanıtlamada kullanılan farklı bir imza oluşturulmaktadır. Her kullanıcı gizli anahtar (private key) ve açık anahtar (public key) olarak adlandırılan anahtar çifti ile iki farklı ancak tamamlayıcı bir anahtar kullanmaktadır (İnalöz, 2003: 31). Açık anahtar gizli dünyaya ilan edilebilmekte ve dağıtılabilmekte iken, gizli anahtar çok dikkatli bir şekilde saklanır. Bireyin açık anahtarı bir grup matematik işlemden geçirilerek şifrelenmekte ve kişiye bildirilmektedir. Şifrelenmiş bilgi gizli anahtar deşifre edebilmekte, dolayısıyla sadece gizli anahtara sahip olan kişi bu bilgiyi okuyabilmektedir (Gaziler, 2006: 42).

Açık anahtar altyapısı ile:

Kimlik Doğrulama: Gönderilen mesajın kimden geldiğinden veya internet ortamından sunuculara bağlanmak isteyen kişinin kim olduğundan emin olunması,

Gizlilik: Gönderilen verilerin şifrelenmesiyle ve istenmeyen üçüncü bir kişi veya kurum tarafından okunamadığından emin olunması,

Bütünlük: "Özetleme" yöntemiyle verinin "parmak izi"nin alınması sayesinde gönderilen verinin veya bilginin gönderildikten sonra herhangi bir değişikliğe uğramadığından emin olunması,

İnkar-Edememezlik: Gönderilen verinin sayısal imza ile imzalanmasıyla yapılan işlemin yasal olarak da bağlayıcılığının bulunması şeklinde güvenlik sağlamaktadır (Orhun, 2003: 48).

Sanal Klavye: Sanal klavye, bilgisayarınızdaki fiziksel klavyeyi kullanmadan, bilgisayarınızın faresini kullanarak ekrandan şifre girişini sağlayan ek bir güvenlik önlemidir. Sanal Klavye, bilgisayara bilgi dışında yüklenebilecek ve şifre bilgilerini çalmaya yönelik olan "keylogger" programlarına karşı korumak amacı ile geliştirilmiştir. Kişisel bilgisayarlarda bilerek ya da bilmeden yüklenmiş olan Key Logging (klavye tuşlamalarının izlenmesi) ve Screen Capturing (ekran fotoğraflama) yapan virüs programlarının riskine karşı şifrelerini çalınmasını engelleyerek şifre güvenliği sağlanmaktadır (HSBC, 2007).

Elektronik Sertifika: Elektronik imzanın doğrulanması için gerekli olan veriyi ve imza sahibinin kimlik bilgilerini içeren elektronik kaydı ifade etmektedir. Elektronik sertifikalar, kanuna uygun olarak faaliyette bulunan elektronik sertifika hizmet sağlayıcılarından belirli bir ücret karşılığında temin edilebilir. Elektronik sertifika hizmet sağlayıcısının sertifika üzerindeki elektronik imzası, sertifikanın bütünlüğünü ve doğruluğunu garanti edecektir. Elektronik sertifikalar, atılan imzanın doğruluğunun teyit edilebilmesi için gereklidir (e-imza.gen.tr). Sertifika sahibi firma, hile veya dolandırıcılık yaptığında Güvenilir Sertifikasyon Örgütleri, olayı araştırır ve firmanın suçlu bulunması durumunda firmaya ceza verir (Aksoy, 2006: 161). Dijital sertifika sahibi firma, sertifikaya sahip olduğunu belirten logoyu web sitesinde yayınlamaktadır. Kişiler sitede bulunan logoyu tıkladığı zaman, Güvenilir Sertifikasyon Örgütlerine ait web sitesine ulaşır; bulunduğu sitenin firmaya ait olduğunu, bilgilerin 128 bit SSL ile şifrelendiğini ve sitenin Güvenilir Sertifikasyon Örgütlerinin programları tarafından korunduğunu ve programın geçerlilik süresini gösteren bir ifade ile karşılaşmaktadırlar. Böylece müşteriler, bu logoyu yayınlayan firmalara güvenerek alışveriş ya da elektronik ödemelerini rahatça yapabilmektedirler (Korkmaz ve Temel, 2006: 993).

Bugün internet bankacılığının en yaygın kullanımı, elde edilmesi oldukça kolay ve gerçek anlamda güvenlik içermeyen doğrulama yöntemi olan, müşteri no veya adı ve şifre kullanımı esasına dayanmaktadır (Orhun, 2003: 36). Bu şifrelerin üçüncü kişilerin eline geçmesi halinde, hesaplarla ilgili her türlü işlem gerçekleştirilir (Çelik, 2002: 17). Son dönemde banka ve finans kurumları tarafından acil ve çok önemli konular içeriyormuş gibi gönderilmiş gibi görünen, sahte e-postalar yayılmaktadır. Bu e-postalarda verilen linkler aracılığı ile banka müşterilerinden, kart bilgileri, kart şifreleri, internet şubesi şifreleri ve kişisel bilgileri istenmektedir. Hemen silinmeli ve maildeki linke asla girilmemesi gereken e-maillerle gönderilen dolandırıcılık işlemlerine Phising (olta) saldırıları denilmektedir (TBB, 2007). İnternet bankacılığı kullanıcıları, giriş yaparken sadece o bankanın web sitesinden giriş yapmalıdırlar.

Dolandırıcılar phishing yöntemiyle kullanıcının gizli bilgilerini elde etmenin yanı sıra bu bilgilere başka bir yöntem olan keylogger adı verilen klavye ve ekran görüntülerini kopyalayabilen programlar vasıtasıyla ulaşabilmektedirler. Bu yöntemde, online işlem şifrelerinin çalınması da yapılabilmektedir. Kullanıcıların bilgisayarlarına yerleştirilen keylogger adlı yazılım, bilgisayarda yapılan her türlü işlemlerin bir kaydını tutar, bu kayıtlar klavyeden girilen bilgilerin yanı sıra ekran görüntüleri de olabilir. Bu kayıtlar ya

sistemde bir txt (metin) dosyası olarak tutulur ya da klavye girdileri e-posta ile saldırgana (hacker) gönderilir (TBB, 2007). İnternet Bankacılığı kullanıcı ve banka güvenlik önlemleri tablo 1 deki gibi özetlenebilir.

Tablo 1: İnternet Bankacılığı Kullanıcı ve Banka Güvenlik Önlemleri

Kullanıcı Güvenlik Önlemleri
- Kimlik ve kişisel finansal bilgileri isteyen e-postalar konusunda dikkatli olunmalı ve kişisel bilgilerin talep edildiği bu tür e-postalar kesinlikle doldurulmamalıdır. - Bankalar tarafından verilen müşteri numarası, parola ve şifre bilgileri üçüncü şahıslarla kesinlikle paylaşılmamalıdır. - Banka ve ticari kurumlardan gelmiş gibi gösterilen ve şifre, kullanıcı adı, müşteri numarası, kredi kartı numarası, kimlik numarası gibi bilgileri talep eden e-postalara güvenilmemelidir. Çünkü bankalar e-posta yoluyla hiç bir şekilde müşterilerin kişisel bilgilerini istememekte ve şifre işlemleri yaptırmamaktadır. Bu nedenle e-postalarda bulunan linkler ile e-postalar içerisinde yönlendirilen linklere girilmemelidir. - Kredi kartı kullanılan ya da kişisel bilgilerin yazıldığı bilgisayarın güvenli olmasına dikkat edilmelidir. (Kullanılan web sitesi http:// yerine https:// olmalıdır). - Phishing web sitesi sahtekarlıklarına karşı uyarılmak için bilgisayara İnternet'ten uyarıcı bir web tarayıcısı yüklenebilir. (http://www.earthlink.net/earthlinktoolbar İnternet'ten ücretsiz olarak yüklenebilen bir tarayıcıdır). - Hesap numaraları, şifreler, parolalar ve kimlik numaralarının yazılı olarak saklanmamalıdır. - Banka hesapları, kredi kartları ve banka kartlarının ekstreleri düzenli kontrol edilmeli, şüpheli görülen durumlarda banka ile irtibata geçilmelidir. - İnternet tarayıcının güncel olması ve tüm güvenlik ayarlarının yüklendiğini kontrol edilmelidir. Microsoft Internet Explorer kullanıyorsanız, Microsoft Security ana sayfasından http://www.microsoft.com/security/'den konu ile ilgili özel güvenlik ayarlarını yüklenmelidir. - Online işlemler gerçekleştirirken, işlem yapılan sayfada, daha önceki bağlantılardan farklı bir görünüm veya ifade varsa, hiçbir işlem yapılmadan ilgili banka ile irtibata geçilmelidir. - Güvenli olmayan internet sitelerine giriş yapılmamalı ve bu tür sitelerden dosya indirilmemelidir. - Bilinmeyen adreslerden gelen e-postalar açılmadan silinmeli, mümkünse bu tür e-postaları engelleyici tedbirler alınmalıdır. - Bilgisayarlarda kullanılan yazılımlara ait güvenlik güncellemeleri

mutlaka yüklenmelidir.
- Anti virüs yazılımları kullanılmalı ve düzenli olarak güncellenmelidir.
- Kişisel güvenlik duvarları (firewall) kullanılmalıdır.
- Kişisel bilgileri ele geçirmek üzere bilgisayara sızan casus yazılımlara karşı "anti-spyware" yazılımları kullanılmalıdır .
- Tahmin edilmesi güç bir şifre oluşturulmalı ve sık sık şifreler değiştirilmelidir.
- Şüphelenilen bir durum olduğunda hemen bankayla irtibata geçilerek, bankalar durumdan haberdar edilmelidir .
- İşlemlerinizi bitirdikten sonra İnternetten çıkarken tarayıcınızı kapatmanın yanı sıra, güvenli çıkış düğmesini de kullanmanızı öneririz. Güvenliğiniz için güvenli bölge çıkış talimatlarına uymak çok önemlidir.

Banka Güvenlik Önlemleri

- Bütün PC'lerde ve serverlerde güncelleştirilmiş virüs programları kullanılması,
- Bütün network bağlantılarının güvenlik altına alınmış olması,
- Personel tarafından kullanılan PC modemlerinin kayıt altına alınması ve güvenliğinin sağlanması,
- E-posta ve ekleri için gerçek zamanlı virüs tarama programları kullanılması,
- Müşterilerin ve çalışanların bilinmeyen kaynaklardan dosya indirmemek hakkında eğitilmesi,
- Şifrelerin belirlenmesi, korunması ve değiştirilmesi ile ilgili yöntemlerin belirlenmesi,
- Online bağlantının belli bir süre kullanmama durumunda otomatik olarak kesilmesi,
- Hackerların bakış açısından bir online bankacılık sitesine girme teşebbüsü ile ilgili olarak periyodik testler yapılmasıdır.

Kaynakça: TBB (2006), 'İnternet Bankacılığı Kullanıcılarının Kişisel Bilgilerini Elde Etmeye Yönelik Virüsler Hakkında Kamuoyu Duyurusu', http://www.tbb.org.tr/turkce/duyurular/tbb/10022006.doc, Erişim Tarihi: 15.05.2007, TBB (2007), 'İnternet Bankacılığı ve Güvenlik', http://www.tbb.org.tr/v12/İNTERNET%20BANKACILIĞI%20VE%20GÜVENLİK.htm, Erişim Tarihi: 29.05.2007, Çelik, Abdullah (2002), 'İnternet Bankacılığı: Uygulamalar ve Bankacılığın Geleceğindeki Muhtemel Etkileri', Active Bankacılık ve Finans Dergisi, Yıl:5, Sayı: 27, Kasım-Aralık, s.19, Active Academy, (2004) 'E-Mailler ve İnteraktif Bankacılık Ne Kadar Güvenli?', http://www.makalem.com/Search/ArticleDetails.asp?nARTICLE_id=3504, Erişim Tarihi: 10.05.2007.

3. İnternet Bankacılığı Kullanımında Güvenlik Unsurlarının Bilinirliğine Yönelik Bir Araştırma

3.1. Araştırma Amaç ve Yöntemi

İnternet bankacılığın kullanılırlığını ve güvenilirliğinin bilinilirliğini araştırma amacında olan bu çalışma bir pilot uygulama ile Zonguldak Karaelmas Üniversitesi İktisadi ve İdari Bilimler Fakültesi İşletme, İktisat ve Maliye Bölümü öğrencileri ve öğretim elemanları üzerinde gerçekleştirilmiştir. İnternet bankacılığı ve güvenilirliğinin bilinirliği hakkında elde edilelen bilgiler teori ile yorumlanacaktır. Çalışmanın amacına uygun olarak ankete dayalı "Tanımlayıcı Araştırma Modeli" uygulanmıştır. Tanımlayıcı araştırma modelinde amaç, durum veya olgunun düzgün bir portesinin çizilmesidir (Altunışık vd, 2005: 61).

Anketler, 12 Mayıs 2007 -8 Haziran 2007 tarihleri arasında Zonguldak Karaelmas Üniversitesi İktisadi ve İdari Bilimler Fakültesi Öğretim elemanlarına ve öğrencilere uygulanmıştır. 25 sorudan oluşan anket formatı ekler kısmında sunulmaktadır. Araştırmanın ana kütlesi, 21 Öğretim üyesi, 33 Araştırma görevlisi ve 1820 öğrenciden oluşmaktadır ve ana kütle gruplaması Tablo 2'dedir.

Tablo 2: Ana Kütle Tanımı

ÖĞRENCİLER			
BÖLÜM	Bayan	Erkek	Toplam
İşletme	332	308	640
İktisat	349	330	679
Maliye	282	219	501
Toplam	963	857	1820
ÖĞRETİM ELEMANI			
STATÜ	Bayan	Erkek	Toplam
Öğretim Üyesi	3	18	21
Araştırma Görevlisi	11	22	33
Toplam	14	40	54

Anket, tabloda görülen ana kütleden 16 Öğretim üyesi 16 Araştırma görevlisi ve 311 öğrenciye uygulanmıştır. Anket dört bölümden oluşmaktadır. Birinci bölümde deneklerin kişisel (demografik) özellikleri tespit etmeye yönelik 5 sorudan oluşmaktadır. İkinci bölüm, deneklerin hangi bankacılık kanallarını tercih ettikleri ve internet bankacılığı kullanma ve güvenme düzeyleri öğrenilmeye yönelik 6 sorudan oluşmaktadır. Üçüncü bölümdeki öğrencilerin internet bankacılığı güvenlik unsurlarının bilinirliği ve internet

bankacılığında yaptıkları işlemleri araştırmaya yönelik 12 sorudan oluşmaktadır. Son bölümde öğrencilerin internet bankacılığı güvenlik bilgi düzeyini belirleme ve bu bilgilendirmenin hangi kanallardan yapılmasıyla ilgili 2 sorudan oluşmaktadır. SPSS (Statistical Package for Social Sciens 15.00) programı kullanılarak yüzde frekans, çapraz tablolar ve ki kare analizleri yapılmıştır.

3.2. Araştırma Sonuçları

Öğrencilere 580 anket uygulanmış, 401 tanesi geri dönmüştür. 90 adet eksik doldurulmuş anketin ayıklanmasıyla, kalan toplam 311 anket değerlendirilmeye alınmıştır. Yanıt verilmeyen soruların daha çok öğrencilerin bu konudaki bilgisizliklerinden kaynaklandığı düşünülmektedir. Öğretim Üyelerine 21 anket verilmiş, 16 adet cevaplanmıştır.

3.2.1. Demografik Değerlendirmeler

Tablo:3: Statüye Göre Cinsiyet Dağılımı ve Medeni Durum Dağılımı

	Cinsiyet			Medeni Hal		
Statü	**Erkek**	**Bayan**	**Toplam**	**Bekar**	**Evli**	**Toplam**
Öğrenci	141	170	311	309	2	311
Arş.Gör	9	7	16	15	1	16
Öğretim Üyesi	15	1	16	2	14	16
Toplam	165	178	343	326	17	343

Tablo 3'de görüldüğü gibi anket yapılan 16 Öğretim üyesinin 15'i (%94) erkek, 1'i (%6) bayandır. 16 araştırma görevlisinin 9'u (%56) erkek, 7'si (%44) bayandır. 311 öğrencinin 141'i (%45) erkek, 170'i (%55) bayandan oluşmaktadır. Ayrıca öğrencilerin % 99.3'ü bekar, % 0.7'si evlidir. Araştırma görevlilerinin %94'ü bekar, %6'sı evlidir. Öğretim üyelerinin ise %12'si bekar %88'si evlidir.

Tablo 4:Statüye Göre Yaş Gruplaması ve Gelir Durumu

	Yaş					Aylık Gelir				
Statü	**17-20**	**21-25**	**26-35**	**35'den fazla**	**Toplam**	**1000 YTL'den az**	**1001-2000 YTL arası**	**2001-2500 YTL arası**	**3001 YTL'den fazla**	**Toplam**
Öğrenci	82	219	10	0	311	123	139	31	16	309
Arş. Gör	0	5	11	0	16	1	13	0	2	16
Öğr.	0	0	1	15	16	0	2	10	3	15

Üyesi										
Toplam	82	224	22	15	343	124	154	41	21	340

Tablo 4'de görüldüğü gibi öğrencilerin % 70'i 21-25 yaş aralığında, %26'sı 17-20 yaş aralığında ve %0.4'ü 26-35 yaş aralığındadır. Araştırma görevlilerinin %69'u 26-35, %31'i ise 21-35 yaş aralığındadır. Öğretim Üyelerinin %94'ü 35'den fazla, %6'sı 26-35 yaş aralığındadır. Genel olarak, öğrencilerin yaş aralıkları 21-25, Araştırma görevlilerinin 26-35 ve Öğretim Üyelerinin 35'den fazla olduğu görülmektedir.

Tablo 4'de statülere göre aylık gelir dağılımları görülmektedir. Öğrencilerin %40'nın geliri 1000 YTL'den az, %45'nin 1001-2000 YTL arası, %10'nun 2001-2500 YTL ve %0.5'nin 3001 YTL'dir. Araştırma görevlilerinin %1'nin geliri 1000 YTL'den az, %81'nin 1001-2000 YTL arası, %12'nin 3000 YTL'dir. Ankete katılanlarda en çok 1000-2000 YTL arası gelir düzeyi çıkmaktadır. Öğrenci ailelerinde en yüksek oran 1000-2000 YTL iken, Akademisyenlerde 2001-2500 YTL'dir.

3.2.2. İnternet Bankacılığı Kullanma Durumu ve Güvenme Düzeyleri

Tablo 5: İnternet Bankacılığını Kullanma Durumu

İnternet Bankacılığını Kullanma Durumu			**Toplam**
Statü	**Evet**	**Hayır**	
Öğrenci	66	245	311
Araştırma Görevlisi	15	1	16
Öğretim Üyesi	14	2	16
Toplam	95	248	343

Tablo 5'de görüldüğü gibi öğrencilerin 66'sı, (%21) Araştırma görevlilerinin 15'i (%94) ve öğretim üyelerinin 14'ü (%87) internet bankacılığını kullanmaktadır. Özellikle öğrenciler arasında internet bankacılığı yaygın görülmemektedir. Genel olarak bakıldığında, ankete katılanların %28'si internet bankacılığını kullanmakta, %72'si kullanmamaktadır. Bu oran çok düşük görülmektedir.

Tablo 6: Bankacılık Kanallarını Tercih Etme Durumu

Banka Şubesini Tercih Edenler				ATM'yi Tercih Edenler		
Statü	**Tercih edenler**	**Tercih etmeyenler**	**Toplam**	**Tercih edenler**	**Tercih etmeyenler**	**Toplam**
Öğrenci	82	228	310	219	91	310
Arş. Gör	2	14	16	6	10	16
Öğr.Üyesi	5	11	16	6	10	16
Toplam	89	253	342	231	111	342
Telefon Bankacılığını Tercih Edenler				**İnternet Bankacılığını Tercih Edenler**		
Öğrenci	7	303	310	29	280	309
Arş. Gör	2	14	16	14	2	16
Öğr.Üyesi	3	13	16	14	2	16
Toplam	12	330	342	57	284	341

Tablo 6'da görüldüğü gibi öğrencilerin 82'si, (%26) Araştırma görevlilerinin 2'si (%13) ve öğretim üyelerinin 5'i (%31) bankacılık işlemlerinde banka şubesini tercih etmektedir. Öğrencilerin 219'u, (%71) Araştırma görevlilerinin 6'sı (%38) ve öğretim üyelerinin 6'sı (%38) bankacılık işlemlerinde ATM'yi tercih etmektedir. Öğrencilerin 7'si, (%2) Araştırma görevlilerinin 2'si (%87) ve öğretim üyelerinin 3'ü (%87) bankacılık işlemlerinde telefon bankacılığını tercih etmektedir. Öğrencilerin 29'su, (%%9) Araştırma görevlilerinin 14'ü (%87) ve öğretim üyelerinin 14'ü (%87) bankacılık işlemlerinde internet bankacılığını tercih etmektedir.

Bankacılık kanalı tercihinde genel bir değerlendirme yapıldığında öğrencilerin özellikle ATM'yi, araştırma görevlilerinin internet bankacılığı ve ATM'yi, öğretim üyelerinin ise internet bankacılığını tercih ettiği görülmektedir.

Tablo 7: İnternet Bankacılığı Kullanmama Nedenleri

İnternet Bankacılığı Kullanmama Nedenleri					
Statü	**İnternet bankacılığına güvenmiyorum**	**İnternet bağlantım yok**	**İnternet bankacılığı hakkında yeterli bilgiye sahip değilim.**	**Diğer**	**Toplam**
Öğrenci	89	34	97	14	234
Öğretim Üyesi	2	0	0	0	2
Toplam	91	34	97	14	236

Tablo 7'de görüldüğü gibi öğrencilerin 89'u, (%38) ve öğretim üyelerinin 2'si (%100) internet bankacılığını kullanmama

nedeni olarak; internet bankacılığını güvenli bulmadıklarını, öğrencilerin 34'ü (%15) internet bağlantılarının olmadığını, 14'ü (%41) diğer sebepleri neden olarak gösterirken, öğrencilerin 97'si (%41) ise İnternet bankacılığı hakkında yeterli bilgiye sahip olmadıklarını belirtmişlerdir.

Ankete katılanların internet bankacılığı işlemlerini güvenli bulmasının frekans analizine bakılırsa %40'ı internet bankacılığı işlemlerini güvenli bulduklarını, %56'sının ise güvenli bulmadıklarını belirtmiştir.

Tablo 8: İnternet Bankacılığı İşlemlerini Güvenli Bulma Durumunun Statüye ve Yaşlara Göre Dağılımı

İnternet Bankacılığı İşlemlerini Güvenli Bulma Durumu							
Statü	**Evet**	**Hayır**	**Toplam**	**Yaş Grubu**	**Evet**	**Hayır**	**Toplam**
Öğrenci	110	185	295	**17-20**	30	48	78
Arş. Gör	11	4	15	**21-25**	79	132	211
Öğr. Üyesi	12	4	16	**26-35**	13	9	22
Toplam	133	193	326	**35'den fazla**	11	4	15
Pearson Chi-Square (Ki-kare)	Value(15,828)	df (2)	Asymp. Sig. (2-sided) 0.000	**Toplam**	133	193	326

Tablo 8'de görüldüğü gibi statülere göre internet bankacılığı işlemlerini güvenli bulma durumuna bakılırsa; öğrencilerin 110'u, (%37) araştırma görevlilerinin 11'i (%73) ve öğretim üyelerinin 12'si (% 75) internet bankacılığı işlemlerine güven duyduklarını belirtmiştir.

Tablodan yaş gruplarına göre bakılırsa; 17-20 yaş grubundaki katılımcıların 30'u, (%38) 21-25 yaş grubundaki katılımcıların 79'u, (%37) 26-35 yaş grubundaki katılımcıların 13'ü (%59) ve 35 yaşından fazla olan katılımcıların 11'i, (%73) internet bankacılığı işlemlerini güvenli bulmaktadır. Genel olarak, 17-20 ve 21-25 yaş grubundaki katılımcılar, 26-35 ve 35'den fazla olan yaş grubundaki katılımcılara göre internet bankacılığı işlemlerini daha az güvenli bulmamaktadır.

H_0: Öğrenci, araştırma görevlisi ve öğretim üyelerinin internet bankacılığına güven durumları aynıdır. H_1: Öğrenci, araştırma görevlisi ve öğretim üyelerinin internet bankacılığına güven durumları birbirinden farklıdır.

P (sig) <0.05 olduğunda H_0 hipotezi red edilir. Ki-kare istatistiği 15,828 ve 0.000 <0.05 olduğu için öğrenci, araştırma görevlisi ve öğretim üyelerinin internet bankacılığına güven durumları

birbirinden farklıdır. Bundan sonraki Ki-kare istatistiği yorumlanırken hipotezler yazılmayacak ve kısaca sig katsayısı ve Ki-kare istatistiği yorumlanacaktır.

Tablo 9: İnternet Bankacılığını Kullanma Sıklığı

İnternet Bankacılığı Kullanma Sıklığı					
Statü	**Her gün**	**Haftada bir veya daha fazla**	**Ayda bir veya daha fazla**	**Yılda bir veya daha fazla**	**Toplam**
Öğrenci	5	15	27	15	62
Araştırma Görevlisi	2	11	2	0	15
Öğretim Üyesi	0	12	2	0	14
Toplam	7	38	31	15	91

Tablo 9'da görüldüğü gibi öğrencilerin 5'i (%8) her gün, 15'i (%24) haftada bir veya daha fazla, 27'si (%44) ayda bir veya daha fazla, 15'i (%24) yılda bir veya daha fazla internet bankacılığını kullanmaktadır. Araştırma görevlilerinin 2'si (%13) her gün, 11'i (%74) haftada bir veya daha fazla, 2'si (%13) ayda bir veya daha fazla internet bankacılığını kullanmaktadır. Öğretim üyelerinin 12'si (%86) haftada bir veya daha fazla, 2'si (%14) ayda bir veya daha fazla internet bankacılığını kullanmaktadır. Özellikle, öğrenciler ayda bir veya daha fazla, araştırma görevlileri ve öğretim üyeleri, haftada bir veya daha fazla internet bankacılığını kullanmaktadır.

Tablo 10: İnternet Bankacılığını Kullanma Kanalları

	Öğrenci	**Araştırma Görevlisi**	**Öğretim Üyesi**	**Toplam**
Masa Üstü Bilgisayar	44	13	14	71
Diz Üstü Bilgisayar	19	11	3	33
Cep telefonu	2	2	-	4
Cep Bilgisayarı	-	-	-	-

Tablo 10'de görüldüğü gibi internet bankacılığını kullanan öğrenciler, araştırma görevlileri ve öğretim üyelerinin çoğu masa üstü bilgisayar kullanmaktadır. Cep bilgisayarı hiç kullanılmamaktadır.

3.2.3. İnternet Bankacılığı Güvenlik Unsurlarının Bilinirliği ve Yapılan İşlemler

Tablo 11: İnternet Bankacılığında Yapılan İşlemler

	Öğrenci	Araştırma Görevlisi	Öğretim Üyesi	Asymp. Sig. (2-sided)
Kart işlemleri	34	13	8	,105
Hesap işlemleri	37	14	12	,028
Para transferleri	28	15	12	,000
Ödemeler	16	13	9	,000
Döviz işlemleri	5	3	2	,424
Yatırım işlemleri	6	3	3	,193

Tablo 11'de görüldüğü gibi genel olarak internet bankacılığında en çok yapılan işlemler; kart işlemleri, hesap işlemleri ve para transferleridir. Buna karşın en az yapılan işlemler ise döviz işlemleri ve yatırım işlemleridir. Tablonun en sağında ki-kare istatistiğinin anlamlılık dereceleri verilmiştir. Daha önce de belirtildiği gibi p (sig) <0.05 olduğunda H_0 hipotezi reddedilir ve gruplar arasında anlamlı bir farklılık olduğu sonucuna varılır. Anlamlılık derecelerine göre; öğrenciler, araştırma görevlileri ve öğretim üyelerinin arasında, hesap işlemleri, para transferleri ve ödeme işlemlerinde anlamlı bir farklılık vardır.

Tablo 12: İnternet Bankacılığı Güvenlik Unsurları Hakkındaki Bilgi Düzeyi

Firewall (güvenlik duvarı) Bilinirliği				**İşletim Sistemi Güvenlik Güncellemeleri Bilinirliği**			
Statü	Evet	Hayır	Toplam	**Statü**	Evet	Hayır	Toplam
Öğrenci	84	221	305	**Öğrenci**	103	204	307
Araş. Gör.	11	5	16	**Araş. Gör.**	12	4	16
Öğretim Üyesi	14	2	16	**Öğretim Üyesi**	11	5	16
Toplam	109	228	337	**Toplam**	126	213	339
Pearson Chi-Square (Ki-kare)	Value (35,150)	df (2)	Asymp. Sig. (2-sided) 0.000	**Pearson Chi-Square (Ki-kare)**	Value 18,360	df (2)	Asymp. Sig. (2-sided) 0.000

Anti-virüs Yazılımları Bilinirliği				Anti- Spy Yazılımları Bilinirliği			
Statü	Evet	Hayır	Toplam	**Statü**	Evet	Hayır	Toplam
Öğrenci	199	108	307	**Öğrenci**	66	240	306
Arş. Gör	16	0	16	**Arş.Gör**	9	7	16
Öğr. Üyesi	16	0	16	**Öğr. Üyesi**	11	5	16
Toplam	231	108	339	**Toplam**	86	252	338
Pearson Chi-Square (Ki-kare)	Value 16,520	df 2	Asymp. Sig. (2-sided) 0.000	**Pearson Chi-Square (Ki-kare)**	Value 26,245	df 2	Asymp. Sig. (2-sided) 0.000
Elektronik (mobil)İmza Bilinirliği				**SSL Protokolü Bilinirliği**			
Statü	Evet	Hayır	Toplam	**Statü**	Evet	Hayır	Toplam
Öğrenci	120	186	306	**Öğrenci**	29	277	306
Arş. Gör	13	3	16	**Arş. Gör**	4	12	16
Öğr. Üyesi	10	6	16	**Öğr. Üyesi**	7	9	16
Toplam	143	195	338	**Toplam**	40	298	338
Pearson Chi-Square (Ki-kare)	Value 13,812	df 2	Asymp. Sig. (2-sided) 0,000	**Pearson Chi-Square (Ki-kare)**	Value 19,908	df 2	Asymp. Sig. (2-sided) 0.000
E-Anahtar Bilinirliği				**Elektronik Sertifika Bilinirliği**			
Statü	Evet	Hayır	Toplam	**Statü**	Evet	Hayır	Toplam
Öğrenci	80	226	306	**Öğrenci**	74	232	306
Arş.Gör.	3	13	16	**Arş.Gör.**	5	11	16
Öğr. Üyesi	6	10	16	**Öğr. Üyesi**	9	7	16
Toplam	89	249	338	**Toplam**	88	250	338
Pearson Chi-Square (Ki-kare)	Value 1,509	df 2	Asymp. Sig. (2-sided) 0,470	**Pearson Chi-Square (Ki-kare)**	Value 8,356	df 2	Asymp. Sig. (2-sided) 0,015

Sanal Klavye Bilinirliği			
Statü	Evet	Hayır	Toplam
Öğrenci	102	204	306
Arş. Gör			
Öğr. Üyesi	14	2	16

Toplam	130	208	338
Pearson Chi-Square (Ki-kare)	Value 35,913	df 2	Asymp. Sig. (2-sided) 0.000

Tablo 12'de gösterildiği gibi öğrencilerin 84'ü, (%28) araştırma görevlilerinin 11'i (%69)ve öğretim üyelerinin 14'ü (%88) internet bankacılığı güvenlik unsuru olan firewall (güvenlik duvarı) hakkında bilgi sahibidir. p (sig) <0.05 olduğunda H_0 hipotezi red edilir. Pearson Chi-Square (Ki-kare) istatistiği 35,150 ve 0.000 <0.05 olduğu için öğrenci, araştırma görevlisi ve öğretim üyelerinin firewall hakkındaki bilgi düzeyi birbirinden farklıdır.

Öğrencilerin 103'ü, (%34) araştırma görevlilerinin 12'si (%75) ve öğretim üyelerinin 11'i (%69) internet bankacılığı güvenlik unsuru olan İşletim sistemi güvenlik güncellemeleri hakkında bilgi sahibidir. p (sig) <0.05 olduğunda H_0 hipotezi red edilir. Ki-kare istatistiği 18,360 ve 0.000 <0.05 olduğu için öğrenci, araştırma görevlisi ve öğretim üyelerinin işletim sistemi güvenlik güncellemeleri hakkındaki bilgi düzeyi birbirinden farklıdır.

Öğrencilerin 199'u, (%65) araştırma görevlilerinin ve öğretim üyelerinin tümü internet bankacılığı güvenlik unsuru olan Anti-virüs yazılımları hakkında bilgi sahibidir.

Burada araştırma görevlileri ve öğretim üyelerinin tümü Anti-virüs yazılımlarını bildikleri için tek bir grup olarak alınmıştır. p (sig) <0.05 olduğunda H_0 hipotezi red edilir. Ki-kare istatistiği 16,520 ve 0.000 <0.05 olduğu için öğrencilerle araştırma görevlisi ve öğretim üyelerinin işletim sistemi güvenlik güncellemeleri hakkındaki bilgi düzeyi birbirinden farklıdır.

Öğrencilerin 66'sı, (%22) araştırma görevlilerinin 9'u (%56) ve öğretim üyelerinin 11'i (%69) internet bankacılığı güvenlik unsuru olan Anti-spy yazılımları hakkında bilgi sahibidir. p (sig) <0.05 olduğunda H_0 hipotezi red edilir. Ki-kare istatistiği 26,245 ve 0.000 <0.05 olduğu için öğrenciler, araştırma görevlisi ve öğretim üyelerinin Anti-spy yazılımları hakkındaki bilgi düzeyi birbirinden farklıdır.

Öğrencilerin 95'i, (%45) araştırma görevlilerinin 14'ü (%88) ve öğretim üyelerinin 15'i (%94) internet bankacılığı güvenlik unsuru olan İnternet bankacılığı güvenli çıkışı hakkında bilgi sahibidir. p (sig) <0.05 olduğunda H_0 hipotezi red edilir. Ki-kare istatistiği 44,408 ve 0.000 <0.05 olduğu için öğrenciler, araştırma görevlisi ve öğretim üyelerinin İnternet bankacılığı güvenli çıkış hakkındaki bilgi düzeyi birbirinden farklıdır.

Öğrencilerin 120'si, (%39) araştırma görevlilerinin 13'i (%81) ve öğretim üyelerinin 10'u (%63) internet bankacılığı güvenlik unsuru olan Elektronik (mobil) imza hakkında bilgi sahibidir. p (sig) <0.05 olduğunda H_0 hipotezi red edilir. Ki-kare istatistiği 13,812 ve 0.001 <0.05 olduğu için öğrenciler, araştırma görevlisi ve öğretim üyelerinin elektronik (mobil) imza hakkındaki bilgi düzeyi birbirinden farklıdır.

Öğrencilerin 29'u, (%9) araştırma görevlilerinin 4'ü (%25) ve öğretim üyelerinin 7'si (%44) internet bankacılığı güvenlik unsuru olan SSL protokolü hakkında bilgi sahibidir.p (sig) <0.05 olduğunda H_0 hipotezi red edilir. Ki-kare istatistiği 19,908 ve 0.000 <0.05 olduğu için öğrenciler, araştırma görevlisi ve öğretim üyelerinin SSL protokolü hakkındaki bilgi düzeyi birbirinden farklıdır.

Öğrencilerin 80'i, (%26) araştırma görevlilerinin 3'ü (%19) ve öğretim üyelerinin 6'sı (38) internet bankacılığı güvenlik unsuru olan E-anahtarı hakkında bilgi sahibidir.p (sig) > 0.05 olduğunda H_0 hipotezi kabul edilir. Ki-kare istatistiği 1,509 ve 0.470 > 0.05 olduğu için öğrenciler, araştırma görevlisi ve öğretim üyelerinin E-anahtarı hakkında bilgi düzeyi aynıdır.

Öğrencilerin 74'ü,(%24) araştırma görevlilerinin 5'i (45) ve öğretim üyelerinin 9'u (%56) internet bankacılığı güvenlik unsuru olan Elektronik sertifika hakkında bilgi sahibidir. p (sig) <0.05 olduğunda H_0 hipotezi red edilir. Ki-kare istatistiği 8,356 ve 0.015 <0.05 olduğu için öğrenciler, araştırma görevlisi ve öğretim üyelerinin elektronik sertifika hakkındaki bilgi düzeyi birbirinden farklıdır.

Öğrencilerin 102'si,(%33) araştırma görevlilerinin 14'ü (%88) ve öğretim üyelerinin 14'ü (%88) internet bankacılığı güvenlik unsuru olan Sanal klavye hakkında bilgi sahibidir. p (sig) <0.05 olduğunda H_0 hipotezi red edilir. Ki-kare istatistiği 35,913 ve 0.000 <0.05 olduğu için öğrenciler, araştırma görevlisi ve öğretim üyelerinin sanal klavye hakkındaki bilgi düzeyi birbirinden farklıdır.

3.2.4. İnternet Bankacılığı Kullanımında Güvenlik Unsurlarının Bilgi Düzeyi ve Bilgilendirme Kanalları

Aşağıda öğrenci, araştırma görevlisi ve öğretim üyelerinin internet bankacılığı kullanırken dikkat ettiği güvenlik unsurları önem derecesine göre tablolaştırılmıştır.

Tablo 13: İnternet Bankacılığı Kullanımında Güvenlik Unsurlarının Bilgi Düzeyi

Anti Virüs Yazılımlarını Kullanmak Ve Bunları Sürekli Güncellemek						Toplam
Statü	1. Öncelik	2. Öncelik	3. Öncelik	4. Öncelik	5. Öncelik	

Öğrenci	87	13	15	8	17	140
Araştırma Görevlisi	5	0	1	0	2	8
Öğretim Üyesi	2	1	2	2	0	7
Toplam	94	14	18	10	19	155
Anti Spy (Casus) Yazılımlarını Kullanmak Bunları Sürekli Güncellemek						**Toplam**
Öğrenci	7	10	12	7	13	49
Araştırma Görevlisi	0	3	1	2	0	6
Öğretim Üyesi	1	2	2	0	0	5
Toplam	8	15	15	9	13	60
Sanal Klavyeyi Kullanmak						Toplam
Öğrenci	13	42	21	11	7	94
Araştırma Görevlisi	3	2	5	2	1	13
Öğretim Üyesi	5	2	0	2	1	10
Toplam	21	46	26	15	9	117
Güvenilmeyen Network ve Bilgisayarları Kullanmamak						Toplam
Öğrenci	20	28	19	13	12	92
Araştırma Görevlisi	0	3	0	1	1	5
Öğretim Üyesi	2	3	3	3	1	12
Toplam	22	34	22	17	14	109
İnternet Sayfasının Güvenliğini Gösteren Kilit İşaretine Dikkat Etmek						Toplam
Öğrenci	7	19	22	23	12	83
Araştırma Görevlisi	0	1	0	1	4	6
Öğretim Üyesi	0	3	1	1	4	9
Toplam	7	23	23	25	20	98
E-Maillerle Gönderilen Sahte İnternet Bankacılığı Linklerine Dikkat Etmek						Toplam
Öğrenci	7	12	24	22	20	85
Araştırma Görevlisi	1	0	2	4	2	9
Öğretim Üyesi	2	0	5	2	2	11
Toplam	10	12	31	28	24	105
Şifreleri Üçüncü Şahıslarla Paylaşmamak ve Sürekli Değiştirmek						Toplam
Öğrenci	18	31	44	36	12	141
Araştırma Görevlisi	3	1	3	1	0	8
Öğretim Üyesi	3	2	0	2	1	8
Toplam	24	34	47	39	13	157
İnternet Bankacılığında Elektronik Sertifikaya Sahip Olup Olmadığına Dikkat Etmek						Toplam
Öğrenci	6	9	5	20	14	54
Araştırma Görevlisi	1	0	2	2	0	5
Öğretim Üyesi	0	1	2	2	4	9
Toplam	7	10	9	24	18	68
Mobil İmza (Elektronik İmza) Kullanmak						Toplam
Öğrenci	7	4	7	22	28	68
Araştırma Görevlisi	0	1	0	0	3	4

Öğretim Üyesi	0	1	0	0	1	2
Toplam	7	6	7	22	32	74
Firewall (Güvenlik Duvarı) Kullanmak						Toplam
Öğrenci	8	9	8	15	42	82
Araştırma Görevlisi	1	3	0	1	1	6
Öğretim Üyesi	0	0	0	1	1	2
Toplam	9	12	8	17	44	90

Tablo 13'e genel olarak bakıldığında öğrencilerin çoğu birinci öncelik olarak anti vürüs yazılımlarını kullanmakta ve bunları sürekli güncellemektedir. İkinci önceliklerinde, şifreleri üçüncü şahıslarla paylaşmamakta ve sürekli değiştirmekte, güvenilmeyen network ve bilgisayarları kullanmamaktadır. Üçüncü önceliklerinde, sanal klavyeyi kullanmakta, yine şifreleri üçüncü şahıslarla paylaşmamakta ve sürekli değiştirmektedir. Dördüncü öncelikte, şifreleri üçüncü şahıslarla paylaşmamakta ve sürekli değiştirmektedir. Beşinci öncelikte ise, firewall (güvenlik duvarı) kullanmakta olduklarını belirtmişlerdir.

Araştırma görevlilerinin çoğu birinci öncelik olarak anti vürüs yazılımlarını kullanmakta ve bunları sürekli güncellemekte ve sanal klavye kullanmaktadır. İkinci önceliklerinde, güvenilmeyen network ve bilgisayarları kullanmamakta ve anti spy (casus) yazılımlarını kullanmakta bunları sürekli güncellemektedir. Üçüncü önceliklerinde, sanal klavyeyi kullanmakta, yine şifreleri üçüncü şahıslarla paylaşmamakta ve sürekli değiştirmektedir. Dördüncü öncelikte, e-maillerle gönderilen sahte internet bankacılığı linklerine dikkat etmektedir. Beşinci öncelikte ise, internet sayfasının güvenliğini gösteren kilit işaretine dikkat etmekte olduklarını belirtmişlerdir.

Öğretim Üyelerinin çoğu birinci öncelik olarak, sanal klavye kullanmaktadır. İkinci önceliklerinde, güvenilmeyen network ve bilgisayarları kullanmamakta ve internet sayfasının güvenliğini gösteren kilit işaretine dikkat etmektedir. Üçüncü önceliklerinde, e-maillerle gönderilen sahte internet bankacılığı linklerine dikkat etmektedir, Dördüncü öncelikte, güvenilmeyen network ve bilgisayarları kullanmamaktadır. Beşinci öncelikte ise, internet sayfasının güvenliğini gösteren kilit işaretine dikkat etmekte ve bankanın internet bankacılığında elektronik sertifikaya sahip olup olmadığına dikkat etmekte olduklarını belirtmişlerdir.

Tablo 14: İnternet Bankacılığı Kullanımı ve Güvenliği Konusunda Bilgilendirilmek İstenmesi

	Frekans	Yüzde	Kümülatif Yüzde
Evet	252	73,5	77,3
Hayır	74	21,6	100,0
Toplam	326	95,0	
Eksik	17	5,0	
Toplam	343	100,0	

Ankete katılanların % 73.5'i İnternet bankacılığı kullanımı ve güvenliği konusunda bilgilendirilmek istenmektedir. Aşağıdaki tabloda ise internet bankacılığı kullanımı ve güvenliği konusunda bilgilendirilmek istenen kanallar tablo halinde verilmiştir.

Tablo 15: İnternet Bankacılığı Kullanımı ve Güvenliği Konusunda Bilgilendirilmek İstenen Kanallar

İnternet Bankacılığı Hakkında Bilgilendirmek İstenen Kanal	Banka Tarafından İnternet Üzerinden Verilen Eğitim	Banka Personeli Tarafından Verilen Eğitim	Üniversite'deki Öğretim Üyeleri Tarafından Verilen Eğitim	Konferans, Seminer Ve Kongrelerde Eğitim Verilmesi
Frekans	95	93	97	112

Tablo 15'de gösterildiği gibi ankete katılanların çoğu yukarıda görülen kanallardan bilgilendirmek istemektedir. En fazla bilgilendirilmek istenen kanal ise konferans, seminer ve kongrelerde eğitim verilmesini belirtmişlerdir.

4. Sonuç

İnternet yüzyılımızın en hızlı gelişen, insanoğluna bilgiye sahip olma ve teknolojinin kullanımı konusunda sınırsız katkı yapan bir buluştur. Bu buluşun bankacılık sektörüne yansıması son dönemde özellikle internet bankacılığında yoğunlaşmaktadır. İnternet bankacılığı yaygınlaşırken aynı zamanda internet bankacılığı yoluyla dolandırıcılık işlemlerinin yapılabilmesi internet bankacılığı güvenirliliğini gündeme taşımaktadır. İnternet bankacılığına güvenilirlik sağlamak amacıyla sistemler geliştirilmektir. Gerek internet bankacılığının sunduğu hizmetlerin bilinilirliği gerek internet bankacılığı güvenlik sistemlerinin bilinilirliğiyle internet bankacılığı kullanımını etkileyecektir. Bilgi düzeyi farklılıklarının kullanım farklılıklarına yol açması kaçınılmazdır.

Bu teoriyi test etme amacıyla anket sistemine dayanan çalışma Zonguldak Karaelmas Üniversitesi İktisadi ve İdari Bilimler Fakültesinin 16 Öğretim üyesi 16 Araştırma görevlisi ve 311

öğrencisine uygulanmıştır. Değerlendirme sonuçlarına göre internet bankacılığı kullanım oranı; öğrencilerde %21, araştırma görevlilerinde % 94 ve öğretim üyelerinde % 88 dolaylarındadır. Özellikle öğrencilerde internet bankacılığı kullanım oranı düşüktür ve internet bankacılığına güvenme düzeyi % 39'dur. Özellikle öğrenciler, birkaç güncel güvenlik unsurunun dışında internet bankacılığı güvenlik unsurları hakkında bilgi sahibi değildirler ve internet bankacılığı hakkında bilgilendirilmek istemektedirler. Öğretim elemanlarında internet bankacığı güvenlik sistemlerinin bilinirliği ve güvenme düzeyi daha yüksek olmasına rağmen bilgilendirilme isteğine sahiptirler. İnternet bankacılığının ve internet bankacılığı güvenilirliğinin bilinilirliği kullanımı artırmaktadır. Gelir düzeylerine göre internet bankacılığı kullanımına bakıldığında, Öğretim üyeleri öğrencilere göre internet bankacılığını daha çok kullanmaktadır ve bundan dolayı gelir düzeyindeki artışın internet bankacılığı kullanımını artırdığı ifade edilebilir. Türkiye'de kişi başına düşen milli geliri artan bir ülke olduğu için internet bankacılığı kullanım potansiyelinin artması kaçınılmazdır. Bankacılık kesiminin de bu artışı dikkate alması gerekmektedir.

İnternet bankacılığının yaygınlaşması hem bankalara hem de kullanıcılara maliyet, zaman tasarrufu sağlamaktadır. Bu avantajlara rağmen, internet bankacılığı işlemleri ve internet bankacılığı güvenlik unsurlarının bilinirliği ve uygulanmasının çok düşük olduğu sonucuna varılmıştır. Bu düzeyi arttırmak için özellikle görsel ve yazılı medyada ve okullarda internet bankacılığı ve güvenlik unsurları hakkında bilgi aktarımı sağlanmalıdır. Görsel basında kısa bilgilendirme filmleri, yazılı basında tanıtım yazıları, okullarda konferanslar verilebilir, okulların ders müfredatlarına eklenebilir. Sonuç olarak; internet bankacılığı yaygınlaşabilmesi için internet bankacılığı hakkında toplum bilgilendirilmeli ve internet bankacılığı güvenlik unsurlarının bilinilirliği artırılmalıdır.

KAYNAKÇA

ACTİVE ACADEMY, (2004), "E-Mailler ve İnteraktif Bankacılık Ne Kadar Güvenli?", http://www.makalem.com/Search/ArticleDetails.asp?nARTICLE_id=3504, Erişim Tarihi: 10.05.2007.

ACTİVE ACADEMY, (2006), "Güvenlik Endişesi, İnternet Bankacılığını Yavaşlatıyor", Activeline Gazetesi, Yıl:6, Sayı:72, Mart.

ALTUNIŞIK Remzi, ve Diğerleri, Sosyal *Bilimlerde Araştırma Yöntemleri: Spss Uygulamalı*, Geliştirilmiş 4.Baskı, Sakarya Kitabevi, Sakarya.

AKÇA, Cem (2005), "Microsoft'tan Anti-Casus Yazılımı: Windows AntiSpyware" http://www.pclabs.gen.tr/2005/01/07/microsofttan-anti-casus-yazilimi-windows-antispyware/

AKSOY, Ramazan (2006) İnternet Ortamında Pazarlama, Seçkin Yayıncılık, Ankara.

BÜYÜKBAHÇECİ, Muharrem, "E- İmza Online Bankacılığın Güveni Artıyor" http://turk.internet.com/haber/yazigoster.php3?yaziid=17422, Erişim Tarihi: 18.05.2007.

BERBER, Keser, Leyla, (2006), İnternet Bankacılığında Güvenli Elektronik İmza'ya Geçiş Zorunluluğu, http://www.e-imza.gen.tr/templates/resimler/File/makaleler/Internet_Bankaciliginda_Guvenli_ Eimzaya_Gecis_LKeser.pdf, Erişim Tarihi: 20.05.2007

CAN, Özgü ve Baki Murat Bozkurt, (1994), "Elektronik Ödeme Sistemlerinin Güvenilirliği Üzerine Bir Çalışma", Pamukkale Üniversitesi, Bilgi Teknolojileri Kongresi III, 7-9 Ekim. Bildiriler Kitabı, ss.107-109.

ÇELİK, Abdullah (2002), "İnternet Bankacılığı: Uygulamalar ve Bankacılığın Geleceğindeki Muhtemel Etkileri", *Active Bankacılık ve Finans Der*gisi, Yıl:5, Sayı: 27, Kasım-Aralık, ss.6-23.

DAYIOĞLU, Burak, 'Ağ ve İşletim Sistemleri', http://www.e-ticaretmerkezi.net/agveisletimsistemi.pdf, Erişim Tarihi: 30.05.2007.

ERTAŞ, Sacit (2000), "Elektronik Ticaret: Tanımı, Gelişimi, Avantajları, Güvenliği," Der:Veysel Bozkurt, Elektronik Ticaret, Alfa Basım Yayın, Bursa.

FORSNET (2007), 'e-imza nedir', http://www.e-imza.gen.tr, Erişim Tarihi: 15.05.2007.

İNALÖZ, Ayşe (2003), "Telekomünikasyon Regülasyonları Çerçevesinde Elektronik Ticaretin İncelenmesi," Telekomünikasyon Kurumu Uzmanlık Tezi, Ankara, Aralık, www.tk.gov.tr/Yayin/Uzmanlik_Tezleri/ tktezler/Ayse_Inaloz_Tez.pdf, Erişim Tarihi: 20.05.2007.

GAZİLER, Volkan (2006), "İnternet Bankacılığı Ve Kullanımının Etkinliği: Kullanım Etkinliği-Eğitim İlişkisini Ortaya Koymaya

Yönelik Bir Araştırma", Gazi Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.
HSBC (2007), "Sanal Klavye" http://www.hsbc.com.tr/BireyselBankacilik/SikcaSorulanSorular/SanalKlavye.asp#2, Erişim Tarihi: 10.06.2007.
KORKMAZ, Turhan ve Halime Temel, (2006), 'E-Finans ve Elektronik Ödemelerde Güven Unsuru', 5. Bilgi Ekonomi ve Yönetim Kongresi, 3-5 Kasım, 2006, Bildiriler Kitabı II. Cilt, Kocaeli, ss. 984-998.
ORHUN, Can (2003), "İnternet Bankacılığında Güvenli İletişim ve Açık Anahtar Altyapısı", Active Bankacılık ve Finans Dergisi, Yıl:6, Sayı: 30, Mayıs-Haziran, ss.46.50.
SEVİNÇ, Eser (2001), "Elektronik Ticaret Güvenlik, Denetim, İdari ve Yasal Düzenlemeler", http://www.ymm.net/e-ticaret/e-ticarette_guvenlik.html, Erişim Tarihi: 01.06.2007
TBB (2006), "İnternet Bankacılığı Kullanıcılarının Kişisel Bilgilerini Elde Etmeye Yönelik Virüsler Hakkında Kamuoyu Duyurusu", http://www.tbb.org.tr/turkce/duyurular/tbb/10022006.doc, Erişim Tarihi: 15.05.2007.
TBB (2007), "İnternet Bankacılığı ve Güvenlik", http://www.tbb.org.tr/v12/İNTERNET%20BANKACILIĞI%20VE%20GÜVENLİK.htm, Erişim Tarihi: 29.05.2007
Microsoft (2005), "Bilgisayar virüsü nedir?", http://www.microsoft.com/turkiye/athome/security/viruses/intro_viruses_what.mspx, Erişim Tarihi: 15.05.2007.
MİCROSOFT (2006), "İşletmenizi Güvenlik Duvarıyla Savunun," http://www.microsoft.com/turkiye/girisimci/products/howto/firewall.mspx, Erişim Tarihi: 19.05.2007.
WALTHER, Stephen-Jonathan Levine-Çev: Taylan Yemliha (2001), *ASP ile E-Ticaret Programcılığ*ı, Sistem Yayıncılık, İstanbul.