

İnternet'te Bireysel Güvenliđi Nasıl Sağlarız?

Günümüzde kişilerin internette bilgilerinin korunması ve bu bilgilere herhangi bir zarar gelmesinin önlenmesi ilk bakışta kolay gibi gözükse de esasında oldukça zor bir durumdur. Bilgileri korumak kredi kartlarını kimseye göstermemek, şifreni kimseyle paylaşmamaktan ibaret değildir. Bilgileri korumak için doğru yazılımların kullanılması, internet üzerinden yapılacak alışverişlerin güvenilir siteler üzerinden yapılması kişinin güvenli bir şekilde bilgilerini koruyarak, kendisine ve kişisel bilgilerine zarar gelmesini önleyebilir.

İnternet üzerinde saldırganların kullandığı çeşitli yollar vardır. Bunlardan bir tanesi bilgisayara bulaştırılacak olan trojan veya bunun gibi yazılmış kötü amaçlı yazılımlardır. Bu tehlikeden korunmanın en hızlı ve verimli yolu antivirüs programları veya casus yazılımlarını önleyici (spyware) programları kullanmaktır. Eğer ortada bir zayıflık yoksa, virüs kendi kendine bulaşamaz. Zayıflığı engellemenin yollarından bir tanesi de güncellemelerin doğru şekilde yapıldığından emin olmaktır. Güvenlik, zararların bir anda engellenerek gelecekte yaşanabilecek sıkıntıları tamamen yok etmesi anlamına gelmemektedir. Güvenliđi sağlamanın yollarından bir tanesi de süreç aşamasında zaman zaman yapılacak güncellemelerden geçmektedir. Eğer bilgisayarınıza zararlı bir program girerse; e-posta hesaplarınız, banka şifreleriniz, diğer kişisel bilgilerinizin zarar görebileceđi gibi bilgisayarınızda ki değerli belgeleriniz silinebilir, kopyalanabilir ve bilgisayar üzerinde yaptığınız her şeyi kaydedebilir. Ayrıca hard diskinizin içinde bulunan tüm verileri silebilir ve diğer kötü amaçlı yazılımların yüklenmesine sebep olabilir.

Saldırganların kullandığı bir diğer yöntemde internet üzerinden kredi kartı hırsızlığıdır. Saldırganlar, şahısların kredi kartı bilgilerini ele geçirmek için phishing (oltalama) ve pharming (yemleme) yöntemlerini kullanmaktadır. Phishing yönteminde; saldırgan kişinin kullandığı bankanın, e-posta hesabının ve bunun gibi bilgilerini girmesi gereken web sitelerinin kopyalarını yaparak kişiye gönderir. Kişi eđer bilgilerini girip devam ederse, bu kopya sitelerin içinde bulunan kod parçacıklarıyla bunu saldırgana yönlendirir ve saldırganın bu bilgileri kullanarak kredi kartı numaralarını, şifreleri, hesap numaralarını çalmasına olanak sağlar. Pharming yöntemi ise daha farklı şekilde işlemektedir. Pharming yönteminde; saldırgan DNS sunucusuna girer ve sunucu cache'nde tutulan yasal adresi sahte adrese yönlendirir veya kişinin bilgisayarına gönderdiği trojanla kişinin ruhu bile duymadan kişisel bilgilerini çalar. Pharming daha tehlikelidir sebebi ise denetlenmesi çok daha zordur. 21 Ekim 2011 tarihinde yaşanan bir çete operasyonunda, çete üyelerinin internette kurdukları bazı alışveriş siteleriyle kişilerin

kredi kartı bilgilerini çalarak milyonlarca lira vurgun yaptığı ortaya çıkmıştır. Bu saldırılara karşı alınacak belli başlı önlemler ise şöyledir; bilgisayarınızın güncellemelerini mutlaka yapmalı ve güncel bir antivirüs programı kullanılmalıdır. Gelen e-postanın kimden geldiğine emin olunmayan durumda bu e-posta 'spam' olarak değerlendirilmelidir. Güvenli olmayan internet siteleri üzerinden alışveriş gerçekleştirilmemeli, kişisel bilgiler kesinlikle kullanılmamalıdır. Ayrıca yapılacak alışverişlerde gerçek kredi kartlarını kullanmak yerine sanal kredi kartlarını kullanılması zararı engellemede fayda sağlar.

Saldırganların kullandığı yollardan biri de internet bankacılığını kullanarak yapılan dolandırıcılık yöntemleridir. İnternet bankacılığı kullanırken dolandırmalar yine phishing ve pharming üzerinden yapılmaktadır. Bankalar güvenlik önlemlerini son derece üst düzeyde tutmaktadır. Ancak saldırganlar da kendilerini her konuda geliştirmektedir. Mart 2011'de internet üzerinde ki hesabından 11 bin TL çekildiğini fark eden çift bankaya açtıkları davayla paralarını faiziyle beraber aldılar. Bu yaşanan olay esasında bankanın güvenlik açığından faydalanarak yapılmış olan dolandırıcılıktır. Kişi güvenilir olmayan ağ üzerinden internet bankacılığı kullanırsa saldırganın eline kişisel bilgilerinin geçmesine olanak sağlayabilir. Bu yüzden güvenilmeyen ağ üzerinden kesinlikle internet bankacılığı kullanılmamalı ve işlem yapılmamalıdır. Açılan oturum kesinlikle kapatılarak daha sonra erişime imkan verilmemelidir. Her banka için ayrı şifre belirlenmeli. Bankanızdan gelen ekstreleri tek tek kontrol edin. Ayrıca internet bankacılığı üzerinden yapılacak işlemleri sanal klavyeler kullanarak daha güvenli hale getirilebilir.

İnternet üzerinden kullanılan kredi kartı hırsızlığında ve internet bankacılığı kullanılarak yapılan dolandırmalara benzer bir durum ise kimlik hırsızlığıdır. Kimlik hırsızlığında kullanılan yöntemlerden birkaçı; kredi kartlarınızın, kimlik kartlarınız ve diğer bilgilerinizin bulunduğu çanta ve cüzdanlarınızı çalarak veya internette paylaştığınız kişisel bilgilerinizi kullanarak gerçekleştirilebilir. Kimlik hırsızlığı ile yaşayabileceğiniz örneklerden birkaçı; kişinin adına alınacak sahte e-posta hesabı, sahte sabit ve cep telefonu numaraları, sahte hesapların açılması gibi durumlara maruz kalınabilir. Örneğin; Nisan 2011'de gerçekleşen hadise de saldırganlar Sony PSN üzerinden gerçekleştirdiği saldırıyla kullanıcıların tamamının hesap numaraları dahil her şeyini ele geçirdi. Kişilerin gördüğü zarar kadar bu durumdan Sony'de yara aldı, güvenilirliğinin sarsılmasına sebep oldu. Açılacak sahte e-posta hesabıyla yapılabilecek en basit işlemlerden biri kişinin çevresinde ki çalışma arkadaşlarına, müşterilerine, yöneticilerine gönderilecek kötü niyetli e-posta hesaplarla kişiyi zor durumda bırakmaktır. Saldırganlar internet üzerinden kişinin kimlik bilgileriyle dolandırıcılık yaparak, adına alışverişler düzenleyerek, kişi adına suç işleyerek yapılabilecek bütün işlemlerden kendine pay sağlayarak kişiyi suçlu durumuna düşürebilir. Saldırgan ayrıca kimlik hırsızlığı yaparak daha özel bilgileri elde ederek kişiye şantaj yapabilir. Ticari yazışmaları takip ederek manipüle sağlayabilir. Bu örneklerin sayısı bir hayli fazladır. Bu

gibi durumları yaşamamak için kişinin yapması gerekenler, bilgilerini sadece çok güvenli internet sitelerine kaydetmek, özellikle banka hesabının bulunduğu sitelerde şifrelerini düzenli olarak değiştirmek, güvenilirliği az olan yerlerde bütün kişisel bilgilerini paylaşmamak, e-posta hesaplarının şifresini düzenli olarak değiştirmek ve kullandığı internet ağının güvenilirliğine emin olarak hareket etmektir.

İnternet son 10 yılda bütün dünyayı ufaltarak, insanları birbirine bağlayarak, bireylerin internet üzerinden para kazanmalarını, kişilerin emeklerini sergileyebilmelerini sağlayan bir platform haline gelmiştir ve teknoloji devrinde bundan sonra daha da yaygın bir şekilde kullanılacağı bir gerçektir. Ancak şöyle de bir gerçek var ki; dolandırıcıları, hırsızları, saldırganları da son derece cezbe çekmekte ve bu kötü amaçlı insanlara para kazanmanın yollarını da açmaktadır. Bu gibi kötü amaçlar karşısında mağdur olmamak, zarar görmemek, sıkıntı yaşamamak için yapılması gerekenler bu yazıda belirtilmiştir. Bireyler, bu yolları kullanarak kendini güvenli hale getirebileceği gibi çevresini de bilinçlendirebilecektir.

Rauf DİLSİZ

Referans:

<http://www.mastercard.com/tr/personal/tr/education/kimlik-hirsizligi-nasil-olusuyor.html>

<http://www.microsoft.com/tr-tr/security/resources/phishing-what-is.aspx>

http://www.cpp.com.tr/identity_protection_types_of_identity_theft.html

<http://www.sayisaldelil.net/files/IdentityTheft.pdf>,

<http://blog.lostar.com/2011/10/kimlik-hirsizligi.html>

<http://blog.csirt.ulakbim.gov.tr/?p=45>

<http://blogs.voanews.com/turkish/bizbize/2011/07/14/amerikada-kimlik-hirsizligi/>