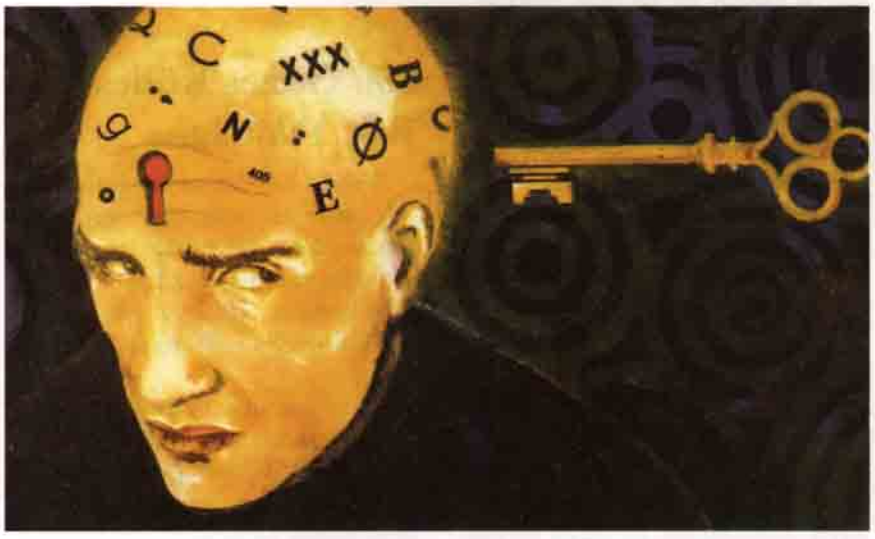
Elektronik Ticaret, Kişisellik ve Güvenlik Üzerine...

İnternet'te Gizlilik



Önce kitabevine uğradınız. İstediğiniz kitapları hemen belirleyip, tutarını ödeyip çıktınız. Bunun peşi sıra bir müzikmarkete girdiniz ve sevdiğiniz grubun uzun zamandır beklediğiniz albümünün çıkmış olduğunu görüp, hemen onu da aldınız. Daha sonra sevgilinizin doğum günü için onun en çok sevdiği çiçekleri ısmarladınız. Ardından evinizin haftalık alışverişini yaptınız ve başka bir şehirde okuyan kardeşinize harçlığını yolladınız.

BUNLARIN tümü çalışan bir insanın ancak hafta sonu gerçekleştirmeye zaman bulacağı etkinlikler; ama siz hepsini 15 dakika içerisinde hem de evinizden, hatta bilgisayarınız başından ayrılmadan yapabilirsiniz. Nasıl mı? Kredi kartı kullanıp, sanal alışveriş yaparak.

Ülkemizde de yavaş yavaş beliren sanal ticaret sayesinde yukarıda anlatılanların tümünü (hatta fazlasını) yapabilirsiniz. Bir İnternet bağlantısı, bir kredi kartı tüm bunlar için fazlasıyla yeterli. Ancak, sanal alışverişin yaygınlaşması bizi bugüne değin hiç düşünmediğimiz bir konu üzerinde zihin yormaya zorluyor: Güvenlik.

Türkiye'de bir kredi kartı sahibi, kartını kullanırken kimliğini de göstermesi istendiğinde bunu kendisini aşağılayıcı bir davranış olarak algılayabileceğinden, dükkan sahipleri (bir bakıma haklı olarak) kredi kartlarının güvenliği konusunda pek de titiz davranmıyorlar. Hatta alışverişi bitirdikten sonra, ödeme yapmak için uzattığınız banka kartının şifresini herkesin önünde söylemenizi bile isteyebilirler. Kredi kartı numaraları, şifreler, hesap numaraları, cep telefonuyla birlikte gündelik yaşamımıza giren PIN (Personal Identification Number, kişisel tanımlama numaraları) konusunda bu denli vurdumduymaz oluşumuz, İnternet kullanırken de güvenliği ön planda tutmayabileceğimiz kaygısını doğruluyor.

WWW'deki Amazon.com gibi kitap siparişinde bulunabildiğiniz sitelerde, alışverişin tutarını almaları için kredi kartı numaranızı vermelisiniz. Ancak WWW'de dolaşmak için kullandığınız yazılımlar (Netscape Navigator, Internet Explorer gibi) aracılığı ile gönderdiğiniz bilgiler, normalde salt metin biçiminde karşıdaki sunucuya iletildiğinden, kötü niyetli herhangi bir kişinin bazı teknikler kullanarak kredi kartı numaranızı ele geçirmesi mümkün. Kredi kartı numaranız da gizli bir bilgi kabul edildiğinden bunun öğrenilmesi sizin için zararlı bazı sonuçlara yol açabilir (örneğin bu kredi kartı numarasını kullanarak sizin adınıza borç yapılması gibi).

Bunu önlemek için İnternet üzerinde "güvenli" kabul edilen WWW servisleri kurulmuştur. Örneğin yine Amazon.com adresinde, sipariş ettiğiniz kitapları ve kredi kartı bilgilerinizi girdiğiniz sayfa "şifrelenmiştir". Yani kullandığınız yazılım karşı taraftaki sunucuya bilgileri salt metin olarak değil, şifrelenmiş metin olarak gönderir.

Kredi kartı işlemleri için İnternet üzerinde yaygın olarak kullanılan protokol, SET'dir (Secure Transactions Protocol, Güvenli İşlem Protokolü). MasterCard ve Visa'nın başı çektiği, Netscape ve Microsoft'un da desteklediği bir endüstri grubunca geliştirilen SET, geçtiğimiz yıl içinde kullanıma girdi. SET dışında WWW üzerin-

de yaygın olarak kullanılan bir güvenli işlem protokolü de SSL'dir (Secure Socket Layers, Güvenli Soket Katmanları). Hali hazırdaki birçok WWW sitesi bu protokolü kullanıyor.

Aslında İnternet üzerinde güvenlik (ve bunun bir parçası olan kişisellik) hiç de yeni tartışmalar değil. E-posta haberleşmesinin ve bununla birlikte doküman değiş tokuşunun kullanımından beri, iletilen bilginin yaptığı yolculuk boyunca güvenliğini sağlama önemli bir sorun olagelmiştir.

Bu sorunu aşmak için de verilerin okunamaz bir biçimde kodlanması, şifrelemenin ilk kullanımıdır. Şifreleme teknikleri, anahtar adı verilen ve bir şifreleme algoritması ile kullanıldığında veriyi özgün bir biçimde kodlayan, gizli bir veri zincirinden oluşmaktadır. Şifrelenmiş mesajı kırma, anahtar zincirinin uzunluğuna bağladır. Örneğin 8 bitlik bir anahtar kullanıldığında sadece 256 olası anahtar oluşturulabilir.

İnternet'teki en büyük sanal kitabevi: Amazon.com

8 bitlik bir anahtarı kaba kuvvet kullanarak (olası tüm durumları bilgisayarın hızından ve gücünden yararıp denemek) kırmak kısa sürecektir. Ancak, örneğin 100 bitlik bir anahtar söz konusu olduğunda, 2^{100} olasılık olduğundan, saniyede 1.000.000 (ki yaklaşık 2^{20}'ye denk gelir) anahtar deneyebilen bir bilgisayar bile doğru anahtarı bulmak için çok uzun süre çalışmak zorunda kalacaktır.

Anahtarlı şifreleme yöntemleri içinde yaygın olarak kullanılanı kamusal (public) anahtarlamadır. Burada kullanıcının biri herkese dağıttığı genel, diğerini de salt kendine sakladığı özel bir çift anahtarı vardır. Ahmet, Ayşe'ye şifrelenmiş bir doküman göndermek isterse, bunu Ayşe'nin genel anahtarıyla şifrelemelidir. Ayşe de gelen şifreli dokümanı kendi özel anahtarıyla açmalıdır.

Çift anahtarlı şifreleme için İnternet kullanıcıların en çok kullandıkları yazılım "Pretty Good Privacy"dir (PGP). Bu programın yazarı Philip Zimmermann, programı yazıp, kaynak kodunu İnternet'e koyduğunda, ulusal güvenliği tehlikeye soktuğu gerekçesiyle başı CIA ile derde girmişti. PGP'nin ABD yasalarına göre ABD dışına çıkarılması hâlâ yasal değil, ancak bir İnternet kullanıcısı ABD dışında yer alan herhangi bir PGP sitesinden bu yazılımı getirebilir. Windows 95, tüm UNIX uyumlu işletim sistemleri, Mac OS gibi popüler işletim sistemlerinin hemen hepsi için uyarlanmış durumda PGP. İnternet üzerinden arkadaşlarınıza yolladığınız kişisel e-postalar ya da dünyanın herhangi bir yerine yollayacağınız ticari bilgilerinizi şifrelemek için PGP'yi kullanabilirsiniz. Bazı yazılım firmaları PGP üzerine ürün de geliştiriyor. Örneğin Eudora posta programında PGP'yi kullanmanızı sağlayan bir eklentiyi bulmanız mümkün.

Bu arada küçük bir not: PGP'nin son sürümü 128 bitten 4096 bite kadar farklı uzunlukta anahtarlar yaratmanıza izin veriyor. Yukarıdaki hesaba göre 4096 bitlik bir anahtarın kaba kuvvet kullanarak kırılması sonlu bir zaman içinde gerçekleşebilir gibi görünmüyor (tabii, şans -daha doğrusu şansızlık- etkeni unutulmamalı). Ancak bu büyüklükte anahtar yaratmanın bir miktar işlem gücü gerektirdiği de göz ardı edilmemeli.

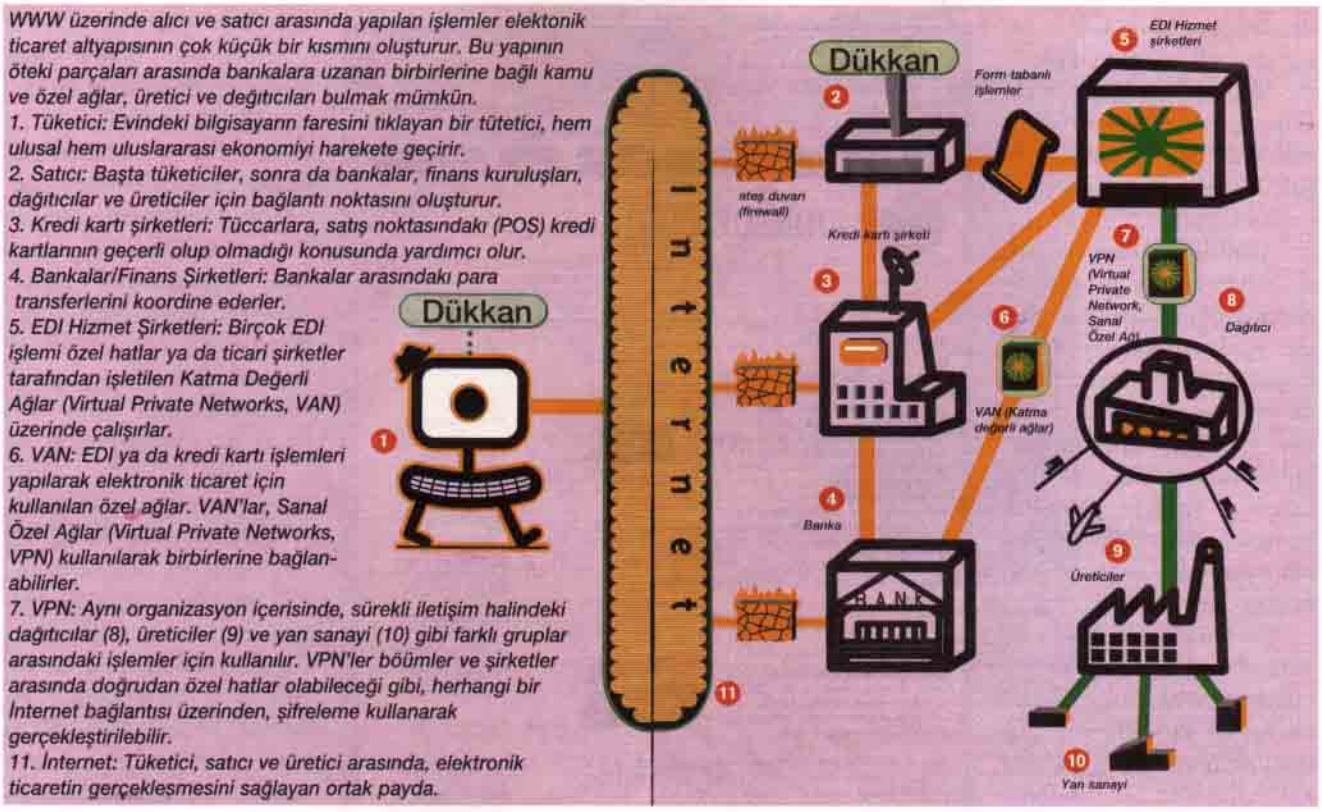
İnternet'te güvenlik deyince akla sadece kişisel e-postaların, kredi kartlarının ve dosyaların güvenliği gelmemeli. İşyerinizdeki müşteri veri tabanının tutulduğu bilgisayarın İnternet üzerinden saldırıya uğrayıp, bilgilerinizin tahrip (kim bilir belki de yok) edilmesi de mümkün.

Geçtiğimiz Şubat sonunda ABD Savunma Bakanlığı Pentagon'un bilgisayarlarına korsanlar tarafından sızılması bunun en yakın ve çarpıcı örneklerinden birisi. Bilgisayar korsanlarınca en çekici hedeflerden birisi olan Pentagon ağına daha önce de benzer saldırılarda bulunulmuştu. Bu seferki saldırıda (aslında peş peşe bir dizi saldırı demek daha doğru) personel kayıtları ve muhasebe gibi pek önemli bilgilerin bulunmadığı yerlere sızılmış. Savunma Bakanlığı sekreterliği olay hakkında pek fazla bilgi veremeyeceklerini, zira Adalet Bakanlığı ile birlikte olası suç etkinlikleri üzerinde incelemeler yaptıklarını açıklamıştı.

Bilgisayar korsanlarının Pentagon kadar favori bir başka hedefleri ise CIA (Central Intelligence Agency, Merkezî Haberalma Teşkilatı). CIA'nin İnternet üzerindeki sitesine 1996 Eylül'ünde saldıran bir grup, ana sayfadaki "Central Intelligence Agency" yazısını "Central Stupidity Agency" (Merkezî Salaklık Teşkilatı) haline çevirmişlerdi.

Hem CIA'nin, hem de Pentagon'un sitesine yapılan saldırılarda, İnternete bağlı olan ağın, önemli ve gizli bilgilerin olduğu ağdan ayrı olması sayesinde saldırganlar bu bilgilere zarar veremediler.

Bu arada Pentagon'un bilgisayar ağına saldırı düzenleyenlerin peşine düşen FBI, iki liseli genci yakaladı. İsrailli, kendine Analyzer (İnceleyici) takma adını veren bir bilgisayar korsanınca yönlendirilen bu gençler, işletim sistemlerindeki bir boşluktan



WWW üzerinde alıcı ve satıcı arasında yapılan işlemler elektonik ticaret altyapısının çok küçük bir kısmını oluşturur. Bu yapının öteki parçaları arasında bankalara uzanan birbirlerine bağlı kamu ve özel ağlar, üretici ve değitıcıları bulmak mümkün.
1. Tüketici: Evindeki bilgisayarın faresini tıklayan bir tütetici, hem ulusal hem uluslararası ekonomiyi harekete geçirir.
2. Satıcı: Başta tüketiciler, sonra da bankalar, finans kuruluşları, dağıtıcılar ve üreticiler için bağlantı noktasını oluşturur.
3. Kredi kartı şirketleri: Tüccarlara, satış noktasındaki (POS) kredi kartlarının geçerli olup olmadığı konusunda yardımcı olur.
4. Bankalar/Finans Şirketleri: Bankalar arasındaki para transferlerini koordine ederler.
5. EDI Hizmet Şirketleri: Birçok EDI işlemi özel hatlar ya da ticari şirketler tarafından işletilen Katma Değerli Ağlar (Virtual Private Networks, VAN) üzerinde çalışırlar.
6. VAN: EDI ya da kredi kartı işlemleri yapılarak elektronik ticaret için kullanılan özel ağlar. VAN'lar, Sanal Özel Ağlar (Virtual Private Networks, VPN) kullanılarak birbirlerine bağlanabilirler.
7. VPN: Aynı organizasyon içerisinde, sürekli iletişim halindeki dağıtıcılar (8), üreticiler (9) ve yan sanayi (10) gibi farklı gruplar arasındaki işlemler için kullanılır. VPN'ler böümler ve şirketler arasında doğrudan özel hatlar olabileceği gibi, herhangi bir İnternet bağlantısı üzerinden, şifreleme kullanarak gerçekleştirilebilir.
11. İnternet: Tüketici, satıcı ve üretici arasında, elektronik ticaretin gerçeklesmesini sağlayan ortak payda.

yararlanarak 200'den fazla kuruluşu kırmışlar. İnternet üzerinden yayın yapan bir derginin Analyzer'la yaptığı röportajda korsan, kırdığı sistemlere aslında yardım ettiğini; çünkü var olan açıkları sistem sorumlularına gösterdiğini söylüyor. Bu arada Analyzer'ın yandaşları, korsanların kırdıkları arşivlerden dolayı sorumlu tutulmaları durumunda misilleme yapacaklarına dair FBI'a uyarıda bulundular.

Saldırıların WWW sitenizdeki ana sayfayı tahrip etmek ya da önemli bilgilerinizi yok etme gibi doğrudan olması gerekmiyor. Bilgisayarınızın sık sık "göçmesine" yol açmak da bir başka çeşit saldırı (Bilgisayar terminolojisinde "çökmek" ya da "göçmek" bir yazılım sorunu nedeniyle bilgisayarın kullanılamaz hale gelmesini tanımlar).

Mart ayının başlarında, yine ABD'deki bilgisayar korsanlarının Microsoft firmasının Windows NT işletim sistemini kullanan bilgisayarlara saldırdıkları haberi geldi. Yalnız bu sefer sisteme sızmaya çalışma yerine, işletim sistemi yazılımının çökmesine yol açıyorlardı.

Aralarında MIT, Kaliforniya Üniversitesi ve Deniz Kuvvetleri gibi önemli kurumların bulunduğu birçok ağda bilgisayarların bir anda, birbirlerinin ardı sıra çöktükleri haberi geldi. Bilgisayarlar herhangi bir sorun olmaksızın yeniden düzgün olarak çalıştırılabildiyse de, o sırada kullanılan uygulamalardaki bilgiler yitirildi. Bu durum birçok insan için çok önemli sorunmuş gibi gelmese de, bir çökme sonrasında oluşan disk sorunları bazen giderilemeyip, diskin yeniden sıfırlanmasına bile yol açabiliyor. Yani korsanlar bilgiyi doğrudan silmeseler bile, silinmesine yol açabiliyorlar.

Korsanlar Windows NT programında, çözülemeyen bir sorunu gidermek için çok fazla bellek ayrılmasına yol açan bir hatadan faydalanmışlar. Üç gün boyunca süren bu saldırı dizisinden sonra Microsoft firması, üründeki bu soruna yol açan hatayı gideren bir yamayı (patch) İnternet üzerinden dağıtmaya başladı.

Bilgisayar ağınızda CIA ya da Pentagon'un bilgisayar ağında olduğu kadar önemli bilgiler yok diye sakın sevinmeyin. Zira birçok bilgisayar korsanı (yukarıda Analyzer'ın da söylediği gibi) bir sistemi sadece içine sızabileceğini göstermek için kırabilir. Bir tür gövde gösterisi. Özellikle İnternetteki haber gruplarında işletim sistemlerindeki boşlukları duyan birisi bunların doğru olup olmadığını görmek için bile sizin bilgisayar ağınıza sızmayı deneyebilir.

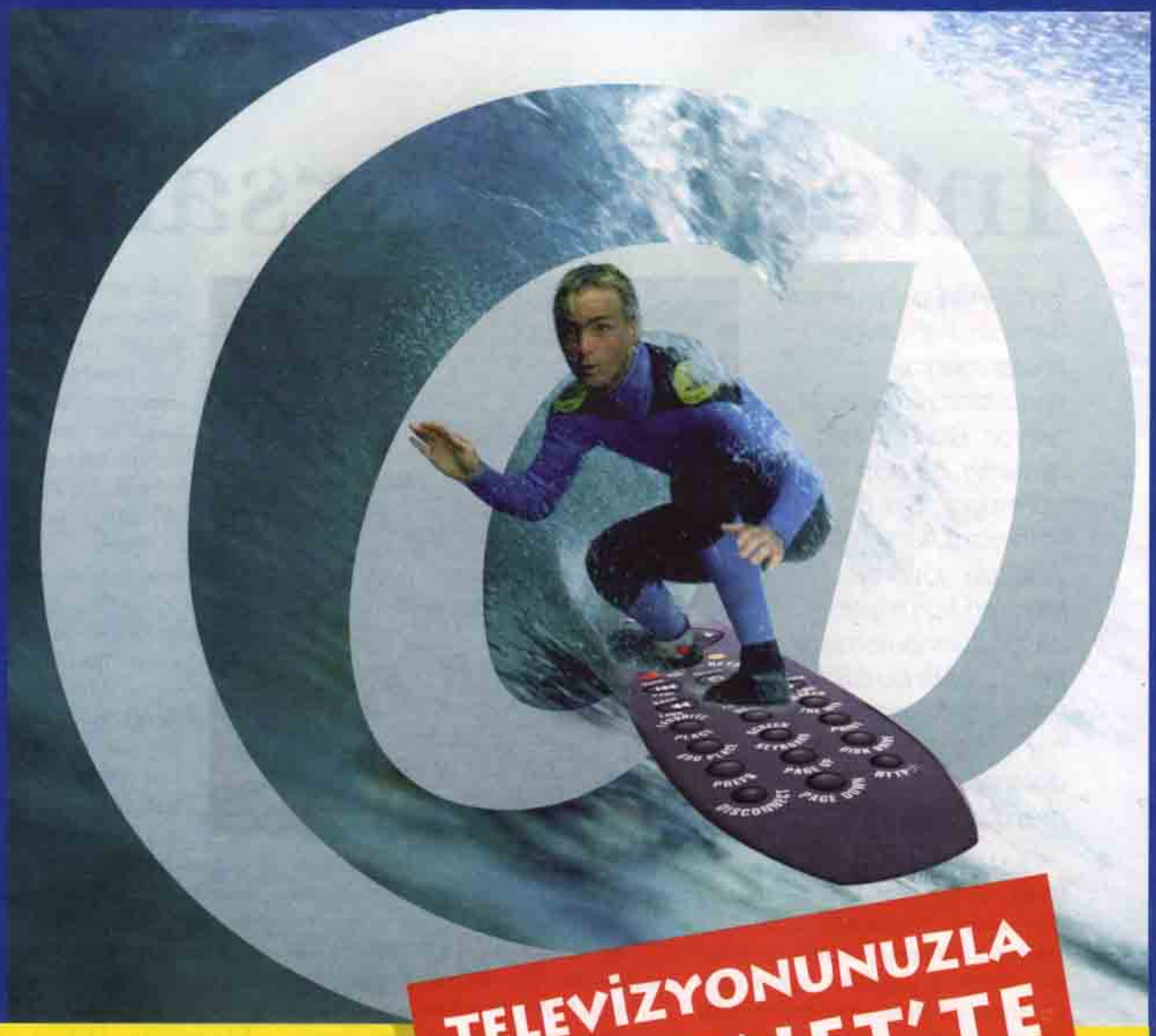
Bilgisayar ağınız olmasa bile sıradan bir İnternet kullanıcısı bilgisayar sitelerinin kırılmasından ötürü önemli sorunlar yaşayabilir. Sürekli sanal alışveriş yapıp, kredi kartı bilgilerinizi verdiğiniz bir siteye yaklaşık bir ay boyunca korsanlar tarafından sızıldığını öğrenmek hiç hoş olmayacaktır.

Amacımız felaket tellallığı yapmak değil. Sanal bankacılık, İnternet üzerinden alış veriş Türkiye'de yeni yeni gelişen sektörlerden. Ancak hem kullanıcıların, hem de bilgisayar ağı sorumlularının bu konuda duyarlı olması gereklidir. Bir İnternet kullanıcısının Netscape Navigator ya da Internet Explorer'ın verdiği "Dikkat yolladığınız bilgi güvenli olarak iletilmemektedir. Üçüncü şahıslar tarafından görülebilir." uyarısını dikkate alması yerinde olacaktır. Bu, WWW sitelerine gönderilen her bilgide paranoya yaşamalı demek değil tabii, ama kişisel bilgiler ya da kredi kartı numarası gönderileceği zaman, karşıdaki sitenin en azından SSL desteklemeyip, desteklemediğine bakılmalı.

Murat Maga

Kaynaklar
ZD Internet, Mart 1997
http://www.cnn.com/TECH/computing/9803/04/microsoft.attack/
http://www.cnn.com/TECH/9609/19/cia.hacker

TELEFUNKEN



TELEVİZYONUNUZLA İNTERNET'TE SÖRF YAPTINIZ MI?

Telefunken İnternet Gezgini'yle, artık görsel bilgi dünyasına açılabilirsiniz! Dünyanın en büyük sanal kütüphanesinden dilediğiniz eseri seçebilir, hatta elektronik postayla, yazarlarıyla sohbet bile edebilirsiniz... En büyük müzik marketlerinden, hayran olduğunuz sanatçıların albümlerini sipariş edebilir, ünlü yönetmen ve oyuncular hakkında bilgi edinebilirsiniz. Bu arada vizyona girecek olan yeni filmleri de herkesten önce öğrenebilirsiniz. Daha yapabileceğiniz o kadar çok şey var ki... Üstelik bilgisayara da ihtiyacınız yok! Telefunken İnternet Gezgini sayesinde tek ihtiyacınız olan; scart socket girişli bir televizyon ve telefon hattı... Şimdi İnternet'te sörf yapmanın tadını çıkarabilirsiniz. Aman, fazla açılmayın!

TELEFUNKEN

GÖRÜNTÜ VE SES TEKNOLOJİSİNDE UZMAN