Internet Safety Tips

Never Assume You're Safe On The 'Net
Established And Emerging Technologies Are Addressing Many Consumers' And Businesses' Security Worries

(NAPSA)—Knowingly or not, consumers often reveal personal data while shopping online, enrolling in a frequent flier program, or just visiting a Web site. Naively, many assume the information is held in confidence. Similarly, businesses large and small worry about protecting online transactions for their customers' security and safely transporting their own data.

The 'Net poses a security risk calling for technology that ensures that proprietary data is not intercepted or misused by cyber-intruders, marketers and other unauthorized parties. Here's a look at some current and percolating security technologies.

Protocol Police

Many merchants provide security by hosting their Web sites on a secure server that uses SSL (secure socket layer). These protocols, or procedures, encrypt the data being transmitted, so when you submit your credit card on an electronic form, it can't be deciphered by anyone who doesn't know the code. Encryption is the translation of data—in this case, all your private information—into a secret code. The key is simply a table used both to encrypt and then to decipher the encoded information.

SSL authenticates, or confirms, for users that a legitimate merchant runs a selected Web site. Once the site's server is authenticated, you can enter a user ID and password over an encrypted connection to that server. To know protective technology is in place, users can check the Web site's
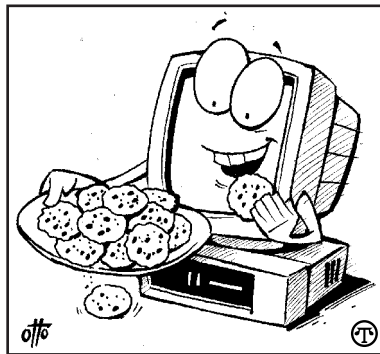
Will too many cookies spoil your appetite for Internet exchanges?

security policy. Also, a site visitor's browser often will indicate whether a transaction is occurring in a "secure session" by showing a padlock icon at the bottom of the screen.

Leaving Crumbs With "Cookies"

Even while innocently clicking around the 'Net, you could be leaving crumbs of your identity behind. Remote servers gather information about your activities using "cookies." A cookie is a piece of information shared between your browser and certain servers that lets the server know you are visiting, or when you return.

The first time you connect to a site that uses cookies, the server sends a small text file to your browser. Each time you return, your browser sends it back, tracking your visits. The information in a cookie is encoded and is generally used for harmless reasons. For example, when you go to a retail site, the shopping basket you use depends on cookies to remember who you are and what

you've placed in your basket. However, cookies can provide marketers a valuable record of your Web site preferences.

In defense, you can set your browser to alert you when a server attempts to send a cookie. You can opt not to accept it, though you may not be able to access certain sites without accepting the cookie. To check for cookie files, and remove them from the hard drive, Netscape Navigator users can access a file called cookie.txt and Microsoft® Explorer users can look in the directory called c:\windows\cookies.

Sniffing Out Sites With P3P

What if you could surf the Web with your privacy assured? With the Platform for Privacy Preferences (P3P), users can know if and how a Web site might gather and use personal information without reading the site's lengthy privacy policy. The P3P software, once installed on a user's browser, automatically checks all Web sites a user visits for a P3P-compliant privacy policy. If the site has such a policy, the browser can automatically compare it with the user's preferences. Ultimately, P3P will help consumers make informed decisions about their interactions with Web sites.

Scaling The Wall

Businesses can prevent outsiders from accessing private data resources and control what outside resources its employees can access with a "firewall." That's a combination of computer hardware and software that separates a LAN (local area network) into two or more parts for security purposes.