CancerLynx.com

We Prowl the Net

Security basics:

Beating hackers, pirates and thieves

Alexandra Andrews and Neil Dunlop

Internet pirates are looting bank accounts, stealing medical research and business secrets and taking over computers for malicious uses. There's no shortage of ways for these thieves to get your company's and your personal sensitive information. Luckily, there are a few ways to thwart these evil-doers, and we'll offer a few in this article.

First, let's look at some ways that information is stolen.

There are many true stories of organizations -- banks, government agencies, universities, hospitals, etc. -- giving laptops loaded with confidential information to contract consultants. Then, the consultant says that the laptop has been lost or stolen. Poof! There goes that confidential data.

Also, it is no secret that there is a high failure rate in websites. Very often, when a site goes belly up, the only thing of value is the database of users. The creditors try to sell that database to the highest bidder. Many sites that sell the personal data of their users have fancy seals of approval and such, but, very often, all that they mean is that someone paid extra to be able to put the seals there -- nice little decorations. Toto, pay no attention to that man behind the curtain.

So, there are many ways in which you and your company are vulnerable to Internet pirates. These unscrupulous folk use phishing, malware and spyware for hostile takeovers of computers, businesses, and identity theft.

Phishing or spoofed e-mails and/or websites pretend to be banks, credit card companies or your very best friend/lover; designed to fool you into divulging your personal financial data.

Spyware lurks in the background of computers to secretly gather information and relay it to advertisers or whoever is buying. Download a freeware version of Spybot Search and Destroy from www.safer-networking.org

Malware is malicious software designed specifically to damage or disrupt a computer system, such as viruses, worms or Trojan horses.

Cookies Many sites offer cookies because they want to be able to recognize you when you return. But there are the sneaks who hide the cookies by using code such as white on white HTML as your mouse travels over the page - a cookie or spyware program is set.

First, dump MS Internet Explorer

Stop using Microsoft Internet Explorer because it is loaded with security problems. That's the advice given by the U.S. Computer Emergency Readiness Team (USCERT), a computer security partnership between the U.S. Government's Department of Homeland Security, the public sector and private sector. Move to another browser, USCERT suggests. Can you take a hint?

If you are on a PC and using Windows Explorer or LookOut (aka Outlook) Express, you are in grave danger. Download other browsers and email clients such as Mozilla Firefox or Thunderbird from Mozilla.org, Netscape from Netscape.com, Opera from Opera.com, Eudora from eudora.com or Slim Browser from Flashpeak.com.

When setting up your browser, read the preferences section, and do not allow pop ups plus consider not allowing graphics. Much of the evil Malware uses graphics to enter your computer system. Browsers like Opera will alert you to a site trying to set an illegal cookie, sending you to a false domain or using a forged security certificate. Opera offers the option of *Delete private data.* This removes your browsing history, clears your cache, deletes cookies, clears email passwords and more. Always use this or a similar option before shutting your machine down.