How to Avoid Becoming a Victim

H. Thomas Milhorn, MD, PhD

Universal Publishers
Boca Raton, Florida

Cybercrime:
How to Avoid Becoming a Victim

Universal Publishers
Boca Raton, Florida
USA • 2007

ISBN: 1-58112-954-8
13-ISBN: 978-1-58112-954-0

www.universal-publishers.com

Preface

Computers and the Internet can be used almost anywhere. Desktop computers are found in homes, schools, libraries, businesses, and cybercafés. The advent of wireless Internet connection has allowed the use of computers in places not envisioned a few years ago—on a train, on a bus, in a restaurant, or even on a busy street corner. In addition, you can plug your laptop into an outlet in many hotel rooms for a traditional, hardwired Internet connection. And more and more people, including the elderly, are taking the necessary steps to learn how to use computers and the Internet.

In teaching basic computer courses for adults, the most frequent question I get asked is "Is using the Internet safe?" The answer is, "well yes and no." Americans lost more than $336 million to online fraud in 2005, and that doesn't count all the headaches, lost hours spent trying to restore their computers to normal functioning states after they were disrupted by viruses and other intrusive programs, or the money paid to computer experts to fix the problems. In addition, dealing with viruses, spyware, computer theft, and other computer-related crimes cost U.S. businesses $67.2 billion a year, according to the FBI. And the criminals are still out are there just waiting to plant a virus that crashes your whole system, install spyware that keeps track of everything you do on the Internet, defraud you out of money, or steal your personal information, including passwords, Social Security number, bank account number, and credit card number. However, there is good news. There are steps you can take to protect yourself and your computer, and they are spelled out in this book.

My interest in cybercrime began after personally experiencing a modem hijacker (dialer program) and having my browser hijacked by an unethical anti-spyware company, not to mention a multitude of viruses. I've also had bogus charges added to my

credit card following online purchases. All this made me very conscious of the need for knowledge of cybercrime and computer security. “Cybercrime: How to Avoid Becoming a Victim” is my attempt to share with fellow computer users what I learned from experience and research on the topic.

I have laid out each chapter in a format consisting of a discussion of the basics of the crime, followed by real-life examples of the particular crime, and then things you can do to avoid becoming a victim of the crime. In addition to the chapters on individual cybercrimes, I have included a chapter on the role of organized crime in Internet fraud and a chapter on Internet hoaxes. Although hoaxes are not crimes as such, some can lead you to damage your own computer if you follow their instructions, and they are a nuisance. In addition, I have included an appendix on where to report various cybercrimes and another appendix on cybercrime terminology.

Being a firm believer that people learn from example, I have used over 200 case reports to illustrate specific crimes. I have no personal knowledge of any of these. They are all taken from various sources, both online and the print media.

I would like to thank Phyllis Millett for proofreading the manuscript and making a number of valuable suggestions.

Tom Milhorn

Meridian, Mississippi

Contents

Chapter 1

Introduction

Computers and the Internet offer great benefits to society. The Internet provides instant access to news, banking, auctions, shopping, reference information, stock trading, travel information, and much more. Chat rooms, emails, and instant messaging have become common methods of communication. Unfortunately, criminals also use the Internet, giving rise to the term *cybercrime*, which refers to any type of activity that uses the Internet to commit a crime. A *cybercriminal*, or *cybercrook*, is defined as a person who uses a computer and the Internet to commit a crime.

The fact is, the more you know about cybercrime the better able you will be to protect yourself and your computer from those out there who wish to do you harm.[1,2]

CATEGORIES OF CYBERCRIME

Cybercrime has been categorized a number of ways. The two presented here depend on (1) the target of the crime and (2) whether the crime occurs as a single event or as a series of events.

Target of the Crime

The target of cybercrime can be (1) persons, (2) property, or (3)

organizations.

Persons

When an individual or group is the target of cybercrime, the computer is said to be the tool of the crime. The goal is to exploit human weaknesses, such as greed and naivety. These crimes, including financial crimes, sale of stolen or nonexistent items, child pornography, copyright violation, harassment, and stalking, have existed for centuries. Criminals have simply been given a new tool which increases their potential pool of victims. It also makes it harder to trace and apprehend the criminals.[3,4]

Property

Crimes against property include stealing a laptop; transmitting harmful programs that disrupt the function of a computer, wipes out the hard drive, or spies on the computer's user; and hijacking a computer, a browser, or a modem.[4]

Organizations

Organizations include governments and companies. Cyberterrorism is one distinct kind of crime against government. In this type of crime the Internet is used by individuals and groups to terrorize the citizens of a country or to threaten international governments. The latter form includes breaking into military computers and stealing secret information. More recently, the definition of cyberterrorism has been extended to include attacks against computers and networks of nongovernmental natures. Various companies, including Internet service providers, are often the target of cybercrimes, such as hacking into a computer network to steal information, damage programs or files, or plant programs that allow control of the network.[4]

Single or Series of Events

Single Event Cybercrime

Single event cybercrime is a single event from the perspective of

the victim. For example, you unknowingly open an email attachment that contains a virus that infects your computer. Or you might receive an email containing what appears to be a link to well-known company, but in reality is a link to a criminal website whose goal is to still your credit card number. Other examples of this type of cybercrime include hacking, spyware, and fraud.[2]

Series of Events Cybercrime

Series of events cybercrime involves repeated interactions with the target. For example, an adolescent is contacted in a chat room by someone who, over time, establishes a relationship. Eventually, the criminal exploits the relationship to commit sexual asault.[2]

In this book I simply present the various types of cybercrime in alphabetical order to make it easy for you, the reader, to find information about individual crimes.

STEPS TO PROTECT YOURSELF

Attacks against home computer users generally fall into two classes—fraud and crimeware, although other crimes, such as stalking, harassment, prostitution solicitation, and child pornography, do occur and are discussed later in this book.

Fraud is a deception deliberately practiced to secure unfair or unlawful gain, usually monetary in nature. Internet fraud includes auction fraud, identity theft, work at home scams, investment scams, and many others. An online fraud is known as a *dotcon,* which is a take off on *.com*. *Crimeware* is defined as software designed to steal personal information or perform some other illegal operation. It is malicious software that allows a crime to be committed.

Two special forms of crimeware are warez and malware. *Warez* refers to pirated software distributed over the Internet. *Malware* is a contraction of *mal*icious soft*ware*. It consists of browser hijackers, dialer programs, viruses, worms, Trojans, and spyware, all of which are designed by people who wish to do you or your computer harm.[5,6] Dialers and browser hijackers are discussed in Chapter 12, and viruses, worms, Trojans, and spyware are discussed in Chapter 35.

As we move from dial-up Internet connections (connected to

the Internet only when you connect them to the Internet) to high-speed connections (always connected to the Internet when the computer is on) the risk of becoming a target of cybercrime increases considerably. So, if you have a high-speed Internet connection and leave your computer on for long periods of time when you're not using it, it's a good idea to disconnect it from the Internet.

In addition, there are six basic steps you can take to reduce the risk of becoming a victim of cybercrime. You should (1) create a virtual shield, (2) beware of impersonators (3) avoid taking the bait dangled by cybercrooks, (4) stay away from high-risk websites, (5) download with caution, and (6) keep an eye on your children. In addition, if you have a wireless home network, use computers made available in public places, or travel with a laptop there are some additional steps to take.

Create a Virtual Shield

Online criminals look for easy targets. To thwart them by creating computer security in the form of a virtual shield you should (1) have a firewall, (2) have antivirus software, (3) have anti-spyware software, (4) choose strong passwords, and (5) update your operating system periodically.

Firewall

A *firewall* serves as a digital barrier that shields your computer from the outside world and monitors all out-going and in-coming programs that connect it to the Internet. A firewall's primary purpose is to alert you to unsolicited connection attempts and to block them.[7,8]

Every program on your computer uses ports to connect to other computers on the Internet. Ports are access ways through which information enters and leaves your computer. There are thousands of ports in use today, numbered from 1 to 65,535. They are logical accesses, not physical or hardware ones. Some applications use specific ports. For instance all regular HTTP (web traffic) uses ports 80 and 1080, and all HTTPS (encrypted web traffic) uses port 443. File sharing and instant messaging systems use a variety of ports. Many of these programs use whatever ports

are available at the time. Because applications use ports to access computers, one job of a firewall is to monitor the ports that are allowed to communicate with your computer.[5]

If you use a modem (dial-up connection), you are at a much lower risk from Internet attackers, since most hackers don't want to waste their time hacking into computers with slow Internet connections and which are rarely connected to the Internet. However, just because you aren't the most desirable target, doesn't mean you shouldn't run a firewall program.

For high-speed DSL, Cable, and Satellite Internet users, a firewall is essential. You are a primary target for Internet hackers for two reasons. First, hackers are interested in high speed transmission to get their fraudulent schemes out to as many people as possible in a short period of time. Second, many people with high-speed Internet connections leave their computers on for hours, days, or even all the time. With a dial-up Internet connection your Internet service provider assigns your computer a new IP (Internet Protocol) address each time you access the Internet. However, with high-speed Internet connections the IP address stays with your computer until you power down or log off. Leaving your computer on for long periods of time makes it easier for cybercrooks to obtain your computer's IP address and then come back at a later time to do their dirty work. Thus, although it might be convenient to have a ready Internet access, it does increase the risk.

Modern operating systems, like Windows XP and Mac OS X, have built-in firewalls, but you have to make sure they are turned on. Commercial firewalls are also available, including Norton Personal Firewall (www.symantec.com), McAfee Firewall (www.mcafee.com), and PC-cillin firewall (www.trendmicro.com). These and others can be purchased for a reasonable price and updated annually for a smaller fee.[7,8]

Antivirus Software

An *antivirus program* is software designed to detect and delete computer viruses, worms, Trojans, and other malicious software from your computer's email, memory (RAM), and hard drive. Such unwanted intruders can slow your computer down, make it difficult to open programs, such as Microsoft Word or Norton

SystemWorks, and even shut your computer down by crashing your hard drive and deleting everything that is stored there.

You should configure your antivirus program to automatically scan incoming and outgoing email for viruses. Most antivirus programs come with a real-time scanner that checks your files each time you open them. And most antivirus programs can be set to run scans at predetermined intervals. Even so, you should probably do a manual scan at least once a week.[7,8,9]

Unfortunately, antivirus software can't protect you from viruses it doesn't know about. New viruses and other forms of malware get a free pass until the antivirus companies can analyze them, create software to get rid of them, test the software, and distribute it. This usually only takes three or four hours after the outbreak of the virus.[5]

Most new computers come with an antivirus programs installed, but it is up to you to update it annually. Since new virus programs are written and released on a daily basis be sure you have your antivirus program set to automatically update itself. The first year of updates is usually free. Many Internet service providers provide free antivirus programs, but some of them you have to download and install.

Never open emails from someone you don't know or a company you have not agreed to receive emails from. But if you should open these emails, don't open any attachment that comes with them or click on any hyperlinks within the body of the email as these are common sources of viruses. It's best simply to delete the emails unopened.

Examples of antivirus programs include Norton Antivirus (www.symantec.com), McAfee Antivirus (www.mcafee.com), and PC-cillin Antivirus (www.trendmicro.com).[7,8,9]

Anti-spyware Software

Anti-spyware programs offer protection from malicious software codes that track your online activities and may capture everything you type, including passwords, credit card numbers, and bank account numbers. Anti-spyware programs can be purchased commercially, and like antiviral programs they need to be updated automatically.[8]

Commercially available anti-spyware programs include Ad-aware SE Personal (www.lavasoft.com) and Stopzilla (www.stopzilla.com). Also, there are some good freeware/shareware programs available on the Internet, such as Spybot-S&D (www.safer-networking.org). Microsoft has a free beta anti-spyware program called Windows Defender (www.microsoft.com).

A word or two of warning—there are a number of commercial anti-spyware websites on the Internet that offer a free spyware scan. Only after the scan is completed do you find out that you have to buy the software to get rid of the spyware they find. Not only that, but many of them grossly over report the amount of spyware they "find" in an attempt to induce you to purchase their product.

Spyware is often installed as a component of freeware programs, so be careful when downloading anything from the Internet that is said to be free.[8,9]

Strong Passwords

Hackers may try to figure out your passwords to gain access to your computer, your bank account, or your credit card company. You can make it tougher for them by doing the following:

Number of Characters. Use passwords that have six or more characters and include numbers and uppercase and lowercase letters. You can make your passwords even more secure by including symbols.

Common Words. Avoid common words, such as apple or crankshaft. Some hackers use programs that can try every word in the dictionary.

Personal Information. Don't use personal information, such as your name or city, as a password.

Change Passwords. Consider changing your passwords regularly—at a minimum every 90 days.

Different Passwords. Use different passwords for every online account you access. For instance, don't use the same password for your Internet service provider, your bank, your credit card company, and your financial investments. That makes it too easy for cybercriminals.[10]

Update Your Operating System Regularly

Microsoft and Apple, on a regular basis, come out with security fixes for their operating systems to help you stave off cybercriminals. It is extremely important that you download these fixes as they are released. If you have your operating system set to download the fixes automatically then you can put this out of your mind. If not, you will have to access the Microsoft or Apple website and do it manually.[9,10]

Other Measures

Other steps you may wish to take include using (1) an alternative operating system or browser, (2) a popup blocker, and (3) a spam filter.

Operating System and Browser. Some experts suggest that you go as far as using an operating system other than Windows, but I find that a bit extreme, provided you take the necessary precautions. Because 90 percent of the computers in the world use the Windows operating system it is only natural that it should be the primary target of cybercrooks. Other less-popular operating systems, such as Mac OS X and Linux, are much less often attacked. Similarly, Internet Explorer, being the most popular browser in the world, is more often attacked than other browsers. Switching to an alternate browser, such as Firefox (www.mozilla.org) or Opera (www.opera.com), will decrease the number of attacks, at least until these browsers become more popular.[6]

Popup Blocker. Many websites generate popup ads as you visit the site. The popup may appear in front of the webpage or under it so that it shows up only after you close the webpage. These ads are potentially dangerous because spyware, among other methods, uses popup windows as a way of tricking you into installing their programs on your computer.

The current Windows operating system comes with a built-in popup blocker that is enabled by default. If you are using an operating system that doesn't have a popup blocker you can download free tools that do this. For instance, Yahoo (www.yahoo.com) and Google (www.google.com) offer browser toolbars that can block popups.[6]

Spam Filter. Unsolicited commercial email is known as *Spam*. It is junk email messages from people you don't know. It has one purpose—to generate income for the senders or the people they represent. Marketers are increasingly using email messages to pitch their products and services, and cybercrooks bombard your inbox with fraudulent offers and attempt to steal your credit card or bank account number.

Approximately 30 million emails are sent across the Internet each day, and it is conservatively estimated that 50 percent of these are spam, although the actual percentage is probably much higher. Internet service providers, such as AOL, Comcast, and MSN, ensure that you get a fairly clean mail stream; however, they tend to err on the side of letting spam in to avoid blocking legitimate email.[5]

Some computer users find spam annoying and time consuming; others have lost money to bogus offers that arrived in emails. A spam filter is helpful in preventing many of these from reaching your in-box. There are a number of spam filters on the market, such as Spam Killer (www.mcafee.com) and Spam Buster (www.spambuster.com).

Symantec (www.symantec.com) offers a free security check that scans your computer for a variety of vulnerabilities, including ports that may respond to unsolicited requests, the presence of Trojan horses, and whether you have an antivirus program or if your antivirus program is active.[6]

Beware of Impersonators

One of the most common cybercriminal tricks is to get you to click on a link that you think will take you to a desired site (eBay, a video store, a bank, a gaming site, and so forth) but instead connects you to a "spoof" site that appears identical, or similar to, the site you wished to go to. When you type in your user name and password to enter the site or give personal information, such as your credit card number, the criminal steals the information and then can use it to purchase items in your name. So, never click on a link in an unsolicited email, even if it seems to be from your bank, your credit card company, eBay, or another familiar source. Simply delete the email. Legitimate companies don't request personal information via email.[8,10]

Don't take the Bait

It's amazing what greed will cause some people to do. If you receive an email telling you that you have won a contest you didn't enter or a Nigerian banker telling you he wants to transfer a large sum of money to your bank account and is willing to share it with you, don't take the bait. The next encounter will involve a request for an advance fee before you "get" that much larger sum of money. Simply laugh at the email because of its poor grammar, misspelled words, and unusual punctuation and then delete it. And when you get popups telling you that you've won a laptop or a sum of money, or anything else, do the same. Trust me, you haven't won anything. They just want your email address so they can start sending you spam.[8]

There are a number of ways to spot an Internet scam, including the following:

Advance Fee. Beware of great sounding offers in which the details of the offer are kept hidden until you pay a fee. Any offer that requests money upfront most likely is a scam.

Capital Letters and Excessive Punctuation. Be skeptical of ads that shout at you, like "MIRACLE CURE!!!" or "Make BIG $$$$$ MONEY in HOURS A WEEK!!!!!"[11]

Credit Card Number. Don't give your credit card number to anyone when it is requested by email or by website that is linked to an email. Don't give it to what appears to be your bank, the IRS, eBay, or anyone. Legitimate companies don't request this type of information via an email.[11]

Hidden Name or Address. Don't conduct business with someone unless the person reveals his or her name, address, and phone number. Beware of users who try to buy or sell things using an anonymous email address or a post office box.[11]

Money Back. Remember, a "money-back-guarantee" from a stranger may be worthless. By the time you decide you want your money back the website may have disappeared or the "company" may simply refuse to answer your emails or phone calls.[11]

Not a Scam. Scammers say "This is not a scam" all the time. Don't fall for this trick. A legitimate business doesn't spend time trying to convince you of its honesty.[11]

Password. Never reveal your password to anyone online, unless you are required to do so to enter legitimate sites, such as

your bank or credit card company. And if someone asks you to change your password to a specific "word" for the purpose of "system testing," be immediately suspicious; this is a well-known trick.[11]

Pyramid. If you are asked to send money to five people, who each send money to five more people, who each send money to five more people, and so on, then you are looking at an illegal pyramid scheme or chain letter. Avoid it. Not only will you lose money, but it is illegal.[11]

References. The ad might state "As appeared in such and such magazine or newspaper." The credentials sound impressive, but you aren't given enough information to look them up.[11]

Secret Method. Beware of ads that say such things as "secret available only to a limited number of people." If it were a secret they wouldn't be advertising it.[11]

Talk about Money. There's too much talk about money and not enough about the deal. Scammers try to blind you with dreams of becoming rich so you won't notice the fine print. Watch out for bogus promises of wealth.[11]

Too Much Knowledge. Beware of emails that know details about you that you have not revealed. Also, if someone you don't know starts asking very personal questions about you, be very suspicious.[11]

Unsolicited Email. If you get an email from a stranger offering to give or sell you something or that leads to a website requesting personal information, treat it with great suspicion. It's best simply to delete it.[11]

Avoid High-risk Websites

Some websites put you at higher risk for getting your computer infected with a virus or spyware than others. Pornography and gaming sites are notorious for this. So the best advice is to avoid them like the plague. Some major Internet companies, including Google, are taking steps to warn computer users if they are about to visit a webpage that could harm their computer. A warning pops up if users click on a link to a page known to host spyware or other malicious programs.[12]

Download with Caution

Be wary of downloading free programs or files over the Internet. Things are seldom completely free. These files or programs may contain spyware, viruses, or other malicious software. Also be wary of floppy, CD, or DVD discs received in the mail if you don't know the sender personally. Buying products online from reputable retailers all but eliminates the threat of an attack in this manner.[13]

Keep an Eye on Your Children

The younger members of your family, if you have children at home, are the most likely to respond to bogus email requests, visit high-risk websites, and use file-sharing programs to download music or other material from the Internet. Music, movie, and software companies take copyright violations very serious. You may find yourself the target of a lawsuit because one of your children downloaded a movie, a song, or a game program.

The following are some guidelines that may keep your children, and you, out of trouble.

Chat Rooms. Be cautious of online chat rooms. Younger children shouldn't be allowed to use them, and the older ones should be allowed to use them only under your supervision. Explain to them that they shouldn't believe everything they are told. A person saying that he is a teenaged girl might actually be an adult male with ulterior motives.[9,15,16]

Comfort. Teach your children to come to you if anything they run across makes them feel uncomfortable, such as inappropriate questions in a chat room, an invitation to a private chat room, or an offensive email.[9,15,16]

Common Area. Put computers in a common area so you can monitor your children's time online. Discuss and set rules with your children for computer use. Post these rules by the computer as a reminder.[9,15,16]

Email and Instant Messaging. When your children are young they should share the family email address rather than have their own. As they get older you can set up separate email addresses, but your children's email should still reside in your account. Tell your children never to respond to emails or instant messaging from

strangers.[9,15,16]

Face-to-face Encounters. Never allow your children to meet someone face-to-face that they've "met" online. This is an invitation to disaster. Early on, explain to them that they might get such an invitation, that it is dangerous, and that such a meeting won't be allowed.[9,15,16]

Filtering. Although far from perfect, browsers and search engines, such as Google and Yahoo, can be set to filter some content. In addition, some Internet service providers, such as AOL and EarthLink, provide parental filtering software. There are a number of commercial parental filtering programs available, including Cyber Patrol (www.cyberpatrol.com), CYBERsitter (www.solidoak.com), and Net Nanny (www.netnanny.com). For your younger children you might want to consider using a children's browser, which has some built in safety factors. There are a number of these available, including Garfield's (www.garfieldisland.com) and Junior Net's (www.juniornet.com).[9,15,16]

Limit Online Time. Limit your children's online time as you would television viewing.[9,15,16]

Personal Information. Teach your children not to give out personal information online, such as phone number, address, last name, name of school, passwords, or credit card information (assuming your older children have their own credit cards).[9,15,16]

Signs. Watch for signs that your child may have been approached by a sexual predator online.[6] These are discussed in Chapter 29.

Webcam. If you have decided to let your children have computers in their bedrooms, whatever else you do don't let them have a webcam as well. That is just begging for trouble.[9,15,16]

ADDITIONAL STEPS

If you have a wireless network, are in the habit of using computers made available in public places, or travel with your laptop, there are some additional steps you should consider.

Wireless Networks

Many households have more than one computer. Quite often these