TechRepublic

10 technologies that cybercriminals love to exploit

Version 1.0
July 10, 2008

By Debra Littlejohn Shinder, MCSE, MVP

New technologies make it easier for all of us to get our work done online, communicate with others, and take advantage of all the Internet-based entertainment that's available today. But many of those same technologies have also made it easier for cybercriminals—the bad guys who use the 'Net for illegal purposes—to do their dirty deeds. We're talking about hackers, attackers, spammers, scammers, phishers, and other criminal types.

In this article, we'll take a look at the top 10 online technologies that they love to exploit and see how you can protect yourself, both at home and at your business, when using those technologies.

1 Broadband connectivity

Broadband has come to most of the United States, with almost 73 million subscribers as of the end of 2007. That's more than 50% of U.S. households and more than 70% of all home Internet subscribers. Experts predict that by 2012, more than 70% of households will have broadband access.

Broadband has many advantages for users, including high speed at relatively low cost and the "always-on" nature that eliminates the need to log onto the ISP each time you want to access Internet resources. But those same characteristics also make it the perfect technology for exploitation by hackers and attackers. Having your computer connected to the 'Net 24/7 means the cybercriminals have a much wider window of opportunity to gain access and steal your data, crash your computer, or otherwise do you harm. And the high speed of new access technologies (for example, Verizon now offers 50Mbps plans and predicts speeds up to 100Mbps or more in the near future) means a "drive-by download" can put even a large malicious file on your machine in just seconds.

2 Wi-fi networking

Another technology that has become incredibly popular is wi-fi, or 802.11 wireless networking. With increasing frequency, both home and business networks are connected by wireless technologies instead of Ethernet cables, and wi-fi hotspots proliferate in public places such as coffee shops, airports, hotels, and city parks. Wi-fi offers maximum convenience because you can move around and stay connected, but it also makes it more convenient for a criminal to get onto your network and into your system without your even knowing, since anyone with a wireless-enabled laptop within range can intercept the signals.

Unlike their older counterparts, new wireless access devices use encryption by default—but you need to check and ensure that yours uses the more secure encryption, such as WPA/WPA2/802.11i rather than WEP, which is easy to crack. You should also use strong encryption for the applications you run over a wireless network (for example, SSH and TLS/HTTPS). You can use a VPN (virtual private network) or IPsec to encrypt traffic traveling over a wireless LAN, and you should create a separate network segment for your wireless communications if you also have a wired LAN. For more information about wi-fi security, see http://www.wardrive.net/.

3 Removable media

Floppy drives have been almost entirely replaced by CD/DVD readers/writers, flash card readers, and USB drives, but whatever the form, cybercriminals love removable media. If they can get physical access to a computer, they can quickly and easily copy files and remove them, often with no one the wiser. Removable media also pose a security risk because it's easy to lose discs, thumb drives, flash cards, and the like.

You can use Group Policy in Vista or edit the registry in XP to disable use of USB devices. You can also get third-party software that will block the use of any I/O devices through USB and IEEE1394 ports or using BlueTooth wireless connections. For example, see http://www.lumension.com/usb_security.jsp

If you're concerned about removable drives or cards being lost or stolen and the data on them accessed, you can encrypt the data on flash cards, CDs, and DVDs so that you can still work with them on different computers but a thief can't. For example, see http://www.dekart.com/howto/howto_disk_encryption/encrypt_flash_drive_cd_dvd/.

4 The Web

The Web is hardly a "new" technology now, but it's still a favorite of cybercriminals because almost everyone who connects to the Internet uses a Web browser. Back when the Web was text-based, browsing was a pretty safe activity, but today's Web pages are expected to do much more, and many of them run programs—such as Javascripts and Active-X controls—to give users a much richer multimedia experience. The problem is that attackers can use these browser capabilities to run their own malicious programs on your computer.

Don't be fooled into thinking that because you use a particular browser, you're safe. All popular browsers have vulnerabilities and can be exploited. More important is the browser's settings. If you disable Javascript and Active-X for most sites, you'll make it more difficult for attackers to get to your computer through your browser (but you may also not be able to properly view some sites). It's also important to install security updates for your browser as they're released.

5 E-mail and instant messaging

E-mail is becoming ubiquitous. Almost everybody has one or more e-mail addresses, and it's one of the most convenient ways to communicate. It has almost the same immediacy as a phone call or instant message without the pressure to answer in real time unless you want to.

Unfortunately, e-mail also has some characteristics that make it attractive to criminals. They can send mail with spoofed return addresses so that it's difficult or impossible to discover the true origin of the messages. Thus, they can get away with sending spam, phishing messages, threats, child pornography, and other types of illegal correspondence. Instant messaging programs can also present a threat. As with e-mail, IMers can pretend to be someone else, and most IM programs now support file transfer, which provides a way for criminals to download malicious software to your machine.

Technologies to authenticate the identity of e-mail senders, such as Microsoft's Sender ID and the more generic SPF, can solve the spoofing problem—but only if all e-mail domain owners use them. Meanwhile, you can protect yourself with spam filtering software that allows you to create a whitelist or safe senders list and by following best practices such as not clicking on hyperlinks in e-mail, viewing your mail in text format only (no HTML mail), and not engaging in IM conversations or file exchange with people you don't know.

6 Unified communications

Unified communications (UC) is a popular trend in the enterprise space, and companies are finding many advantages in combining their e-mail, telephony, IM, and conferencing applications so that these programs can interact with each other. With voice over IP (VoIP) slowly replacing traditional telephone services, all these communications technologies can be run over the same network.

However, this also means that now your phone calls are subject to some of the same threats to which your data has always been vulnerable: VoIP packets can be intercepted or even modified in transit just as other data traffic can. For more about UC security threats, see http://blogs.techrepublic.com.com/security/?p=406.

To protect yourself in a unified world, use encryption to keep important data confidential—whether it's text, voice, or other. Also make sure UC software is updated regularly (along with the underlying operating system) and use authentication to verify the origin of messages and to ensure that messages haven't been tampered with.

7 Peer-to-Peer (P2P) programs

The most popular means of exchanging large files quickly across the Internet is through the use of P2P software and networks, such as BitTorrent, KaZaA, Gnutella, and Napster. People use them to share music and movies in violation of copyright laws, but also for legitimate purposes, such as distributing their own home movies and pictures. The number of songs swapped via P2P networks is estimated to be in the billions per year.

Criminals love P2P networks because they can mislabel the files they share and cause you to download malware (such as a program that allows the criminal to take over your computer) when you think you're downloading a song. Most of these networks also strive to protect the anonymity of users, so the bad guys have little risk of being caught. The best way to protect yourself from the dangers of using P2P applications is not to use them at all.

8 E-commerce and online banking

More and more of us are conducting more and more of our business over the Internet. It’s convenient to buy what we need from home and have it delivered to our doorsteps and to pay our bills and transfer money between our accounts without a trip to the bank. Criminals love this trend, because it gives them additional opportunities to get hold of your money. They can intercept information as it travels across the network, break into the databases of online businesses or financial institutions to steal information, or set up their own fake e-commerce sites and lure you into giving them your credit card number and other information under the pretense of selling you something.

To protect yourself when buying or banking online, do business only with well-known sites and ensure that your Web traffic is encrypted (your browser will indicate when a site is secure). Navigate to those sites directly. (Don’t click a link in e-mail to get there.) Don’t save your credit card information on the Web sites, either—type it in each time. Keep a close watch on your credit card statements and bank statements and immediately report any suspicious or unauthorized activity.

9 Mobile computing

Computing has become increasingly mobile and devices ranging from small PDA phones to full-size laptops are being used to store important data and connect to home and company networks. Because of their mobility, however, these devices can easily be lost or stolen—and the data goes with them. If the device contains your personal information, you could be subject to identity theft. If it contains client information for your company, you could put those clients at risk and possibly put your company in violation of regulatory compliance requirements. Luckily, there are a number of ways to protect yourself from these threats.

Many portable computers today come with built in TPMs (Trusted Platform Modules), which are hardware-based cryptography chips that work with software technologies such as Microsoft’s BitLocker (included in some editions of Vista and Server 2008) to encrypt the drive and prevent a thief from being able to log on or access any of the files. More and more laptops also include fingerprint recognition software and other extra security measures. You can also install tracking software that will cause the laptop to "phone home" when connected to the Internet if you fail to enter the correct password.

Many PDA phones provide for password protection and you can buy third-party programs to encrypt data on the phone. The latest versions of Windows Mobile allow you to encrypt the information on the storage card without a third-party program, and you can also remotely wipe the device and card.

10 Universal connectivity

Closely related to mobility is universal connectivity. We are putting not just our computers but our entire lives online. Kitchen appliances and laundry machines can connect to the Internet, pool and spa equipment can be accessed online, and so forth. Many of us have security surveillance cameras with built-in Web servers, which we can monitor from anywhere in the world as long as we have an Internet connection. All of this connectivity is great, but it opens up avenues by which criminals can invade our homes without ever setting foot inside.

We also put ourselves online in another way. We have personal Web sites, MySpace or FaceBook accounts, Second Lives, and other venues where we reveal more about ourselves than we realize. Criminals love these social networking tools because it makes it easy for them to pick victims and get to know them, sight unseen.

What’s the solution, then? Should we disconnect from the global network, erase our presences from the Web, and go hide in our rooms? Even if that were possible (and it’s not), the cure would be worse than the disease. In today’s world, functioning without the technology is becoming increasingly difficult, and once you’ve taken the technological plunge, the information is "out there"—there’s no going back.

The key is increased awareness and constant vigilance. Use common sense, as you do in the real world. Don’t automatically trust strangers. Don’t wander into places (virtual or physical) where you’re unfamiliar with the terrain. Don’t divulge sensitive information, such as credit card and bank accounts numbers, social security numbers, and birthdates, that can be used to steal your identity. Most cybercriminals are like most other predators: they go for the easy marks. By taking some precautions, you can still use the technologies that they exploit—so long as you use them wisely—without becoming a victim.

Additional resources

- TechRepublic's Downloads RSS Feed XML
- Sign up for the Downloads at TechRepublic newsletter
- Sign up for our IT Leadership Newsletter
- Check out all of TechRepublic's free newsletters
- Investigate computer forensics: Concepts, needs, and solutions
- Fight corporate fraud through computer forensics
- Computer crime evidence-preservation checklist

Version history

Version: 1.0
Published: July 10, 2008

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to drop us a line and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Content Team