Every time you access the Internet, a world of criminals is trying to steal personal information – yours and your patients'. Here's how to stop them.

KEITH NEGLEY

How to Protect Your Data When You're on the Web

Adarsh K. Gupta, DO, MS

A computer connected to the Internet without proper protection can be hijacked in a matter of seconds. It's troubling enough that your personal information, such as financial data, can be vulnerable. But if your computer is part of an electronic health record system, then your patients' health data can be stolen as well.

As physicians know well, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires practices to protect patients' personally identifiable information. It also requires regular reviews and, if necessary, modifications of a practice's security policies and procedures to secure this information. Providers are subject to stiff civil and criminal penalties if they violate HIPAA's security requirements, including fines of up to $25,000 for multiple violations of the same standard in a calendar year and fines of up to $250,000 and/or 10 years in jail for knowing misuse of individually identifiable health information.

Protecting your patients' health information and identities (not to mention your practice's financial information and your own personal information) is as important as locking your doors at home every night. This article discusses strategies and tools to minimize your risk of being hacked. You need to understand and employ these strategies even if you are part of a large practice with an established computer network and a dedicated technology staff because the biggest security threat to even the most secure network is the user. ➤

The best software and the most secure network can be undone with one unfortunate mouse click by a careless computer user.

You can take steps to protect your personal information and your patients' data from being hacked.

"Phishers" send spam e-mails that appear to be legitimate, hoping you'll reply with critical information, such as your login name and password.

Malware is any unwanted program designed to damage your computer; it can arrive in the form of a virus, a worm, a Trojan, spyware, adware or cookies.

What you're up against

To better understand how to protect clinical patient data and personal information, you need to first be aware of how someone can access your private data via the Internet. Here are the most common frauds, which you've probably already encountered in some form:

Phishing/identity theft. You can fall into these frauds without even knowing it. "Phishers" send spam e-mails claiming to be from a legitimate business or organization (e.g., an Internet service provider, a bank or a government agency). The e-mail message might say: "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity." The message usually says that you need to "update" or "validate" your account information, threatening some dire consequence if you don't respond. The e-mail appears legitimate because it contains an official-looking logo and a clickable link that, to all appearances, leads to a Web site that looks just like a legitimate organization's. But, of course, it isn't. The criminals hope the bogus site will trick you into divulging your login name, password and personal information so they can steal your identity, run up bills or commit crimes in your name.

Most financial institutions have made it clear that they will never send their customers e-mails requesting personal information. If you receive a suspicious e-mail and can't decide on your own whether it's a fraud, try looking it up at http://www.millersmiles.co.uk, an anti-phishing Web site that constantly updates its archives with actual phishing attempts.

About the Author

Dr. Gupta is a family physician with Stratford Family Medicine in Stratford, N.J. Author disclosure: nothing to disclose.

Malware. With this type of fraud, you receive an e-mail from a friend containing a brief message – "Check out this file!" – and an attachment. Again, the e-mail appears to be from a reliable source. But the attached file is a destructive computer virus sent to you from your friend's e-mail without your friend's knowledge, ready to infect your computer as soon as you open it. Some of these programs will use your e-mail program's address book and send out e-mails with the same attachment to all your friends.

The attached file sent from your friend is an example of "malware," an unwanted program that was designed to damage your computer – and perhaps others on your computer network. Malware can be broken down into the following intruder programs:

- Virus: A self-replicating, malicious code that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence. Most viruses only replicate; however, many do a large amount of damage as well.

GOOD DESKTOP-USE POLICY

1. Do not write down passwords.
2. Do not use the "Save Password" feature on login forms.
3. Use unique passwords, and change them regularly.
4. Do not share computer accounts.
5. Use screen-saver locking, which requires a password to wake your computer from screen-saver mode (handy for when you're away from your desk but don't want to log out).
6. Log out at the end of the day.
7. Lock your laptop by picking a password only you know.

GOOD INTERNET-USE POLICY

1. Think twice before opening e-mail attachments you aren't expecting or e-mails from people you don't know. Before opening them, ask yourself the following questions:
   - *Is it from someone I know? Does it appear to have some legitimate connection to my business?* If not, don't open it.
   - *Was I expecting this particular attachment?* If not, don't open it.
   - *What type of file is it?* Don't open it if it has any of these extensions: .BAT, .EXE, .PIF, .SCR, .VBS or a double extension (e.g., .JPG.COM).
2. Avoid clicking on pop-up ads. This could lead to installation of malware programs on your computer.
3. Make sure that every financial transaction you make online is encrypted. A padlock icon will be displayed in one of the lower corners of your browser to indicate a secure site. Alternatively, check for "https" at the beginning of the Web site's address. The "s" indicates that it's a secure site.
4. Never click on links in e-mails asking for your passwords, account numbers or other private information, no matter how legitimate they appear. The best phishing (fake) sites and fraud e-mails lack obvious flaws. Always type in your bank's URL yourself or use a bookmark.
5. Don't fall victim to a hoax message. Any message that contains dire warnings or asks you to send it to everyone you know is almost surely a hoax. Only your restraint can stop hoaxes from spreading.

• Worm: An independent program that replicates from machine to machine across network connections, often clogging networks and information systems as it spreads. The worm may do damage and compromise the security of the computer. It may arrive in the form of a joke program or software.

• Trojan: A program that does not replicate itself, but causes damage or compromises the security of the computer. Trojan programs do their evil work without the user's knowledge or consent. They can collect data and send it to a criminal, destroy or alter your data, cause your computer to malfunction, or use your computer for malicious or criminal purposes, such as sending spam. Again, a Trojan program often arrives in your e-mail in the form of a joke program or software.

• Spyware: Unwanted software that monitors what you do on your computer.

• Adware: A program that typically shows up as unwanted pop-up ads or changes your browser's home page to an unwanted Web site.

• Cookie: A small file placed on your hard drive by a Web site that can transmit information about you back to the Web site. Many anti-virus programs allow you to decide which sites can create cookies on your computer, as not all cookies are malicious.

Software to stop the intruders

The categories of malware listed above are all very difficult to remove from your computer. This makes it critical that you use the best strategies to make sure they never get a chance to infect your computer in the first place.

The only sure way to protect your data from the outside world is to disconnect it from the Internet. That, of course, isn't an option for most of us. The next best way is to install the appropriate software programs. You need firewall software, anti-virus software and anti-spyware software. This is true for both your office computer and your computer at home. If you are accessing your practice's computer network from a home computer, then your home computer may be a weak point on your practice network.

Firewall software. A firewall is a "lock" for your computer against outside intruders. A network-based firewall is your best option. In lieu of that, most operating systems have firewalls installed, but it's up to you to make sure that they are on. See "Turning on a firewall" on page 32 for instructions on activating the built-in firewall for Windows XP and Mac OS X operating systems. (Note: The instructions provided in this article are

Your computers should be protected by three types of software: firewall, anti-virus and anti-spyware.

You might find one software bundle that can handle all three functions, or you might buy separate programs for each.

If you access work files from home, make sure your home computer is not a weak link on your practice's network.

TURNING ON A FIREWALL

If your computer's operating system is Windows XP or Mac OS X, it has a built-in firewall. Here's how to make sure that firewall is activated. Video tutorials of these instructions are available at http://onguardonline.gov/tutorials under "Security/Tools."

Windows XP	Mac OS X
1. Click once on the "Start" button in the lower left corner of your Desktop. 2. Select "Control Panel" from the menu that pops up. 2. Click once on the "Network and Internet Connections" link. 3. Click once on the "Windows Firewall" link. 4. If it is not already checked, check the "On (recommended)" button. 5. Click once on the "OK" button to activate the firewall.	1. Click once on the Apple icon in the top left corner of your Desktop. 2. Select "System Preferences" from the drop-down menu. 3. Click once on the "Sharing" icon. 4. Make sure the "Firewall" tab is selected. 5. Click once on the "Start" button to activate the firewall.

Shop for an anti-virus program that scans your e-mails, files and Web sites in real time.

Make sure your anti-virus software is set to run a complete deep scan at least once per week.

Your computer should be configured to receive automatic updates for its operating system whenever they are released.

for Windows XP because it is used by more people than the newer Windows Vista operating system.[1] It is important to note, however, that so far Vista has proven to be less vulnerable than XP.[2])

Anti-virus software. Always use anti-virus software, and keep it updated. Hundreds of new viruses are discovered in a typical month. With anti-virus programs, you are protecting yourself as well as others you communicate with. When shopping for an anti-virus program, make sure that it does two things:

1. Performs real-time scans on your e-mail messages, files and Web sites;

2. Updates its virus definitions automatically and frequently (some programs perform hourly updates).

After you've picked an anti-virus program, make sure that you configure it to run a complete deep scan at least once a week.

Anti-spyware software. Think of anti-spyware programs as your computer's policeman, constantly scanning your computer for spyware or malware and removing any that it finds.

To find the best programs for your computer setup, take the time to shop around and educate yourself further before buying. You might decide on one software bundle to handle all three functions, or you might prefer to buy separate programs for each. A good starting point is CNET, http://reviews.cnet.com/4566-3667_7-0.html, which offers unbiased reviews and information.

Other technical tricks

In addition to installing and updating the appropriate software, there are other things you should do to keep your computer fortified.

Update your operating system and applications. Apple and Microsoft are constantly updating their operating systems and application suites to address glitches in both security and function that are uncovered over time. It's important that these updates make their way to your computer. The easiest way to handle this is to configure your computer to download and apply these updates automatically. Instructions for how to do this in Windows can be found at http://www.microsoft.com/protect/computer/updates/mu.mspx. Instructions for Mac OS X users are available at http://docs.info.apple.com/article.html?artnum=106704.

Use a Virtual Private Network (VPN) for remote access to your practice's data. Data transferred on a VPN are better protected than data transferred on other types of networks because VPNs encrypt the data at both the sending end and the receiving end. Because of this, a VPN allows you to access the office network from home without jeopardizing the network's security.

The human factor

The best software and the most secure network can be undone with one unfortunate mouse click by a careless computer user. For this

Because technology and employees can change rapidly, your security safeguards should be checked and tweaked at least once a year.

reason, your practice needs to use the following strategies to make sure its employees are as security-focused as the computers they're using.

Educate users. It's critical that every computer user in your practice, from the front office staff to the nursing staff to the physicians, follow smart and safe practices that, ideally, are written down as part of official company policy. Make every employee aware of his or her information security responsibilities, which will vary depending on how much access to patient information each employee has. See "Good desktop-use policy" on page 30 and "Good Internet-use policy" on page 31 for recommendations.

Appoint a security official. This is a HIPAA requirement. The security official could be a physician or the office manager. This individual is responsible for all policy development, training and security compliance activities.

Perform a risk analysis. Identify the potential security loopholes based on your practice's individual history and situation. This risk assessment simply requires you to determine

INTERNET SECURITY IN A NUTSHELL

Internet threats	How do you get it?	What can it do?	How can you protect yourself?
Spyware	Downloading files from file-sharing services; playing interactive games online; installing free software from unknown, untrusted sources.	• Your computer can become unstable or unusable; • Others may be enabled to record your keystrokes and steal your personal information.	• Install and regularly update anti-spyware software; • Perform frequent spyware scans; • Avoid sites and activities that can invite spyware.
Viruses, worms, Trojan horses, malware	Reading e-mail from unknown senders; opening unknown e-mail attachments; clicking on pop-up ads.	• Your computer files can be destroyed; • Hackers can gain control over your computer; • Viruses can quickly spread to other computers; • Your personal data can be stolen.	• Install and regularly update antivirus and firewall software; • Perform frequent antivirus scans; • Be cautious about opening e-mail attachments you aren't expecting or e-mails from people you don't know; • Never click on pop-up ads.
Phishing scams/ identity thieves	Replying to e-mails that appear to be from legitimate institutions but aren't; shopping, banking or conducting other financial transactions at insecure online sites or on insecure connections.	• Replying to a phishing scam can cause you to unknowingly provide criminals with your personal financial information, such as your social security number, credit-card number and banking passwords, costing you thousands of dollars.	• Make sure every online financial transaction is encrypted; • Avoid clicking on pop-up ads; • Don't allow "cookies" to be downloaded onto your computer without notification; • Never reply to e-mails asking for your passwords, account numbers or other private information – no matter how legitimate they may appear to be.

Guard against human error by putting your Internet-use and desktop-use policies in writing for your employees.

Making the changes required to secure your computers is much less trouble than dealing with the fallout of a security breach involving your patient records.

whether someone – such as an ex-employee – could compromise your network's security and how you could block such a breach.

Develop a contingency plan. What if the worst happens – your systems go down, a security breach occurs or a natural disaster interrupts your access to electronic information? Identify the most vulnerable systems and data, and then create a data backup plan, a disaster recovery plan and an emergency operations plan. Train personnel and test these plans to see if they will be effective when needed.

Develop security incident procedures. Create a process to respond to, contain, investigate and mitigate the damage caused by security incidents. Keep records of actions you take and the results.

Reevaluate your security safeguards annually. Because technology and employees can change rapidly, your security safeguards should be checked and tweaked at least once a year.

Control facility and equipment access. This includes keeping computers, printers and fax machines out of patient or high-traffic areas, locking rooms containing sensitive assets, destroying paper and electronic information when no longer needed, and only allowing certain individuals to access sensitive areas or data applications.

The cost of inaction

Patients are becoming more educated about their rights under HIPAA and state medical privacy laws. If your practice does not take security safeguards seriously and a patient asks questions about your security standards, or if a security breach occurs that results in a publicized violation, the practice will be hit with financial penalties as well as negative publicity. It's much cheaper to implement reasonable compliance solutions today. FPM

Send comments to **fpmedit@aafp.org.**

1. Larkin E. Vista resistance: why XP is still so strong. *PC World*. Sept. 25, 2007. Available at: http://www.pcworld.com/article/id,137635/article.html. Accessed Feb. 26, 2008.

2. Broersma M. Vista more secure than XP and open source. *Techworld*. Jan. 24, 2008. Available at: http://www.techworld.com/news/index.cfm?newsID=11228. Accessed Feb. 26, 2008.