



Real solutions for real business

CARE's WorkLife Solutions Weekly Wire

Stop, Click, Think: Seven Practices for Computer Security

December 2011

This month's Wire is taken from one of the many articles found on our website. The article, "Stop, Click, Think: Seven Practices for Computer Security," relates to our December Webinar topic, "Tune up Your Search Engine," which is attached. To access this article, log-on to www.caresworklivesolutions.com, click on the World Icon and enter your unique company password. (If you do not have a company password, contact CARE's WorkLife Solutions to request a temporary password.) Next, click on the Site Search tab on the right, click on Advanced Search and enter "Computer+Security," in the Search the Website by Title field. You may need to click View All to see the article. We encourage you to use the Site Search feature to locate many topics by your specific area of interest.

Stop, Click, Think: Seven Practices for Computer Security

Seven Practices for Computer Security

Access to information and entertainment, credit and financial services, products from every corner of the world—even to your work—is greater than ever. Thanks to the Internet, you can play a friendly game with an opponent across the ocean; review and rate videos, songs, or clothes; get expert advice in an instant; or collaborate with far-flung coworkers in a "virtual" office.

But the Internet—and the anonymity it affords—also can give online scammers, hackers, and identity thieves access to your computer, personal information, finances, and more. With awareness as your safety net, you can minimize the chance of an Internet mishap. Being on guard online helps you protect your information, your computer, and your money. To be safer and more secure online, make these seven practices part of your online routine.

1. Protect your personal information. It's valuable.

To an identity thief, your personal information can provide instant access to your financial accounts, your credit record, and other assets. If you think no one would be interested in your personal information, think again. Anyone can be a victim of identity theft. In fact, according to the Federal Trade Commission (FTC), millions of people become victims every year. Visit the FTC's Identity Theft Web site (<http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html>) to learn what to do if your identity is stolen or your personal or financial information has been compromised—online or in the "real" world.

How do criminals get your personal information online? One way is by lying about who they are, to convince you to share your account numbers, passwords, and other information so they can get your money or buy things in your name. The scam is called *phishing*: criminals send e-mail, text, or pop-up messages that appear to come from your bank, a government agency, an online seller, or another organization with which you do business. The message asks you to click to a Web site or call a phone number to update your account information or claim a prize or benefit. It might suggest something bad will happen if you don't respond quickly with your personal information. In reality, legitimate businesses should never use e-mail, pop-ups, or text messages to ask for your personal information.

To avoid phishing scams

- Don't reply to an e-mail, text, or pop-up message that asks for personal or financial information, and don't click on links in the message. If you want to go to a bank or business's Web site, type the Web address into your browser yourself.
- Don't respond if you get a message—by e-mail, text, pop-up, or phone—that asks you to call a phone number to update your account or give your personal information to access a refund. If you need to reach an organization with which you do business, call the number on your financial statement, or use a telephone directory

Some identity thieves have stolen personal information from many people at once, by hacking into large databases managed by businesses or government agencies. While you can't enjoy the benefits of the Internet without sharing some personal information, you can take steps to share only with organizations you know and trust. Don't give out your personal information unless you first find out how it's going to be used and how it will be protected.

If you are shopping online, don't provide your personal or financial information through a company's Web site until you have checked for indicators that the site is secure, like a lock icon on the browser's status bar or a Web site URL that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some scammers have forged security icons. And some hackers have managed to breach sites that took appropriate security precautions.

Read Web site privacy policies. They should explain what personal information the Web site collects, how the information is used, and whether it is provided to third parties. The privacy policy also should tell you whether you have the right to see what information the Web site has about you and what security measures the company takes to protect your information. If you don't see a privacy policy—or if you can't understand it—consider doing business elsewhere.

2. Know with whom you're dealing.

And what you're getting into. There are dishonest people in the bricks and mortar world and on the Internet. But online, you can't judge an operator's trustworthiness with a gut-affirming look in the eye. It's remarkably simple for online scammers to impersonate a legitimate business, so you need to know with whom you're dealing. If you're thinking about shopping on a site with which you're not familiar, do some independent research before you buy.

- If it's your first time on an unfamiliar site, call the seller's phone number, so you know you can reach them if you need to. If you can't find a working phone number, take your business elsewhere.
- Type the site's name into a search engine: If you find unfavorable reviews posted, you may be better off doing business with a different seller.
- Consider using a software toolbar that rates Web sites and warns you if a site has gotten unfavorable reports from experts and other Internet users. Some reputable companies provide free tools that may alert you if a Web site is a known phishing site or is used to distribute spyware.

File-Sharing: Worth the hidden costs?

Every day, millions of computer users share files online. File-sharing can give people access to a wealth of information, including music, games, and software. How does it work? You download special software that connects your computer to an informal network of other computers running the same software. Millions of users could be connected to each other through this software at one time. Often, the software is free and easy to access.

But file-sharing can have a number of risks. If you don't check the proper settings, you could allow access not only to the files you intend to share, but also to other information on your hard drive, like your tax returns, e-mail messages, medical records, photos, or other personal documents. In addition, you may unwittingly download malware or pornography labeled as something else. Or you may download material that is protected by the copyright laws, which would mean you could be breaking the law. If you decide to use file-sharing software, be sure to read the End User Licensing Agreement to be sure you understand and are willing to tolerate the potential risks of free downloads.

3. Use security software that updates automatically.

Keep your security software active and current: at a minimum, your computer should have *antivirus* and *anti-spyware* software, and a *firewall*. You can buy stand-alone programs for each element or a security suite that includes these programs from a variety of sources, including commercial vendors or from your Internet Service Provider (ISP). Security software that comes pre-installed on a computer generally works for a short time unless you pay a subscription fee to keep it in effect. In any case, security software protects against the newest threats only if it is up-to-date. That's why it is critical to set your security software to update automatically.

Some scam artists distribute malware disguised as anti-spyware software. Resist buying software in response to unexpected pop-up messages or e-mails, especially ads that claim to have scanned your computer and detected malware. That's a tactic scammers have used to spread malware.

Antivirus Software

Antivirus software protects your computer from viruses that can destroy your data, slow your computer's performance, cause a crash, or even allow spammers to send e-mail through your account. It works by scanning your computer and your incoming e-mail for viruses, and then deleting them.

Anti-Spyware Software

Installed on your computer without your consent, spyware software monitors or controls your computer use. It may be used to send you pop-up ads, redirect your computer to Web sites, monitor your Internet surfing, or record your keystrokes, which, in turn, could lead to the theft of your personal information.

A computer may be infected with spyware if it:

- Slows down, malfunctions, or displays repeated error messages
- Won't shut down or restart
- Serves up a lot of pop-up ads, or displays them when you're not surfing the Web
- Displays web pages or programs you didn't intend to use, or sends e-mails you didn't write

Firewalls

A *firewall* helps keep hackers from using your computer to send out your personal information without your permission. While antivirus software scans incoming e-mail and files, a firewall is like a guard, watching for outside attempts to access your system and blocking communications to and from sources you don't permit.

Don't let your computer become part of a *BotNet*.

Some spammers search the Internet for unprotected computers they can control and use anonymously to send spam, turning them into a robot network, known as a *botnet*. Also known as a *zombie army*, a botnet is made up of many thousands of home computers sending e-mails by the millions. Most spam is sent remotely this way; millions of home computers are part of botnets.

Some spammers search the Internet for unprotected computers they can control and use anonymously to send spam, turning them into a robot network, known as a *botnet*. Also known as a *zombie army*, a botnet is made up of many thousands of home computers sending e-mails by the millions. Most spam is sent remotely this way; millions of home computers are part of botnets.

Spammers scan the Internet to find computers that aren't protected by security software, and then install bad software—known as *malware*—through those "open doors." That's one reason why up-to-date security software is critical.

Malware may be hidden in free software applications. It can be appealing to download free software like games, file-sharing programs, customized toolbars, and the like. But sometimes just visiting a Web site or downloading files may cause a "drive-by download," which could turn your computer into a *bot*.

Another way spammers take over your computer is by sending you an e-mail with attachments, links or images which, if you click on or open them, install hidden software. Be cautious about opening any attachments or downloading files from e-mails you receive. Don't open an e-mail attachment—even if it looks like it's from a friend or coworker—unless you are expecting it or know what it contains. If you send an e-mail with an attached file, include a text message explaining what it is.

4. Keep your operating system and Web browser up-to-date, and learn about their security features.

Hackers also take advantage of Web browsers (like Firefox or Internet Explorer) and operating system software (like Windows or Mac's operating systems) that don't have the latest security updates. Operating system companies issue security patches for flaws that they find in their systems, so it's important to set your operating system and Web browser software to download and install security patches automatically. In addition, you can increase your online security by changing the built-in security and privacy settings in your operating system or browser. Check the "Tools" or "Options" menus to learn how to upgrade from the default settings. Use your "Help" function for more information about your choices.

If you're not using your computer for an extended period, disconnect it from the Internet. When it's disconnected, the computer doesn't send or receive information from the Internet and isn't vulnerable to hackers.

5. Protect your passwords.

Keep your passwords in a secure place, and out of plain sight. Don't share them on the Internet, over e-mail, or on the phone. Your Internet Service Provider (ISP) should never ask for your password. In addition, hackers may try to figure out your passwords to gain access to your computer. To make it tougher for them:

- Use passwords that have at least eight characters and include numbers or symbols. The longer the password, the tougher it is to crack. A 12-character password is stronger than one with eight characters.
- Avoid common words—some hackers use programs that can try every word in the dictionary.
- Don't use your personal information, your login name, or adjacent keys on the keyboard as passwords.
- Change your passwords regularly (at a minimum, every 90 days).
- Don't use the same password for each online account you access.

6. Back up important files.

If you follow these tips, you're more likely to be free of interference from hackers, viruses, and spammers. But no system is completely secure. If you have important files stored on your computer, copy them onto a removable disc or an external hard drive, and store it in a safe place.

7. Learn what to do in an "e-emergency."

If you suspect malware is lurking on your computer, stop shopping, banking, and other online activities that involve user names, passwords, or other sensitive information. Malware could be sending your personal information to identity thieves.

Confirm that your security software is up-to-date, then use it to scan your computer. Delete everything the program identifies as a problem. You may have to restart your computer for the changes to take effect. If the problem persists after you exhaust your ability to diagnose and treat it, you might want to call for professional help. If your computer is covered by a warranty that offers free tech support, contact the manufacturer. Before you call, write down the model and serial number of your computer, the name of any software you've installed, and a short description of the problem. Your notes will help you give an accurate description to the technician.

If you need professional help, if your machine isn't covered by a warranty, or if your security software isn't doing the job properly, you may need to pay for technical support. Many companies—including some affiliated with retail stores—offer technical support via the phone, online, at their store, or in your home. Telephone or online help generally are the least expensive ways to access support services—especially if there's a toll-free helpline—but you may have to do some of the work yourself. Taking your computer to a store usually is less expensive than hiring a technician or repair person to come into your home.

Once your computer is back up and running, think about how malware could have been downloaded to your machine, and what you could do to avoid it in the future. Also, talk about safe computing with anyone else who uses the computer. Tell them that some online activity can put a computer at risk, and share the seven practices for safer computing.

Tips for Parents

Parents sometimes can feel outpaced by their technologically savvy kids. Technology aside, there are lessons that parents can teach to help kids stay safer as they socialize online. Most ISPs provide parental controls, or you can buy separate software. But no software can substitute for parental supervision. Talk to your kids about safe computing practices, as well as the things they're seeing and doing online.

Social Networking Sites

Many adults, teens, and "tweens" use social networking sites to exchange information about themselves, share pictures and videos, and use blogs and private messaging to communicate with friends, others who share interests, and sometimes even the world-at-large. Here are some tips for parents who want their kids to use these sites safely:

- Use privacy settings to restrict who can access and post on your child's Web site. Some social networking sites have strong privacy settings. Show your child how to use these settings to limit who can view their online profile, and explain to them why this is important.

- Encourage your child to think about the language used in a blog, and to think before posting pictures and videos. Employers, college admissions officers, team coaches, and teachers may view your child's postings. Even a kid's screen name could make a difference. Encourage teens to think about the impression that screen names could make.
 - Remind your kids that once they post information online, they can't take it back. Even if they delete the information from a site, older versions may exist on other people's computers and be circulated online.
 - Talk to your kids about bullying. Online bullying can take many forms, from spreading rumors online and posting or forwarding private messages without the sender's OK, to sending threatening messages. Tell your kids that the words they type and the images they post can have real-world consequences. They can make the target of the bullying feel bad, make the sender look bad—and, sometimes, can bring on punishment from the authorities. Encourage your kids to talk to you if they feel targeted by a bully.
 - Talk to your kids about avoiding sex talk online. Recent research shows that teens who don't talk about sex with strangers online are less likely to come in contact with a predator.
 - Tell your kids to trust their instincts if they have suspicions. If they feel threatened by someone or uncomfortable because of something online, encourage them to tell you. You can then help them report concerns to the police and to the social networking site. Most sites have links where users can immediately report abusive, suspicious, or inappropriate online behavior.
-
-

OnGuardOnline.gov. (n.d.). *Stop - think - click: Seven practices for safer computing*. Retrieved October 23, 2009, from <http://www.onguardonline.gov/>