STOP • THINK • CLICK™

7 PRACTICES FOR SAFER COMPUTING

OnGuard Online | YOUR SAFETY NET™

EFFICIENT SHOPPING

ACCESS TO INFORMATION, MUSIC, AND GAMES

EDUCATIONAL RESOURCES

TRAVEL PLANNING

SPORTS, HOBBIES, AND SOCIAL NETWORKS

CONNECTIONS TO FAMILY AND FRIENDS

CONVENIENT FINANCIAL MANAGEMENT

NEWS FROM AROUND THE WORLD

DIGITAL PHOTOGRAPHY

Access to information and entertainment, credit and financial services, products from every corner of the world — even to your work — is greater than earlier generations could ever have imagined. Thanks to the Internet, you can order books, clothes, or appliances online; reserve a hotel room across the ocean; download music and games; check your bank balance 24 hours a day; or access your workplace from thousands of miles away.

The flip-side, however, is that 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.

But 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, even yourself. To be safer and more secure online, adopt these seven practices.

THE SEVEN PRACTICES

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

Why? 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. The reality is that anyone can be a victim of identity theft. In fact, according to a Federal Trade Commission (FTC) survey, there are millions of victims a year. It's often difficult to know how thieves obtained their victims' personal information, and while it definitely can happen offline, some cases start when online data is stolen. Visit ftc.gov/idtheft to learn what to do if your identity is stolen.

Unfortunately, when it comes to crimes like identity theft, you can't entirely control whether you will become a victim. But following these tips can help minimize your risk while you're online:

- If you're asked for your personal information — your name, email or home address, phone number, account numbers, or Social Security number — find out how it's going to be used and how it will be protected before you share it. If you have children, teach them to *not* give out your last name, your home address, or your phone number on the Internet.
- If you get an email or pop-up message asking for personal information, don't reply or click on the link in the message. The safest course of

action is not to respond to requests for your personal or financial information. If you believe there may be a need for such information by a company with whom you have an account or placed an order, contact that company directly in a way you know to be genuine, like using a phone number from directory assistance. In any case, don't send your personal information via email because email is not a secure transmission method.

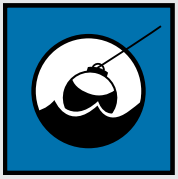
- If you are shopping online, don't provide your personal or financial information through a company's website until you have checked for indicators that the site is secure, like a lock icon on the browser's status bar or a website URL that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some scammers have forged security icons.
- Read website privacy policies. They should explain what personal information the website 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 website 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.

WORDS FOR THE WISE

A **hacker** is a person who uses the Internet to access computers without permission. A **spammer** is someone who sends mass amounts of unsolicited commercial email. A **virus** is software that spreads from computer to computer and damages files or disrupts your system.

2 Know who you're dealing with.

And know 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 who you're dealing with. If you're shopping online, check out the seller before you buy. A legitimate business or individual seller should give you a physical address and a working telephone number at which they can be contacted in case you have problems.



PHISHING

BAIT OR PREY?

"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."

"Phishers" send spam or pop-up messages claiming to be from a business or organization that you might deal with — for example, an Internet service provider (ISP), bank, online payment service, or even a government agency. The message usually says that you need to "update" or "validate" your account information. It might threaten some dire consequence if you don't respond. The message directs you to a website that looks just like a legitimate organization's, but isn't. The purpose of the bogus site? To trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name. Don't take the bait: never reply to or click on links in email or pop-ups that ask for personal

information. Legitimate companies don't ask for this information via email. If you are directed to a website or told to call a phone number to update your information, verify that the request is legitimate by calling the company directly, using contact information from your account statements. Or open a new browser window and type the URL into the address field, watching that the actual URL of the site you visit doesn't change and is still the one you intended to visit. Forward spam that is phishing for information to spam@uce.gov and to the company, bank, or organization impersonated in the phishing email. Most organizations have information on their websites about where to report problems.

FREE SOFTWARE AND 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 easily accessible.

But file-sharing can have a number of risks. If you don't check the proper settings, you could allow access not just to the files you intend to share, but also to other information on your hard drive, like your tax returns, email messages, medical records, photos, or other personal documents. In addition, you may unwittingly download 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, set it up very carefully. Take the time to read the End User License Agreement to be sure you understand the side effects of any free downloads.

3 Use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly.

Dealing with anti-virus, anti-spyware, and firewall protection may sound about as exciting as flossing your teeth, but it's just as important as a preventive measure. Having intense dental treatment is never fun; neither is dealing with the effects of a preventable computer virus.

ANTI-VIRUS SOFTWARE

Anti-virus 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 email through your account. It works by scanning your computer and your incoming email for viruses, and then deleting them.

To be effective, your anti-virus software should update daily with antidotes to the latest "bugs" circulating through the Internet. Most commercial anti-virus software includes a feature to download updates automatically when you are on the Internet.

ANTI-VIRUS SOFTWARE

What to Look For and Where to Get It

You can download anti-virus software from the websites of software companies or buy it in retail stores. Look for anti-virus software that:

- Removes or quarantines viruses.
- Updates automatically.

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 websites, monitor your Internet surfing, or record your keystrokes, which, in turn, could lead to the theft of your personal information.

Clues that spyware is on a computer include:

- A barrage of pop-up ads
- A hijacked browser — that is, a browser that takes you to sites other than those you type into the address box
- A sudden or repeated change in your computer's Internet home page
- New and unexpected toolbars
- Unexpected icons on the system tray at the bottom of your computer screen
- Keys that don't work
- Random error messages
- Sluggish or downright slow performance when opening programs or saving files.

You can take steps to limit your vulnerability to spyware:

- Update your operating system and Web browser software. Your operating system (like Windows or Linux) may offer free software "patches" to close holes in the system that spyware could exploit. Make sure to set your browser security high enough to detect unauthorized downloads.
- Download free software only from sites you know and trust. It can be appealing to download free software like games, file-sharing programs, customized toolbars, or other programs that may change or customize the functioning of your computer. Be aware, however, that many free software applications bundle other software, including spyware.

FIREWALLS

Don't be put off by the word "firewall." It's not necessary to fully understand how it works; it's enough to know what it does and why you need it. Firewalls help keep hackers from using your computer to send out your personal information without your permission. While anti-virus software scans incoming email 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.

Some operating systems and hardware devices come with a built-in firewall that may be shipped in the "off" mode. Make sure you turn it on. For your firewall to be effective, it needs to be set up properly and updated regularly. Check your online "Help" feature for specific instructions.

If your operating system doesn't include a firewall, get a separate software firewall that runs in the background while you work, or install a hardware firewall — an external device that includes firewall software. Several free firewall software programs are available on the Internet.

DON'T BECOME A ZOMBIE DRONE

Some spammers search the Internet for unprotected computers they can control and use anonymously to send unwanted spam emails. If you don't have up-to-date anti-virus protection and a firewall, spammers may try to install software that lets them route email through your computer, often to thousands of recipients, so that it appears to have come from your account. If this happens, you may receive an overwhelming number of complaints from recipients, and your email account could be shut down by your Internet Service Provider (ISP).

4 Be sure to set up your operating system and Web browser software properly, and update them regularly.

Hackers also take advantage of Web browsers (like Internet Explorer or Netscape) and operating system software (like Windows or Linux) that are unsecured. Lessen your risk by changing the settings in your browser or operating system and increasing your online security. Check the "Tools" or "Options" menus for built-in security features. If you need help understanding your choices, use your "Help" function.

Your operating system also may offer free software "patches" that close holes in the system that hackers could exploit. If possible, set your operating system to automatically retrieve and install patches for you. If your system can't do this, bookmark the website for your system's manufacturer so you can regularly visit and update your system with defenses against the latest attacks. Updating can be as simple as one click. Your email software may help you avoid viruses by giving you the ability to filter certain types of spam. It may be up to you to activate the filter.

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 view. Don't share your passwords on the Internet, over email, 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.

One way to create a strong password is to think of a memorable phrase and use the first letter of each word as your password, converting some letters into numbers that resemble letters. For example, "How much wood could a woodchuck chuck" would become HmWc@wcC.

6 Back up important files.

If you follow these tips, you're more likely to be more secure online, 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 drive, and store them in a safe place.

7 Learn who to contact if something goes wrong online.

Hacking or Computer Virus

If your computer gets hacked or infected by a virus:

- Immediately disconnect your machine from the Internet. Then scan your entire computer with fully updated anti-virus and anti-spyware software, and update your firewall.
- If your computer is infected and you can't get it to recover any other way, you can buy software to "wipe" — or erase — the hard drive. You'd then have to reinstall the operating system, and any other files you wish to use.
- Take steps to minimize the chances of another incident.
- Alert the appropriate authorities by contacting:
  - your ISP and the hacker's ISP (if you can tell what it is). You can usually find an ISP's email address on its website. Include information on the incident from your firewall's log file. By alerting

the ISP to the problem on its system, you can help it prevent similar problems in the future.

- the FBI at www.ic3.gov. To fight computer criminals, they need to hear from you.

Internet Fraud

If a scammer takes advantage of you through an Internet auction, when you're shopping online, or in any other way, report it to the Federal Trade Commission, at ftc.gov. The FTC enters Internet, identity theft, and other fraud-related complaints into a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Deceptive Spam

If you get deceptive spam, including email phishing for your information, forward it to spam@uce.gov. Be sure to include the full header of the email, including all routing information. You also may report phishing email to reportphishing@antiphishing.org. The Anti-Phishing Working Group — a consortium of ISPs, security vendors, financial institutions, and law enforcement agencies — uses these reports to fight phishing.

Divulged Personal Information

If you believe you have mistakenly given your personal information to a fraudster, file a complaint at ftc.gov, and then visit the Federal Trade Commission's Identity Theft website at ftc.gov/idtheft to learn how to minimize your risk of damage from a potential theft of your identity.

PARENTS

Parental controls are provided by most ISPs, or are sold as separate software. Remember that 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.

RESOURCES

OnGuardOnline.gov
ftc.gov/idtheft

OnGuard Online provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information.

To order more copies of this publication, visit OnGuardOnline.gov/order.

Test your knowledge about safe computing: Visit OnGuardOnline.gov/quiz.

To keep up to date with information about the latest computer threats, sign up for alerts from the Department of Homeland Security at www.US-CERT.gov.

September 2007