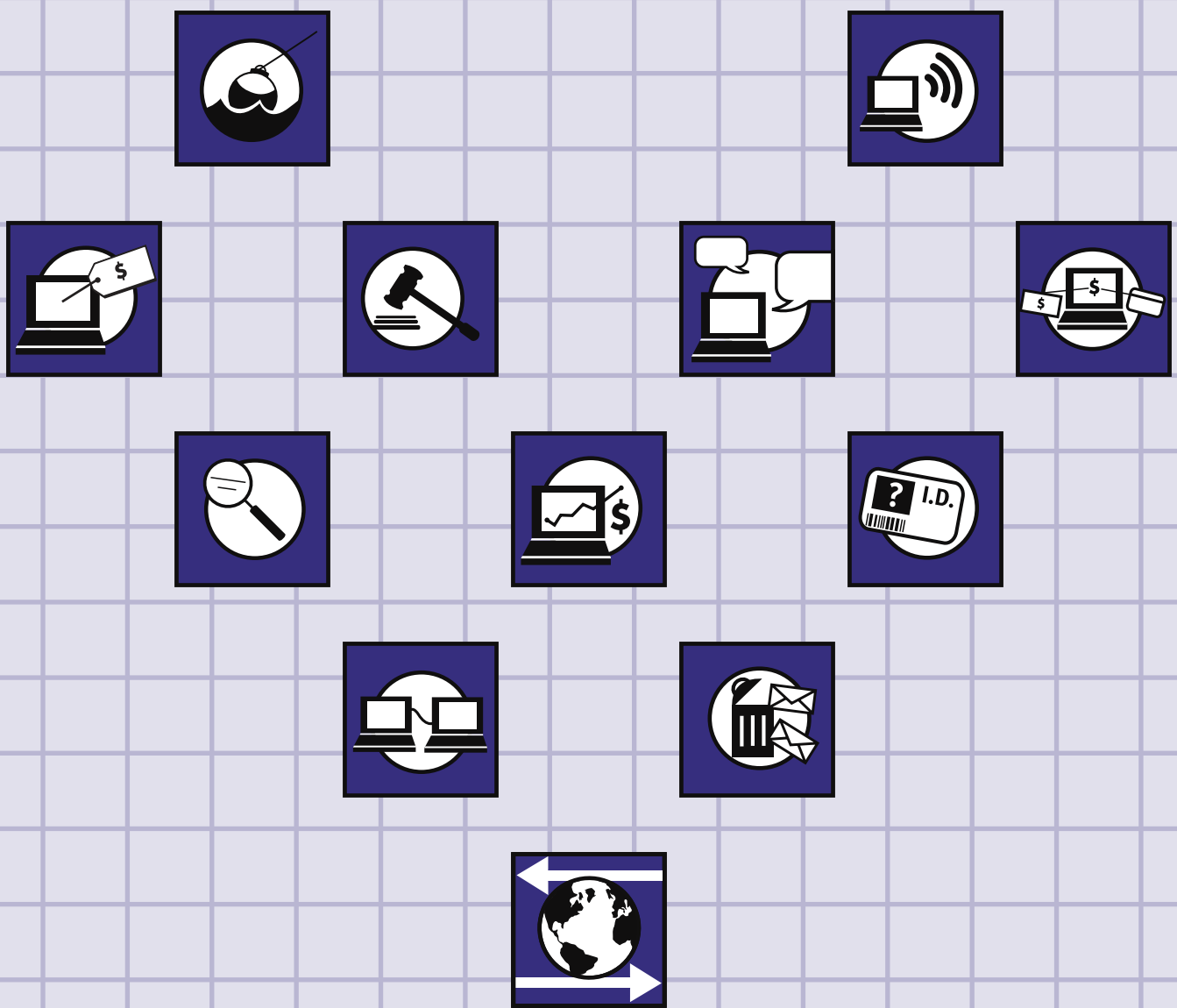
STOP • THINK • CLICK

7 PRACTICES

FOR SAFER COMPUTING



The Internet can give you access to information, entertainment, financial offers, and countless other services. At the same time, it can leave you vulnerable to online scammers or identity thieves. Learn experts' top seven practices for safer computing, as well as some terms and remedies.

The Federal Trade Commission is the nation's consumer protection agency. The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them.

Consumers can contact the FTC for free information on a wide range of issues, including:

Advertising Claims • Buying, Leasing, and Renting Cars
Credit • Debt Collection • Employment and Job Placement
Identity Theft • Investment Schemes
Online Shopping • Scholarship Scams
Sweepstakes • Telemarketing
Work-At-Home Schemes... and More

To file a complaint or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

The FTC manages OnGuardOnline.gov, a joint project of the federal government and the technology industry providing practical tips to help you guard against Internet fraud, secure your computers, and protect your personal information.

Dear Student:

Thanks to the Internet, you can buy just about anything online, watch movies and t.v. shows, catch the latest news, discuss a topic that interests you, take classes, buy a book or download music and games, communicate with friends and family, meet new people...the list goes on.

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.

The FTC believes that consumer education truly is the first line of defense for computer users against fraud and deception online.

With awareness as your safety net, you can minimize the chance of an Internet mishap. An aware computer user is more likely to recognize a phishing e-mail, more likely to download a spyware detector, and far less likely to disclose, expose, or unwittingly share personal information.

The Federal Trade Commission (FTC), the nation's consumer protection agency, prepared this supplement. The articles provide practical tips to help you be on guard against Internet fraud, secure your computer, and protect your personal information. I hope you will keep them in mind as you take advantage of all the Internet has to offer – safely.

Sincerely,
Deborah Platt Majoras
Chairman
Federal Trade Commission

7 Practices for Safer Computing

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

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 target your personal information, think again. The reality is that anyone can be a victim of identity theft. According to a Federal Trade Commission survey, there are almost 10 million victims every year. It's often difficult to know how thieves obtained their victims' personal information. While it definitely can happen offline, some cases start when online data is stolen.

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

- If asked for 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. In general, its a good idea to keep your last name, home address, and phone number to yourself.
- If you get an email or pop-up message asking for personal information, don't reply or click on the link in the message. To check if a company with whom you have an account or placed an order may need such information, contact them directly in a way you know to be genuine, like a phone number from directory assistance. In any case, don't send personal information via email because email is not a secure transmission method.
- When shopping online, don't provide personal or financial information through a company's website until you check that the site is secure. Look for indicators 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. These 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 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.

Test Your Knowledge: Check Out the Interactive Quizzes at OnGuardOnline.gov.

2 Know who you're dealing with.

And know what you're getting into. There are dishonest people in the bricks and mortar world as well as 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. 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."

"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."

Have you received email with a similar message? It's a scam called "phishing" – and it involves Internet

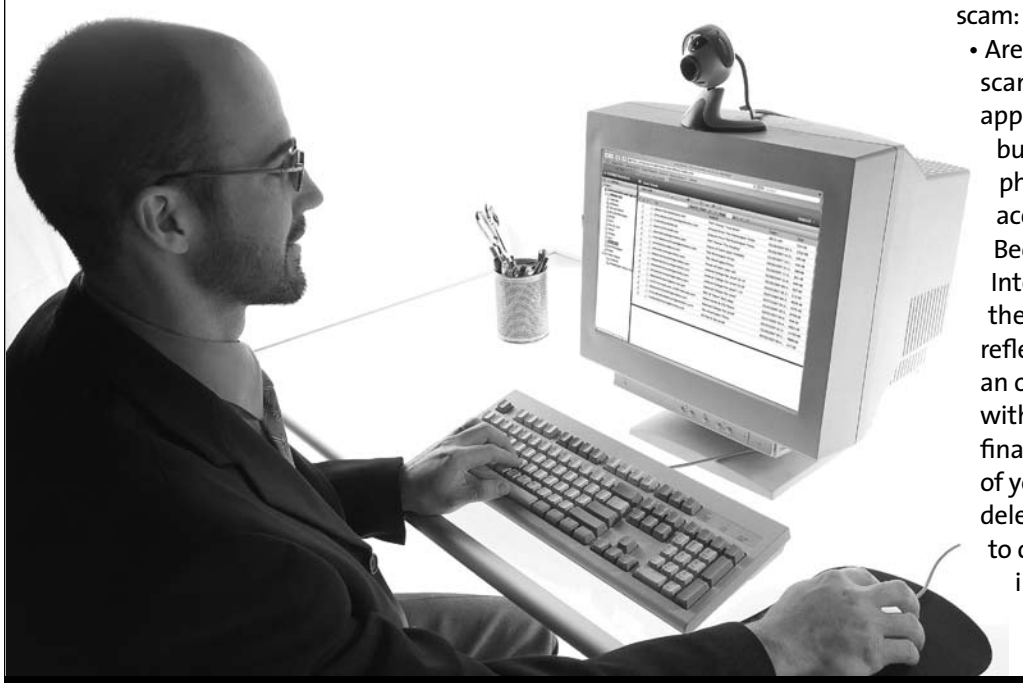
fraudsters who send spam or pop-up messages to lure personal information (credit card numbers, bank account information, Social Security number, passwords, or other sensitive information) from unsuspecting victims.

"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 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. 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 information this way. If you are directed to a website to update your information, verify that the site 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.

These additional tips may help you avoid getting hooked by a phishing scam:

- Area codes can mislead. Some scammers send an email that appears to be from a legitimate business and ask you to call a phone number to update your account or access a "refund." Because they use Voice Over Internet Protocol (VoIP) technology, the area code you call does not reflect their real location. To reach an organization you do business with, call the number on your financial statements or on the back of your credit card. In any case, delete random emails that ask you to confirm or divulge your financial information.
- Review credit card and bank account statements as soon as you receive them to check for unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security.



FREE SOFTWARE AND FILE-SHARING: Worth the hidden costs?

Every day, millions of computer users share files online. File-sharing gives access to a wealth of information, including music, games,

"Some 'free' software comes with spyware."

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 poses a risk. If you don't check the proper settings, you could permit 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 carefully. Read the End User Licensing Agreement to be sure you understand and are willing to tolerate the side effects of any free

True or False:

To do file-sharing, your computer needs special software that connects it to an informal network of computers running the same software.

Answer: True.

True or False:

When downloading from another computer, the only way to know what you're really getting is to check the file name.

Answer: False

3 downloads.

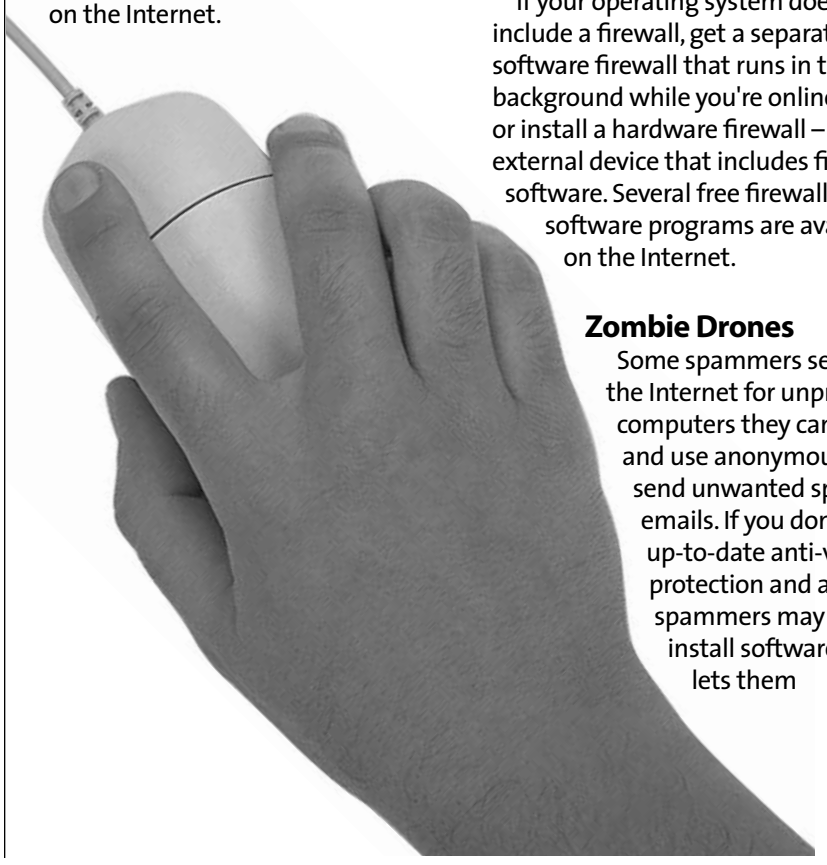
Use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly.

Dealing with anti-virus and firewall protection may sound about as exciting as flossing your teeth, but it's just as important. 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 those viruses.

To be effective, your anti-virus software should update routinely 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.



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

Firewalls

Don't be put off by the word "firewall." You don't need to know how it works; just know what it does and why you need it. Firewalls help prevent 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're online, or install a hardware firewall – an external device that includes firewall software. Several free firewall software programs are available on the Internet.

Zombie Drones

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).

Spyware

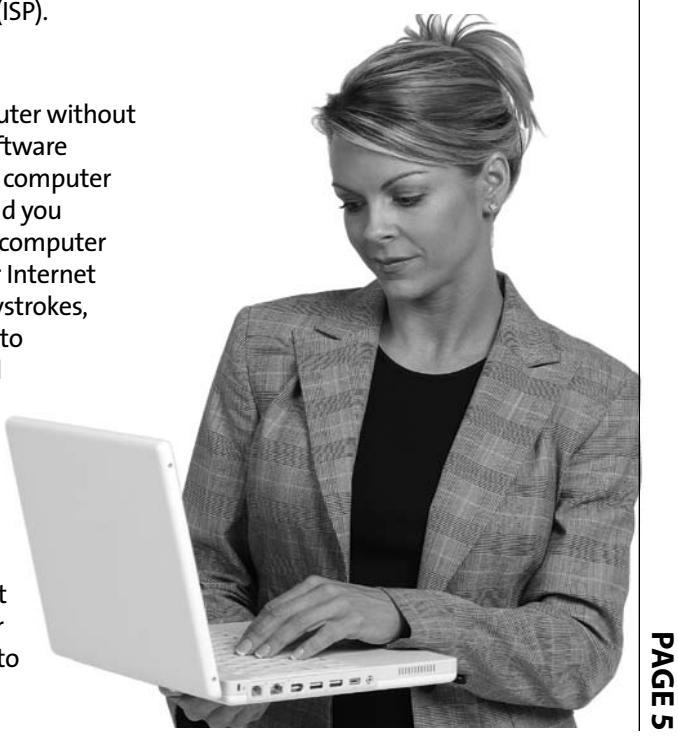
Installed on your computer without your consent, spyware software monitors or controls your computer use. It may be used to send you pop-up ads, redirect your computer to websites, monitor your Internet surfing, or record your keystrokes, which, in turn, could lead to the theft of your personal information.

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 (for example, the "Tab" key that might not work when you try to move to the next field in a Web form)
- Random error messages
- Sluggish or downright slow performance when opening programs or saving files

You can take steps to limit your vulnerability to spyware:

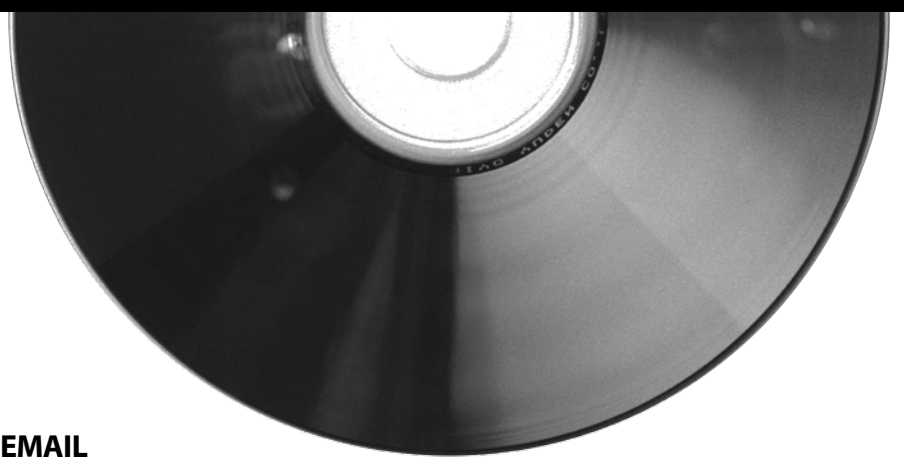
- Update your operating system and Web browser software. Your operating system (like Windows or Linux) may offer free software "patches" to close holes in the system that spyware could exploit. Make sure to set your browser security high enough to detect unauthorized downloads.
- Download free software 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.



True or False:

File-sharing programs will find and remove spyware that has been secretly installed on your computer.

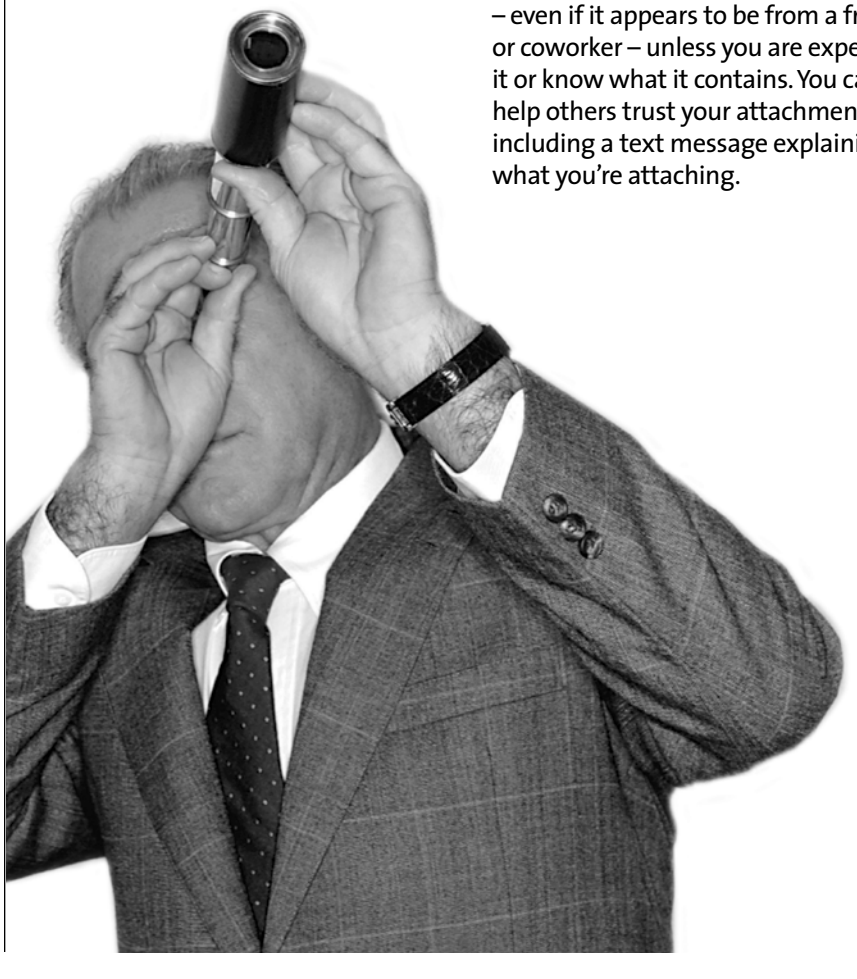
Answer: False



- Don't install any software without knowing exactly what it is. Take the time to read the end-user license agreement (EULA) before downloading any software. If the EULA is hard to find – or difficult to understand – think twice about installing the software.
- Don't click on any links within pop-up windows. If you do, you may install spyware on your computer. Instead, close pop-up windows by clicking on the "X" icon in the title bar.
- Don't click on links in spam that claim to offer anti-spyware software. Some software offered in spam actually installs spyware.

If you think your computer might have spyware on it, experts advise that you:

- Get an anti-spyware program from a vendor you know and trust.
- Set it to scan on a regular basis – at least once a week – and every time you start your computer, if possible.
- Delete any software programs the anti-spyware program detects that you don't want on your computer.

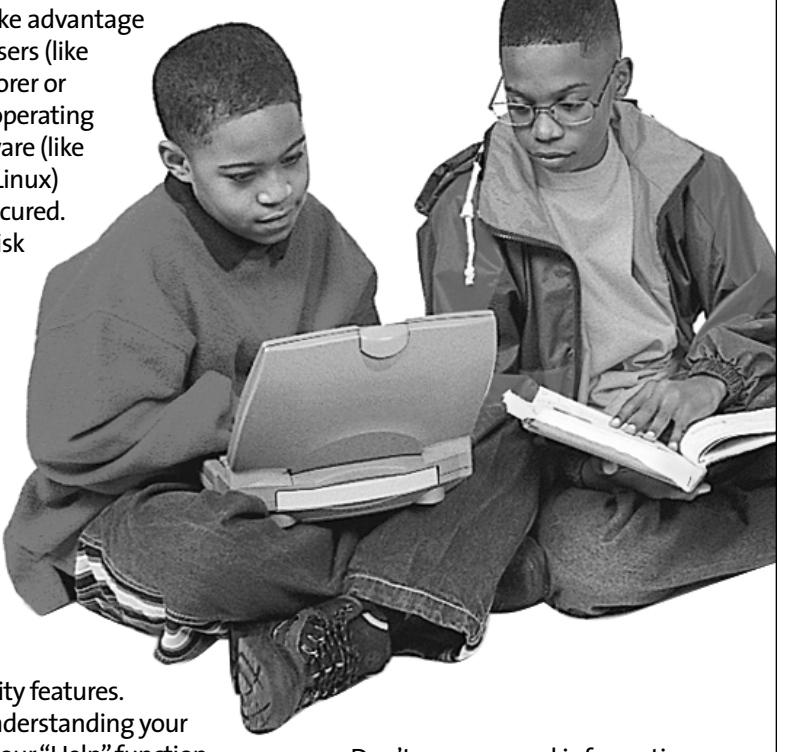


EMAIL ATTACHMENTS AND LINKS: Legitimate or virus-laden?

Most viruses sent over email or Instant Messenger won't damage your computer without your participation. For example, you would have to open an email or attachment that includes a virus or follow a link to a site that is programmed to infect your computer. That's why hackers often lie to get you to open the email attachment or click on a link. Some virus-laden emails appear to come from a friend or colleague; some have an appealing file name, like "Fwd: FUNNY". Others promise to clean a virus off your computer if you open it or follow the link.

Don't open an email or attachment – even if it appears to be from a friend or coworker – unless you are expecting it or know what it contains. You can help others trust your attachments by including a text message explaining what you're attaching.

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



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

Your operating system also may offer free software "patches" that close holes that hackers could exploit. Many popular operating systems can be set to automatically retrieve and install patches. If your system does not do this, bookmark the manufacturer's website so you can visit often and update your system with defenses against the latest attacks. 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.

5 Protect your passwords.

Keep your passwords in a secure place, and out of plain view. Don't share passwords on the Internet, over email, or on the phone. Your Internet Service Provider (ISP) should never ask for your password.

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 personal information, your login name, or adjacent keys on the keyboard as passwords.

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.

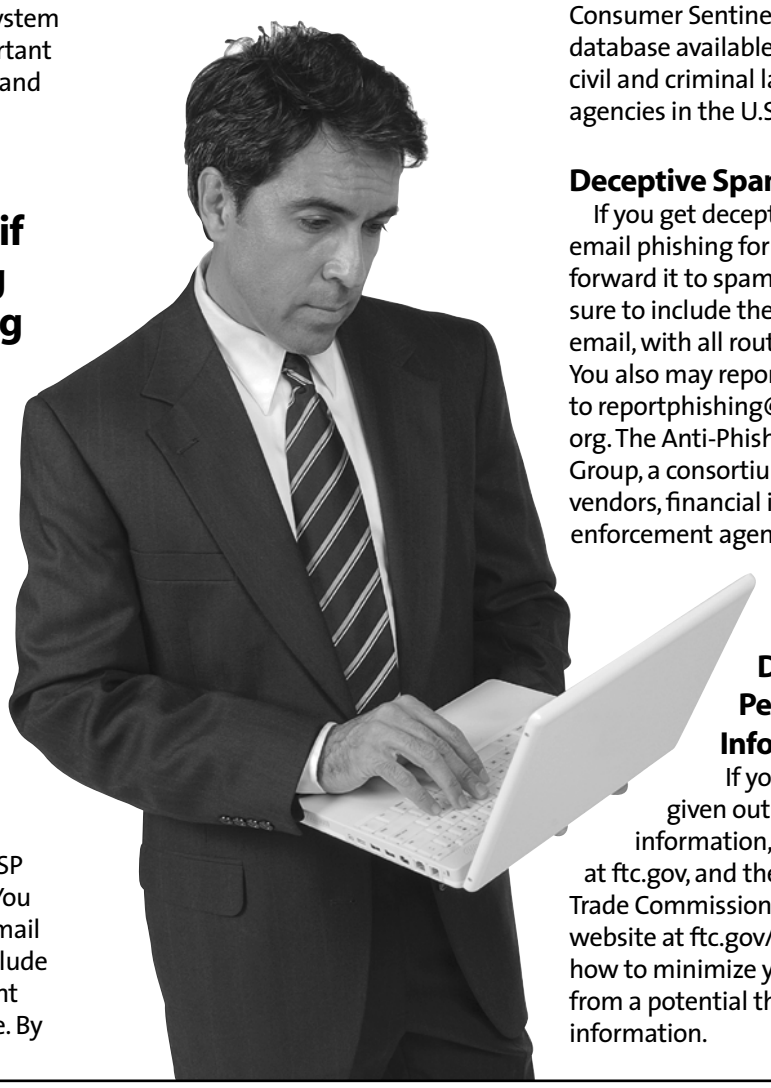
Following these tips, you're more likely to stay secure online, free of interference from hackers, viruses, and spammers. But no system is impenetrable. Copy your important files onto a disc you can remove, and store it in a safe place.

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.
- Alert the appropriate authorities. Contact:
  - Your ISP and the hacker's ISP (if you can tell what it is). You usually can 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's Internet Crime Complaint Center at 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 Consumer Sentinel, 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, with 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 have mistakenly given out personal information, 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 personal information.

You get an email that asks for your personal and financial information. What should you do?

a. Do not respond. Send the spam to the FTC at spam@uce.gov so that it can be available to law enforcement.

b. Always avoid emailing personal and financial information – like your Social Security number or account numbers.

c. a. and b.

Answer: c. If you get an unexpected email from an organization asking for your personal information, contact the organization using a telephone number you know to be genuine. Or open a new Internet browser window and type in the Web address you know is correct.

identitytheft

If your information is accidentally disclosed or deliberately stolen, take these steps quickly to minimize the potential damage from identity theft.

The bottom line for online threats like phishing, spyware, and hackers is identity theft. ID theft occurs when someone uses your name, Social Security number, credit card number or other personal information without your permission to commit fraud or other crimes.

Place a "Fraud Alert" on your credit reports, and review the reports carefully. The alert tells creditors to follow certain procedures before they open new accounts in your name or make changes to your existing accounts. The three nationwide consumer reporting companies have toll-free numbers for placing an initial 90-day fraud alert; a call to one company is sufficient:
Equifax: 1-800-525-6285
Experian: 1-888-EXPERIAN (397-3742)
TransUnion: 1-800-680-7289

Close accounts. Close any accounts that have been tampered with or established fraudulently.

- Call the security or fraud departments of each company where an account was opened or changes were made without your okay. Follow up in writing; include copies of supporting documents.
- Use the ID Theft Affidavit at ftc.gov/idtheft to support your written statement.
- Ask for verification that the disputed account has been closed and the fraudulent debts discharged.
- Keep copies of documents and records of your conversations about the theft.

File a police report. File a report with law enforcement officials to help you deal with creditors who may want proof of the crime.

Report the theft to the Federal Trade Commission. For more information, visit ftc.gov/idtheft.

SOCIAL networking sites

Safety Tips for Tweens and Teens

You've probably learned a long list of important safety and privacy lessons in your life: Look both ways before crossing the street; buckle up; don't talk to strangers; hide your diary where your nosy brother can't find it.

Add one more lesson to the list: Don't post information about yourself online that you don't want the whole world to know. The Internet is the world's biggest information exchange: many more people could see your information than you intend, including your parents, your teachers, your employer, the police – and strangers, some of whom could be dangerous.

Social networking sites have added a new factor to the "friends of friends" equation. By providing information about yourself and using blogs, chat rooms, email, or instant messaging, you can communicate, either within a limited community, or with the world at large. But while the sites can increase your circle of friends, they also can increase your exposure to people who have less-than-friendly intentions. You've heard the stories about people who were stalked by someone they met online, had their identity stolen, or had their computer hacked.

- Find out how different sites work before deciding to join. Some sites allow only a defined community of users to access posted content; others allow anyone and everyone to view postings.

- Keep some control over the information you post by restricting access to your page.

- Keep your full name, Social Security number, address, phone number, and bank or credit card account numbers to yourself. Don't post them.

- Make sure your screen name doesn't say too much about you. Even if you think it makes you anonymous, it doesn't take a genius to combine clues to figure out who you are and where you can be found.

- Post only information that you are comfortable with others seeing and knowing.

- Consider not posting your photo. It can be altered or broadcast in ways you may not be happy about.

- Flirting with strangers online could have serious consequences. Some people lie about who they really are.

- Be wary if a new friend wants to meet you in person. If you decide to meet them, meet in a public place, during the day, with friends you trust. And tell a responsible adult where you're going.

- Trust your gut if you have suspicions. If you feel threatened by someone or uncomfortable because of something online, tell an adult you trust. If threats continue, report them to the police.

For more information, visit OnGuardOnline.gov/socialnetworkingsites

True or False:

If you accidentally put something on your page that's too personal or private, you can delete it. But you won't be able to "take it back" completely.

Answer: True. Even if you delete information from your page, it may still be available in older versions of your page that exist on the computers of anyone who visited while the information was posted.

ONLINE shopping

Shopping online offers lots of benefits that you won't find shopping in a store or by mail. The Internet is always open and bargains can be numerous. With a click of a mouse, you can buy an airline ticket, book a hotel, send flowers to a friend, or buy your favorite fashions. But sizing up your finds on the Internet is a little different from checking out items at the mall.

If you're buying items online, here are ways to make the most of your shopping experience:

- **Know who you're dealing with.** Anyone can set up shop online under almost any name. Confirm the online seller's physical address and phone number in case you have questions or problems. If you get an email or pop-up message while you're browsing that asks for financial information, don't reply or click on the link in the message. Legitimate companies don't ask for this information via email.

- **Know exactly what you're buying.** Read the seller's description of the product closely, especially the fine print. Words like "refurbished," "vintage," or "close-out" may indicate that the product is in less-than-mint condition, while name-brand items with "too good to be true" prices could be counterfeits.

- **Know what it will cost.** Check out websites that offer price comparisons and then compare "apples to apples." Factor shipping and handling – along with your needs and budget – into the total cost of the order. **Do not send cash** under any circumstances.

- **Pay by credit or charge card.** If you pay by credit or charge card online, your transaction will be protected by the Fair Credit Billing Act. Under this law, you have the right to dispute charges under certain circumstances and temporarily withhold payment while the creditor is investigating them. In the event of unauthorized use of your credit or charge card, you generally would be held liable only for the first $50 in charges. Some companies offer an online shopping guarantee that ensures you will not be held responsible for any unauthorized charges made online, and some cards may provide additional warranty, return, and/or purchase protection benefits.

- **Check out the terms of the deal, like refund policies and delivery dates.** When you will receive your order? Can you return the item for a full refund if you're not satisfied? If you return it, find out who pays the shipping costs or restocking fees. A Federal Trade Commission rule requires sellers to ship items as promised or within 30 days after the order date if no specific date is promised.

- **Keep a paper trail.** Print and save records of your online transactions, including the product description and price, the online receipt, and copies of every email you send or receive from the seller. Read your credit card statements as you receive them and be on the lookout for unauthorized charges.

- **Check the privacy policy.** It should let you know what personal information the website operators are collecting, why, and how they're going to use the information. If you can't find a privacy policy – or if you can't understand it – consider taking your business to another site that's more consumer-friendly.

For more information, visit OnGuardOnline.gov/shopping

Newspaper Activities

Find articles about Internet frauds. Summarize the story by identifying the 5W's and the H (who, what, when, where, why & how) of the story. Then read commentaries in the newspaper. Using them as examples, write a brief commentary suggesting ways to stop this type of crime and how perpetrators should be punished.

Find positive stories about use of the Internet by the government, non-profits or other organizations. How was the Internet used? What were the positive results?

Look at ads in the newspaper. Do most companies now have web addresses in their ads? What might be the reasons for them to display their URL? How might that help you as a consumer?

Find stories about social networking sites, chat rooms, or other Internet stories featuring young people. What are the issues being addressed? Are there concerns or bad outcomes because of how the Internet what used? Are there lessons to be learned about Internet safety, what are they?

True or False:

Online sellers must ship items as promised or within 30 days after your order is placed if no date is promised.

Answer: True. The FTC states that a company should ship your order within the time stated in its advertisements. If no time is promised, the company should ship your order within 30 days after receiving it. If the company is unable to ship within the promised time, they must give you an option notice, giving you the choice of agreeing to the delay or canceling your order and receiving a prompt refund. One exception to the 30-day rule: If a company doesn't promise a shipping time, and you're applying for credit to pay for your purchase, the company has 50 days to ship after receiving your order.

Some email users have lost money to bogus offers that started as spam in their in-box. Con artists are very cunning; they know how to make their claims seem legitimate. Some spam messages ask for your business, others invite you to a website with a detailed pitch.

Here are some basic tips to help you avoid being a victim of a scam:

- Protect your personal information. Share credit card or other personal information only when you're buying from a company you know and trust.
- Know who you're dealing with. Don't do business with any company that won't provide its name, street address, and telephone number.
- Take your time. Resist any urge to "act now" despite the offer and the terms. Once you turn over your money, you may never get it back.
- Read the small print. Get all promises in writing and review them carefully before you make a payment or sign a contract.
- Never pay for a "free" gift. Disregard any offer that asks you to pay for a gift or prize. If it's free or a gift, you shouldn't have to pay for it. Free means free.

FILTER TIPS: SCAMS TO SCREEN FROM YOUR EMAIL

While some consumers find spam informative, others find it annoying and time consuming. Still others find it expensive: They're among the people who have lost money to spam that contained bogus offers and fraudulent promotions.

Many Internet Service Providers and businesses offer filtering software to limit the spam in their users' email in-boxes. In addition, some old-fashioned 'filter tips' can help you save time and money by avoiding frauds pitched in email. When you screen spam for scams, send unwanted spam on to the appropriate enforcement authorities, and then hit delete. Here's how to spot some common spam scams:

Work-at-Home Scams

The Bait: Advertisements that promise steady income for minimal labor – in medical claims processing, envelope-stuffing, craft assembly work, or other jobs. The ads use similar come-ons: Fast cash. Minimal work. No risk. And the advantage of working from home when it's convenient for you.

The Catch: The ads don't say you may have to work many hours without pay, or pay hidden costs to place newspaper ads, make photocopies, or buy supplies, software, or equipment to do the job. Once you put in your own time and money, you're likely to find promoters who refuse to pay you, claiming that your work isn't up to their "quality standards."

Your Safety Net: The FTC has yet to find anyone who has gotten rich stuffing envelopes or assembling magnets at home. Legitimate work-at-home business promoters should tell you – in writing – exactly what's involved in the program they're selling. Before you commit any money, find out what tasks you will have to perform, whether you will be paid a salary or work on commission, who will pay you, when you will get your first paycheck, the total cost of the program – including supplies, equipment and membership fees – and what you will get for your money. Can you verify information from current workers? Be aware of "shills" – people who are paid to lie and give you every reason to pay for work. Get professional advice from a lawyer, an accountant, a financial advisor, or another expert if you need it.

Weight Loss Claims

The Bait: Emails promising a revolutionary pill, patch, cream, or other product that will result in weight loss without diet or exercise. Some products claim to block the absorption of fat, carbs, or calories; others guarantee permanent weight loss; still others suggest you'll lose lots of weight at lightening speed.

The Catch: These are gimmicks, playing on your sense of hopefulness. There's nothing advertised through email you can wear or apply to your skin that can cause permanent – or even significant – weight loss.

Your Safety Net: Experts agree that the best way to lose weight is to eat fewer calories and increase your physical activity so you burn more energy. A reasonable goal is to lose about a pound a week. For most people, that means cutting about 500 calories a day from your diet, eating a variety of nutritious foods, and exercising regularly. Permanent weight loss happens with permanent lifestyle changes. Talk to your health care provider about a nutrition and exercise program suited to your lifestyle and metabolism.

Cure-All Products

The Bait: Emails claiming that a product is a "miracle cure," a "scientific breakthrough," an "ancient remedy" – or a quick and effective cure for a wide variety of ailments or diseases. They may announce limited availability, require payment in advance, and offer a no-risk "money-back guarantee." Case histories or testimonials by consumers or doctors claiming amazing results are not uncommon.

The Catch: There is no product or dietary supplement available via email that can make good on its claims to shrink tumors, cure insomnia, cure impotency, cure cancer, and prevent severe memory loss. These kinds of claims deal with the treatment of diseases; companies that want to make claims like these must follow the FDA's pre-market testing and review process required for new drugs.

Your Safety Net: When evaluating health-related claims, be skeptical. Consult a health care professional before buying any "cure-all" that claims to treat a wide range of ailments or offers quick cures and easy solutions to serious illnesses. Generally speaking, cure-all is cure none.

Check Overpayment Scams

The Bait: A response to your ad or online auction posting, offering to pay with a cashier's, personal, or corporate check. At the last minute, the so-called buyer (or the buyer's "agent") comes up with a reason for writing the check for more than the purchase price, and asks you to wire back the difference after you deposit the check.

The Catch: If you deposit the check, you lose. Typically, the checks are counterfeit, but they're good enough to fool unsuspecting bank tellers; when they bounce, you are liable for the entire amount, even if the check had cleared.

Your Safety Net: Don't accept a check for more than your selling price, no matter how tempting the plea or convincing the story. Ask the buyer to write the check for the purchase price. If the buyer sends the incorrect amount, return the check. Don't send the merchandise. As a seller who accepts payment by check, you may ask for a check drawn on a local bank, or a bank with a local branch. That way, you can visit personally to make sure the check is valid. If that's not possible, call the bank the check was drawn on using the phone number from directory assistance or an Internet site that you know and trust, not from the person who gave you the check. Ask if the check is valid. Forward check overpayment scams to spam@uce.gov and your state Attorney General. You can find contact information for your state Attorney General at naag.org. For more information, visit OnGuardOnline.gov/spam.

FIGHTING BACK

Con artists are clever and cunning, constantly hatching new variations on age-old scams. Still, skeptical consumers can spot questionable or unsavory promotions in email offers. Should you receive an email that you think may be fraudulent, forward it to the FTC at spam@uce.gov, hit delete, and smile. You'll be doing your part to help put a scam artist out of work.

An online ad promises good money for working a few hours a day at home. For a "small" fee, you'll find out how to earn money stuffing envelopes. The ad might not say:

a. You might have to work many hours without pay.
b. You may have to pay for your own supplies.
c. There might NOT be any customers willing to pay for your service.
d. All of the above.

Answer: d. We don't know of anyone who has gotten rich stuffing envelopes at home. Check out ftc.gov/workathome for more information.

Newspaper activity:
Find stories in the newspaper about the FTC or other federal, state or local consumer agencies. How are these agencies helping consumers deal with various issues of fraud? Are new rules or laws being enacted to help consumers? What do you think should be done?

Answer: True. Credit cards allow buyers to seek a credit from the credit card issuer if the item isn't delivered or isn't what they ordered. Some online payment services also offer protections, but you should read each service's terms of agreement before you use it. With other kinds of payments – like money wiring services, or even a check – you'll have no recourse if there's a problem.

True or False:
It's a good idea to use a credit card when paying for items on an Internet auction.

Internet auctions

Internet auction sites give buyers a "virtual" flea market with new and used merchandise from around the world; they give sellers a global storefront from which to market their goods. But the online auction business can be risky business.

OnGuard Online wants to help buyers and sellers stay safe on auction websites. Among the thousands of consumer fraud complaints the FTC receives every year, those dealing with online auction fraud consistently rank near the top of the list. The complaints generally deal with late shipments, no shipments, or shipments of products that aren't the same quality as advertised; bogus online payment or escrow services; and fraudulent dealers who lure bidders from legitimate auction sites with seemingly better deals. Most complaints involve sellers, but in some cases, the buyers are the subject.

Thinking of bidding in an online auction, or selling some of your stuff? Internet auctions are a great resource for shoppers and sellers, but you need to watch out for some pitfalls.

Here's how:

- Evaluate how soon you need to receive the item you're bidding on, and whether you can tolerate it being delivered late, or even not delivered. Many complaints about Internet auction fraud involve late shipments, no shipments, or shipments of products that aren't the same quality as advertised.
- Carefully consider your method of payment. Learn what recourse you have if something goes wrong. Don't send cash, and don't use a money wiring service.
- Whether you're a buyer or a seller, read each auction site's Terms of Use before using it for the first time – sites may charge fees, follow different rules, or offer different protections.
- Know exactly what you're bidding on. Read and print a copy of the seller's description of the product, especially the fine print. Save copies of all emails you send and receive from the auction site or seller, too.
- Know who you're dealing with. Avoid doing business with sellers you can't identify, especially those who try to lure you off the auction site with promises of a better deal. Confirm the seller's telephone number in case you have questions or problems.
- Don't reply to "phishing" emails. Delete messages that look like they've been sent by an auction website or payment service and ask for your password or other personal information.
- Watch out for fake check scams. If a "buyer" sends you a check for more than your agreed-upon price, don't ship the item you are selling, don't cash the check, and don't send the "buyer" any money. It's almost certainly a scam.

If you have problems during a transaction, try to work them out directly with the seller, buyer, or site operator. If that doesn't work, file a complaint with:

- The attorney general's office in your state;
- Your county or state consumer protection agency (check the blue pages of the phone book under county or state government);
- The Better Business Bureau; and
- The Federal Trade Commission. File a complaint online at ftc.gov.

For more information, visit OnGuardOnline.gov/auctions

wireless security

Increasingly, computer users interested in convenience and mobility are accessing the Internet wirelessly. Today, business travelers use wireless laptops to stay in touch with the home office; vacationers beam snapshots to friends while still on holiday; and shoppers place orders from the comfort of their couches. A wireless network can connect computers in different parts of your home or school without a tangle of cords, and enable you to work on a laptop anywhere within the network's range.

Going wireless generally requires a broadband Internet connection into your home, called an "access point," like a cable or DSL line that runs into a modem. To set up the wireless network, you connect the access point to a wireless router that broadcasts a signal through the air, sometimes as far as several hundred feet. Any computer within range that's equipped with a wireless client card can pull the signal from the air and gain access to the Internet.

The downside of a wireless network is that, unless you take certain precautions, anyone with a wireless-ready computer can use your network. That means your neighbors, or even hackers lurking nearby, could "piggyback" on your network, or even access the information on your computer. And if an unauthorized person uses your network to commit a crime or send spam, the activity can be traced back to your account. Here's how you can protect your wireless network and the computers on it.

1. Use encryption. The most effective way to secure your wireless network from intruders is to encrypt, or scramble, communications over the network. Most wireless routers, access points, and base stations have a built-in encryption mechanism. If your wireless router doesn't have an encryption feature, consider getting one that does.

Manufacturers often deliver wireless routers with the encryption feature turned off. You must turn it on. The directions that come with your wireless router should explain how to do that. If they don't, check the router manufacturer's website.

Two main types of encryption are available: Wi-Fi Protected Access (WPA) and Wired Equivalent Privacy (WEP). Your computer, router, and other equipment must use the same encryption. WPA is stronger; use it if you have a choice. It should protect you against most hackers.

Some older routers use only WEP encryption, which is better than no encryption. It should protect your wireless network against accidental intrusions by neighbors or attacks by less sophisticated hackers. If you use WEP encryption, set it to the highest security level available.

2. Use anti-virus and anti-spyware software, and a firewall.

3. Most wireless routers have a mechanism called identifier broadcasting. Turn it off so your computer won't send a signal to any device in the vicinity announcing its presence.

4. Change the identifier on your router from the default. The identifier for your router is likely to be a standard, default ID assigned by the manufacturer to all hardware of that model. Even if your router is not broadcasting its identifier to the world, hackers know the default IDs and can use them to try to access your network. Change your identifier to something only you know, and remember to configure the same unique ID into your wireless router and your computer so they can communicate. Use a password that's at least 10 characters long. Again, the longer your password, the harder it is for hackers to break.

5. Change your router's pre-set password for administration to something only you know. The longer the password, the tougher it is to crack.

6. Allow only specific computers to access your wireless network. Every computer that is able to communicate with a network is assigned its own unique Media Access Control (MAC) address. Wireless routers usually have a mechanism to allow only devices with particular MAC addresses access to the network. Some hackers have mimicked MAC addresses; so don't rely on this step alone.

7. Turn off your wireless network when you know you won't use it.

8. Don't assume that public "hot spots" are secure. Assume that other people can access any information you see or send over a public wireless network.

For more information, visit OnGuardOnline.gov/wireless

True or False:

You can set your wireless router to only allow certain computers access to your network.

Answer: True. All modern computers have their own unique MAC addresses, so you should be able to set your router to allow only computers you know to use your network. But be forewarned – some hackers have "spoofed" MAC addresses, so this step alone is not enough to secure your wireless network.

ONLINE-SPEAK

Learning the Language

You don't have to be a computer expert to go online, but it certainly helps to know the language. The Federal Trade Commission has prepared this glossary to help you better understand techno terms.

Adware: A type of software that often comes with free downloads. Some adware displays ads on your computer, while some monitors your computer use (including websites visited) and displays targeted ads based on your use.

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.

Bandwidth: A measure of the "speed" of an Internet connection.

Biz Opps: Shorthand for "business opportunity;" some schemes involve extravagant and unfounded earnings claims and are actually fraudulent business ventures.

Blocking Software: Computer programs that filter content from the Internet and block access to some websites or content based on specified criteria.

Blog: Short for Web log. A blog is a website to which one or more people post their personal observations on particular subjects.

Bookmark: A Web browser feature that allows you to save the addresses of interesting or frequently used websites, so that you can readily revisit them.

Browser: A program that allows a user to find, view, hear, and interact with material on the Internet.

Browser Hijacker: A common spyware program that changes your Web browser's home page automatically, even if you change it back.

Cache: A form of computer memory that allows you to access stored information, such as Web addresses you've recently typed into your browser, more quickly. Pronounced, "cash."

CAN-SPAM Act: A law that prohibits senders of unsolicited commercial email from using false or misleading header information or deceptive subject lines, and requires them to identify each email as an advertisement, among other provisions.

Chat Room: The name given to a place or page in a website or online service where people can type messages that are displayed almost instantly on the screens of others who are in the "chat room."

Cookies: A small text file that a website can place on your computer's hard drive to collect information about your activities on the site or to allow other capabilities on the site.

Cyberspace: Used to distinguish the physical world from the digital, or computer-based, world.

Domain: A segment of Internet space, denoted by the function or type of information it includes; current domains include ".com" for commercial sites, ".gov" for government ones, and ".org" for non-commercial organizations.

Download: To copy files from one computer to another.

Drive-by Download: Software that installs on your computer without your knowledge when you visit certain websites. To avoid drive-by downloads, make sure to update your operating system and Web browser regularly.

DSL(Digital Subscriber Line): A means of accessing the Internet at high speed using standard phone lines.

Encryption: The scrambling of data into a secret code that can be read only by software set to decode the information.

End User Licensing Agreement (EULA): A provider's legal terms. You, as the "end user," may be required to "click" to accept before you can download software.

Exposure: When sensitive data is released to someone without authorization.

Extended Service Set Identifier (ESSID): The name a manufacturer assigns to a router. It may be a standard, default name assigned by the manufacturer to all hardware of that model. Users can improve security by changing to a unique name. Similar to a Service Set Identifier (SSID).

Filter: Software that screens information on the Internet, classifies its content, and allows the user to block certain kinds of content.

File Sharing: Accessing files on one computer from another computer.

Firewall: Hardware or software that helps keep hackers from using your computer to send out your personal information without your permission. Firewalls watch for outside attempts to access your system and block communications to and from sources you don't permit.

Gigabyte: A measure of computer memory equaling 1,024 megabytes.

Hacker: Someone who uses the Internet to access computers without permission.

Hardware: The mechanical parts of a computer system, including the central processing unit, monitor, keyboard, and mouse, as well as other equipment like printers and speakers.

Hypertext Markup Language (HTML): A coding language used to create documents on the Internet and control how Web pages appear.

Hidden Dialers: Programs that you may unknowingly download that can use your computer to silently dial expensive phone calls, which later show up on your phone bill.

HTTP (Hypertext Transfer Protocol): The standard language that computers connected to the World Wide Web use to communicate with each other.

Instant Message (IM): Technology, similar to a chat room, which notifies a user when a friend is online, allowing them to "converse" by exchanging text messages.

Internet Protocol (IP): The computer language that allows computer programs to communicate over the Internet.

IP Address: A computer's "address," it consists of a series of numbers separated by periods.

ISP (Internet Service Provider): A company that sells direct access to the Internet.

Java: A computer programming language that enables Web pages to include animations, calculators, scrolling text, sound effects, and games.

JPEG: Shorthand for "Joint Photographic Experts Group," a computer file format that reduces the size of graphics by using compression.

Keystroke Logger: A device or program that records each keystroke typed on a particular computer.

LAN (Local Area Network): A network of connected computers that are generally located near each other, such as in an office or school.

Media Access Control (MAC) Address: A unique number that the manufacturer assigns to each computer or other device in a network.

Monitoring Software: Programs that allow a parent or caregiver to monitor the websites a child visits or email messages he or she reads, without blocking access.

Netiquette: The informal rules of Internet courtesy, enforced exclusively by other Internet users.

Network: A group of two or more computers that are able to communicate with one another.

Online Profiling: Compiling information about consumers' preferences and interests by tracking their online movements and actions to create targeted ads.

Operating System: The main program that runs on a computer. An operating system allows other software to run and prevents unauthorized users from accessing the system. Major operating systems include UNIX, Windows, MacOS, and Linux.

Opt-in: When a user explicitly permits a website to collect, use, or share his or her information.

Opt-out: When a user expressly requests that his or her information not be collected, used and/or shared. Sometimes a user's failure to "opt-out" is interpreted as "opting in."

P2P, Peer-to-Peer: An informal network that allows users to share music, games, software, or other files with other users online.

Parental Controls: Tools that allow parents to prevent their children from accessing certain Internet content they might find inappropriate.

Patches/ Software Patches: Software updates that fix a particular problem or vulnerability within a program.

Personal Information: Information that can identify you, like your bank and credit card account numbers; your income; your Social Security number; or your name, address, and phone numbers.

Pharming: Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing.

Phishing: A scam that involves Internet fraudsters who send spam or pop-up messages to lure personal information (credit card numbers, bank account information, Social Security number, passwords, or other sensitive information) from unsuspecting victims.

Pop-up Messages or Ads: Unsolicited advertising that appears as its own browser window.

RAM: Shorthand for "Random Access Memory," it's the hardware inside your computer that retains memory on a short-term basis and stores information while you work.

Router: A device that connects two or more networks. A router finds the best path for forwarding information across the networks.

Secure Socket Layer (SSL): A protocol used to transmit sensitive data, like credit card information, securely via the Internet.

Social Networking Sites: Websites that allow users to build online profiles; share information, including personal information, photographs, blog entries, and music clips; and connect with other users.

Sock Puppet: A secret alias used by a member of an Internet community, but not acknowledged by that person.

Software: A computer program with instructions that enable the computer hardware to work. System software – such as Windows or MacOS – operates the machine itself, and application software – such as spreadsheet or word processing programs – provides specific functionality.

Spam: Unsolicited commercial email, often sent in bulk.

Spam Zombies: Home computers that have been taken over by spammers who then use them to send spam in a way that hides the true origin.

Spammer: Someone who sends unsolicited commercial email, often in bulk.

Spoofing: Forging an e-mail header or Web addresses to make it appear as if the message or website came from somewhere or someone other than the actual source.

Spyware: A software program that may be installed on your computer without your consent to monitor your use, send pop-up ads, redirect your computer to certain websites, or record keystrokes, which could lead to identity theft.

Trojans: Programs that, when installed on your computer, enable unauthorized people to access it and sometimes to send spam from it.

Upload: To copy or send files or data from one computer to another.

URL (Uniform Resource Locator): The address for a webpage, such as www.ftc.gov.

Virus: A program that can sneak onto your computer – often through an email attachment – and then make copies of itself, quickly using up all available memory.

VoIP (Voice Over Internet Protocol): A category of hardware and software that lets you use the Internet as the transmission medium for telephone calls.

Wi-Fi Protected Access (WPA): A security protocol developed to fix flaws in WEP. Encrypts data sent to and from wireless devices within a network.

Wired Equivalent Privacy (WEP): A security protocol that encrypts data sent to and from wireless devices within a network. Not as strong as WPA encryption.

Wireless Network: A method of connecting a computer to other computers or to the Internet without cables.

World Wide Web: An Internet system, which distributes graphical, hyperlinked information through a browser.

Worm: A program that reproduces itself over a network and can use up your computer's resources and possibly shut your system down.

Zombies: Home computers that have been taken over by spammers, who then use them to send spam in a way that hides the true origin.

Visit **www.OnGuardOnline.gov/quiz**
to test your knowledge about safe computing.