



Internet Safety Trainer's Manual

QUESTIONS AND ANSWERS ABOUT PROTECTING YOUR
PRIVACY AND SECURITY ON THE COMPUTER

A Consumer Action Publication

TABLE OF CONTENTS

<i>Page 1</i>	Introduction Potential Risks for Internet Users
<i>Page 4</i>	Protecting Your Computer and Data
<i>Page 8</i>	Protecting Your Privacy from Online Marketers
<i>Page 10</i>	Protecting Your Kids Online
<i>Page 11</i>	Tips and Tools
<i>Page 13</i>	Assistance and Information

Introduction

People of all ages and backgrounds use personal computers and Internet-enabled devices to be more productive at work, surf the Web, and stay in touch with friends and family. Being online has become such a part of daily life for most people that it can be easy to forget the risks associated with the enjoyment and convenience. While there have been great advances in computer and Internet security, scam artists, hackers and stalkers still find ways to reach vulnerable targets. The Internet Crime Complaint Center (IC3) reported that there were 275,000 complaints and \$265 million in losses from Internet scams in 2008, a jump from the previous year. Many people could avoid becoming victims by taking simple but effective precautions and avoiding unnecessary risks.

The “Internet Safety Trainer’s Manual” can help answer many questions about how to keep children, computer data and personal information safer and more secure. This publication is part of an educational module that includes a multilingual brochure, “Internet Safety: A computer user’s guide to privacy and security” (available in Chinese, English, Korean, Spanish and Vietnamese); a training guide for classes and seminars; PowerPoint slides; and class activities.

This Consumer Action module is free for individuals, nonprofits and community-based organizations. To learn more about our training modules, visit Consumer Action’s website (www.consumer-action.org/modules). See the back of this booklet for more ways to contact Consumer Action.

Potential Risks for Internet Users

What are some of the risks that Internet users face?

The main risks Internet users face include:

- ✓ Inappropriate or unwanted contact (cyberbullying and spamming, for example)
- ✓ Inappropriate or inaccurate content (pornography and hate sites, for example)
- ✓ Deceptive or fraudulent commerce (counterfeit and malicious sites, for example)

How do crooks and con artists find their victims online?

Crooks and scammers have many ways to find their potential victims, and they’re

constantly coming up with new ones. Beware of:

- ✓ **Phishing**—an attempt to “hook” you into revealing your personal and confidential information by sending emails that seem to come from a legitimate business.
- ✓ **Spam**—unwelcome email and instant messages, which may offer goods of no or little value or a promise of financial rewards if you give the sender money.
- ✓ **Malware**—malicious software (spyware, Trojans, viruses and worms) that can be remotely installed on your computer, making it possible for the person who controls the malicious software to steal, damage or delete your files and other data.
- ✓ **Malicious websites**—harmful sites that lure users by promising content on popular breaking news stories, offers from retailers or other desired information. Links to such sites can appear among online search results or can be sent to you via email or on social network pages (such as Facebook or MySpace, etc.).
- ✓ **Transactions that are not secure**—sites that don’t have secure payment forms or companies that store debit and credit card information without proper safeguards may give crooks the opportunity to intercept your personal information.
- ✓ **Social networking**—users who reveal too much personal information in their online profiles or who arrange to meet online contacts in person may be at risk; or the sites may compromise your personal information.

What does a phishing email look like?

Typically, a phishing email appears to come from a financial institution, a large company, a chain store, a social networking site, or a government agency. The messages try to mimic a legitimate site by using the same or similar colors, logos, fonts and layout. And they often include a link to a legitimate-looking but phony Web page that asks you to enter personal information.

One tip-off that an email may be phishing is the use of phrases such as “Verify your account” and “Your account will be closed” if you don’t provide certain sensitive information such as login name and password. A legitimate business will never ask for such personal information via email.

Promising big lottery winnings, prizes or other type of windfall if you pay money upfront is another common phishing scam.

Misspellings, bad grammar, incorrect punctuation and awkward language—things you wouldn't expect in a legitimate email message from a business or organization—are a tip-off that the message is phony.

The best advice is to trust your instincts. Always contact the financial institutions and other companies you do business with directly, by phone or by typing the company's URL (Web address) into your browser. Look for legitimate phone numbers on your billing statement or phone directory. And remember, if something appears too good to be true, it probably is.

What should I do if I suspect an email message I receive is a phishing attempt?

Do not reply to the email. Forward the message to your Internet service provider (ISP), contact the company the email claims to be from, and file a complaint with the Federal Trade Commission (FTC) at www.onguardonline.gov. Large companies often have special "abuse" email addresses you can forward the email to, such as abuse@companyname.com.

What if I have already responded and fear I may be a victim of identity theft?

Immediately change the passwords on your online accounts, and notify the fraud department at the institution that was mimicked. Request your credit report from the three main credit reporting agencies: Equifax, Experian and TransUnion (Equifax.com or 800-525-6285; Experian.com or 888-397-3742; TransUnion.com or 800-680-7289). The reports are free to victims of identity theft. You can also request free reports from all three agencies at www.AnnualCreditReport.com.

When you receive your credit reports, review them carefully for accounts you don't recognize, which may be signs of identity theft. Consider placing a security freeze on each report, which means that no new credit can be extended without your personal approval.

What's the difference between a virus, a worm, a Trojan and spyware?

All these types of malicious software, or malware, pose a serious threat to your computer and data.

- ✓ A virus invades a computer and copies, deletes or damages data.
- ✓ A worm is a virus that reproduces itself and spreads to other computers.

- ✓ A Trojan (short for Trojan horse) is a virus that, despite appearing to be good or helpful, actually destroys your data, damages your computer, and steals your personal information.
- ✓ Spyware is software that tracks your online activity, can launch numerous pop-up ads, and may steal your personal information or change your computer settings without your knowing.

How can I avoid malicious websites?

Never click on, or copy and paste, links that are sent to you by people or companies you don't know. If you want to verify that the site is legitimate, type (don't copy) the homepage portion of the URL (ending with .com or .net, etc.) directly into your browser address bar. When doing an online search, visit only results that are well known and trusted sources of information.

Protecting Your Computer and Data

Why would someone want to steal or damage the data on my computer?

Some people commit malicious acts with no other goal than to create problems for others. Theft, on the other hand, generally has the goal of financial gain through the use of the stolen information.

What can I do to protect myself?

There are many practices and tools that will help you protect your computer and data.

- ✓ Use a firewall.
- ✓ Install antivirus software.
- ✓ Install antispyware.
- ✓ Use a spam filter.
- ✓ Perform timely updates.
- ✓ Create strong passwords.
- ✓ Secure your wireless network.

What is a firewall?

A firewall is a virtual barrier between your computer and the Internet. Everything coming into or leaving your computer must go through the firewall, which blocks anything that doesn't meet specific security criteria.

Before purchasing separate firewall hardware or software, check your operating system (OS) (Mac OS X and Windows 8, for example) to locate the built-in firewall and determine whether it's turned on.

What is antivirus software?

Antivirus software scans everything that goes into your computer, looking for known viruses. Because new viruses are created all the time, you have to update your antivirus software regularly. You can subscribe to virus protection software that automatically installs updates to your computer as they become available.

What is antispyware?

Spyware is software that tracks your computer activity, gathering information without your knowing it. Antispyware is software that blocks or removes spyware. Some virus protection products include antispyware features. Like antivirus software, antispyware needs to be updated regularly.

How does a spam filter work?

Most ISPs and email programs now include an automatic spam filter, which reduces the number of unwelcome email messages that make it to your inbox. Delete, without opening, any spam or "junk mail" that gets through the filter. Check your "junk mail" folder on a regular basis to make sure that emails you want to see are not being flagged as junk. You can also add the email addresses of people and companies you want to hear from to your address books, which may save them from being flagged as junk.

What does it mean to "update" my computer and software?

Computer and software companies frequently update their programs to include protection against the newest security threats. So, simply updating your operating system and software whenever new versions become available gives you an added measure of security. If available, activate automatic updates so you will be alerted when updates are

issued. Updates sometimes slow your computer down, so set your computer to update at times you are not using it.

What makes a password strong?

A strong password includes a seemingly random string of letters, numbers and symbols. It should never include personal information such as your birth date, address or pet's name. The longer your password is, the harder it is to decipher. Try for least eight characters, including upper and lowercase letters, numbers and symbols, if allowed.

What is a wireless network, and how do I make mine secure?

A wireless network (wi-fi) is a common way for computer users to access the Internet at home or work using radio waves rather than cables to transmit data. Leaving your network "unlocked" means that anyone within range of your wi-fi signal can access it—and possibly capture the data you send and receive. Securing your wireless network can be as simple as creating a strong password for your router and enabling its built-in encryption tool. When you buy a router, it comes with instructions for accessing security settings. This generally requires you to type an Internet Protocol (IP) number into your Web browser address bar. This allows you to get inside your router, choose a replacement for the default password that comes from the manufacturer and ensure that you have a secure connection.

What precautions should I take when using public wi-fi?

Today most laptops have the ability to connect to wireless Internet networks (wi-fi). These can be found in public places such as coffee shops, airports, hotels, etc. Be cautious about entering personal information on a website when using public wi-fi. Avoid entering credit card numbers, bank account numbers or passwords while using public wi-fi. If you must enter a password or payment card number while using a public wireless network, make sure the Web address begins with https: (the "s" stands for secure). Turn off your wireless connection when you're not using it.

Is it safe to use the Internet at my local library?

If you follow some basic guidelines, you can use your library's computers without compromising your safety or privacy:

- ✓ Never save your log-on information to websites on a public computer. When you visit sites that require a password, always log out by clicking “log out” or “sign out” on the site when you are done.
- ✓ Many browsers allow you to surf the Web “in private.” This means you can browse the Internet without the computer saving any data about which sites you have visited. Use your browser’s Help function to find out how to use private—or “incognito”—browsing.
- ✓ When you step away, or leave the public computer, log out of all programs and close all windows that might display sensitive information.
- ✓ If possible, disable the feature that stores passwords. Read the Help section of the browser (Internet Explorer, Firefox, Safari, Chrome, etc.) for more information.
- ✓ Don’t enter your credit card or bank account number or other sensitive information into any public computer.

Is it safe to send sensitive data via email or instant messaging (IM)?

No, you shouldn’t send sensitive personal information like credit card numbers, passwords, your date of birth or Social Security number using email or IM on your computer or any other Web-enabled devices such as a smartphone, tablet or personal digital assistant (PDA).

I’m having trouble updating my old computer. Why?

If you have an older computer, you may no longer receive updates and security “patches,” and the manufacturer probably does not offer support for your computer. New versions of browsers have important security features that may not run on older operating systems. Firewalls, a relatively new technology, are activated by default by the manufacturer on newer computers, and may be turned off on older machines. Older computers connected to “always on” high-speed Internet may be at risk for security and privacy breaches.

The good news is, over the past four or five years, computers have dropped in price so that a new—and more powerful—computer can be purchased for around \$400.

Protecting Your Privacy from Online Marketers

Why should I care about reducing my exposure to online marketers?

Unwanted marketing messages can be a nuisance and even, in some cases, an invasion of your privacy. Parents of children and teens should be vigilant about websites that market to youngsters, because young people are more susceptible to certain kinds of marketing than previously believed. Marketers can easily exploit young people by inducing them to desire things that are not in their best interest.

How do online marketers get my information?

Anytime you fill out a form, enter an online contest, or otherwise submit information electronically there is the potential it will be used for marketing purposes—by the company whose site you are visiting, or by a third party that buys the information. Personal information is the currency we provide to access free Web services, join social networks, play online games and visit virtual worlds.

How do I know if a site will use my information for marketing purposes?

Read the “Privacy Policy” for sites you interact with to learn how they could use your information and whether or not they will sell or trade your contact information.

What is a privacy policy, and where do I find it?

Legitimate companies will have a privacy policy that clearly states when and how the company might use your information. Leave the site if you are not satisfied that your privacy will be protected.

There should be a link to the privacy policy somewhere on the site’s homepage, or you may be able to reach it through a general information page such as “About Us.” If the site allows searching, enter “privacy policy” in the search box.

Look for “trust mark” logos on the site, such as TRUSTe and BBBOnline, that certify trustworthy privacy policies.

How can I avoid online marketers?

The best way to reduce the amount of online marketing you’re subjected to is by guarding your personal information while on the Web. In other words, reveal as little as

possible about yourself at unfamiliar sites until you have decided you want to establish a relationship. And always ignore and delete spam completely. Do not respond, even to unsubscribe, because your response confirms that the address is “live.”

Consider getting an alternate email address that you use for certain online activities. This will help keep your regular email inbox as clear of unwanted messages as possible. There are many free email services to choose from.

You may also want to manage your cookies (*see next question*).

What are cookies, and what do they do?

A cookie is a piece of information stored on an Internet user’s computer by a Web browser. It allows the site being visited to record such things as the visitor’s shopping cart contents and user preferences. Cookies also are used to target a company’s marketing efforts. “Behavioral targeting” involves monitoring computer users’ online habits and directing ads to them based on that information.

Pop-up ads and banners sponsored by third parties often use cookies as well. If you want to limit the marketing messages you receive, think twice before clicking these. To get rid of a pop-up ad, click the X in the upper-right corner of the window or press ALT+F4 on your keyboard.

Most modern browsers give users the option to accept or reject cookies. Rejecting cookies may seem like a good way to further protect your privacy, but some websites won’t work if cookies are disabled. You can also set your browser preferences so that cookies are deleted whenever you exit the browser. This means the site will not retain any of your information or recognize you as a returning visitor.

Can companies and marketers collect data from my children?

The Children’s Online Privacy Protection Act [COPPA] requires sites to obtain parental consent for the collection or use of any personal information from children under 13. Still, instruct your children not to reveal private information at websites they visit, and monitor Web activity by teens, who may be susceptible to activities that are not in their best interest.

Protecting Your Kids Online

Should I be worried about my children and teens using the Internet?

You shouldn't be worried, but you should be cautious. Here are some tips:

- ✓ **Discuss** the various risks of Internet use.
- ✓ **Set** clear rules about what your kids can do and which websites they can visit. Consider writing out the rules and posting them near the computer. (SafeKids.com offers a 10-point list of online safety rules for kids that you can print out. Go to www.safekids.com/kids-rules-for-online-safety.)
- ✓ **Manage** and monitor their online activities—there are tools to help you with this.
- ✓ **Read** your child's favorite blogs (short for weblog), and become a "friend" on your child's social networking sites.
- ✓ **Discuss** what information is appropriate to share and what should be kept private.
- ✓ **Establish** that it is never okay to go alone to see someone they "meet" on the Internet.
- ✓ **Let them know** it's not okay to share their passwords for social networking and other sites with friends. Accounts can be compromised and personal information stolen.
- ✓ **Keep** the lines of communication open. Encourage children to share their questions and online experiences with you. Make sure they understand that you will not punish them or take away Internet access if they let you know about any threatening or inappropriate communication, including bullying.
- ✓ **Explain** why it's wrong to bully others.

What kind of tools are available to help keep my children safe online?

Special software designed to manage Internet use can help you keep your children and teens safer. Most operating systems also include settings you can use to keep your kids safe online. Learn about family safety tools at kids.getnetwise.org/tools.

What should I do if my child is being harassed or stalked online?

Report "cyber-bullying," harassment and predatory behavior to the proper authorities,

which may include school officials, local police, or the CyberTipline (www.cybertipline.com or 800-843-5678). Children and teens are extremely susceptible to peer pressure and may lack the critical judgment to know when something is not in their best interest.

Tips and Tools

How can I make sure I don't permanently lose important data on my computer?

Because there's no guarantee that a virus or malware won't corrupt your data, your best defense is to back up your files regularly—that means at least once a week. StaySafe.org offers information and instructions for backing up important files. Most new computers come with automatic backup settings.

How do I know when to update my software?

Set your operating system and other software to update automatically. You can choose to run updates at convenient times when you are not using the computer.

I plan to get rid of my computer and get a new one. How can I make sure nobody can access the data on my old machine?

It's necessary to erase your hard drive completely and permanently before selling, donating or disposing of your computer. (Simply deleting files isn't enough.)

Some operating systems come with their own built-in "disk cleanup" software. If yours doesn't, you can use third-party software. If you need help, and your computer is still under warranty, you may be able to call the computer manufacturer's tech support line. Or, you can take your computer or hard drive to a trusted local computer repair shop and ask them to overwrite your files.

I like to shop online, but I worry about entering my personal information at various sites. How can I tell if a site is safe?

First of all, shop only with online merchants you trust. Consider entering your payment card numbers each time you purchase something, instead of allowing the site to store your number for future purchases.

Then, make sure any shopping site is secure by looking for the SSL encryption ("https://", not just "http://") in the browser's address bar and a closed padlock or unbroken key in

the browser window frame. Never enter debit or credit card information or bank account numbers unless you check this first. Most legitimate commercial websites have SSL encryption to make it safe to shop online.

And confirm the website is authentic. Click (or double-click if necessary) the padlock and key icons to check for a match between the name in the Web address and on the security certificate. If the names are different, you may be on a bogus site. Before shopping on a site you have never heard of, do some online research to see if anyone has complained about the site. Simply enter the site's name plus the word "complaints" in a Web browser.

Can I use a debit card when shopping online?

You can, but it is safer to use a credit card. The maximum liability for unauthorized charges on a credit card is \$50. Liability for unauthorized use on a debit card can be much higher, depending upon when you report the loss. And most debit cards are linked to your bank account, which means a thief could wipe you out and you would be without money until your bank investigates the loss and makes provisional credit.

Are there any special precautions for users who access the Internet on a public computer?

It's a good idea not to let your Web browser save sensitive ID and passwords, like your bank account login or your credit card info for "one-click" shopping. This is especially important at shared or public computers. Clear this info by clicking on the "Tools" in most browsers and then "Delete Browsing History." Or, begin your session by enabling the private browsing option, available in many browsers. This means you can browse the Internet without the computer saving any data about which sites you have visited. Use your browser's Help function to find out how to use private—or "incognito"—browsing.

I received an email with an attachment from someone I don't know. What should I do?

Be careful about opening attachments—the file you receive could contain a virus, spyware, or inappropriate content.

Likewise, be careful about visiting unfamiliar websites, downloading "free" software, or downloading or sharing music or movie files with strangers. Free music, games and other downloads often include unwanted software in the download. And unauthorized file sharing of copyrighted material is illegal.

My friend says I shouldn't forward chain letters? Why not?

Your friend is correct. Electronic chain letters (email messages that are intended to be passed on from one person to another, or to a large group) and other junk email can be risky. You could be seen as a spammer or you could forward a destructive file to someone else. Check out all emails on anti-hoax sites (www.snopes.com or www.quatloos.com) before you hit the forward button so you don't spread something others don't want.

Assistance and Information

Where can I get more information about online safety?

There are many sources of computer and online safety information, including:

✓ ***Fosi.org***

The nonprofit Family Online Safety Institute works to make it safer online for children and their families.

✓ ***OnGuardOnline.gov***

The federal government and the tech industry help you avoid fraud, secure your computer and guard your personal information.

✓ ***PrivacyRights.org***

The nonprofit Privacy Rights Clearinghouse offers a library of information on privacy, from tips for online job seekers to how to shop safely on the Internet.

✓ ***SafeTeens.com***

The site offers information for teens and their parents about safe, civil and responsible use of the Internet. There also is information about safety on cell phones and when texting.

✓ ***SafeKids.com***

Kids can learn about Internet safety and civility, and take an online safety quiz.

✓ ***ConnectSafely.org***

This site focuses on information related to safe blogging and social networking.

Consumer Action, a nonprofit education and advocacy organization, offers news and information about privacy, including what your rights are and how to avoid scams.

Consumer Action

www.consumer-action.org

221 Main Street, Suite 480

San Francisco, CA 94105

415-777-9635 / TTY: 415-777-9456

hotline@consumer-action.org

523 W. Sixth Street, Suite 722

Los Angeles, CA 90014

213-624-8327

Chinese, English and Spanish spoken

This publication was created by Consumer Action in partnership with Microsoft. © Consumer Action 2010

Rev. 4/13