The Cyber Safety Handbook

AARP Washington

Microsoft®
Microsoft is a registered trademark of Microsoft Corporation.

This booklet is provided by The Cyber Safety Program, a campaign to reduce victimization of older persons in Washington State, sponsored by AARP Washington, Microsoft, the Attorney General of Washington, and the Federal Trade Commission.

Cyber Safety

10 Practices for Staying Safer on the Internet

Stop, Think, Click

The world has changed. Today you can work, check your bank balances, book travel, research medical questions, talk to friends and family members, order books and music, bid on auction items, and even buy a car without leaving your home.

Thanks to the Internet, you have access to entertainment, shopping, your own personal financial transactions, email and other information, 24 hours a day.

This unprecedented access to information is greater than earlier generations could have ever imagined. The Internet has unlimited information available to you upon demand.

For most people, most of the time, the Internet is a positive place. However, the Internet is not without hazards. The Internet and the anonymity it affords can give online scammers, hackers, and identity thieves access to your computer, personal information, finances and more.

Consumer education and awareness is your safety net. This booklet on cyber safety will provide you with tools and resources to protect yourself, your family, and your computer.

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

1 Protect Yourself

Protect your privacy and personal information online

Your personal information can provide an identity thief instant access to your financial accounts, your credit record and other assets. Anyone can be a victim of identity theft. According to the Federal Trade Commission, there are almost nine million victims a year nationwide.

Here are a few tips to help minimize your risk online:

- If you are asked for personal information such as your name, email, address, telephone number, account numbers, or Social Security number, find out how the information is going to be used before you share it. Find out how the requester protects your personal information. Remember, it is *your* information.
- Whether you are shopping, banking, or conducting other business online, do not provide your personal or financial information through a company's website until you have checked for indicators that the site is secure.

Website Safety Tips

Look for "https" in the Web address (the "s" stands for secure).

Look for a padlock or an unbroken key in the lower right corner of the status bar.

Double-click the padlock or key to ensure that the "issued by" name on the security certificate matches the name in the address bar.

- Read website privacy policies. Privacy policies should explain what personal information the website collects, how the information is used, and if the site shares the information with third parties. The policy should also tell whether you have the right to see what information the website has about you. The policy should explain measures the company takes to protect your information. If you do not see a privacy policy or cannot understand it, consider doing business elsewhere.
- "Phishers" send email or pop-up messages claiming to be from a business or organization that you might have a business relationship with such as your Internet Service Provider, bank, online payment service or a government agency. The message appears to be official and urges you to take immediate action to update or validate your account information. It may threaten that your account will be closed or frozen if you do not respond. The message directs you to a website that looks legitimate, but is not. The bogus site operators are "phishing" for your personal information so they can steal your identity. Do not take the bait. Never reply to or click on links in email or pop-ups that ask for personal information. Legitimate businesses do not ask for your personal information by email.
- If you get an email or pop-up message asking for personal information, do not reply or click on the link in the message. If you think there may be a need to provide information to the requester (you have an account with the company or have placed an order) contact the company directly by telephone. Do not send your personal information via email; it is not a secure transmission method.

Resources

How to Protect Your Personal Information
www.microsoft.com/athome/security/privacy

What You Should Know about Phishing Scams
www.microsoft.com/athome/security

2 Be alert online

Anyone can set up shop online. It is a good practice to know whom you are dealing with and what you are getting into. Proceed with caution in your online activities.

- If you shop 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 you can call in case you have problems. Call the telephone number before you buy.
- If you do shop online, pay by credit or charge card. If you pay by credit or charge card online, the Fair Credit Billing Act, a federal law, protects your transactions. In the event your card is used without your knowledge or permission, you are only liable for up to $50. Many companies do not hold consumers responsible for any unauthorized charges made online. And some card issuers may provide additional warranty, return and/or purchase protection benefits.
- Never send cash, personal checks or money orders for online purchases.
- Check out the terms of the deal, like refund policies and delivery dates. The law requires sellers to ship items as promised or within 30 days after the order date if no specific date is promised.

Resources

Credit Cards
www.ftc.gov/bcp/conline/edcams/credit/coninfo_loans

How to Shop Online More Safely
www.microsoft.com/athome/security/online

Shop Safely and Wisely Online
www.ftc.gov/onlineshopping

3 Junk email—what to do about spam

If you have email, you have probably received junk email or unsolicited commercial email also known as spam. It is estimated that 80 percent or more of all email that is sent is spam.

Many Internet Service Providers provide junk email filters to help stop 3.2 billion messages from reaching customers' email accounts daily. As a computer user, there are also things you can do to protect yourself.

- Delete junk email without opening the message. If you open the email, it can alert the spammer that the address is good.
- Never reply to spam. This includes responding to an option to "Remove me from your list."
- Do not buy anything or give to any charity marketing through spam. Spammers may swap or sell email addresses of their customers. If you make a purchase as the result of a spam email, it may result in more spam.
- Do not forward chain email messages. You lose control over who sees your email address. You might also be forwarding a hoax aiding in the delivery of a virus.
- Read website privacy policies before you submit your email address to a site. See if it allows the company to sell your email address.
- Read website "opt out" policies about information sharing. You may have to uncheck a pre-checked box if you want to opt out. Read the fine print.

- Consider using two email addresses, one for friends and family, and another for online transactions. If you start getting too much email at one address, you can close it.
- Use a unique email address. Spammers use "dictionary attacks" to sort through possible name combinations, hoping to find valid addresses. A common name such as ssmith may get more email than ssmithzyx321.
- See if your Internet Service Provider provides an email filter to help you filter out potential spam.
- Treat unsolicited email like you would a telemarketing call. Use caution. Old-fashioned scams, schemes, and moneymaking opportunities now arrive in your email inbox.

Resources

Dealing with Spam Email
www.microsoft.com/athome/security/email

Spam
www.ftc.gov/spam

4 Use strong passwords—protect them and change them regularly

Passwords are the key to unlocking your computer and online accounts. A strong password provides better security against hackers and thieves.

- Strong passwords should be over eight characters in length, combine letters, numbers and symbols, and should avoid using common words. Do not use your name, your spouse's name, your birthday or location.
- Change your passwords regularly or at least every 90 days. Do not use the same password for each online account you use.
- Keep your passwords secret. Do not give passwords out to family or friends or send your passwords over email. Do not enable the "Save Password Option" if you receive a dialog box asking you if you would like the computer to remember your password.
- Do not store written passwords on or near your computer. Record passwords and store in a safe, secure place.

One way to create a strong and memorable password is to think of a "passphrase." Think of a phrase that is easy to remember like "I save my pennies for a rainy day." Use the first letter of each word as your password, converting some letters into numbers that resemble letters for example "Ism¢4ard." Notice the combination of upper and lower case letters, numbers and symbols.

Resources

Strong Passwords
www.microsoft.com/athome/security/privacy/password.mspx

5 Protect Your Computer

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

A Web browser is software that gives a user access to the World Wide Web. Web browsers often provide a graphical interface that lets users click buttons, icons, and menu options to view and navigate Web pages.

An operating system is the software that manages the computer system and makes the computer functional.

Hackers can take control of Web browsers and operating systems that are unsecured. Security settings should be set at medium or higher. Lessen your risk by changing settings in your browser or operating system and increasing your online security.

Your operating system may offer free software patches that close the holes in the system that hackers could exploit. Some operating systems can be set to automatically retrieve and install patches for you. If your system does not do this, bookmark the website for your system's manufacturer so you can regularly visit the site and update your system. Sometimes updating can be as simple as one click.

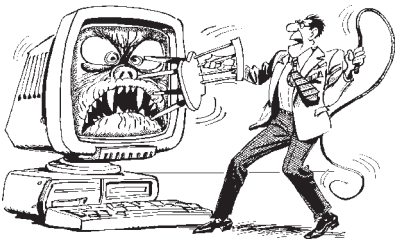
If you are not using your computer for an extended period, turn it off or unplug it from the telephone or cable line. When your computer is off, it does not send or receive information from the Internet and is not vulnerable to hackers.

Resources

Software Updates
www.apple.com/support

Updates & Maintenance
www.microsoft.com/athome/security/update/default.mspx

6 Use antivirus software and a firewall—update both regularly



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

- You can download antivirus software from the websites of software companies or buy it. Look for antivirus software that recognizes current viruses, as well as older viruses, effectively reverses the damage, and updates automatically.
- Firewalls help keep hackers from using your computer to send out your personal information without your permission. While antivirus 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 do not permit.

Some operating systems include built-in firewalls in the "off" mode. Make sure you turn it on. For a firewall to be effective, it needs to be set up properly and regularly updated.

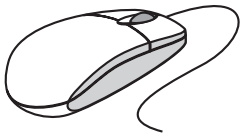
If your operating system does not include a firewall, you can either download free firewall software programs on the Internet or purchase firewall software or hardware.

Resources

Protect Your PC
www.microsoft.com/athome/security/viruses

Protect Your Mac
www.apple.com/support

7 Stop and think before you click



Before you provide information, open files or attachments, or download files from unknown senders, take a minute to stop and think before you click.

- Free downloads can contain spyware. Spyware is software installed on your computer without your knowledge or consent that adversely affects your ability to use your computer, sometimes by monitoring or controlling how you use it. To avoid spyware, resist the urge to install any software unless you know exactly what it is. You can install antispyware software and then use it regularly to scan for and delete spyware programs that may sneak onto your computer.
- Email attachments and links sent over email will not damage your computer without your participation. You 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. Hackers use a variety of enticing file names such as "Per your request!" or "Fwd: FUNNY" to get you to open the email attachment or click on the link. Do not open an email attachment, unless you expect it and know what it contains. You can help others trust your attachments by including a message in your text that explains what you are attaching.
- "Instant messaging" is a form of online communication like email. You can type messages to someone and they can see the messages almost immediately. Files attached to instant messages can also contain viruses. In most cases, viruses spread when you open an infected file attached to an instant message appearing to come from someone you know.

Resources

Defending Yourself Against Viruses and Worms
www.microsoft.com/athome/security/viruses

FTC Consumer Alert - Spyware
www.ftc.gov/bcp/conline/pubs/alerts/spywarealrt.htm

Spyware
www.microsoft.com/athome/security/spyware

8 Back up important files

No system is completely secure. If you have important files stored on your computer, copy them onto a removable disc and store them in a safe place. Maintain a home computer backup schedule so you do not lose important files.

Resources

Backup Basics
www.microsoft.com/athome/security/update/backup.mspx

9 Protect Your Friends and Family

Share information to help keep kids, grandkids, friends and family safe online

Now that you have a basic knowledge about how to stay safer on the Internet, share this booklet with a friend or family member. If you reach just one person whom you think might be vulnerable to unsafe Internet practices, you will be doing a tremendous community service.

- Pay attention to what kids do and whom they meet online. Consider a rule that no child reveals personal information, including photos, without permission. Warn kids never to meet Internet "friends" in person.
- Parental controls are provided by most Internet Service Providers, or sold as separate software. No software can substitute for parental supervision. Talk to your kids and/or grandkids about safe computing as well as things they are seeing and doing online.

Resources

Child Safety

www.microsoft.com/athome/security/children

Kidz Privacy

www.ftc.gov/kidzprivacy

By law, websites that ask for certain information about kids under 13 have to get their parents permission to get the information.

Staysafe.org

www.staysafe.org

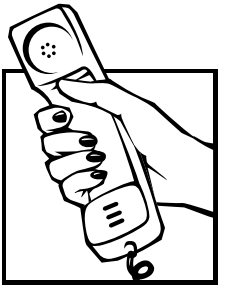
This is an educational site intended to help consumers understand both the positive aspects of the Internet as well as how to manage a variety of safety and security issues that exist online.

Web Aware

www.bewebaware.com

This site provides you with tools you need to help keep your kids safe online.

10 Report Fraud



Join the fight against fraud

All across Washington State, people are becoming Fraud Fighters, citizens volunteering to help stop fraud by educating others.

As a fraud fighter, you become the eyes and ears of law enforcement. Research has shown that less than one in four fraud victims ever report the crime to the authorities. Now that you know what to look for and can identify spam, phishing emails and other online dangers, make a report to the proper agency or to your Internet Service Provider.

Identity Theft

If you believe you have mistakenly given your personal information to a fraudster, file a complaint at www.ftc.gov and then visit the Federal Trade Commission's Identity Theft website at www.consumer.gov/idtheft to learn how to minimize your risk of damage from a potential theft of your identity. You can also call the Identity Theft Hotline at 1-877-IDTHEFT (438-4338).

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 www.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.

Internet Service Provider

Report abusive, harassing, or threatening email messages to your Internet Service Provider.

Phishing

Report phishing attempts to the company that has been misrepresented. You also may report phishing email to reportphishing@antiphishing.org. The Anti-Phishing Working Group, a consortium of Internet Service Providers, security vendors, financial institutions and law enforcement agencies use these reports to fight phishing.

Spam (unsolicited commercial email)

If you get deceptive spam, forward it to spam@uce.gov. Be sure to include the full header of the email, including all routing information. The FTC uses the spam stored in this database to pursue law enforcement actions against people who send deceptive email.

Many Internet Service Providers also provide features to report spam directly from your email account to your ISP.

Steps I will take to stay safer online

Immediate steps

- ☑ I will keep my operating system up-to-date. I will bookmark the website for my operating system and check for updates. I will also enable the automatic update feature.
- ☑ I will regularly update my Web browser and other major software, using the update instructions provided by the manufacturer.
- ☑ I will check my browser security settings. I will keep my security settings set at medium or higher.
- ☑ I will ensure my Internet firewall is enabled. If I do not have firewall protection, I will either download or purchase firewall protection.
- ☑ I will use antivirus software. I will check to see if my ISP provides additional virus protection or purchase software from a manufacturer or retail outlet. I will enable the auto-protect and update features or if I am a subscriber, will keep my subscription current.
- ☑ I will use antispyware software. I will check to see if my ISP provides additional spyware protection or purchase software from a manufacturer or retail outlet. I will enable the auto-protect and update features or if I am a subscriber, will keep my subscription current.
- ☑ I will make sure my ISP provides security such as spam filtering and virus scanning for no additional charge.

Cyber safety practices

- ☑ I will ensure websites are secure and investigate website privacy policies.
- ☑ I will be an alert online shopper, investigating merchants, products, and services before I buy.
- ☑ I will be cautious of email and instant message attachments.
- ☑ I will never open an attachment that I was not expecting, even from a friend.
- ☑ I will never reveal personal or financial information in response to an email.
- ☑ I will delete spam or report spam. I will never respond to spam or buy products or services from spammers.
- ☑ I will consider two email addresses, one for family and friends, and one for online transactions.
- ☑ I will use strong passwords and change them frequently.
- ☑ I will regularly back up important computer files.
- ☑ I will keep my friends and family safe online by sharing cyber safety tips, resources and information.

Internet Terms

Attachment	A file sent along with an email message.
Cookies	Computer code that is placed on a hard drive when Internet users go to websites and allow the sites to identify the computer if it returns to the site.
Hacker	A person who uses the Internet to access computers and information without permission.
Phishing	Spam or a pop-up message to lure personal and financial information from unsuspecting victims.
Spam	Unsolicited commercial email. There are two types of spam, legal and illegal. The subject line is considered legally deceptive if it has a tendency or capacity to deceive consumers.
Spammer	Someone who sends mass amounts of unsolicited commercial email.
Spim	Instant message spam is also known as spim.
Spyware	Programs installed without your explicit consent. Spyware can remotely control your computer or collect your personal information and send it to a third party.
Virus	Software that spreads from computer to computer and damages files or disrupts your system.
Worms	Self-propagating malicious code that can automatically distribute itself from one computer to another through network connections.

Security Software Terms

Antispam Software	Antispam software automatically intercepts and filters email before it reaches your inbox.
Antispyware Software	Antispyware software helps protect your computer from spyware and other potentially unwanted software by detecting and removing known spyware programs. It can be scheduled to scan your computer at times that are convenient for you.
Antivirus Software	Antivirus programs help protect you from malicious programs, called viruses, that attach themselves to a program or file in order to spread from computer to computer.
Firewall	A firewall will help protect your computer from hackers who might try to delete information from your computer, make it crash or even steal personal information, such as passwords or credit card numbers over the Internet. If you use the Internet from home, installing a firewall before connecting to the Internet is the most important first step you can take to protect your computer.
Spam or Junk Email Filters	Spam or junk email filters can serve as the first line of defense against spam. Many Internet Service Providers and email programs provide email filters.

To File Complaints

Attorney General of Washington

www.atg.wa.gov

If you are a Washington State resident or the business is located in the state, and have been the victim of an unfair or deceptive business practice, file a complaint with the Attorney General's Office online or call 1-800-551-4636 to request a complaint form.

Federal Bureau of Investigation and the National White Collar Crime Center

www.ic3.gov

Consumers can report suspected Internet frauds to the Internet Fraud Complaint Center.

Federal Trade Commission

www.ftc.gov

The FTC does not resolve individual consumer complaints; your complaint helps the FTC investigate fraud and may lead to law enforcement action. The FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into the Consumer Sentinel®, a secure online database available to hundreds of civil and criminal law enforcement agencies worldwide. You can call 1-877-FTC-HELP (382-4357).

Resources

AARP

www.aarp.org/wa

Visit AARP Washington's website for cyber safety resources and an online tool kit.

www.aarp.org/learntech/computers/

Your place for online training, classes and more. Sign up to receive a free online newsletter on computers and technology.

www.aarp.org/money/wise_consumer/scams/

Information about online scams and many other subjects of interest to older adults.

Attorney General of Washington

www.atg.wa.gov

The Attorney General's Office investigates and brings legal actions to stop fraudulent and deceptive business practices. The office also facilitates the resolution of consumer complaints and educates consumers.

Federal Trade Commission

www.ftc.gov

Contains up-to-date information about consumer protection issues. It lets you file a complaint about a business online, including privacy violations.

www.onguardonline.gov

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.

Microsoft

www.microsoft.com/athome/security

Get continuous antivirus protection and maintenance for your computer. This site provides information on how to protect yourself, your family and your computer.

Other Resources

Better Business Bureau

www.bbb.org

Site lets you check the reliability of a business, get consumer tips, and file a complaint against a business online.

Child Pornography CyberTipline

www.missingkids.com/cybertip

If you know about a child who is in immediate risk or danger, call law enforcement at 1-800-843-5678.

Consumer Reports WebWatch

www.consumerwebwatch.org

Consumer Reports WebWatch is a grant-funded project of Consumers Union, the non-profit publisher of Consumer Reports magazine and ConsumerReports.org.

Direct Marketing Association

www.dmaconsumers.org

Describes ethical practices on online marketing and privacy, and handles consumer complaints. Maintains services to remove your name from lists used for unwanted mail, telephone calls, and email.

Federal Consumer Information Center

www.pueblo.gsa.gov

The federal government's clearinghouse for consumer education materials.

Federal Government Agencies

www.consumer.gov

A gateway to consumer protection offices of several federal agencies. Lets you file a complaint online.

GetNetWise

www.getnetwise.com

The GetNetWise coalition wants Internet users to be only "one click away" from the resources they need to make informed decisions about their and their family's use of the Internet.

National Fraud Information Center

www.fraud.org

Run by the National Consumers League. Maintains information about online scams, and lets you file a consumer complaint online.

Disclaimer

The information contained in this presentation and materials is provided for educational and informational purposes only. AARP, Microsoft, the Federal Trade Commission, and the Attorney General of Washington make no representations that the suggestions and recommendations provided will prevent any harmful conduct. Microsoft and the Microsoft logo are either registered trademarks or trademarks of the Microsoft Corporation in the United States and /or other countries. The names and logos of actual companies and products mentioned herein may be trademarks of their respective owners.

FRAUD FIGHTER ALERT!

You can help stop fraud in Washington by joining the Fraud Fighters!

Learn how to spot fraud and stop it! If you would like to become a Fraud Fighter—no matter what age you are—clip and fill out the form below to receive regular updates on current scams and fraudulent activity in Washington state.

☐ Yes, I'd like to receive regular updates from AARP on fraud and scams in Washington by mail. (Please print.)

Name _____

Address _____

_____

Telephone ( ) _____

☐ I'd prefer to receive this information by email (this will reduce mailing costs). Please include the information above. My email is:

_____

Choose from four easy ways to submit this information:

1. Return this form to any AARP staff person.
2. Mail this form: Fraud Fighters
   AARP Washington
   9750 3rd Avenue NE, Suite 450
   Seattle, WA 98115
3. Fax this form: 206-517-9350
4. Email: submit your name, mailing address, city, state, zip code and telephone number to aarpwa@aarp.org. Type "Fraud Fighter" in the subject line.

Please clip and return this form by mail or fax.