AARP®

Mini Edition

Internet Safety Tips

FOR DUMMIES®

Linda Criddle
Nancy C. Muir

Internet Safety Tips For Dummies

In This Book

- Recognizing how online risks occur
- Staying safer with technology
- Taking care with shared photos
- Understanding how crooks collect information
- Reporting fraud and abuse

News stories about Internet risks sometimes cause people to avoid going online, and that's a real shame because the Internet is a fantastic place to learn, communicate, meet people, shop, bank, get help, and be entertained.

By learning a few safety precautions, you can be as risk-free online as you are when you go about your business in the offline world every day.

Understand What's Going On

Six factors allow crimes to take place online:

- **Lack of knowledge:** Consumers of every age and at every level of technical expertise lack online safety education.

- **Carelessness:** People often click a link or reply to an e-mail without thinking.
- **Unintentional exposure:** You or others may provide publicly accessible information that exposes you.
- **Technology flaws:** Online products and services can expose consumers.
- **Holes in consumer protection standards:** Because of the rapid growth of the Internet, governments have not yet been able to create a full set of standards and laws.
- **Criminal acts:** The Internet offers some powerful tools that criminals take advantage of.

Lucky for you, a little knowledge can keep you safer.

Use Technology to Stay Safer

No matter how safely you act online, if you allow your computer to be infected with viruses or spyware, your information could still be stolen and your safety compromised. Here are some steps you can take:

- **Protect your computer.** Install antivirus and antispyware software and set these to automatically update.
- **Use a reputable browser.** Use Internet Explorer, Firefox, or Safari, and keep the default security and privacy settings intact.
- **Keep up to date.** Set your system so that it automatically checks for, and installs, software updates for your Operating System and browser.

- **Don’t trade safety for savings.** There are good, free antivirus and anti-spyware services.
- **Turn on your firewall.** A firewall is a part of your computer system or network that blocks unauthorized access while permitting outward communication.

  You access and manage the Windows Firewall through the Control Panel. To access and manage the firewall on a Mac, you go through System Preferences. A knowledgeable friend can help you check your firewall’s status.
- **If you’re using a home wireless network, make sure security is enabled for it.** Check your settings. A knowledgeable friend can help you in this arena, too.

Secure Your Browser and Search the Internet Safely

Browsers help you move around the Internet, and search engines make it easy to find information on the Internet. A secure browser, combined with an antivirus/ anti-spyware program, helps you identify safe and unsafe websites:

- If you get a notification from your antivirus/ malware program that a site you are trying to visit is unsafe, believe it. Don’t go there.
- If a site asks you to change your browser settings in order to “improve your experience,” ignore the request and use a different website.

- Allow downloads and execution of programs only when you absolutely trust and understand what the program will do.

E-Mail Safety Basics

Adopt the following e-mail practices to keep you safer every time you send messages:

- **Don't share sensitive personal information.** Never share passwords, Social Security numbers, and credit card numbers in e-mail.
- **Choose who you e-mail.** Just because someone sends you an e-mail doesn't mean you need to read it or respond. Set up your spam filters to be restrictive, and check your spam folder periodically for legitimate messages.
- **Think twice before you open attachments or click links in e-mail.** If you don't know the sender, delete the e-mail. If you do know the sender but weren't expecting an attachment, double-check that the person actually sent the e-mail.
- **When sending e-mail to a group of people who don't know each other, use the Bcc line to protect everybody's identity.** Place all the e-mail addresses on the Bcc (or Blind Carbon Copy) line of the message. That way, no recipient can see the e-mail addresses of other recipients. This respects their privacy and protects their accounts from spammers.

Passwords Made Easy

Strong passwords don't have to be hard to remember, just hard to guess. Though strong passwords use at least ten characters, and include uppercase letters, special characters (such as @ or :), and numbers, they don't have to be intimidating. To make it easy, use a phrase, incorporate shorthand, or use the site to give you clues:

- **2BorNot2B?** (to be or not to be)
- **It's@MyBank** (it's at my bank)
- **Matt6:9-13** (Biblical verse)

Recognize Fraud and Scams

Most e-mail spam and scams are easy to spot. Learn these common red flags to help you spot e-mail scams:

- You don't know the person sending the e-mail.
- The claims sound too good to be true.
- Someone is promising to send you money or a prize.
- A financial institution or store asks for your account information or password.
- You're asked to click on a link in the e-mail or download a file.
- The message has misspellings or sounds unprofessional.

The more dangerous scams are the ones that look like they *might* be legitimate. These look like they're from a company you have an account with but are fake. These guidelines can help you navigate safely through these types of scams:

- Be very skeptical if you receive an e-mail that looks like it is from your bank, broker, or other trusted company but asks you to verify or re-enter personal or financial information through e-mail, a website it directs you to, or a phone number it provides.
- Follow this rule: "Drive, don't be pulled." Don't let a link in an e-mail "pull" you to a site of the sender's choosing. Instead, navigate to the legitimate site on your own by looking up the URL in a search engine or on an old bill. Stay safe by always navigating to websites yourself.

Sharing Photos Safely

Posting pictures online is a wonderful way to share experiences with others. If you share only with people who know you well, on reputable sites, and with privacy protections in place, then you can be fairly worry-free because your friends and family probably already know the information being shared. Just have fun and enjoy. But be cautious.

If you want to share photos publicly, there are a few things you need to know to stay safer:

- **Understand what information is in a photo:** Consider not what you think you are sharing, but what a criminal or bully can glean. Can you see the ages of people in the photos? Socio-economic status? Emotional vulnerabilities? Identifying information like house numbers or landmarks? Is there a caption under the photo or information in the person's blog or album that adds to what a criminal can learn?

- **Some types of information can be used in unintended ways:** Unintended uses can include ways to embarrass you, threaten you, or steal from you or someone else.
- **Decide who should be allowed to see photos:** Some information should only be shared privately.

Look at photos over the next few days and practice seeing what is there and who you might feel comfortable sharing those photos with.

How Information Is Spread and Collected

Sharing personal information with friends and family enriches relationships. Sharing personal information with untrustworthy people or companies is taking a big risk.

Criminals and bullies often collect information in a systematic way. Each piece of personal information contributes to forming a picture of your life, emotions, and finances, and may help them exploit you.

Fortunately, you have a great deal of control over your information exposure. Be careful when sharing the following pieces of information:

- Addresses and phone numbers
- Names of family members (including mother's maiden name), siblings, children, and grandchildren
- Information about your personal property, work history, or financial status

REMEMBER Always be careful about sharing information; the more sensitive the information, the fewer the people who should have access to it.

WARNING! Every detail you or others share online about your life and the people you interact with is stored *somewhere.* That information may be copied and posted in other locations, and could stay online forever.

Avoid Emotional Exposure

Just as some offline criminals read birth, wedding, graduation, and obituary announcements in newspapers to find possible victims, some online criminals also watch for information about significant life events.

The joy of a wedding, the arrival of a new grandchild, or a death in the family may inspire individuals to share information on publicly viewable registries and memorial sites that they would otherwise keep private.

Follow four simple guidelines for safely sharing joy or grief, in any public online setting:

- Make a conscious choice about whether you want the site *private* (only those whom you allow) or *public* (available to anyone). Then decide what information you want to provide.

- ✓ Let others know your safety boundaries so they can participate online in a way that respects your privacy choices.
- ✓ If you're too busy, ask a friend to monitor the site for information risks so you can focus on other matters.
- ✓ If you choose to place contact information online, create a *separate* e-mail address for this purpose to protect your main e-mail address.

Report Abuse

Often, people don't know where to turn when something has gone wrong online.

Every site should have an easy-to-find "Report Abuse" feature and a way to contact customer support.

Additionally, if your safety is threatened, or a crime has been committed, contact your local law enforcement office. It will bring in other agencies if needed.

Immediately report identity theft to your local law enforcement agency, as well as to credit reporting agencies. Learn more about identity theft by visiting http://www.ftc.gov/bcp/edu/microsites/idtheft/.

It's Never the Victim's Fault

Offenders bear complete responsibility for their actions.

REMEMBER

If you or a loved one have been abused in any way, report it, and get the support you need.

Protect your privacy and stay secure online

Isn't the Internet amazing? Though you've heard of online risks, there's no reason you can't enjoy your Internet experience while still feeling safe and secure. Here's the mini guide you need to steer through the hazards with confidence, so you can shop, visit, explore, pay bills, play games, and do dozens of other things online — and maintain your peace of mind.

Open the book and find:

- How to create strong passwords
- Advice on spotting scams
- Tips for sharing photos and personal info
- The basics of e-mail safety
- When and how to report abuse

Making Everything Easier!™

For Dummies®
A Branded Imprint of
WILEY

Linda Criddle is an internationally recognized Internet safety and technology expert. **Nancy C. Muir** is a writer, consultant, and author of more than 60 books, including *Using the Internet Safely For Seniors For Dummies*.

ISBN 978-1-118-35460-5
9 781118 354605