Computer Security

Scammers, hackers, and identity thieves are looking to steal your personal information – and your money. But there are steps you can take to protect yourself, like keeping your computer software up-to-date and giving out your personal information only when you have a good reason.

Use Security Software That Updates Automatically

The bad guys constantly develop new ways to attack your computer, so your security software must be up-to-date to protect against the latest threats. Most security software can update automatically; set yours to do so. You can find free security software from well-known companies. Also, set your operating system and web browser to update automatically.

If you let your operating system, web browser, or security software get out-of-date, criminals could sneak their bad programs – malware – onto your computer and use it to secretly break into other computers, send spam, or spy on your online activities. There are steps you can take to detect and get rid of malware.

Don’t buy security software in response to unexpected pop-up messages or emails, especially messages that claim to have scanned your computer and found malware. Scammers send messages like these to try to get you to buy worthless software, or worse, to “break and enter” your computer.

Treat Your Personal Information Like Cash

Don’t hand it out to just anyone. Your Social Security number, credit card numbers, and bank and utility account numbers can be used to steal your money or open new accounts in your name. So **every time** you are asked for your personal information – whether in a web form, an email, a text, or a phone message – think about whether you can really trust the request. In an effort to steal your information, scammers will do everything they can to appear trustworthy. Learn more about scammers who phish for your personal information.

Check Out Companies to Find out Who You’re *Really* Dealing With

When you’re online, a little research can save you a lot of money. If you see an ad or an offer that looks good to you, take a moment to check out the company behind it. Type the company or product name into your favorite search engine with terms like “review,” “complaint,” or “scam.” If you find bad reviews, you’ll have to decide if the offer is worth the risk. If you can’t find contact information for the company, take your business elsewhere.

Don’t assume that an ad you see on a reputable site is trustworthy. The fact that a site features an ad for another site doesn’t mean that it endorses the advertised site, or is even familiar with it.

Give Personal Information Over Encrypted Websites Only

If you’re shopping or banking online, stick to sites that use encryption to protect your information as it travels from your computer to their server. To determine if a website is encrypted, look for **https** at the beginning of the web address (the “s” is for secure).

Some websites use encryption only on the sign-in page, but if any part of your session isn’t encrypted, the entire account could be vulnerable. Look for https on every page of the site you’re on, not just where you sign in.

Protect Your Passwords

Here are a few principles for creating strong passwords and keeping them safe:

- The longer the password, the tougher it is to crack. Use at least 10 characters; 12 is ideal for most home users.
- Mix letters, numbers, and special characters. Try to be unpredictable – don’t use your name, birthdate, or common words.
- Don’t use the same password for many accounts. If it’s stolen from you – or from one of the companies with which you do business – it can be used to take over all your accounts.
- Don’t share passwords on the phone, in texts or by email. Legitimate companies will not send you messages asking for your password. If you get such a message, it’s probably a scam.
- Keep your passwords in a secure place, out of plain sight.

Back Up Your Files

No system is completely secure. Copy important files onto a removable disc or an external hard drive, and store it in a safe place. If your computer is compromised, you’ll still have access to your files.