

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](/articles/0011-malware) (/articles/0011-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 really can 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](/articles/0003-phishing) (/articles/0003-phishing).

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](/articles/0027-researching-products-online) (/articles/0027-researching-products-online). 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).