
# Cybersecurity Without the Jargon: What Can Actually Hurt Your Computer?

Cybersecurity can sound intimidating. We hear about viruses, ransomware, hackers, spyware, phishing, data breaches and identity theft. The terminology alone can make an ordinary computer user wonder whether safely going online requires a degree in computer science. It doesn't. You don't need to understand the technical details of malicious software to protect yourself from most everyday cyber threats. What you do need is a basic understanding of what the bad guys are trying to accomplish, how they try to reach your computer, and what you can do to make their job much harder.

## What Exactly Is Malware?

The word **malware** is short for *malicious software*. It is an umbrella term covering software deliberately created to damage a computer, steal information, spy on its user or gain unauthorized access to a system.

The familiar computer **virus** is one kind of malware. A virus attaches itself to files or programs and spreads when those files are opened or shared. A **worm** can spread from one computer to another without attaching itself to another program. A **Trojan horse**, named after the famous trick from ancient history, disguises itself as something legitimate or useful while concealing malicious software.

**Spyware** secretly collects information about the computer user, while **ransomware** can encrypt important files or otherwise make them inaccessible and then demand payment to restore them. There are many more technical varieties, but most home computer users don't need to memorize them. Knowing whether something is technically a virus, worm or Trojan won't help much after you've clicked the wrong attachment.

# From Mischief to Money

The motivations behind malware have changed considerably. Early computer viruses were sometimes created simply to demonstrate the programmer's abilities or to cause disruption. They traveled from computer to computer on floppy disks and other removable media.

The arrival of email and the World Wide Web changed everything. A malicious program could suddenly travel around the world in hours instead of moving from one floppy disk to another. One famous example was the **Melissa virus of 1999**. Melissa arrived as an infected Microsoft Word document attached to an email. If the recipient opened it, the malware could use Microsoft Outlook to send itself to other people. The resulting avalanche of email disrupted corporate and government systems. Melissa demonstrated something that remains important more than a quarter-century later: the computer itself doesn't always have to be fooled. Sometimes the criminal only has to fool **you**.

# Today's Criminal Wants Something

Modern cybercrime is increasingly about making money. A criminal may want your credit-card information, bank credentials, email password or personal information. Another may want access to your computer so it can be used in further attacks. Ransomware criminals may simply make your valuable files inaccessible and demand payment for their return.

Your email account is particularly valuable because it can become a gateway to the rest of your digital life. Password-reset messages for other accounts frequently arrive by email. A criminal who takes control of your email may therefore have an opportunity to attack your other accounts as well. This is why cybersecurity today is about much more than keeping a virus off your hard drive. It is about protecting your **digital identity**.

# The Criminal's Favorite Target May Be You

Computers have become much more secure since I originally wrote about cybersecurity in 2017. Windows and macOS have built-in security protections. Modern browsers can warn about suspicious websites. Email services filter enormous quantities of junk and malicious mail before we ever see it. Security updates continually repair newly discovered vulnerabilities.

So cybercriminals adapted. Rather than always trying to defeat the computer's defenses, they increasingly try to persuade the computer's owner to open the door for them. An email might announce that your bank account has been compromised. A text message might claim that you owe a small toll-road charge. A delivery notice might tell you that a package cannot be delivered until you verify some information. A pop-up window might warn that your computer is infected and provide a telephone number for "Microsoft Support."

The common ingredient is **urgency**. Click here. Call immediately. Verify your account. Pay now. The criminal doesn't want to give you time to think.

# Your Computer Already Has Bodyguards

Fortunately, the situation isn't hopeless. In fact, today's ordinary computer user starts with considerably better protection than users had when the Internet first became popular. Windows and macOS include security features that should normally remain turned on. Modern browsers receive frequent security updates. Reputable email providers filter suspicious messages. Computers and smartphones can automatically install important operating-system updates.

Those updates deserve special attention. Sometimes users postpone them because restarting a computer is inconvenient. But many updates repair security weaknesses that criminals already know about. When your Mac, PC, iPhone or other trusted device says an important security update is available, installing it is usually a good idea.

# Don't Help the Bad Guys

The most useful cybersecurity principle may also be the simplest: **don't help the criminal get in.** Be cautious with unexpected attachments. Don't install software merely because a pop-up tells you to. Be suspicious of alarming messages demanding immediate action. Obtain applications from sources you trust, and keep your computer and applications updated.

If something doesn't look right, stop and investigate before doing anything. You don't lose anything by taking another minute to examine an email before clicking its link. You can contact your bank directly rather than using the convenient button in the message. You can ask a friend whether that strange attachment really came from him. You can close a suspicious browser window instead of following its instructions. That moment of hesitation can be one of the most effective cybersecurity tools available.

# You Don't Have to Be an Expert

Cybersecurity professionals deal with enormously complicated threats, and organizations spend billions of dollars protecting their systems. Fortunately, protecting a home computer doesn't require becoming one of those experts. For the ordinary user, good cybersecurity mostly consists of sensible habits: keep your software current, protect your accounts, maintain backups, be careful about what you download, and become suspicious whenever someone unexpectedly asks for money, passwords or personal information.

In the next articles we'll look more closely at phishing, ransomware, passwords and the practical security measures that can make everyday computing considerably safer. The Internet has its share of bad neighborhoods and shady characters, but you don't have to stop traveling. You just need to learn how to lock the doors.