

The seemingly limitless information, images, and opportunities on the web can lead us to forget that access comes with risk to our computers—and to us.

Cybercriminals work shrewdly and relentlessly to seize control of your computer, use your email or instant messages (IM) to spread spam, or spy on your online activities—ultimately in an attempt to steal personal information or money.

Criminals use two broad strategies to try to break through a computer's defenses:

- > They try to trick you into installing their adware, worms, and other malicious software (*malware*). They can deliver it in downloads that you think are innocent, such as photos or music, or in links that you click in email or IM, on a social network (like Facebook), or in a game. Or, they may try to scare you into responding to fake warnings that your computer has a virus or needs repair.
- > They install malicious software on computers that haven't been updated by exploiting older weaknesses in its software or by breaking into accounts guarded by simple passwords.

So how do you better secure your computer? Strengthen its defenses and train yourself to act cautiously as you make your way across the web.



What to do if your computer isn't running as usual

If your computer is unusually slow, crashes frequently, or shows other problems, it might be infected with malware. (These issues might also indicate a malfunctioning computer.) Microsoft can help you diagnose the problem and solve it: consumersecuritysupport.microsoft.com.

More helpful info

- > Find out how to create strong, memorable passwords: aka.ms/passwords-create.
- > Find out how to spot fake virus alerts and what to do about them: microsoft.com/security/antivirus/rogue.aspx.
- > For more information to help you better defend your computer: microsoft.com/security/pypc.aspx.



Defend Your Computer

- > Build up your computer's defenses
 - > Don't be tricked into downloading malicious software
 - > What to do if your computer isn't running as usual

This material is provided for informational purposes only. Microsoft makes no warranties, express or implied.

1011 PN 098-108790



Strengthen your computer's defenses

Install antivirus and antispyware programs from a trusted source

These programs scan and monitor your computer for known viruses and spyware. When they find something, they notify you and help you take action.

- > Never download anything in response to a warning from a program you didn't install or don't recognize that claims to protect your computer or offers to remove viruses. It's highly likely to do the opposite.
- > Get reputable malware protection from a vendor you trust.
 - > Microsoft Security Essentials offers free real-time protection against malware: [microsoft.com/security_essentials](https://www.microsoft.com/security_essentials).
 - > Or choose from a list of Microsoft partners who provide antimalware software: [microsoft.com/windows/antivirus-partners](https://www.microsoft.com/windows/antivirus-partners).

Keep all software up to date

Cybercriminals are endlessly inventive in their efforts to exploit vulnerabilities in software, and many software companies work tirelessly to combat these threats.

- > Regularly install updates for *all* your software—antivirus and antispyware programs, browsers (like Windows Internet Explorer), operating systems (like Windows), and word processing and other programs.
- > Subscribe to automatic updates whenever they are offered. For example, to automatically update all Microsoft software, go to update.microsoft.com.
- > Uninstall software that you don't use. You can remove it using Windows Control Panel.

Protect accounts with strong passwords


- > Strong passwords are long long phrases or sentences that mix letters, numbers, and symbols.
- > Keep passwords secret. Don't share them with anyone.
- > Don't use the same password on multiple sites.
- > Create different strong passwords for the router and wireless key of your wireless connection at home. Find out how from the company that provides your router.

Never turn off your firewall

A firewall puts a protective barrier between your PC and the Internet. Turning it off for even a minute increases risk.

Use flash drives cautiously

Minimize the chance that you'll infect your computer:

- > Don't put *any* unknown flash (or thumb) drive into your PC.
- > To block malware, hold down the Shift key when you insert the flash drive into your computer. If you forget to do this, click  in the upper-right corner to close any flash drive-related pop-up windows.
- > Don't open files on your drive that you're not expecting.



Don't be tricked into downloading malware

- > Be very cautious about opening attachments or clicking links in email or IM, or on social networks—even if you know the sender. Confirm with him or her that the message is legitimate. If not, delete the message or close the IM window.
- > Avoid clicking **Agree**, **OK**, or **I accept** in banner ads, in unexpected pop-up windows or warnings, on websites that may not seem legitimate, or in offers to remove spyware or viruses.
 - > Instead, press Ctrl + F4 on your keyboard to close the window.
 - > If that doesn't close the window, press Alt + F4 on your keyboard to close the browser. If asked, close all tabs and don't save any tabs for the next time the browser starts.
- > Only download software from websites you trust. Be cautious of "free" offers of music, games, and the like. They're notorious for including malware.