# Defend Your Devices Against Internet Dangers

Practical advice to help you secure your computers, tablets, and phones

Enjoy the limitless information, images, and opportunities on the web—but don't forget that all that comes with risk, too.

Criminals work relentlessly to seize control of your devices, compromise your email or text messages, or spy on your online activities—ultimately in an attempt to steal your identity or financial information:

- They try to trick you into installing software that is infected with malicious software (*malware*) like worms and viruses. They can deliver it through seemingly innocent downloads such as photos or music, or in links that you click in email or IM, on a social network, or in a game. Or they may try to scare you with a fake warning that your device has a virus or needs repair, or swindle you with offers of something "free."
- They install malware on devices by taking advantage of weaknesses in software or systems that don't have adequate antivirus protection, or by using bots to guess account passwords.

So how do you better secure your devices? Strengthen their defenses and pay attention as you make your way across the web.

## Strengthen the defenses of your devices

### 1 Install reputable antimalware programs from a trusted source

- These programs monitor and scan your devices for known viruses and spyware. When they find something, they notify you and help you take action.
- Never download anything that claims to protect your device or offers to remove viruses in response to a warning from a program you didn't install or don't recognize. They are likely to do the opposite, even though they look "real."

### 2 Keep all software up to date

Criminals are constantly trying to break into software, and software companies are constantly adding updates to help thwart them, so keeping software current is the most effective way to stay ahead of the crooks.

- Accept and install updates offered for *all* your software—apps, antimalware programs, browsers (like Windows Internet Explorer), operating systems (like Windows), and spreadsheet and other programs.
- Subscribe to automatic updates whenever possible.
- Remove apps and software that you don't use—outdated versions of Java, for example.

### Protecting Windows computers and tablets

- For protection against malware, choose:
  - Microsoft Security Essentials, which offers free real-time protection: microsoft.com/security_essentials.
  - From a list of software that Microsoft partners provide: microsoft.com/windows/antivirus-partners.
- Get help setting up automatic updates of Microsoft software: update.microsoft.com.
- You can remove software using Windows Control Panel.
- If your device is unusually slow, crashes frequently, or shows other problems, it might be infected with malware. Microsoft can help you diagnose the problem and solve it: consumersecuritysupport.microsoft.com.

Find out...

- How to create strong, memorable passwords: aka.ms/passwords-create
- How to protect yourself from malware: aka.ms/malware_protection
- More ways to help you better defend your devices: microsoft.com/security/pypc.aspx

### 3 Protect devices and accounts with PINs and strong passwords

Strong passwords are long phrases or sentences that mix letters, numbers, and symbols. For PINs, avoid personal numbers, such as your birthdate or phone number.

- Keep passwords and PINs secret. Period.
- Avoid using the same password or PIN everywhere. In particular, create different strong passwords to protect accounts that hold sensitive information like credit card numbers.

### 4 Minimize the chance you'll infect your device

- Don't give an app access to data when it doesn't make sense. For example, a calculator app doesn't need access to your contacts or location.
- Do not disable the security features of your devices: don't unlock (or *jailbreak*) your phone or turn off your firewall (say, for a game).
- Don't put any *unknown* flash drive or secure digital (SD) card into your device. Do not open files on these drives or cards that you weren't expecting.

## Don't be tricked into downloading malware

### 1 Download reputable apps

- Download apps, games, and software only from major stores and stick to those that are well-reviewed. Purchasing games and other apps from proprietary stores like Windows Store or iTunes helps reduce the risks of viruses and scams.
- "Free" offers of music, games, and the like are notorious for including malware.

### 2 Accept incoming content with care

- If someone sends an attachment or link that you didn't expect or isn't typical of the sender, it could be a virus or spyware—so confirm with the sender that the message is legitimate (preferably using another device).
- To block unwanted downloads and keep intruders from reading your data, turn off Bluetooth connectivity when you're not using it. Also, use near-field radio communications (NFC) cautiously: only tap tags with physical protections like glass or plastic, and bump phones only with people you trust.

### 3 Think before you click

Avoid clicking **OK**, **Agree**, or **I accept** in banner ads, in unexpected pop-up windows or warnings, on websites that may seem suspicious, or in offers to remove spyware or viruses.

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

0614 PN 098-108790