Fight Back! Tips for a Malware-Free Life

Prevent

The bad guys are constantly thinking up ways to trick us into downloading malware. They load it into Web sites, applications, videos, PDFs, photos – you name it. If they can convince us to click, link, install, or download their malware-packed offerings, we're sunk! The best advice to thwart their efforts comes from security expert Brian Krebs, who suggests three basic rules:

Rule #1: If you didn't go looking for it, don't install it!

Email attachments and links

Never click on a link or open an attachment in an email from an unknown sender. Even an email that appears to have been sent from someone you trust may actually be part of a twisted malware scheme. When in doubt, contact the sender and verify the email. Learn the signs of phishing emails.

Pop-ups

Never click on a pop-up window – especially if it mentions malware. Ironically, pop-ups claiming to scan for malware most likely carry malware. Don't click the "X" in the upper right-hand corner to close the pop-up – that, too, may load malware. Instead, right click over the ad and select "Close." Better yet, set your computer to block pop-up windows.

Downloads

Whenever possible, download software only from Web sites you know and trust. Be suspicious of free downloads from unknown companies. Think twice about downloading free screensavers and toolbars – they often carry malware and viruses.

Anti-Virus

Your computer should have anti-virus, and a firewall.

- Install security software from a reliable company and set it to update automatically.
- Set your operating system and web browser to update automatically too.
- If you are not sure how, use the help function and search for "automatic updates."

Rule #2: If you installed it, update it.

Cybercriminals try to exploit "vulnerabilities" (security flaws) in popular software (such as Java, Adobe PDF Reader, Flash, and QuickTime) to create openings for malware; in response, application vendors develop "patches" to fix vulnerabilities and distribute them to customers by way of free updates. Updating a software program effectively closes a door on malware. Update often at home but check with IT before trying anything like that at work - managing system updates is their responsibility.

Rule #3: If you no longer need it, remove it.

Unfortunately, new home computers often come loaded with lots of “bloatware” – software we didn’t ask for and won’t use. This stuff just sits on our machines and gets ignored. Plus there’s all that other junk we downloaded, then outgrew, that’s sitting on our system too. The problem? Unused software – whether we put it on the computer or not it – makes us more vulnerable to malware because we don’t update it. Get rid of the junk!

Detect

The goal of malware makers is generally mischief or money. Malware can be used to monitor or control what you do online, steal information, steal your identity, or send spam.

Got Malware?

- Your computer is slower than normal
- Excessive pop-up windows appear
- Your battery drains quickly
- Familiar or unknown software starts up unexpectedly
- Files, folders, or icons disappear
- Your browser displays a webpage you didn’t intend to visit
- Your computer won’t shut down or restart
- New toolbars or icons appear without your permission
- Your computer experiences unexpected errors or crashes
- Your contacts receive email messages from your account that you didn’t send
- You can’t download software updates
- Your antivirus software vanishes
- Your firewall becomes disabled

Act!

What to do if you suspect malware

- Stop shopping, banking, and any other online activity that requires passwords.
- Change all of your passwords – if possible use your work computer to do so.
- Update your security software, run a system scan, and delete anything that’s flagged as a problem.
- If you think your computer has malware, the Federal Trade Commission wants to know. File a complaint at www.ftc.gov/complaint.