First Financial
FEDERAL CREDIT UNION
Putting people first since 1936.

How to boost your malware defense and protect your PC

Protecting your home computers is essential in preventing virus infections and critical to keep your sensitive information and identity private.

Please review the following information from Microsoft and perform necessary action to protect your information from falling into wrong hands.

Free protection is available to help secure your computer against malware:

Build up your computer's defenses

Install antivirus and antispyware programs from a trusted source

- Never download anything in response to a warning from a program you didn't install or don't recognize that claims it will protect your PC or offers to remove viruses. It is highly likely to do the opposite.
- Get reputable anti-malware programs from a vendor you trust.
    - Windows 8 includes antivirus protection called Windows Defender. It's turned on by default.
    - If your computer is not running Windows 8, download Microsoft Security Essentials for free.
    - Choose security software that is compatible with Windows 7.

Update software regularly

Cybercriminals are endlessly inventive in their efforts to exploit vulnerabilities in software, and many software companies work tirelessly to combat these threats. That is why you should:

- 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 software updates whenever they are offered—for example, you can automatically update all Microsoft software. Windows 8 and Windows 7 turn on automatic updating during installation.
- Uninstall software that you don't use. You can remove it using Windows Control Panel.

Use strong passwords and keep them secret

- Strong passwords are at least 14 characters long and include a combination of letters, numbers, and symbols. Learn more about how to create them.
- Don't share passwords with anyone.
- Don't use the same password on all sites. If it is stolen, all the information it protects is at risk.
- Create different strong passwords for the router and the wireless key of your wireless connection at home. Find out how from the company that provides your router.
- Use our password checker.

First Financial
FEDERAL CREDIT UNION
Putting people first since 1936.

Never turn off your firewall
A firewall puts a protective barrier between your computer and the Internet. Turning it off for even a minute increases the risk that your PC will be infected with malware.

Use flash drives cautiously
Minimize the chance that you'll infect your computer with malware:

- Don't put an unknown flash (or thumb) drive into your PC.
- Hold down the SHIFT key when you insert the 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 any files on your drive that you have not expected to see.

Don't be tricked into downloading malware

Instead, follow this advice:

- Be very cautious about opening an attachment or clicking a link in an email, instant message, or post on social networks (like Facebook)—even if you know the sender. Call to ask if a friend sent it; if not, delete it or close the IM window.
- Avoid clicking **Agree, OK**, or **I accept** in banner ads, in unexpected pop-up windows with warnings or offers to remove spyware or viruses, or on websites that may not seem legitimate.
    - Instead, press **CTRL + F4** on your keyboard to close the window.
    - If the window doesn't close, 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 you start the browser.
- Only download software from websites you trust. Be cautious of "free" offers of music, games, videos, and the like. They are notorious for including malware in the download.
- Take advantage of technology—such as Windows SmartScreen in Windows 8—designed to help protect you from phishing scams and new malware that your anti-malware software hasn't detected yet. Learn more about Windows SmartScreen.

*Source: Microsoft.com