Computer Protection Tips

We use computers for everything. BUT….what happens when your computer is hacked? Here are some simple, yet very important steps you can take to help prevent hackers from accessing your computer and personal information.

Use strong passwords.

- **Back up your information often.** You can save your data to a CD, DVD, USB device or an external hard drive. That way, if your computer ever crashes or is hacked, you will not lose all of your information.
- **Never give someone remote access to your computer.** If you receive a call from someone claiming to be from Microsoft or any other company stating you have a virus or that they can fix other issues on your computer, hang up immediately. Scammers will try to convince you to pay for unnecessary services and get access to your computer to obtain personal information or install malicious software.
- **Update your operating system regularly.** Computer operating systems are periodically updated to stay current with technology requirements and to fix weak spots that may be targeted by hackers. Install updates to make sure your computer has the latest version. Often there are settings in your operating system to make these updates automatic.
- **Use strong passwords and change them often.** Do not use the same password for multiple accounts. Use passwords that contain upper and lower case letters, numbers, and symbols. Change your password every three months and do not reuse passwords. This is especially true for passwords that are used to access your email and bank accounts.
- **Use two-factor authentication.** Two-factor authentication is an added layer of security that combines something you have, a physical token

such as a card or a code, with something you know, something memorized such as a personal identification number (PIN) or password.

- **Do not click on pop-ups.** Pop-up windows on the internet are quick advertising tools, but beware of "too good to be true" offers. Not only can these pop-ups slow your computer and internet speed down, but by clicking on these you can accidentally sign up for unauthorized services. Set your browser's information bar to not allow pop-ups.
- **Be careful what you download.** Some of the most destructive viruses have been hidden in internet programs and applications or e-mail attachments. Download only from a trusted source. As for e-mails, never click on links or attachments if you do not recognize the sender. Even if you do know the sender, beware! It is possible their computer was hacked and is sending out infected e-mails. Those emails may also be very well disguised to look like often used financial institutions or retail websites, sent to phish for your personal information.
- **Do not send sensitive or private information via email.** Email is not usually encrypted, or in other words not in a "secret code," and can be intercepted and read by hackers.

- **Use antivirus software and set it to update itself daily.** There are many commercial products that can help you protect your computer from various viruses. Most virus protection software has a feature that will scan downloaded files automatically and some will even scan incoming emails by default.
- **Avoid installing unnecessary, unfamiliar, or untested software.** This includes games, toolbars or screensavers that could leave your computer open to attacks. Spyware and viruses are often installed by downloading unfamiliar programs. When you install software, choose a program that is not piggybacking other toolbars or software onto the installation. Look for automatically checked box items in the agreement page giving your permission to install these other items.
- **Use a personal firewall.** A firewall acts as a barrier between you and the internet. It helps keep hackers out and prevents malicious software from sending your personal information to criminals. There are free and retail versions available that come in both software and hardware.
- **Be careful of wireless networks.** For your home network, make sure your router is password protected. For public wireless access (such as at restaurants, libraries or cafes), be aware if the network is unsecured. Cyber criminals take advantage of unsafe networks to hack into your computer and access your personal data.
- **Turn your computer off when not in use.** Leaving your computer on and unattended could leave it open for an attack by hackers. Protect your computer, and save energy by turning your computer off when you are not using it.
- **Dispose of your old computer safely.** Make sure all personal data is removed by the wiping or physical destruction of your computer's hard drive.

If your computer has been hacked and you feel your safety is in jeopardy, or think that the hacker is someone you know, you should call your local police.

Contact a trusted, local computer professional to remove any malicious software that may have been installed.

Technology continues to change and evolve. You may not be able to prevent all hacking, but you can help equip yourself with the tools and knowledge to protect your computer from cyber criminals.

You may also find more helpful tips in our publication "Social Networking."

For more information or to file a complaint, visit our website or contact:

Wisconsin Department of Agriculture, Trade and Consumer Protection
Bureau of Consumer Protection
2811 Agriculture Drive, PO Box 8911
Madison, WI 53708-8911

Email: DATCPHotline@wi.gov
Website: datcp.wi.gov
(800) 422-7128 TTY: (608) 224-5058

IDTheftComputerProtection643 (rev 10/23)