Protecting Ohio's Families

Stay safe in cyberspace

Learn how to protect
your personal information
and avoid common
cyber scams.

Cybersecurity Help
Information, and Protection Program
(CHIPP)

MIKE DEWINE
OHIO ATTORNEY GENERAL

Cybersecurity has never been more important

Ohioans increasingly use multiple devices to connect to the Internet. From desktop and laptop computers, to smartphones and tablets, we are online more often and in more places than ever before. That's why cybersecurity, which helps protect computers and mobile devices from attacks and harm caused by malicious software, or malware, is so important.

Ohio Attorney General Mike DeWine's Cybersecurity Help, Information, and Protection Program (CHIPP) informs consumers about staying safe and protecting personal information while browsing the Internet, connecting through social media, and shopping online. Through CHIPP, you can learn how to protect your devices from malware and hackers, keep your personal information private, and avoid common cyber scams.

This guide provides a range of cybersecurity tips.

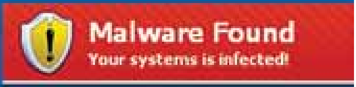
For additional information, call **800-282-0515** or visit **www.OhioAttorneyGeneral.gov/Consumers**.

Learn to recognize malware

Malware comes in many forms, but its aim is generally the same: to steal your personal information or harm your devices. With it, cybercriminals can infect your computer when you download files, access unfamiliar links, or click on pop-up windows disguised as messages or advertisements.

Common types of malware include:

- Viruses, designed to infect your computer and spread to other devices.
- Spyware, which tracks or “spies” on your devices to steal personal information, such as passwords and credit card numbers.
- Adware, programs that may display unwanted advertisements based on your Internet browsing habits.
- Ransomware, malware that holds devices hostage and demands you pay a fee to remove it.



Malware Found

Your systems is infected!

Beware of malware scams

Some scammers try to gain access to your devices by pretending to represent a technology or computer repair company. They falsely claim you have downloaded viruses that must be removed, then offer to “fix” the supposed problem by remotely accessing your computer. Instead of solving any problems, the scammers load malware onto your device or threaten to lock it until you pay.

Secure your home network

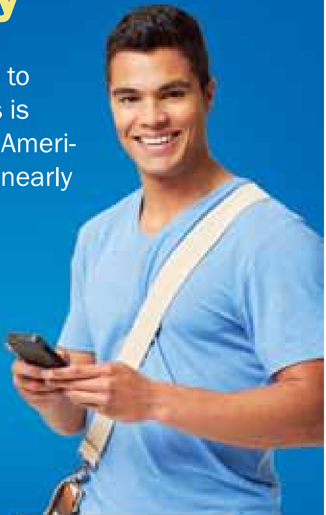
A home wireless network can include computers, gaming systems, printers, tablets, and other devices. To ensure yours is safe:

- Make sure your home Internet connection is behind a firewall, which is hardware and/or software that controls what comes and goes from your network. A firewall helps keep would-be intruders off home networks.
- Set and use a password on your wireless routers and network connections.
- Enable encryption, which scrambles data into an unreadable format when available.

Use mobile devices wisely

The number of people who connect to the Internet through mobile devices is constantly rising. More than half of American adults have smartphones, and nearly that many own tablets.

Mobile devices pose specific security concerns. Personal information can easily be taken if the device is lost or stolen. Also, the devices typically have geolocation features, allowing them to pinpoint your exact physical location in real time.



To boost privacy and security when using mobile devices:

- Set and use the locking feature, which requires users to have a password or passcode for entry.
- Remember that mobile phones are susceptible to malware and other viruses, just like computers.
- Disable geolocation and geotagging features. Geotagging occurs when an application or program displays and sometimes broadcasts the device's location to others.
- Turn off Bluetooth and Wi-Fi features when not in use.
- When you download apps, do so from reputable sources such as well-known Web-based stores.
- Keep apps and mobile operating systems updated to ensure any newly released security patches are loaded. Delete apps you no longer use.
- Beware of "SMiSHing," when scammers phish for information through text messages. Such text messages may include a link to a phony, but legitimate-looking website that asks consumers to update, validate, or confirm account information.
- Download a locator app, if available, from your mobile device's manufacturer. This app can trace the device if it is lost or stolen. It may also include features to remotely lock the device and/or wipe out the information it contains.

Safeguard your computer

Maintaining a clean computer is the key to combating malware. Following these suggestions will help:

- Install and maintain an anti-virus and anti-spyware program. Set the program to update automatically or check regularly for updates since new viruses are launched all the time.
- Scan the hard drive for viruses on a regular basis.
- Visit **www.staysafeonline.org** for a list of free security products to detect malware.
- Do not buy protection software or services based on telephone calls, pop-up advertisements, or email messages that allege your device has malware. They are probably scams.
- Install and use a pop-up blocker. They are often available free, including within some Internet browsers.
- Install and update personal firewalls, which filter incoming and outgoing data.
- Delete suspicious emails and text messages, even if they appear to be from a friend or trusted source. Do not click on links, open attachments, or download anything from a suspicious message.

Take precautions on public Wi-Fi

Using unfamiliar, unsecured wireless or Wi-Fi networks can put you at risk of downloading malware to your computing devices. To protect yourself:

- Verify the specific network name with the network owner before connecting to Wi-Fi in a public area.
- Never disclose personal information, such as logins, passwords, or credit card numbers when using an unsecure connection.
- Assume everyone can see what you are doing when you use a public network.

Protect your accounts

To prevent access to your personal information:

- Use strong passwords for each of your online accounts and change them regularly.
- Use unique passwords for each program, website, and application.
- Disable any automatic login functions on websites.
- Log off from each website and account when finished.

Please Login

Username: Username

Password: ●●●●●●

□ Remember Password

Set strong passwords

- All passwords should be at least eight characters long and include capital and lowercase letters, numbers, and symbols.
- Create passwords based on a phrase that uses a combination of letters and numbers. For example, "My dog's name is Brutus" plus a random number creates the password "MdniB239."

Use the Internet wisely

The Internet has made a world of information and networking options available at our fingertips. But it has also given scam artists and other criminals a powerful tool to carry out their crimes.

Keep up your guard and follow these tips for safe Internet usage:

- Each computer, Internet browser, and mobile phone has different ways to adjust security and privacy features. An Internet search can help determine how to best protect a specific device or browser.
- Operating systems and Internet browsers typically allow you to adjust security and/or privacy settings to your comfort level. Adjust Internet browser settings to at least “medium” security. These settings may, for example, filter out potentially harmful data and control the types of “cookies” that can be loaded by websites you visit. Cookies are sometimes used to track a user’s activity for marketing purposes.
- Whenever you disclose personal or financial information over the Internet, look for the lock symbol and the “s” in “https:” at the beginning of the website address. The “s” means the site is secure.

- If making online purchases, use a credit card instead of a debit card to best limit your financial risk in case personal information is misused.
- Know that some scammers “phish” for personal information using e-mails or phone calls that appear to be from your bank or a government agency and seek personal information, such as bank account numbers, pass words, or Social Security numbers.
- Never respond to unexpected requests for your personal information. Instead, contact the “source” at a phone number you trust. For example, call the phone number on your billing statement or the back of your credit card.

Exercise caution on social media

Follow these suggestions to protect yourself when using social media sites:

- Social media websites and apps each have their own default, or automatic privacy settings that control what you share. Familiarize yourself with the settings, understand what they mean, and know how to change them to meet your privacy needs.
- Privacy settings on one type of device may not carry over to your other devices. Be sure you're comfortable with the settings for all devices you use to connect to social media.
- Know whom you're sharing with on each site and device you use.
- Don't give out more personal information than necessary.
- Think about how others could use the information you share.
- Understand how your information will be used, saved, and shared, even after you're done visiting the site or using the app.
- If you're a parent, look at the age restrictions of the social media your children use and monitor their usage of such sites.

Dispose of devices responsibly

Make cybersecurity a priority whenever you dispose of, sell, or recycle a computer, mobile device, or USB jump drive.

- Take the device to a trusted source, such as a local electronics store, and have them wipe the hard drive and any other memory hardware clean.
- If you have any question about whether personal information has been completely removed from a device, talk to a trusted computer professional before disposing of the device.

RESOURCES

Ohio Attorney General's Office
800-282-0515
www.OhioAttorneyGeneral.gov

Federal Trade Commission
877-382-4357 (Consumer Complaints)
www.ftc.gov
www.FTC.gov/OnGuardOnline

Federal Communications Commission
888-225-5322
www.fcc.gov

Internet Crime Complaint Center
www.ic3.gov
www.VictimVoice.org

National Cyber Security Alliance
www.StaySafeOnline.org

STOP. THINK. CONNECT.
www.stopthinkconnect.org

U.S. Computer Emergency Readiness Team
www.US-CERT.gov

MIKE DEWINE
OHIO ATTORNEY GENERAL

For more information, to report a scam, or to schedule a speaker on consumer protection issues, contact Ohio Attorney General Mike DeWine's office at **www.OhioAttorneyGeneral.gov** or **800-282-0515**.

For TTY, please call Relay Ohio at **800-750-0750**.