Cybersecurity Help, Information and Protection Program (CHIPP)

Stay Safe in Cyberspace

Learn how to protect yourself online and avoid common cyberscams

DAVE YOST
OHIO ATTORNEY GENERAL

Cybersecurity has never been more important

From computers and smartphones to tablets and gaming systems, we are online more often than ever before. Cybersecurity is essential because it helps protect our devices, personal information and wallets.

Ohio Attorney General Dave Yost'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, keep your personal information private and avoid common cyberscams.

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 — short for malicious software — comes in many forms, and is aimed at stealing your money and personal information or harming your devices. Cybercriminals can infect your device with malware when you download files, access unfamiliar links or click on pop-up windows disguised as messages or advertisements.

Common types of malware include:

- Viruses, which are designed to infect your computer.
- Spyware, which tracks or "spies" on your devices to steal passwords, credit-card numbers or other personal information.
- Ransomware, which holds devices hostage and demands that you pay a fee to remove it.

Beware of computer-repair scams

Some scammers pretend to be a technology or computer-repair company. By phone or through a pop-up message, they falsely claim that you have downloaded a virus, then offer to "fix" the problem by accessing your computer. Instead of solving the problem, the scammers load malware onto your device or threaten to lock it until you pay them. Beware: If you're asked for payment via gift card, cryptocurrency or wire, it's likely a scam!

Secure your home network

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

- Set and use a password on your wireless routers and network connections. Change any default passwords.
- Enable encryption when it is available; it scrambles data into an unreadable format.
- Back up your hard drive regularly so you have a recent copy in case your device gets infected with ransomware or another harmful virus.

Use mobile devices wisely

Many people connect to the internet through mobile devices, which means personal information can easily be taken if the device is lost or stolen.

To boost privacy and security when using mobile devices:

- Set and use the locking feature, which requires facial recognition, a password or a passcode for entry.
- Remember that mobile phones, like computers, are susceptible to malware and other viruses.
- Disable geolocation and geotagging features except on a locator app. 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 that any newly released security patches are loaded. Delete apps you no longer use.
- Beware of text messages with a link asking you to update, validate or confirm your account information; such links are often fake and are used to take your personal information or money.
- 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 since new viruses are launched all the time.
- Scan the hard drive for viruses, and back up your data regularly.
- Do not buy protection software or services based on unexpected calls or messages that allege your device has malware. They are probably scams.
- Install and use a pop-up blocker. The program is often available for free, including within some internet browsers.
- Delete suspicious emails and texts, 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.
- Never allow a stranger remote access to your device.

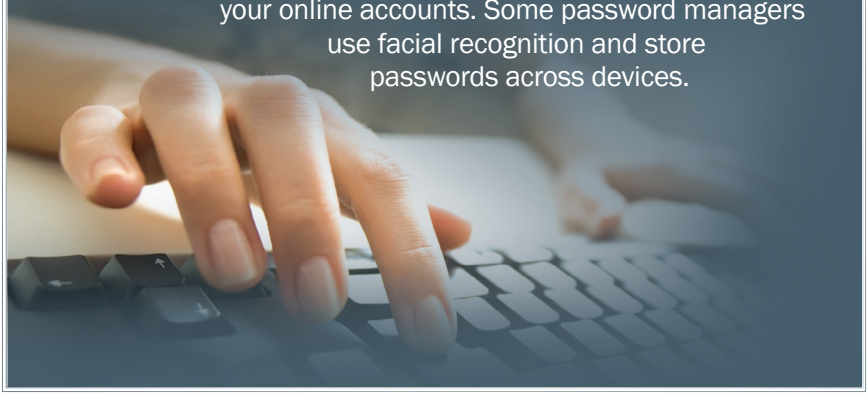
Take precautions on public Wi-Fi

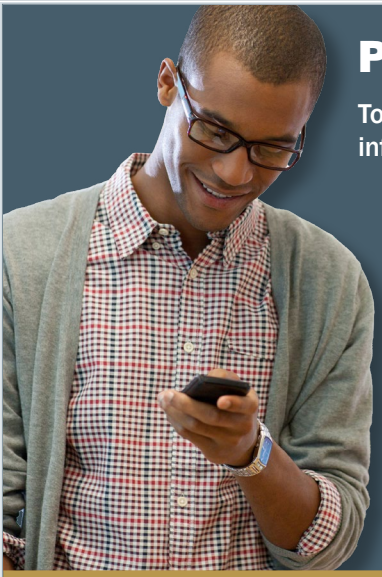
Using unfamiliar, unsecured wireless or Wi-Fi networks can put you at risk. To protect yourself:

- Verify the specific network name with the network owner before connecting to Wi-Fi in a public area.
- Never disclose personal information — logins, passwords, and credit card numbers — when using an unsecure connection.
- Assume everyone can see what you are doing when you use a public network.
- Consider using a reputable virtual private network (VPN) to help better secure your data and protect your privacy.

Set strong passwords

- All passwords should be at least 12 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 first dog’s name was Max” plus a random number and a symbol create the password “MfdnwM@x239!”
- Consider using a reputable password manager. Typically, a password manager requires you to remember a “master password,” then can develop long, unique passwords for your online accounts. Some password managers use facial recognition and store passwords across devices.





Protect your accounts

To prevent access to your personal information:

- Use strong and unique 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 and Wi-Fi networks.
- Log off from each website and account when finished.

Use the internet wisely

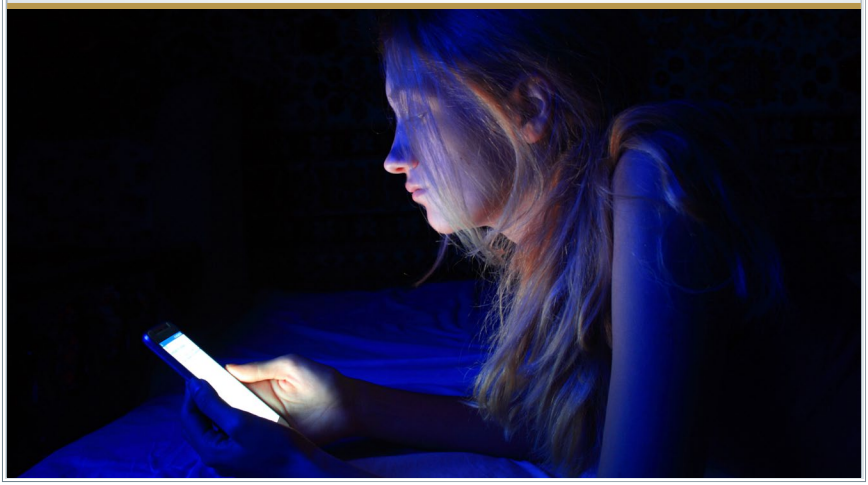
Keep up your guard and follow these tips for safe internet usage:

- Enable multifactor authentication whenever offered. This feature requires an additional step beyond entering your password to access your account such as entering a passcode sent to you.
- Each device and internet browser has different ways to adjust security and privacy features. Run an internet search to help determine how to protect your devices.
- Whenever you disclose personal or financial information online, 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.
- Know that some scammers “phish” for personal information using emails or phone calls that appear to be from your bank or a government agency and seek personal information, such as bank-account numbers, passwords 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:

- Every social-media site and app has its own 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.
- Know who you're sharing with on each site you use.
- Don't give out more personal information than necessary.
- Think about how others can access and 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.
- Beware that social-media accounts can be hacked, and remain suspicious if a "friend" contacts you with an out-of-the-ordinary request.
- 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 your device.

- Take the device to a trusted source — a local electronics store, for example — and have the hard drive and any other memory hardware wiped clean.
- If you have any questions about whether your information has been completely removed, talk to a trusted computer professional; if you can restore your data, so can a scam artist.
- Remember that even small pieces of equipment — such as jump drives or memory cards — may contain information that you'll want to clear before disposing of them.
- **Final Tip!** Remember to exercise extreme caution with anyone who unexpectedly contacts you via the internet, especially if they ask for payment via cryptocurrency, gift card or cash.

DAVE YOST

OHIO ATTORNEY GENERAL

Resources

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

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

National Cyber Security Alliance
www.StaySafeOnline.org

STOP. THINK. CONNECT.
www.stopthinkconnect.org

U.S. Cybersecurity & Infrastructure Security Agency
www.cisa.gov

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

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