

Cybersecurity tip emails

Tip 1

Subject line:

Cybersecurity Tip: Create Strong Passwords and Update Them Frequently

- **Lock down your login:** Fortify your online accounts by enabling the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device. Your usernames and passwords are not enough to protect key accounts like email, banking, and social media.
- **Make your password a sentence or phrase:** A strong password is a sentence with at least 12 characters. Focus on positive sentences or phrases that you like to think about and are easy to remember (for example, "I love country music."). On many sites, you can even use spaces.
- **Unique account, unique password:** Having separate passwords for every account helps to thwart cybercriminals. At a minimum, separate your work and personal accounts and make sure your critical accounts have the strongest passwords.
- **Write it down and keep it safe:** Everyone can forget a password. Keep a list stored in a safe, secure place away from your computer. Or use a service like a password manager to keep track of your passwords.

For more information, visit: stopthinkconnect.org

Tip 2

Subject line:

Cybersecurity Tip: Connect It. Protect It.

- **Protect all devices that connect to the internet:** Along with computers, smartphones, gaming systems, and other web-enabled devices also need protection from viruses and malware.
- **Keep security software current:** Having the latest security software, web browser, and operating system is the best defense against viruses, malware and other online threats.
- **Get savvy about Wi-Fi hotspots:** Limit the type of business you conduct and adjust the security settings on your device to limit who can access your machine.
- **Plug and scan:** USBs and other external devices can be infected by viruses and malware. Use your security software to scan them.
- **Back it up:** Protect your valuable work, music, photos, and other digital information by making electronic copies of your important files and storing them safely.

For more information, visit: staysafeonline.org and stopthinkconnect.org

Tip 3

Subject line:

Cybersecurity Tip: Securing Your Wireless Network

Widespread teleworking provides new opportunities for cybercriminals. Your home Wi-Fi network is a potential path for unauthorized access to not only your private information but also to State of Ohio information. What can you do to secure your wireless network?

- **Change the default name of your home Wi-Fi network.** The service set identifier, or SSID, is the name of your network. Many manufacturers give every wireless router the same default network name. If you don't change this default name, you are giving a hacker a much better chance of breaking into your network. Choose an unusual name that doesn't disclose any personal information.
- **Make your Wi-Fi network password unique and strong.** Most wireless routers have a pre-set default password that hackers can easily guess. Change your password to a pass phrase that is at least 20 characters long and includes numbers, letters, and symbols. Make sure your password is stored safely and is not readily accessible to others.
- **Enable network encryption.** Almost all wireless routers include an encryption feature, but it may be disabled by default. Look for WPA2 or WPA3 protocols. Activating encryption on your wireless router can help to secure your network and data.
- **Keep your router firmware up to date.** Check periodically for updates that address known security exploits. Your product manual or the manufacturer's support website can provide the steps you'll need to complete these critical tasks.
- **Ensure your router's administrative password is unique and strong.** Also, disable the remote administration option to prevent access to your router configuration from the internet.
- **Update your network devices too.** A network is only as secure as its weakest device. We typically think about PC patches and updates, but lots of other devices on your network have security vulnerabilities. These too need to be updated regularly. Examples include printers, smart televisions, speakers, streaming media controllers, phones, watches, tablets, home security systems, game consoles, and even appliances. Think about anything that connects to your home network.
- **Consider disabling Wi-Fi when you are away.** If you plan to be away from home for more than a day, one simple security measure is to turn off wireless access. But remember that some devices, like connected thermostats, may require internet access.

For more information, visit: staysafeonline.org and stopthinkconnect.org

Tip 4

Subject line:

Cybersecurity Tip: Avoid Phishing Attempts

Phishing is a common way wanna-be data thieves prey on State employees. Phishing occurs when scammers, usually posing as a trustworthy source, use email to attempt to get you to divulge personal information such as usernames and passwords.

Be aware if a message:

- Is from **someone you don't know**.
- Is from someone you know but **isn't expected**. Check the underlying email address, not just the name.
- **Contains hyperlinks**. They may not take you to the site you are expecting. Always check the URL.
- **Contains an attachment** you were not expecting. Only open attachments you are expecting.
- **Urges you to take immediate action**, especially if it elicits fear: "Your account has been hacked!" Or "Your account will be deactivated."

If you think you have received a phishing email, **contact your IT department or click the "Phish Alert" button** in the upper right of your email, if you have one.

For more information, visit the U.S. Cybersecurity and Infrastructure Security Agency's website at cisa.gov.