Ring in the new year cyber-safely!

It's a new year! Let's start with some new habits to keep you cyber-safe!

Hover over links

Links in emails, texts or direct messages can contain malware. One way to verify whether the link is legitimate is to hover your pointer over the link (do not click!) and check the URL at the bottom of the screen. This URL will show you where the link will take you — and if it says the website you were expecting, great! If it doesn't match what you expected, it's time to be cautious.

If you aren't certain, the best thing to do is go to the website through your browser. This way, you know you are getting there safely.

Report suspicious messages and ask for help

If you receive a suspicious message or phone call at work, immediately report it to the correct point of contact. The more quickly you report suspicious activity, the sooner the security team can tackle any issues.

Cybersecurity can be confusing. Don't hesitate to reach out if you have any questions or concerns about these matters. The experts will know how to handle tough situations.

Use a lock screen

People often walk away from their computers without thinking about locking them. Now that many people are back in the office or able to work outside of the house, such as in a coffee shop, it is critical that we get in the habit of locking our screens every time we step away from our devices. It may only take a hacker a few clicks or even a quick glance to obtain sensitive information from your device.

Create different passwords for each account

Using different passwords for each account ensures that if one password has been compromised, others won't be. Using unique passwords for each account reduces the risk of a security incident.

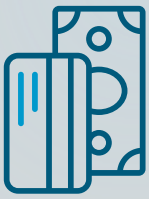
Complete security awareness training

Security awareness training is important to keep you and your organization safe. Completing awareness training ensures that people know to act appropriately when there is a cybersecurity situation. Training helps develop important skills and habits to be better employees. You are an important part of cybersecurity!

Brrr — Leave hackers out in the cold!

With the number of data breaches, everyone's information has been exposed at some point. A hacker can use your personal information to open credit cards in your name. One way to stop this from happening is to freeze your credit. You can freeze your credit with the big three credit bureaus — Experian, Equifax and TransUnion. You do this by creating a PIN that only you know. This will stop anyone from opening a credit card in your name.

Hot tip: You will need to unfreeze your information if you are applying for a loan or opening a credit card, as your credit information will need to be available.



Cybersecurity roles — Penetration tester

Have you ever wondered what your friendly cybersecurity team is up to? Each month we will share a cybersecurity job role to give you an inside look!

Penetration tester

Penetration testers act like hackers and hack into their organization's resources. The purpose is to simulate a real hack and cyber security penetration testing is a safer way for organizations to gauge their security than to wait for a real-time hack.

E-TECH