TECH LINK

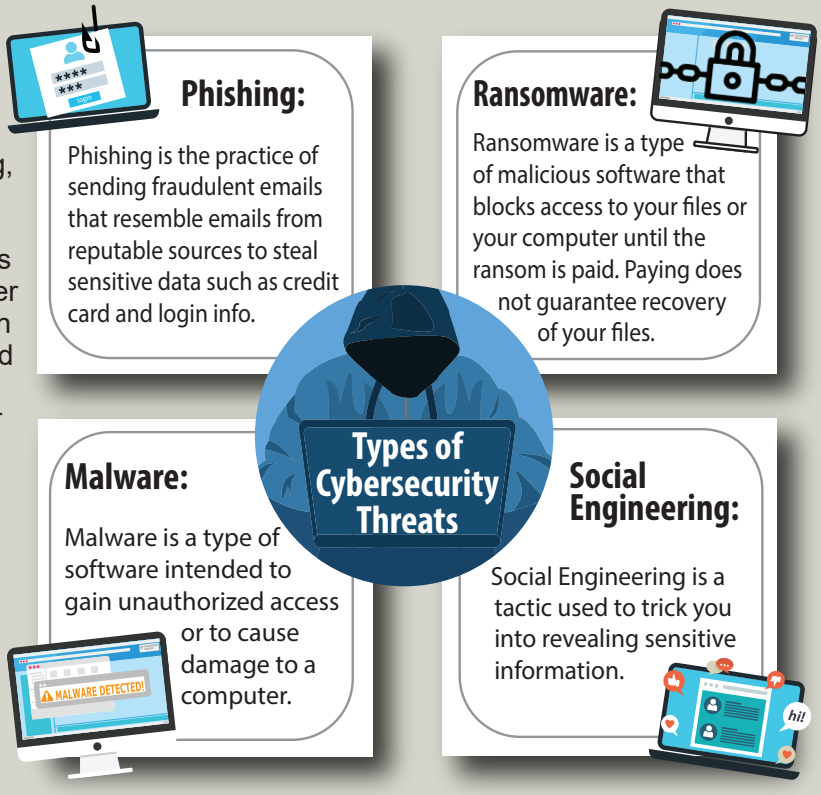
October is National Cybersecurity Awareness Month

In today's digital world, many of us use multiple devices that are connected to the internet every day for personal and business use. As the amount of digital devices increases, so does the risk of cybersecurity threats. Since October is National Cybersecurity Awareness month, we are taking this opportunity to share these valuable reminders from Cisco.

What is Cyber Security?

Cybersecurity is protecting systems, networks, and programs from digital attacks. Cyber-attacks are usually aimed at accessing, changing, or destroying sensitive info. On an individual level, a cybersecurity attack can result in anything from identity theft to the loss of valuable data like family photos. On a larger scale, we all rely on critical infrastructure such as power plants, healthcare organizations and banking institutions. Keeping these types of organizations secure is crucial to keeping our society functioning.

While MVEC takes the necessary steps and precautions to protect the company's data as well as our members' confidential information within the company's network, MVEC does not provide cybersecurity for our MVlink members' personal data on their own devices on their own network. It is up to you to understand the threats listed and do what you feel is necessary to protect your own devices and network.



Top 10 Cybersecurity Tips

1. Realize attacks can happen to anyone, anytime, anywhere, on any device.
2. Practice good password management. Use a strong mix of characters, and don't use the same password for multiple sites.
3. Never leave your devices unattended. Lock the screen so no one can use.
4. Always be careful when clicking on attachments or links in email. If an email is unexpected or suspicious for any reason, don't click on it.
5. Sensitive browsing, such as banking or shopping, should only be done on a device that belongs to you, on a network that you trust.
6. Back up your data. Make sure your antivirus software is always on and up to date.
7. Be conscientious of what you plug in to your computer. Malware can be spread through infected flash drives, external hard drives, and even smartphones.
8. Watch what you're sharing on social networks.
9. Be wary of social engineering, where someone attempts to gain information from you through manipulation.
10. Be sure to monitor your accounts for any suspicious activity.