MITIGATING CYBERSECURITY RISKS WHILE WORKING FROM HOME

PROTECT YOUR DATA

Cybercriminals create email addresses and website that look legitamite. Hackers can even take our company social media accounts and send seemingly legitimate messages. Be careful!

AVOID POP-UPS, UNKNOWN EMAILS, & LINKS

Phishers try to trick you into clicking on a link that may result in a security breach. It's important to be cautious of links & attachments in emails from senders you don't recognize.

USE STRONG PASSWORD PROTECTION & AUTHENTICATION

Strong, complex passwords (at least 10 characters, including numbers, sybols, and capital and lowercase letters) can help stop cyberthieves from accessing company information.

CONNECT TO SECURE WI-FI

Public wi-fi networks can be risky and make your data vulnerable to interception.

ENABLE FIREWALL PROTECTION AT WORK & HOME

A firewall for your home network is the first line of defense in protecting data against cyberattacks.

INVEST IN SECURITY SYSTEMS

All the devices you use at work and home should have protection of strong antivirus and malware detection security software.

INSTALL SECURITY SOFTWARE UPDATES & BACK UP YOUR FILES

Following IT security best practives means keeping your security software, web browsers, and operating sustems updated with the latest protections.

TALK TO THE IT DEPARTMENT

Your IT department is here to assist you! Reach out to your support team about information secuty.

EMBRACE EDUCATION & TRAINING

Your responsibility includes knowing company cybersecurity policies, what's expected of you, and following those policies. If you have questions or are unsure of a IT policy, ask!