CYBER SECURITY

WHEN WORKING FROM HOME

When working remotely, it's important to stick to the same cyber safety guidelines as though you were in the office. With the FBI reporting an uptick in cyber crime related to coronavirus,[1] it's important to stay vigilant while connected at home.

Cyber Security Tips:

Use Strong Passwords

Passwords for WiFi and work accounts should be unique and tough to crack. Start with a special phrase that is at least 12 characters. Incorporate uppercase and lowercase letters, numbers and special characters. Avoid including personal information, and don't use the same password for everything.

Double Up on Security

Multi-factor authentication gives your work accounts an extra layer of security. This feature requires you to confirm your identity by way of another device when logging in somewhere new. Also consider requiring a password for online video conference calls.

Updates Matter

Install the latest updates for all devices, programs and apps, which typically include improved security measures. Where possible, opt for automatic updates.

Consider a VPN

If your company does not use a Virtual Private Network (VPN), consider investing in your own. This software secures your network to reduce your risk of a hack. Popular services include NordVPN and ExpressVPN.

New message

Watch Out for Fake Emails!!!

Cc Bcc

Hackers often target individuals first with personalized fake emails, or phishing emails. Before you act:

Review the Sender's Email Address: It may look like a message from your bank or a colleague, but a misspelled or incorrect email address indicates it's fake.

Hover, Not Click: Place your cursor over the link to read the URL. An unrecognizable site is a big red flag, so don't click it.

Check the Tone: Urgent, fearful messages requiring immediate action and a deadline are typically fake — even if they look like they're from a co-worker.

Report It: Notify your IT department immediately of the message following company protocol.