

CYBER SECURITY

When Working from Home

With the FBI reporting an uptick in cyber crime related to COVID, it's important to stay vigilant while connected at home.

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.

WATCH OUT FOR FAKE EMAILS

Hackers often target individuals first with personalized fake emails, or phishing emails. **Review** the sender's email address to make sure it is not misspelled. **Hover**, don't click, to read a URL before proceeding. **Check the tone**, and remember that 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** and notify your IT department immediately of the message following company protocol.

KEEPING YOUR KIDS SAFE ONLINE



KNOW WHAT YOUR KIDS ARE UP TO

Understand your kids' Internet habits. Know what sites they visit for school and for fun, and talk to them if you see something unusual.



BLOCK DANGEROUS WEBSITES

Talk to your Internet provider if you want to block certain websites from your network.



SET THE GROUND RULES

Consider asking your kids to stay nearby when they're using their devices and setting rules for what sites they can visit and when — i.e. YouTube allowed after school hours only.



HAVE A CONVERSATION

Outline the rules and set expectations for responsible online behavior.

Educate kids on cybersafety so they understand for themselves the risks of unfamiliar websites, mysterious downloads and conversations with strangers on the web.

Share tips on creating strong passwords, protecting personal information and using social media safely — especially relevant for teens and tweens.

SHOUT OUTS!

Congrats to Joe and JoAnn P. on your South Loop sale!

Congrats to Mike and Ellen P. on your sale and move to a new city!

Congrats to Britta R. on your great new LP condo!!