CYBERSECURITY *Checklist*

Whether you're working from home or in the office, it is important to keep your professional devices secure so that you are strengthening your organization's defense against cyber attacks and data breaches. Here's what you need to know to protect your devices and your organization.

- **Familiarize yourself with your company's data security policies** and be sure to follow them.
- **Set a strong password or PIN** for all work devices. Strong passwords have a combination of upper and lower case letters, numbers, symbols, with eight or more characters to be guess-proof.
- **Set up multifactor authentication** for any software that offers it. One example includes using both a password and a code sent to your phone to log in. If you have two factor authentication, you can choose long passphrases, at least 16 characters, that include a string of unrelated words.
- **Don't click on links** or open attachments in unsolicited emails or text messages.
- **Watch out for phishing emails and phone scams.** Always verify requests for sensitive information via phone using a company directory and not any contact information in the email itself.
- **Regularly participate in cybersecurity training** to stay informed of new cyber threats. New scams emerge daily, so keep up with the latest information!
- **Use a Virtual Private Network (VPN)** to protect your internal network. If your company provides VPN, be vigilant in connecting to the VPN each workday
- **Keep all antivirus software and security patches** from your organization current. When your computer advises you that a restart is needed, be sure to do so as soon as possible.
- **Remember that IT support is available** as a resource. If you see anything suspicious, contact your IT department for guidance before clicking or taking action.