MINNESOTA TRUCKING ASSOCIATION'S

CYBERSECURITY quick start guide

PROTECT THE ENDPOINTS. Install or turn on Microsoft's free Defender. If you can invest in further protection, MalwareByte's Pro is an essential next step.

PROTECT THE NETWORK. A next generation firewall (NGFW) like Meraki, Fortinet, even Cisco's small business offerings are essential. Buy what you can afford, as much as you can afford for this.

FILTER EMAILS. Put in place Spam filtering and protection. Check with your email provider first to see what they offer (e.g. Office 365 or Gmail) or look at best of breed solutions like Mimecast or Avanan.

PROTECT PASSWORDS. Turn on strong passwords (12 or more characters long, mix upper and lower case as well as non-standard characters like !@#$%^&* etc.), and if possible use Multi Factor Authentication (MFA) over SMS messaging to your cell phones. Use 1Password, Dashlane or other password managers. Do not save passwords in your browsers.

BACKUP DATA. Backup your data at least nightly and store a copy in the cloud as well as on a different local device (preferably one you can rotate off site). Wasabi is an inexpensive cloud storage for backups.

SECURE WIFI. Secure your WiFi access points. Change any new hardware's default passwords as soon as you set them up. Secure the new passwords in your password manager shared folder. Share only with "Need To Know" people.

RESTRICT ACCESS. Remove all local administrator access for end users. Check with your IT resource if you need assistance with this.

AUTOMATIC UPDATES. Setup automatic software patching wherever possible for each device (PC, laptop, mobile). Access this via your computer's control panel, select "Update and Security".

REMOTE OR PERSONAL THREATS. Whatever threatens a device working remotely, whether issued by the company or personal (e.g. cell phone) threatens the company. Look to make proper provisions for employees who work remotely or use their own devices as part of their roles. Implement best practices as noted above to ensure remote devices do not allow bad actors to compromise your systems.

EDUCATE YOUR EMPLOYEES. Educating your employees may be the most critical step. If you can build a "Human Firewall" you can greatly reduce your attack surface. Knowbe4 is an affordable option. You may also find that your email services and/or spam filtering vendor has this available at nominal or even free prices.

SHRED. Shred that paperwork before throwing it out. Dumpster divers can find ways to compromise employees and vendors alike.

ENGAGE A SECURITY MONITORING SERVICE. There are free trials that can show you what to fix, and even free accounts that are a good gauge of things changing in your environment and even those of customers and vendors. Panorays or Security Scorecard trial will give you a list of what to fix and establish a patch/update cadence.

SECURE THE PROPERTY. If physical security is a concern find a reasonable camera system that has cloud capabilities like Spot.Ai.

DEVELOP AN INCIDENT RESPONSE PLAN. With the basics in place, work with your team to develop a robust Incident Response Plan (IRP). The MTA offers a model plan free to all members.