TSG's Digital Security "Quick Wins"

Take the following actions once a week or twice a month at minimum. Make sure you have time to shut your computer down without interrupting any pending work. There are three custom scripts that will be doing the heavy lifting for you.

Email Security:

- Use a password manager to generate and store strong, unique passwords on email accounts
- Turn on two-factor authentication
- Do not use personal email accounts for company business Employees should know not to open suspicious links in email, tweets, posts, online ads, messages or attachments – even if they know the source.
- Employees should also be instructed about your company's spam filters and how to use them to prevent unwanted, harmful email

Mobile Devices:

- Update security software regularly. Go ahead, update your mobile software now.
- Delete unneeded apps and update existing apps regularly
- Always download apps from a trusted source and check reviews prior to downloading
- Secure devices with passcodes
- Turn off Discovery Mode
- Configure app permissions immediately after downloading

Wi-Fi Security:

- Use separate Wi-Fi for guests or customers than you do for business
- Physically secure Wi-Fi equipment
- Use a virtual private network (VPN) when using public Wi-Fi
- Do not connect to unknown, generic or suspicious Wi-Fi networks. Use your mobile carrier's data plan to connect instead
- Turn off Wi-Fi and Bluetooth when not in use on your devices
- Secure your internet connection by using a firewall, encrypt information and hide your Wi-Fi network

Routers:

- Change from manufacturer's default admin password to a unique, strong password
- Use a network monitoring app to scan for unwanted users
- Restrict remote administrative management Log out after configuring
- Keep firmware updated

Point-of-Sale Systems:

- Use a password manager to generate and store strong, unique passwords
- Separate user and administrative accounts
- Keep a clean machine: Update software regularly
- Avoid web browsing on POS terminals

Website Security:

- Keep software up-to-date
- Require users to create unique, strong passphrases to access
- Prevent direct access to upload files to your site Use scan tools to test your site's security – many are available free of charge
- Register sites with similar spelling to yours

Social Media:

- Limit who has administrative access to your social media accounts
- Set up 2-factor authentication
- Configure your privacy settings to strengthen security and limit the amount of data shared. At the very least, review these settings annually
- Avoid third-party applications that seem suspicious, and modify your settings to limit the amount of information the applications can access.
- Make sure you're accessing your social media accounts on a current, updated device and web browser or app.

Software:

- Make sure your computer operating system, browser, and applications are set to receive automatic updates
- Ensure all software is up-to-date.
- Get rid of software you don't use, Your company should have clear, concise rules for what employees can install and keep on their work computers
- When installing software, pay close attention to the message boxes before clicking OK, Next or I Agree
- Make sure all of your organization's computers are equipped with antivirus software and antispyware. This software should be updated regularly
- Limit access to data or systems only to those who require it to perform the core duties of their jobs.