CYBERSECURITY CHECKLIST
for Employees

Hackers pose a critical threat to your business' cybersecurity, and incidents are increasing. Why? Because most employees don't know how to identify phishing scams and other cyber threats that can lead to a network infection or intrusion.

When your staff is properly trained they're your first line of defense – and this training should not only include things like strict passwords and policies, but extend to their workspace and behaviors. Here are a few tips to start off your training.

- [ ] **Always keep your system, software and web browsers up to date.**
  If you don't, you're leaving your system exposed to viruses, malware and intrusions.

- [ ] **Lock down your computer.**
  Never leave your laptop or desktop computer on when you step away from your desk. Make sure they are set to lock within a very short period of time.

(703) 600-3301 • sales@nachnet.com
Nachnet.com • 14001C Saint Germain Dr • Suite 194 • Centreville, VA

nachman NETWORKS
Networks Done Right

☐ **Be cautious when online.**
Don't open websites that appear suspicious, and never open a link or advertisement from an email unless you know who it's from. Do the same on social media sites like Facebook, LinkedIn or Twitter. These links and ads could contain malicious viruses.

☐ **Watch out for phishing scams on email.**
Phishing attacks are increasingly sophisticated and becoming more difficult to spot. You must be vigilant:

- Hover over links to see the actual email address of the sender. Don't open attachments unless you're 100% sure of where they came from.
- Beware of banner ads, especially those offering gifts that are too good to be true.
- Never share personal information from a link clicked in an email. Stick to the phone or a website that you proactively navigated to over a secure connection.
- Be cautious when receiving a non-personalized email from an individual you only know slightly, and that asks you to open an attachment or share information.
- If you have the slightest question about whether activity is suspicious or not, report it to your IT service provider or technical team.
- Bump up spam filters to their max settings. Yes, you will likely miss a few emails from friendly sources, but you're more likely to block criminal activity with tighter security settings.

☐ **Use strong passwords and user names.**
The difference between a good password, and a weak one is the major determining factor in protecting your online information. The best practice in terms of password security is to NOT use words that can be found in the dictionary. Use long codes with 10 distinct characters or more, that also contain symbols and other special characters to increase complexity. The same goes for usernames – avoid common ones such as "User1". Consider using a Password Manager like LastPass or DashLane.

☐ **Always use a PIN or Password to open your computer devices including your phone and tablet.**
It's important to password protect these devices to keep others from accessing your data if they're lost or stolen. You can also use locator apps like Find my iPhone, and set it to automatically wipe sensitive data from it after a number of failed login attempts.

Questions? Need help training your employees?
Contact Nachman Networks at (703)600-3301 or sales@nachnet.com

(703) 600-3301 • sales@nachnet.com
Nachnet.com • 14001C Saint Germain Dr • Suite 194 • Centreville, VA

nachman NETWORKS
Networks Done Right