CYBER CHECKLIST:
Securing Your Cyber Infrastructure

This cybersecurity checklist was developed to assist you in protecting your infrastructure against malicious actors. This is not an exhaustive list, as good security requires constant attention based upon evolving risk. Implementing these protocols, and instilling a culture of digital vigilance, will put your team in the best position to focus on fighting fires instead of battling the consequences of a cyber incident.

Use Multi-Factor Authentication (MFA)

Multi-factor authentication allows an extra layer of security for email, social media, and database accounts by requiring users to provide a second login beyond the user's password. Request free MFA tokens at: **State and Local Cybersecurity Grant Program**

Implement Strong Password Practices

- Use password managers to secure all of your passwords. Password managers allow you to manage all your accounts in one place. Make sure to review a password manager before selecting.
- Use a long password to access the password manager. We recommend using a unique string of words or a passphrase that can be easily remembered, but difficult to guess.
- Use different passwords for all accounts, including email and social media.

Enable Auto-Update to Install Security Patches in a Timely Manner

Once patches are available, quickly install onto the operating systems of your computers, mobile devices, and databases. Unpatched systems pose unnecessary risks to your systems.

Ensure Your Team is Well Trained on Basic Cyber Hygiene

Did you know that human error accounts for up to 95% of cybersecurity breaches? A well-trained and informed workforce is your first and most important line of defense.

- Request free cybersecurity training for leadership and fire departments at: **NH Municipal Cyber Defense Program**
- Have a municipal employee covering your IT? Request free Security+ training for them at: **State and Local Cybersecurity Grant Program**
- Not sure where to start implementing organizational cybersecurity practices? Check out: **Cyber Essentials/CISA**
- Don't have a lot of time for training? Micro-trainings are available for Primex members at: **Micro-Trainings/Primex**

Have a Plan to Respond to Cyber Incidents

Despite following these practices, cyber incidents may occur. Have a plan in place to respond and know which authorities to contact depending on the type and severity of the incident.

- If you are a Primex member, reach out to Cori Casey at **ccasey@nhprimex.org** for tailored assistance in developing a municipal incident response plan covering your fire department.
- If you are not a Primex member, contact **richard.rossi@cisa.dhs.gov** for assistance

Ensure Your Network is Managed and Technology is Supported

- Active management and patching of a network is critical to preventing cyber attacks.
- Use of unsupported (or end-of-life) software and hardware s dangerous and significantly elevates risk of cyber attack. This dangerous practice is especially egregious in technologies accessible from the Internet

Beware of Phishing Attempts

Phishing is a common attack where emails, texts, or other communication are sent to entice a user to provide their username and password, open an attachment that has destructive software hidden in it, or click a link that directs them to a website containing malicious software.
Protect yourself from phishing attacks:

- If the content of a message seems unusual or out of the norm for the sender, or it is from a sender you do not recognize, do not open an attachment or click a link until you have contacted the sender.
- Take a second to review links and attachments before opening.
- Haven't migrated to a .gov domain? Request free assistance at: **State and Local Cybersecurity Grant Program**

New Hampshire DoIT