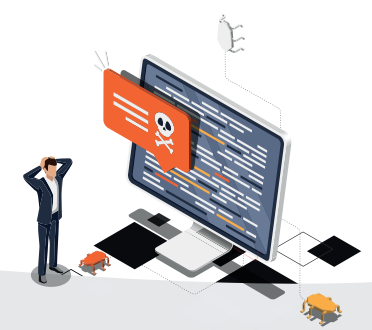# Cyber Security Checklist

12 Steps to Protect Your Business

Security Assessment

Perform a review of your current systems to identify where you may be vulnerable today and what must be done to protect your business.

Security Awareness Training

Train your employees. Teach them about data security and email attacks. Ongoing semi-annual training plans should be implemented for all employees.

Endpoint Protection

Protect your computers and data from malware, viruses, and cyber attacks. Replace your outdated antivirus solution with endpoint protection to guard against file-less and script based threats.

Firewall Hardening

Your router is the gateway to your business from the internet. Turn on Intrusion Protection and Prevention features. Ongoing network monitoring should be considered essential.

Spam Email Protection

Secure your email. Most attacks originate in your email. It is critical to employ advanced phishing prevention, detection and response.

Computer Updates

Keep Windows, Office and other software updated to ensure protection from the latest known attacks. Cyber criminals exploit software vulnerabilities to gain access to computers and data.

Web Filtering

Internet security is a race against time. Implement Web Filtering to block malicious links & websites to protect employees when they are on the internet.

Passwords

Apply security policies on your network to force strong passwords. Set user screen timeouts and limit user access. Provide users with a password security vault to encrypt their passwords.

Data Backup

Have an online backup that can be restored so you can immediately recover from any data corruption or loss resulting from security breaches.

Dark Web Research

Monitor the Dark Web and take corrective action to protect your business from stolen credentials that have been posted for sale on the internet.

Mobile Device Security

Cyber criminals can steal data or access your network by way of your employees' phones and tablets. They're counting on you to neglect this piece of the puzzle. Mobile device security closes this gap.

Two-Factor Authentication

Setup Two-Factor Authentication whenever you can—including on your network, email and business applications. By adding this additional layer of protection, even if a password is compromised, your data stays protected.