303.786.7474 | info@pei.com | www.pei.com

IT SECURITY ESSENTIALS FOR BUSINESS CHECKLIST

ESSENTIAL PIECES YOU NEED FOR IT SECURITY

You know IT security is an essential piece of your business strategy, but where should you start? For a strong foundation that protects users, data, and devices across your entire security ecosystem, use our checklist. If you need help, ask about our **Advanced Security Package, where we implement, manage, and monitor all these elements and more** to provide comprehensive coverage against current and evolving threats.

☐ MULTI-FACTOR AUTHENTICATION

Both Microsoft and Google have stated implementing multi-factor authentication would eliminate 99% of account breaches.

Multi-factor authentication prevents attacks even when user credentials have been compromised and is essential for all accounts—admins especially.

☐ EMAIL FILTERING & SCANNING

91% of cyber attacks start with an email. Advanced email filtering and capabilities like safe links and safe attachments can prevent emails from even landing in user inboxes—because you can't rely on users to always be vigilant!

☐ DNS FILTERING

DNS filtering is your last line of defense when users click on malicious links, blocking malicious destinations before a connection is established. DNS filtering can stop infections from phishing, malware, ransomware, and more.

☐ FAILED LOGIN MONITORING

It's not enough to enforce strong password policies and hope brute force attacks fail.

You need reporting that captures login events for each of your devices. Equally important is analyzing these reports regularly to assess patterns and detect malicious behavior before a data breach occurs.

☐ ANTIVIRUS & ANTIMALWARE

New exploits are being found and sold with alarming frequency, and even the most cautious web user can fall prey to these "zero-day" exploits. Antivirus solutions are essential for protecting devices from viruses and malware.

☐ REGULAR & TIMELY PATCHING

If patching isn't performed regularly, your business is not protected from the latest threats. Some of the biggest malware attacks have targeted vulnerabilities for which patches had already been released.

☐ OFFICE 365 SECURE SCORE

Your Office 365 environment holds essential business data and is responsible for essential business processes, like your email or phone system.

Keeping this environment protected with consistent reviews of and improvements to your Secure Score should be a top priority.

☐ OFFICE 365 DATA BACKUP

Keeping backups of your essential data—files, mailboxes, etc.—can mean all the difference between a business setback and business closure. This means keeping up-to-date backups and consistently validating them through reporting.

☐ USER TRAINING & AWARENESS

Your users are your weakest link, and the most likely factor to introduce vulnerabilities to your security practice. Consistently testing and training your users can significantly lower your risk.