10 Tips To Help Your Small Business Avoid a $255K Cyberattack

$255,000! The average cost of a cyberattack on SMBs in 2024, according to Microsoft Security. The same year, fully one-third of SMBs were hit by a phishing, ransomware, malware, or other cyberattack. Yet, too many small businesses remain unprotected against such attacks. **Let's start changing that right now**.

Use strong passwords. No, seriously.

Using the same, simple passwords practically invites hackers. Use passwords that combine numbers, upper and lower case letters, and symbols — and use different passwords across platforms. Can't keep track? No problem. Use a password manager.

Keep software, devices up to date

Cybersecurity is a cat-and-mouse game. Hackers scan the internet for security holes in outdated software, while manufacturers issue software updates to "patch" these holes. Don't be a soft target; regularly install updates to operating systems, apps, browsers, etc.

Protect your personal information

Hackers can use your personal information (PII), including your social media posts, to guess passwords and answer security questions. PII can also be used to impersonate you, write phishing emails, and identify security weaknesses. Be careful what you share.

Install essential protections

Antivirus/endpoint protection. Firewalls. Encryption. SIEM/log management. Must-haves, increasingly, for businesses. Here's the thing: All software isn't equal. Quality matters. So does proper installation, management. Make your business a fortress.

Train your team

Cyberattacks usually result from human error, so teach your team about phishing, passwords, 2FA, etc. Start with this tip sheet. Ensure every member of your team understands the basics of cybersecurity. Then, implement regular, online training for your team.

Always use two-factor authentication

Two-factor authentication (2FA) locks down access to software/online portals (e.g., email, banking) beyond passwords by requiring a second form of proof (e.g., authenticator app, SMS code). Done right, 2FA is a formidable barrier to hackers. Always use 2FA!

Secure that email inbox

Your inbox is a battlefield; it's the entry point for most cyberattacks today. Require 2FA. Learn to spot phishing emails. Use well-secured email clients (e.g., Microsoft 365) and advanced spam filters. Tighten up your inbox to stick it to these hackers.

Secure your **personal** devices

Businesses often protect work computers but neglect personal, on-the-go devices like mobile phones. Don't store sensitive info on mobile devices. Enable auto updates. Use biometrics. Be cautious with public hotspots. Turn on remote wipe (for lost devices).

Back up data regularly

Your data is your business. Accidental deletion or hardware failure can wipe out years of work in seconds. And hackers can hold your data hostage — demanding a huge ransom. Unless you regularly update your files. Preferably to the cloud.

Start being proactive — **today**

"An ounce of prevention is worth a pound of cure." Never has this been more true than here. After an attack is $255K too late to get serious about cybersecurity. Train, prepare, test. Resist the temptation to delay. Be proactive.