Cybersecurity Tips for Small Businesses

Recognize the Psychology Behind Hacks

Hackers exploit human nature through persuasion. Teach your team to spot manipulation tactics like urgency, authority, social proof, liking, and scarcity. Train them to slow down and question high-pressure requests.

Be 'Politely Paranoid'

Adopt cautious skepticism. Always verify sensitive requests using two different communication methods. Example: If someone emails for a wire transfer, call them on a known number to confirm.

Use Strong, Unique Passwords + Password Managers

Avoid password reuse. Use a password manager to generate and store complex passwords. These tools help detect phishing by refusing to autofill on fake websites.

Enable Multi-Factor Authentication (MFA)

MFA adds a layer of protection using a password plus something you have or are. It greatly reduces risk even if passwords are compromised.

Know Your Threat Model

Some roles face higher risk-like execs or those with financial access. Offer them extra protection and training.

Watch for AI-Generated Attacks

Hackers now clone voices and copy brand tone using AI. Don't trust tone alone-verify sensitive messages through multiple channels.

Use Tools That Support You Now-and Later

Embrace password managers now, and prepare for passkeys in the future for effortless, secure authentication.

Build a Security-First Culture

Security is everyone's responsibility. Train regularly, normalize asking questions, and simulate phishing scenarios.

Train Against Social Engineering

Run simulated phishing tests and debrief employees. Use real-world examples to reinforce learning.

Patch Software Promptly

Keep all operating systems and applications up-to-date to reduce vulnerabilities.

Restrict Admin Access

Use the principle of least privilege. Give users only the access they need.

Secure Mobile Devices

Enable remote wipe and use device encryption for smartphones and tablets.

Backup Regularly

Use automated, off-site backups and test your restore process monthly.

Monitor Logins and Devices

Enable alerts for new logins, unfamiliar devices, or geographical anomalies.

Set a Breach Response Plan

Know who to call and what to do if you're compromised. Test your response at least annually.

Lock Down Public Wi-Fi

Use a VPN when accessing sensitive data over public networks. Educate your team to never send confidential information over unsecured Wi-Fi.

Limit Use of Personal Devices

Implement a Bring Your Own Device (BYOD) policy that includes security software, encryption, and monitoring.

Use Encrypted Messaging

Adopt secure messaging apps for business conversations-especially for executives and VIPs.

Disable Unused Services

Minimize attack surfaces by disabling unused accounts, ports, and applications.

Audit User Accounts Regularly

Remove ex-employee access immediately and review active accounts monthly.

Educate Against Deepfakes

Warn team members that attackers can mimic voices and video calls using AI.

Establish a Password Policy

Set standards for password complexity, reuse bans, and auto-expiration.

Use Browser Security Plugins

Encourage browser plugins that block known phishing and malicious sites.

Implement Email Filtering

Deploy tools to block spam, phishing attempts, and malicious attachments.

Cybersecurity Tips for Small Businesses

Know Your Compliance Requirements

If handling personal or payment data, stay compliant with HIPAA, PCI-DSS, or CCPA depending on your business type.

Secure Your Website

Use HTTPS, secure hosting, and regularly check for vulnerabilities on your public-facing websites.

Schedule Quarterly Security Reviews

Review all security tools, processes, and incidents every 3 months.