The Top 7 SMB Cyber Threats

Prevention Checklist

A practical guide to protecting your business from cyber attacks

How to Use This Checklist

Priority

Start with items marked as high priority, then work through the rest systematically.

Timeline

Focus on "This Week" actions first, then "This Month," then "This Quarter."

Track Progress

Check off each item as you complete it. Use the notes section to track who's responsible and when tasks were completed.

Review Regularly

Revisit this checklist quarterly to ensure all protections remain in place.

⏱️ Recommended Timeline

- **This Week:** Enable MFA, schedule training, test backups
- **This Month:** Security assessment, access controls review, system patching
- **This Quarter:** Implement comprehensive tools (EDR, MDM, CASB), ongoing training, cyber insurance

Threat #1: Phishing Attacks

Deceptive emails and messages designed to steal credentials or install malware - the #1 entry point for 90% of breaches.

Email Protection

- Implement email filtering and anti-phishing tools - use advanced threat protection
- Display external email warnings - configure email to tag messages from outside the organization
- Disable auto-forwarding rules or monitor for suspicious forwarding

Employee Training

- Conduct security awareness training - initial training plus monthly refreshers
- Run simulated phishing tests regularly to identify vulnerable employees
- Train employees to verify sender authenticity - check actual email address, not just display name

Verification Protocols

- Establish verification protocols for unusual requests (financial transfers, password resets, etc.)
- Implement the "$10,000 test" - always verify unusual financial requests via phone using a separately-obtained number
- Create easy reporting mechanism - make it simple for employees to report suspicious emails

- Enable MFA on all accounts - provides protection even if credentials are phished
- Review reported phishing attempts and use as training opportunities

Threat #2: Ransomware

Malware that encrypts your data and demands payment can shut down business operations for days or weeks.

01

Backup Strategy

- Implement 3-2-1 backup rule - 3 copies, 2 different media types, 1 offsite/offline
- Test backup restoration regularly - monthly or quarterly verification that backups actually work
- Keep offline/air-gapped backups - ensure ransomware cannot access backup files

02

System Protection

- Implement Endpoint Detection and Response (EDR) solution
- Keep all systems patched - ransomware often exploits known vulnerabilities
- Restrict user permissions - apply principle of least privilege
- Disable unnecessary services and ports to reduce attack surface

03

Incident Response

- Create incident response plan - document steps, contacts, and priorities
- Test incident response plan - conduct tabletop exercises at least annually
- Educate employees on ransomware delivery methods (phishing, malicious links)
- Consider cyber insurance - after implementing basic security controls

Threat #3: Weak/Stolen Passwords

Compromised credentials are the leading cause of unauthorized access and account takeovers.

1

Multi-Factor Authentication

- Enforce multi-factor authentication (MFA) on ALL accounts - email, cloud, financial systems, VPN
- Consider passwordless authentication where possible (biometrics, security keys)

2

Password Management

- Deploy a business password manager (**Keeper**, LastPass, 1Password, Bitwarden, etc.)
- Require strong password policy - minimum 12 characters, unique for each account
- Prohibit password reuse across work and personal accounts

3

Monitoring & Response

- Monitor for compromised credentials using services like Have I Been Pwned or dark web monitoring
- Force password resets for all accounts if a breach is suspected
- Disable accounts after repeated failed login attempts

- Train employees on password security - no sharing, no writing down, no reusing

Threat #4: Insider Threats

Both malicious and negligent employee actions can lead to data breaches, data loss, and security compromises.

Access Controls

- Implement role-based access controls - follow principle of least privilege
- Create immediate offboarding procedures - revoke all access on employee's last day
- Conduct quarterly access reviews - verify who has access to what and whether they still need it
- Separate duties for critical functions - require multiple approvals for sensitive actions

Monitoring & Culture

- Monitor user activity patterns for unusual behavior (mass downloads, after hours access, etc.)
- Conduct background checks for positions with access to sensitive data
- Create clear acceptable use policies and ensure all employees understand them
- Foster positive security culture - make it safe for employees to report mistakes

- Implement data loss prevention (DLP) tools to prevent accidental or malicious data exfiltration

Threat #5: Unsecured Cloud Applications

Misconfigured cloud services and shadow IT create data exposure risks and unauthorized access points.

Cloud Inventory

- Create an inventory of all cloud applications currently in use (approved and unapproved)
- Create an approved software list and make it easy for employees to request new tools

Access Security

- Require MFA for all cloud services - especially Google Workspace, Microsoft 365, Dropbox, etc.
- Review and restrict default sharing settings - change "anyone with link" to specific permissions
- Implement Cloud Access Security Broker (CASB) if budget allows

Monitoring

- Conduct quarterly cloud access audits - review who has access to what and revoke unnecessary permissions
- Configure activity alerts for unusual downloads, sharing, or access patterns
- Review external sharing regularly - schedule quarterly "cloud clean-up days"

- Train employees on secure sharing practices

Threat #6: Unpatched Software & Systems

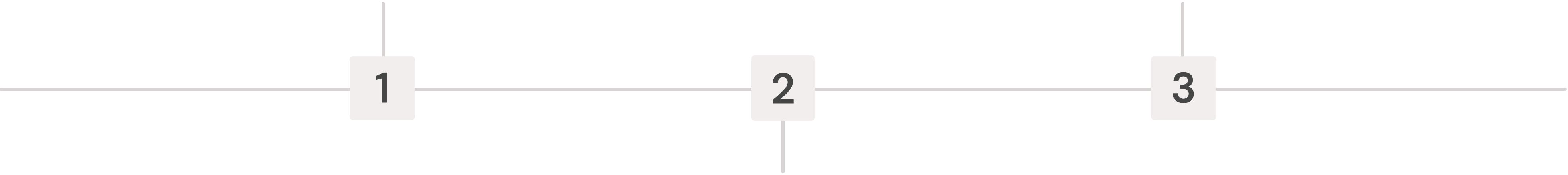
Outdated software with known vulnerabilities provides easy entry points for attackers to compromise your systems.

Immediate Actions

- Enable automatic updates for workstations and non-critical applications
- Create an asset inventory - document all hardware and software in use, including versions

Long-term Planning

- Identify end-of-life systems - create a replacement plan for Windows 7, outdated routers, etc.
- Budget for technology refresh cycles - plan for regular hardware/software updates
- Subscribe to security bulletins for your critical software vendors



Ongoing Management

- Establish a patch management schedule - set regular maintenance windows (e.g., Tuesday nights, Sunday mornings)
- Prioritize critical security patches over feature updates
- Test patches in non-production environment when possible before wide deployment

Threat #7: Inadequate Mobile Security

Lost or stolen devices, insecure mobile apps, and public Wi-Fi risks expose your business data to unauthorized access.

1

Device Management

- Implement Mobile Device Management (MDM) solution to remotely manage and secure all work devices
- Enable device encryption and strong passcodes on all mobile devices (minimum 6-digit PIN or biometric authentication)
- Enable remote wipe capabilities before devices are lost or stolen

2

Network Security

- Deploy VPN for remote work - require VPN use for any work on public or untrusted Wi-Fi networks
- Separate work and personal data using containerization features in MDM

3

Policies & Updates

- Create a lost device protocol - document who to call and what steps to take immediately
- Require security updates - ensure mobile OS and apps are kept current
- Disable unauthorized app installation - restrict app downloads to approved stores only

🎯 Quick Priority Actions (Start Here)

1 Implement DMARC, SPF, and DKIM email authentication protocols

2 Deploy password manager for all employees

3 Test your backups – restore at least one file to verify

4 Schedule security training – even 30 minutes makes a difference

5 Implement email filtering – stop phishing at the gate

6 Create asset inventory – you can't protect what you don't know about

📝 Implementation Notes

Person Responsible: ______________

Target Completion Date: ______________

Budget Allocated: ______________

Additional Notes: ______________

For questions or support, contact your cybersecurity provider