Cyber Hygiene

Checklist for SMEs

Cyber security doesn't need to be complicated. For small- and medium-sized businesses, a few simple habits can make a big difference. Use this quick checklist to cover your bases, reduce risk, and stay one step ahead of cyber threats.

Keep Software Updated

- [ ] **Download the Apex Cyber Security Essentials Checklist**
- [ ] Enable automatic updates for:
  - [ ] Windows
  - [ ] Microsoft 354
  - [ ] All browsers
- [ ] Set a weekly reminder to manually check for updates on third-party applications (Adobe, Zoom, etc.)

Use Antivirus and Endpoint Protection

- [ ] Install business-grade antivirus on all endpoints (laptops, desktops, phones, etc.)
- [ ] Ensure your antivirus includes:
  - [ ] Ransomware protection
  - [ ] Real-time threat detection and response

Backup Your Data (and Test It)

- [ ] Use automated and encrypted backups, both cloud-based and offline/local if possible
- [ ] Perform quarterly restoration tests to confirm backup integrity

Remove Ex-Employee Access

- [ ] Immediately disable all accounts and logins when an employee leaves
- [ ] Schedule a monthly access review to check for:
  - [ ] Unused accounts
  - [ ] Permission creep

Secure Admin Accounts

- [ ] Enforce Multi-Factor Authentication (MFA) for all admin users
- [ ] Use unique, strong passwords for each admin account
- [ ] Restrict admin roles: avoid assigning Microsoft 365 Global Admin to non-essential users

Block Unused Ports and Applications

- [ ] Configure a business-grade firewall to block unused ports
- [ ] Use application whitelisting to control which apps can run:
  - [ ] Company laptops
  - [ ] Mobile devices

Train Staff to Spot Threats

- [ ] Deliver quarterly phishing and cyber hygiene training
- [ ] Include short (30-minute) refresher sessions for ongoing awareness
- [ ] Make cyber security part on onboarding for new hires

Regularly Review Devices

- [ ] Maintain an up-to-date inventory of:
  - [ ] Laptops
  - [ ] Smartphones
  - [ ] Tablets with network access
- [ ] Remove or remotely lock devices that are lost, stolen, or no longer needed

Monitor for Breach Signs

- [ ] Look out for indicators like: unfamiliar login locations, sudden file encryptions, unexpected email behaviour, etc.
- [ ] Use monitoring systems like Microsoft Defender

Have a Simple Incident Plan

- [ ] Create a 1-page cheat sheet with:
  - [ ] Who to contact
  - [ ] What actions to take
  - [ ] When and how to escalate
- [ ] Make this plan accessible and part of staff training

Print it, pin it, use it!

Cyber threats don't wait - and neither should you. Keep this checklist handy and make it part of your regular business routine.

Visit our Cyber Security Awareness Hub here