CSC

CYBER-SECURITY CHECKLIST FOR UK SMES

A practical, security-first checklist for UK small and medium-sized businesses

Prepared by

Computer Support Centre

https://computersupportcentre.com

Cybersecurity checklist for UK SMEs

Executive Summary

- The emphasis of cybersecurity for small and medium-sized enterprises (SMEs) is on decreasing risk as opposed to completely mitigating it.
- The majority of successful cyber-attacks arise from failure to close basic vulnerabilities rather than through any highly sophisticated techniques.
- Cyber-attacks on UK-based SMEs typically take the form of phishing scams, account credentials theft, ransomware, and loss of data.
- Adopting only a few controls will provide the majority of your company's cybersecurity protection if appropriately applied.
- There is a shared responsibility for cybersecurity, which exists between the individual, the Information Technology and the Supply Chain.
- The Cyber Essentials standard should be regarded as a good starting point, but must not be relied upon exclusively.
- While a backup solution may assist in recovery from a cyber-attack, it does not negate the requirement for other security measures.
- Responsibility and ownership are more important than having advanced technological solutions.
- This matrix will help you to determine where to place priority on your improvement efforts, based on whether your improvement efforts are minimum, better, or best practices.
- Implementing an improvement project should occur over a time frame of 30 to 90 days, not expected to be completed all at once.

Who This Guide Is For

This guide is intended for:

- UK SMEs that employed between one and 250 of their staff,
- Owners/directors, office managers and non-techy leaders,
- Businesses that do not have dedicated cyber security teams,
- Organisations that use Cloud services such as Microsoft 365 and Google Workspace,

One-page: Minimum Cybersecurity Baseline for UK SMEs

All SMEs should have, or be working to implement, the following minimum level of cybersecurity:

- A designated Owner of Cybersecurity
- Encryption of All Devices
- Multi-Factor Authentication (MFA) enabled for Email and Cloud Services
- No Shared Admin Accounts. Each user should only have one account (standard users)
- Email Phishing Protection
- Backups of Key Systems and Data
- Regular Device and App Patching
- Secure Wireless Network and a Firewall
- An Incident Response Plan
- Staff educated about the basics of cyber threats

Most SMEs should be able to establish this baseline within 30 days.

Full Cybersecurity Checklist

1) Governance & responsibility

Why it matters

When "everyone thinks that someone else has to be accountable" is the main reason - Cyber security has failed.

Checklist

Item	Minimum	Better	Best practice	Owner	Frequency
Cyber owner	Named person	Role documented	Board oversight	Director/Ops	Annual
Policies	Basic AUP	Reviewed annually	Staff acknowledgement	Ops	Annual
Risk review	Informal	Documented	Regular reporting	Director	Quarterly

Common mistakes

- No defined owner; no clear accountability.
- Policies established but not adhered to.
- Assuming the IT services provider assumes full liability.

Quick wins

- Assign ownership and accountability.
- Storing policies centrally.
- Reviewing and updating risk assessments every quarter.

2) Devices & endpoint security

Why it matters

Data breaches have been frequently caused by devices that were either stolen or compromised.

Checklist

Item	Minimum	Better	Best practice	Owner	Frequency
Encryption	Enabled	Enforced	Verified	IT	Continuous
Malware protection	Installed	Centrally managed	EDR + alerts	IT	Continuous
Device lifecycle	Informal	Planned	Automated	Ops	Annual

Common mistakes

- Old unsupported devices
- Encryption assumed, not checked
- Consumer antivirus only

Quick wins

- Enable BitLocker/FileVault
- Remove admin rights
- Replace end-of-life devices

3) User accounts & access control

Why it matters

Most breaches start with stolen credentials.

Checklist

Item	Minimum	Better	Best practice	Owner	Frequency
MFA	Email only	Cloud services	Conditional access	IT	Continuous
Admin rights	Limited	Separate admin	Privileged access	IT	Quarterly
Joiners/leavers	Manual	Checklist	Automated	Ops	Per event

Common mistakes

- Using shared administrative accounts
- Deferring Multi-Factor Authentication (MFA) to a later date
- Failure to promptly remove access for employees who have left the company

Quick wins

- Implementing MFA today
- Creating distinct administrative accounts
- Performing a review of active users

4) Email & phishing protection

Why it matters

Phishing is the primary method of entry for SME attacks.

Checklist

Item	Minimum	Better	Best practice	Owner	Frequency
Spam filtering	Enabled	Tuned	Advanced policies	IT	Continuous
User awareness	Ad-hoc	Annual reminder	Ongoing training	Ops	Annual
Reporting	Informal	Button	Central triage	IT	Continuous

Common mistakes

- Only relying on filtering systems to identify phishing attempts
- Having no procedure to document Phishing Reports
- Not addressing any Phishing Attempts that were detected but were not successfully exploited

Quick wins

- Creating a button to report Phishing Attempts
- Hosting a Brief Awareness Session about Phishing
- Blocking common Domain Name Service (DNS) Spoofing Domains.

5) Data protection & backups

Why it matters

Importance of Having a Backup are Your Last Resort, Not Your First Option.

Checklist

Item	Minimum	Better	Best practice	Owner	Frequency
Backup scope	Key data	Systems + M365	3-2-1 strategy	IT	Daily
Restore testing	Rare	Periodic	Scheduled	IT	Quarterly
Ransomware resilience	Basic	Immutable	Isolated	IT	Continuous

Common mistakes

- No restore testing
- Believing that the cloud is a backup.
- Allowing attacks to access your backups.

Quick wins

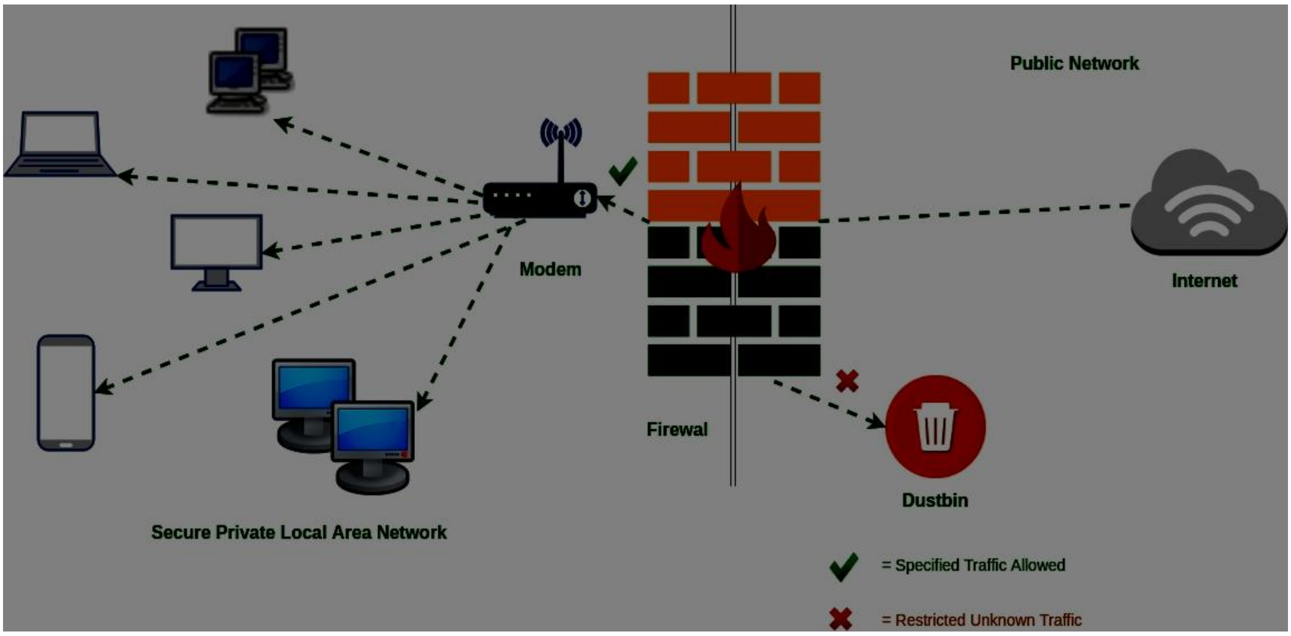
- Test one restoration from your back up.

- Verify your M365 (Microsoft 365) backup exists.
- Limit access to your backups.

6) Network & Wi-Fi security

Why it matters

Vulnerable Wi-Fi & Networks Expose All Devices/Sensitive Data.


Public Network
Modem
Internet
Firewal
Dustbin
Secure Private Local Area Network
✓ = Specified Traffic Allowed
✗ = Restricted Unknown Traffic

Checklist

Item	Minimum	Better	Best practice	Owner	Frequency
Firewall	Business-grade	Managed	Monitored	IT	Continuous
Wi-Fi	Secured	Separate guest	Segmented	IT	Annual
Remote access	VPN	MFA + VPN	ZTNA	IT	Continuous

Common mistakes

- Using consumer grade routers.
- Using publicly shared Wi-Fi passwords.
- Not upgrading Firewall Software with New Patches when released.

Quick wins

- Change wireless network login credentials.
- Enable guest networking.
- Upload Firewall Software for current versions.

7) Cloud services & SaaS security

Why it matters

Cloud security is a **shared responsibility**.

Checklist

Item	Minimum	Better	Best practice	Owner	Frequency
MFA	Enabled	Enforced	Conditional	IT	Continuous
Audit logs	Enabled	Reviewed	Retained	IT	Monthly
Sharing controls	Basic	Restricted	Reviewed	IT	Quarterly

Common mistakes

- Leaving default settings unchanged;
- Over-sharing links;
- No Audit Visibility.

Quick wins

- Reviewing Sharing Settings;
- Enabling Audit Logging;
- Restricting External Access.

8) Remote & mobile working

Why it matters

The attack surface increases when workers work from home;

Checklist

Item	Minimum	Better	Best practice	Owner	Frequency
Device rules	Informal	Written	Enforced	Ops	Annual
BYOD	Allowed	Controlled	Managed	IT	Continuous
Home networks	Advice	Guidance	Secure configs	Ops	Annual

Common mistakes

- Unmanaged personal devices;
- Family members using work devices;
- No guidance on working from home;

Quick wins

- Create remote work guidance;
- Reinforce device locking;
- Create separate work profiles.

Common SME cyber risks & failure points

- Phishing attacks may lead to email compromise.
- The absence or bypassing of MFA
- Old devices are still being used.
- Untested backups
- Users with more permissions than they require.
- Attackers have no means of monitoring who owns each device.
- The cloud configuration is incorrect.
- There is confusion among staff about what should be reported.

30-day improvement plan

Week 1: Secure logins	Week 2: Secure devices
✓ Appoint an individual to oversee Cybersecurity. ✓ Delete old or unused user accounts. ✓ Enable Multi-Factor Authentication (MFA) on all important systems, including Email. ✓ **Reason for Action:** Most Cybercrime begins with stolen passwords.	✓ Create a complete listing of Work Devices. ✓ Enable Automatic Update Feature on Devices. ✓ Install Basic Anti-Virus Software and enable Screen Lock feature. ✓ **Reason for Action:** Software updates address known security vulnerabilities.
Week 3: Protect data	**Week 4: Be ready for incidents**
✓ Verify that backups are created, ✓ Run a test to restore at least one piece of data, ✓ Instruct staff on identifying Phishing Scam Emails. ✓ **Reason for Action:** Backups are necessary to protect against ransomware attacks, and email is the primary means of attack.	✓ Create a simple document outlining What To Do If You Are Hacked. ✓ Review your Home/Remote Working Security Measures. ✓ Use Administrative Accounts only when Necessary. ✓ **Reason for Action:** Preparation reduces panic during a Cyber Attack and reduces the overall impact of the attack.

90-day maturity plan

- Review Alignment to Cyber Essentials.
- Improve on Monitoring and Alerts.

- Formalise your Policy and Training.
- Test Your Backup Restore Process.
- Review Your Vendor(s) Security Posture.

FAQs

➢ Is it true that SMEs are susceptible to being targeted?

Yes, hackers automate their attacks so they do not discriminate based on company size.

➢ Is it sufficient for SMEs to have antivirus protection?

No, antivirus is only one of many layers. It is not a strategy.

➢ Does my business require Cyber Essentials certification?

Cyber Essentials certification can be a useful starting point for many businesses, but it is dependent on the business.

➢ How much cybersecurity coverage does my business require?

It depends on the amount of risk you are willing to accept, as well as how quickly you need to be able to recover from an incident.

➢ What should I do after experiencing a cyber attack?

1) Contain the incident

2) Assess the impact

3) Preserve evidence

4) Recover from the incident

5) Learn from the cyber attack

Final soft CTA

If you would like a cyber health check, then typically this includes:

- A review of your current controls against this checklist,
- Identification of priority control deficiencies,
- Confirmation of confidence in your backup and recovery processes,
- Alignment with Cyber Essentials and the UK GDPR,
- And the development of a realistic 30-90 day improvement plan.

No sales pressure, just clarity.

About This Guide

Computer Support Centre is an IT support and managed service provider, focused on helping small and medium-sized businesses in the UK and their day-to-day operations. **Computer Support Centre** has spent time supporting companies with day-to-day operations, reacting to security incidents and assisting organisations in enhancing their Cybersecurity posture without being over-complicated.

The purpose of the guide is for UK SMEs to have a simple, practical baseline to implement. It is intended to focus on sensible controls, good habits, and making decisions based on knowledge; not out of fear or through unnecessary over-engineering.

If you learn more about **Computer Support Centre**, our services, and our approach, please visit our official website:
□ **https://computersupportcentre.com**

Conclusion

In order to safeguard their network, UK SMEs don't have to spend a lot of money on comprehensive or elaborate cyber-security solutions because the majority of these businesses can significantly reduce their cyber-risk by doing the basics well: establishing clear lines of accountability for their cyber-security, protecting their networks with secured devices, protecting the network users with secure user accounts, establishing a process for backing up their data and establishing basic procedures for responding and recovering from cyber attacks.

By keeping the business cyber-security checklist as a living document, the business has a framework for building resilience, decreasing the level of disruption their business suffers due to cyber-attacks, using technologies with an increased level of confidence, and moreover, it will grow as a business.