Ransomware Prevention Guide for UK Offices

Executive Summary

- Ransomware has become one of the leading causes of IT downtime in small and medium sized enterprises (SMEs) throughout the UK.
- The vast majority of ransomware attacks are initiated by a phishing email or a compromised password (not through advanced hacking techniques).
- Having tested and isolated backups as part of your disaster recovery plan is the most important protection against all forms of data loss.
- Implementing Multi-Factor Authentication (MFA) to secure user accounts will prevent the vast majority of account compromise attacks.
- There is still a widespread culture of delayed patching and weak password controls in small office environments.
- Under UK GDPR, your organisation remains responsible for the protection of your data regardless of where you have chosen to outsource your IT services.
- Implementing a simple 30-day structured plan can significantly reduce your exposure to ransomware attacks at minimal cost.
- Preventing a ransomware incident is significantly less expensive and stressful than recovering from one.

Who This Guide Is For

This guide has been specifically developed for:

- UK SMEs (1-50 employees).
- Owner-managed enterprises.
- Office and Operational Managers.
- Financial Managers with an IT responsibility.
- Non-technical decision makers.

You do not need to hold any technical qualifications to follow the majority of the instructions provided within this document.

What You Will Achieve

After completing this course, you will have an understanding of how ransomware generally arrives at UK small office environments (as of 2026), a short collection of the most effective prevention controls that will support your efforts in defending against these types of attacks, and detailed steps for implementing those controls. Also included in this course are short examples of successful implementation of these measures, a ready-to-use 30 day checklist, and responses to Frequently Asked Questions (FAQs) regarding ransomware threats. When finished with this course, you will be able to make significant improvements to your protection against ransomware within the next week; without having to be a highly technical individual or having a huge budget.

What Is Ransomware?

Ransomware is a malicious software (malware) program that

- Hacks into your information technology (IT) systems
- Encrypts your data (i.e. rendering it inaccessible)
- Requests a ransom payment (which is usually made using digital/cryptocurrency) to provide you with the key(s) to unlock (i.e. access) the data encrypted by the ransomware program.

If your organisation is a victim of ransomware, you will no longer be able to use:

- Your accounting system,
- Shared drive,
- Email system,
- Client database,
- Production system.

Also, with most modern day ransomware attacks, cybercriminals will usually threaten to publish any exfiltrated data unless they receive the requested ransom payments.

RANSOMWARE ATTACK
Your personal files are encrypted
You have 5 days to submit the payment!!!
To retrieve the Private key you need to pay
Your files will be lost

Why Ransomware Matters to UK SMEs

Ransomware is a type of malware that will either lock or encrypt your files and then demand a ransom (typically paid in cryptocurrency) to release them. Ransomware can also be used to steal your data and threaten to publish it.

Small UK businesses are attractive targets for ransomware for a variety of reasons:

- Weak security measures
- Heavy reliance on email for work
- Lack of internal IT staff
- No regular testing of backups
- Belief that they are more likely to pay the ransom

The UK's National Cyber Security Centre (NCSC), which is the UK's national authority for cyber security, regularly advises that phishing and ransomware are two of the most frequent threats to UK businesses.

The Information Commissioner's Office (ICO) has also advised that if ransomware is used to obtain your personal data (that you are responsible for), then you must report it under the General Data Protection Regulation (GDPR) in the UK.

A 15-person accountant located in Manchester

- One employee clicks on an e-mail (phishing) pretending to be a client in their Office 365 environment.
- Their Office 365 login credentials are compromised by attackers who remotely access the account overnight.
- User's shared drive is encrypted by the attackers.
- Backup is also encrypted since it is accessed via the same LAN.
- Therefore, the firm is unable to pay their clients' salaries for 4 days.
- A data breach investigation will have to be conducted.
- The excess on the insurance is £5,000.
- Reputational harm.

Total impact will be far greater than the actual ransom demanded.

Common Ransomware Attack Methods

➢ **Phishing Emails:** Email impersonors send fake invoices and delivery notifications or "Microsoft password reset" email messages to make it easy for employees to click on a phishing link.

➢ **Weak or Recycled Password:** Attackers use credentials stolen through Credential Stuffing to access e-mail accounts -or- (Remote Desktop Protocol) services.

➢ **Unpatched Software:** Out-dated version of Windows Servers. Firewalls, VPNs, and etc... provide common point of entry.

➢ **Unsecured Remote Desktop Protocol (RDP) Connections:** Unsecured RDP ports without MFA are one of the most frequent reasons for an SME to experience a breach.

➢ **Unsafe Supply Chain:** A third party IT services provider or software vendor may be able to compromise the security of your operational environment.

Core Prevention Measures

1. Regular Backups

What it is:

A backup is the storing of copies of your business data in a separate location from your operational systems.

How to implement

- Minimum Requirements: Automated Daily Backups
- Stored using Off-site or Cloud Storage

Better

Preferred: 3-2-1 Rule

- 3 Copies of Data
- 2 Types of Storage (i.e., External Drive, Cloud)
- 1 Copy Must be Offline or Immutable

Best

- Encrypted Immutable Cloud Backup + Encrypted Offline Backup
- Quarterly Restore Testing

Common mistakes

- Backups Stored on Same Network
- Non-Tested Backups
- No Disaster Recovery Procedures in Writing

Quick wins

- Automate Daily Backups
- Remove External Drives After Backup
- Test Restore One File This Week

2. Patch Management (Updates)

What it is:

Updating your software and operating systems regularly to ensure their continued operation.

How to implement

- **Minimum Requirements:** Automatic Updates for Mac and Windows

- **Preferred:** Monthly Update Schedule for All Devices, Update Routers & Firewalls
- **Optimal:** Centralised Patch Management Tool, Maintain a Patch Log

Common mistakes

- No Firmware Updates
- Patch Delays for Convenience Reasons
- Forgetting to Update Printers/Network Devices

Quick wins

- Enable Automatic Updates Today
- Check Your Router's Firmware Version
- Update Microsoft 365 Apps

3. Antivirus / EDR Protection

What Is It:

- Software that helps detect and block malicious activity with security.
- EDR solutions (Endpoint Detection & Response) are designed to protect your devices with more advanced ways than traditional Antivirus software could do alone.

How To Implement

Minimum: A reputable Antivirus solution on any PC

Better: Business-grade Endpoint Protection

Best: Managed EDR Solution with Monitoring

Common Mistakes

- Relying on "free" Antivirus programs
- Turning off protection because the system runs too slowly
- Not having any monitoring alerts

Quick Wins

- Verify that Antivirus application was installed on each device
- Confirm that automatic updates are turned on for all users and devices
- Review the expiration dates for licenses for Antivirus software

4. Multi-Factor Authentication (MFA)

What it is:

- A second verification step before allowing access to your accounts e.g., using an authenticator app.

- **Why Does It Matter?** MFA has been shown to stop many account takeover attacks.

How to implement

Minimum: MFA may work on email accounts

Better: MFA works on Cloud Services

Best: MFA will work for VPNs, Admin accounts, and Remote Access

Common mistakes

- Using only SMS messages
- Allowing "MFA fatigue" approvals for authentication

Quick wins

- Activate MFA on any email accounts using Microsoft 365 or Google Workspace
- Utilise authenticator apps instead of SMS messages for authentication

5. Access Control & Least Privilege

What it is:

Users receive access to the resources they need without additional access beyond that.

How to implement:

Minimum: Remove local administrator privileges

Better: Implement Role Based Access Control

Best: Conduct access reviews on a quarterly basis

Common mistakes:

- Everyone has Administrator access,
- Old employee accounts are not disabled.

Quick Wins:

- Disable local administrator access for standard users
- Disable former employee accounts immediately

6. Network Segmentation

What is it?

Creating separate systems from each other so that ransomware cannot spread through the network.

How to implement:

Minimum: Create a separate guest wireless network

Better: Physically separate servers and user's machines

Best: Implement VLAN segmentation along with firewall rules

Quick Wins:

- Isolate the guest wireless
- Ensure that you are using devices that are not permanently connected for your backup's.

Backup & Disaster Recovery

Without backups, ransomware could be devastating for small businesses. Here are some best practices (2026).

- 3-2-1-1-0. This is three copies of your data on two types of media (e.g., disks + tapes), one of which is off-site, one of which is immutable or air-gapped (cannot be changed by cybercriminals), and zero errors (must test all restores).
- At least one of your copies must be immutable (cannot be changed by cybercriminals).
- You must restore at least one folder or file once per quarter to confirm that it can be restored.
- You must keep backups separate from the main network (e.g., cloud plus disconnected drive).

Quick Wins: Set up OneDrive folder protection and buy at least one external HDD for £50 - £80 for weekly off-site backup.

Staff Training & Awareness

Human beings continue to be the biggest risk and the best protection. The best way to mitigate risk is by providing training and awareness to employees. Minimum actions include:

- Every 1/2 year, hold a 15 - 20 minute meeting with all employees to discuss phishing, safe links, and reporting suspicious emails.
- Establish a simplified process for employees to report a suspicious email.
- Explain multi-factor authentication (MFA) and its importance in the workplace.

Best approach: Conduct real-life phishing simulations (numerous Microsoft or Google partners provide either free or low-cost opportunities).

30-Day Implementation Checklist

Days 1–10 – Quick wins that are of critical importance
• MFA must be enabled for all email and cloud accounts • Windows and macOS must have all updates run on all devices • Ensure that Defender is installed on every device and updated • Create a new administrator password for your router
Days 11–20 – Protecting your data and email from future loss
• Backup the contents of your desktop and documents to OneDrive • Create a backup of your data and store it offline

• Test the restoration of at least one file from your backup in OneDrive • Turn on the external sender flag for messages
Days 21–30 – Raising security standards and awareness
• Stop using a shared account; review and confirm your admin login information • Conduct a 15-minute briefing with your staff on phishing • Document your organisation’s basic process for reporting a data breach • Schedule a follow-up meeting to take place in 3 months.

FAQ

- **Do SMEs get attacked by cyber criminals?**

They do, typically through automated means.

- **Is cloud computing a safer option than on-premises infrastructure?**

Cloud computing has lessened the risk, but it also doesn't shift any responsibility from you.

- **Is Microsoft's 365 offering sufficient protection?**

No, multi-factor authentication (MFA), backups & monitoring are still necessary.

- **How quickly do we need to notify the ICO regarding a breach?**

Within 72 hours, as long as there is a risk to the personal data involved.

- **Is an antivirus program sufficient protection?**

Not by itself; use it along with MFA and backup plans.

- **Should we obtain cyber insurance?**

It is highly recommended for SMEs who are managing the data of others.

- **How frequently should we test our backups?**

At least every quarter.

- **Is MFA inconvenient?**

There are many more inconveniences associated with extended periods of downtime than there are with the minor inconvenience of using MFA.

- **What is the biggest risk factor?**

Weak passwords when using MFA.

- **Can my IT services provider do everything for me?**

Only if it is clearly defined in your contract with them.

About This Guide

This guide was created by **Computer Support Centre**, a consultancy in IT and cybersecurity at a UK-based company that works with small- and medium-sized companies. The guide is based on actual incidents at offices in the UK, therefore, it aligns with the recommendations of the National Cyber Security Centre (NCSC), the UK Information Commissioner's Office (ICO), and UK General Data Protection Regulation (GDPR).

The guide is designed to be read in 'plain English' by non-technical managers and their staff in offices and to assist them with the steps they can report back to you as a result of each of the recommendations in order to take practical action to reduce their risk to ransomware attacks, with as little complexity and/or expense as required. The overall goal is to provide affordable and useful recommendations to build a more resilient office and to ensure continuity for the business.

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

Conclusion

Ransomware is a major disruption for UK offices today however, with appropriate prescriptive controls in place, it can also be prevented. Small businesses have the potential for significant programming for ransomware-related attacks through backup strategies, multi-factor authentication (MFA), periodic patching, the use of secure devices and establishing a level of awareness among their staff which can significantly limit their exposure to such attacks. Preventative programmes do not require an enterprise-level budget; however, they do require some inherent consistency, documentations and practical action. Begin improving your organisations level of resilience this week, generate momentum within the next 30 days and create a safer and more secure working environment for your entire business.