How UK Small Businesses Get Hacked: Real Scenarios Explained

Why Most UK Hacks Aren’t “Targeted”

- What is the biggest misconception about cyber attacks on small businesses?
- The reasons hackers do not need to "target" SMEs
- Automated hacking attacks vs human hackers
- Why SMEs experience a proportionately greater impact from cyber attacks
- The purpose of this guide is to help you understand what being hacked means for your business without creating panic

What “Getting Hacked” Really Means for a Small Business

Typically, the term "being hacked" doesn't refer to an actual person gaining access to your business while you are there

Examples:

- Lost or compromised password(s)
- Unauthorised accesses
- Malware executing
- Data being exposed

Typically, breaches will go unnoticed for a period of time before the business will be aware of them

The Most Common UK Small Business Attack Paths

According to recent NCSC reports and the results of the 2025 breaches survey. Here are the most Common Methods of Compromising UK Small and Medium Enterprises (SMEs):

1. **Phishing:** 85% of reports, through phish emails tricking users into unknowingly submitting credentials and installing malware.
2. **Ransomware:** 100% increase year on year, causing files to be encrypted for a ransom, mostly through unpatched software.
3. **Business Email Compromise (BEC):** Fake invoices or payment changes, costing businesses millions each year.
4. **Unpatched systems:** Old software that has been compromised by way of known vulnerabilities, and emails are sent automatically exploiting them.
5. **Remote Access Exploits:** For example, exposing Remote Desktop Protocol (RDP) and having a direct path to the company.
6. **Supply Chain Attacks** Attackers comprise via 3rd party providers, as we’ve seen in retail attacks in 2025.
7. **Device Loss/Theft:** Unencrypted Laptops causing a data breach.
8. **Insider Errors:** Unknowingly sharing files or poor home office setup.

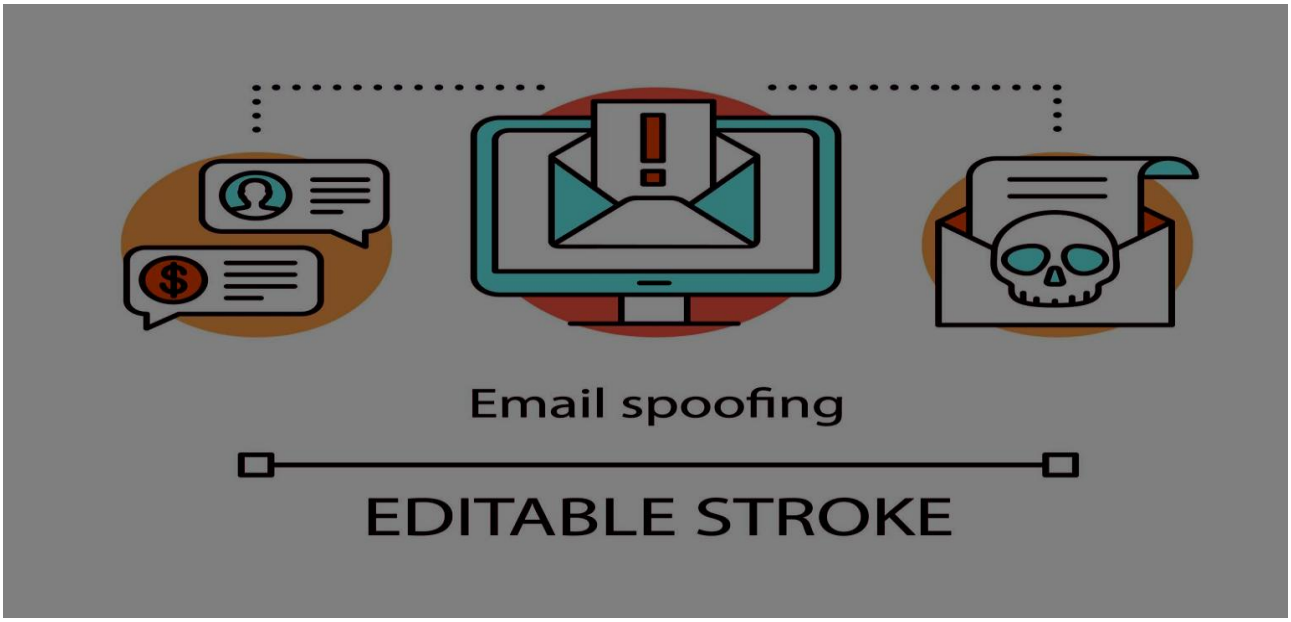
None of these are complex attacks rather they are just exploiting common mistakes.

Real-World UK-Style Scenarios

The reports from 2025 will provide some insight into the stories compiled from a number of common occurrences reported to the UK Government's (NCSC) cyber-crime during 2025 through Annual Reviews and Annual Breaches Survey of 2025 will contain many examples of how incidents happen in businesses across the UK.

Scenario 1: Phishing Email & Fake Microsoft 365 Login

- **Industry:** Business Services (15 employees)
- Business's assessment of the situation:
- Business was phished and its clients were victimised through the compromise.
- How the incident occurred: Unauthorised access through phishing attack.
- Length of time the attack went undetected:
- Impact of the attack: Phished client, lost client trust and revenue.
- **Simple controls that could have helped stop this incident:** Multi-Factor Authentication (MFA) & User Awareness.



Scenario 2: Password Reuse Across Multiple Services

- **Industry:** Residential Real Estate Office
- The passwords for both email and a third country web site were the same.
- How the incident happened: Another company was compromised and email access wa granted to the purchasing company.
- Length of time before discovery:
- Impact of the attack on operations and reputation:

- **Simple controls that could have helped stop this incident:** A password management program and appointing each employee with a different password for each service.

Scenario 3: Unpatched Legacy Software

- **Industry:** Small Manufacturer
- The company had an old Computerised Inventory Control (CIC) system still functioning.
- How the incident occurred: The vulnerability in the CIC software was known, and the attacker was able to exploit the known vulnerability automatically.
- Length of time the attack went undetected:
- Impact of the situation: Production stopped.
- **Simple controls that could have prevented this incident:** Patch management process and system life-cycle reviews not completed.

Scenario 4: Exposed RDP / Remote Access Misuse

- I**ndustry:** Construction business
- RDP was not closed when COVID started.
- Brute-force or credential stuffing occurred.
- An attacker obtained encryption keys due to open access to files.
- **Quick control:** Disable the RDP, VPN, and MFA

Scenario 5: Infected Email Attachment

- **Industry:** Accounting firm
- Open email attachment with the word “invoice.”
- Malware was running in the background.
- Malware spread to other drives.
- **Quick controls:** Email filtering and user awareness

Scenario 6: Fake Invoice & Payment Redirection Fraud

- **Industry:** Marketing firm.
- The supplier’s email was compromised.
- The payment method was altered.
- The money was paid to the hacker.
- **Quick control:** A method for verifying changes in payment processes.

Scenario 7: Lost or Stolen Laptop Without Encryption

- **Industry:** HR consulting.

- A laptop was stolen from a vehicle or train.
- No hard drive encryption.
- Potential risk of information exposure.
- **Quick controls:** Disk Encryption and remote wipe

Scenario 8: Home Working Security Failure

- **Business Type:** Recruitment Organisation
- Incorrectly Configured Home Wi-Fi
- Shared Household Computer Devices
- Malware or Session Hijacking
- **Simple Solution:** How to Work Securely from Home

Scenario 9: Poor Backups or Failed Restore

- **Business Type**: Retail / E-commerce Small- to Medium-sized Enterprise (SME)
- Ransomware Attack
- Backups were Available but not Successful
- Extended Outage to Business
- **Simple Solution:** How to Test Your Backups

Scenario 10: Insider Mistake (Non-Malicious)

- **Business Type:** Charity (or Other Small Office)
- An Employee Shared a Document in a Wrong Way
- Public Link has Documentary Evidence and Created a Public/Private Mix of Data
- **Simple Solution:** Employee Training & Access Control

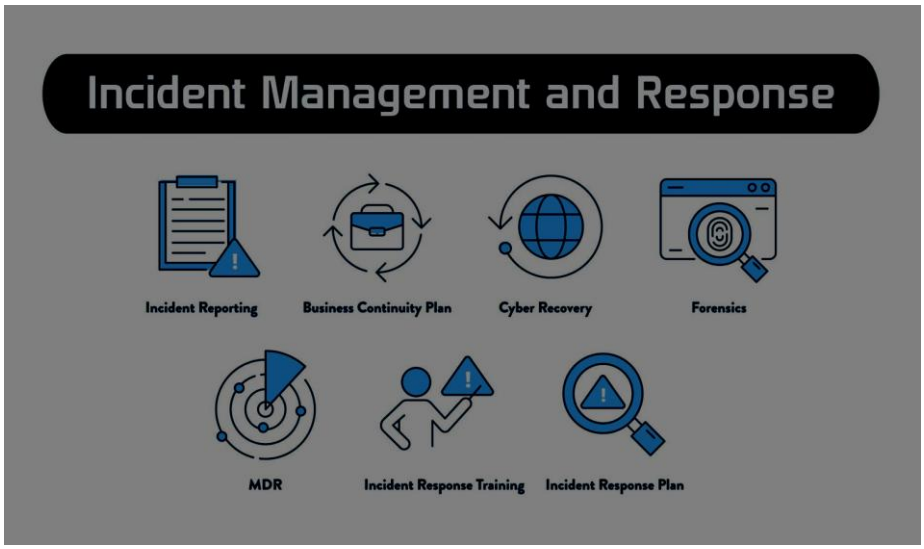
Why Attackers Choose Small Businesses

Small UK businesses tend to attract cybercriminals because they usually have weak cyber defences due to not employing full-time IT personnel, using outdated information technology systems and have a modest budget. Survey data from 2025 shows that 42% of small businesses reported being attacked by cybercriminals, as they are considered to be "easy pickings". Cyber criminals use automated scanning tools to search for large volumes of businesses and look for easy targets to exploit, such as small ransom demands paid or data they can resell after they have accessed it. Additionally, small businesses can be a means to gain access to larger businesses through third-party relationships such as bookkeeping or accounting firms. The National Cyber Security Centre (NCSC) has reported growth in the number of supply chain attacks occurring where a smaller, lower-tier supplier is attacked in order to reach a larger-tier supplier's network.

What Happens After the Breach (Real Consequences)

The clock is ticking once a data breach occurs. If you have an incident involving personal data, you're required under UK GDPR (General Data Protection Regulation) to report it to the ICO (Information Commissioner's Office) within 72 hours. You also must notify individuals affected as soon as possible to help you avoid financial penalties. With fines averaging £10,830 per incident, delays can be very costly. Companies may lose days of productivity due to downtime after a breach; 67% of small businesses that were breached in 2025 reported severe financial hardships shortly after the breach occurred.

Actual outcomes include: recovering from backups (if they're good), accessing insurance claims (if they're available), and repairing your organisation's reputation. In retail data breaches in 2025, companies needing to shift previous processes to manual operations and had to warn shareholders about likely reductions in profits. The pressure and stress placed on owners can be overwhelming; however, many businesses have bounced back stronger than ever with the development of stronger controls. 62% of small businesses received assistance in recovering from data breaches through cyber insurance policies.



FAQs

- **Why would hackers pick on smaller companies?**

They generally have lower levels of protection, and they are likely to respond quickly to pay small ransoms. According to NCSC, small to medium-sized enterprises are sometimes simply an opportunity, not necessarily personal attacks.

- **How frequently do these types of attacks occur in the UK?**

Quite frequently 43% of businesses will fall victim in 2025 (612,000 total), with 42% of those attacks being carried out on small firms. Phishing is responsible for 85% of the attacks.

- **Would antivirus protection stop this?**

In many instances yes with malware and malicious attachment, but frequently no with phishing attacks because you will need some type of training. NCSC has stated that antivirus should be used as part of a layered approach to security.

- **Do cyber criminals use manual processes to target businesses**?

Very rarely with small and medium-sized enterprises. Most criminals will do their scanning processes with automation. Manual processes are used to target large corporations, according to NCSC's review.

- **What should companies do when they experience a cyber breach?**

Privately isolate any affected devices, reset access passwords, and contact your ICO to report any breaches that are related to data. After reporting to the ICO; businesses should contact NCSC or Action Fraud for assistance.

About This Guide

This guide was created by the C**omputer Support Center,** a British-based IT support company that specialises in investigating real life situations related to cyber attack victims in small to medium sized businesses.

The guide was compiled using real life on-site experience rather than hypothetical or sensationalised information.

The guide is designed to provide non-technical business owners and managers with a clear understanding of the way that cyber incidents occur.

The contents of this guide are intended to be educational and are to assist with making board-level decisions in a reasoned, unhurried manner.

This guide should not be used as legal or regulatory advice.

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

Conclusion

The majority of cyber incidents impacting small UK companies arise from weaknesses in ordinary activities being used against them. The examples in this guidance demonstrate that everyday actions, using antiquated equipment, and having your protection measures out of date or missing, can create scenarios that may adversely affect your business.

The good news is that the majority of these incidents could have been avoided with straightforward, reasonable solutions. Cyber security does not have to be complicated or invoke fear to provide a level of protection.

Awareness, having the right level of prevention in place, and conducting periodic reviews are the most efficient methods for mitigating risk.