Small Business Cyber Security Starter Guide

Practical steps every organisation should take to reduce cyber risk

Introduction

Cyber attacks increasingly target small organisations because attackers assume security protections may be weaker than in large enterprises. Many successful breaches occur because simple practices have not been implemented.

This guide outlines key cyber security measures that can significantly reduce risk for small businesses, micro businesses and charities.

Strong Passwords

Why this matters

Weak or predictable passwords remain one of the most common causes of cyber breaches.

Real-world example

A small consultancy used simple passwords such as companyname123 for several staff accounts. An attacker used automated password guessing tools against the company's cloud email service and gained access to an account, sending fraudulent invoices to clients.

Practical actions

1. Use passwords of at least 12-16 characters
2. Avoid predictable words or patterns
3. Use a password manager
4. Enable multi-factor authentication

Multi-Factor Authentication

Why this matters

Passwords alone are often not enough to protect modern systems.

Real-world example

A small business relied only on passwords for their Microsoft 365 accounts. When one employee reused their password on another site that later suffered a breach, attackers logged in to the company email system.

Practical actions

1. Enable MFA on email systems
2. Enable MFA for cloud services
3. Use MFA for remote access systems

Software Updates

Why this matters

Outdated software often contains known vulnerabilities attackers actively exploit.

Real-world example

A company delayed updating website software. Attackers exploited a vulnerability in an outdated plugin and inserted malicious code.

Practical actions

1. Enable automatic updates
2. Regularly update operating systems and applications
3. Remove unused plugins and software

Phishing Awareness

Why this matters

Phishing emails attempt to trick staff into revealing information or clicking malicious links.

Real-world example

An employee received an email appearing to come from a supplier requesting an urgent payment with new bank details. The payment was sent to criminals.

Practical actions

1. Train staff to recognise phishing emails
2. Verify payment changes by phone
3. Be cautious with unexpected attachments

Data Backups

Why this matters

Without reliable backups, ransomware attacks can halt business operations.

Real-world example

A small accountancy firm suffered ransomware that encrypted their files. No recent backups existed so the business had to rebuild systems.

Practical actions

1. Follow the 3-2-1 backup rule
2. Keep one backup offline or off-site
3. Test restoring backups regularly

Network Security

Why this matters

Insecure networks allow attackers to gain access to internal systems.

Real-world example

A company left the default password on its office router and attackers accessed the network.

Practical actions

1. Change router default passwords
2. Use WPA2 or WPA3 encryption
3. Separate guest Wi-Fi networks

Access Control

Why this matters

Too many users with administrative privileges increases risk.

Real-world example

A former employee retained administrator access to cloud services and accessed company data after leaving.

Practical actions

1. Use least-privilege access
2. Remove accounts when staff leave
3. Review permissions regularly

Incident Response

Why this matters

Without a response plan organisations struggle to respond effectively to cyber incidents.

Real-world example

A business discovered suspicious activity but had no defined process to contain the issue.

Practical actions

1. Create a simple incident response plan
2. Know who to contact for support
3. Document recovery procedures

About Wellis Technology

Wellis Technology supports organisations with cyber security guidance, technology resilience and standards based best practice. The focus is on practical improvements that help organisations reduce cyber risk.

Website	www.wellis-technology.co.uk
Email	wellis.technology@gmail.com
Telephone	07976 806151

Guide written by John Ellis - Wellis Technology