Cyber Security for Micro Businesses

Practical cyber security guidance for organisations with fewer than 10 staff

Contents

Introduction

Cyber attacks increasingly target micro businesses because attackers assume security protections may be weaker than those used by larger organisations. Many successful breaches occur because simple security practices have not been implemented.

This guide highlights practical cyber security steps that can significantly reduce risk for micro businesses, charities and small organisations.

Strong Passwords

Why this matters

Weak passwords remain one of the most common causes of cyber security breaches in small organisations.

Real-world example

A small design business used passwords such as design123 and companyname. Attackers used automated tools to guess the password and gained access to the company's Microsoft 365 email account. The attacker then sent fraudulent invoices to customers.

Practical actions

1. Use passwords of at least 12-16 characters
2. Avoid dictionary words
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 online services.

Real-world example

An employee reused their password on another website that later suffered a breach. Attackers used the stolen password to access the company email account because multi-factor authentication was not enabled.

Practical actions

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

Software Updates

Why this matters

Outdated software often contains known security vulnerabilities.

Real-world example

A company delayed updating its website software. Attackers exploited a vulnerability in an outdated plugin and inserted malicious code that redirected visitors to a phishing site.

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 passwords or authorising fraudulent payments.

Real-world example

A business received an email appearing to come from a supplier requesting an urgent payment with new bank details. The message was fraudulent and the payment was sent to criminals.

Practical actions

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

Data Backups

Why this matters

Without reliable backups ransomware attacks can stop a business.

Real-world example

A small accountancy firm suffered ransomware that encrypted client files. Because there were no recent backups the firm had to rebuild systems from scratch.

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 allowing attackers to access 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 security risk.

Real-world example

A former employee retained administrator access to cloud services and later accessed company files 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 detected suspicious activity in their systems but had no defined process for responding. The delay allowed attackers to access additional systems.

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, resilience planning 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