PRACTICAL CYBERSECURITY FOR SMALL BUSINESS OWNERS

Simple steps that genuinely reduce risk

Cyber Centre of Excellence for Local Public Services

Executive Summary

Small and micro-businesses are now routine targets for cyber attacks. Automated ransomware campaigns, AI-generated malware, and ongoing geopolitical cyber conflict mean that even one-person businesses can be compromised.

In 2025, most UK organisations publicly listed by ransomware groups had fewer than 200 employees, and more micro-businesses were impacted than companies with over 10,000 staff.

The good news: most successful attacks exploit basic weaknesses, not advanced technology. Simple, affordable controls — such as, changing router defaults, separating home and work networks, enabling MFA, protecting laptops and phones, and backing up data — stop most threats, including many zero-day attacks.

1. Understand the Reality of Today's Threats

Cyber conflict is global and continuous, involving state-backed actors from China, Russia, Iran, and North Korea. While they often target governments and critical infrastructure, small businesses are frequently compromised as they are easier to breach and can act as stepping stones into larger supply chains.

Real-world testing has shown that even highly sophisticated malware, which costs enormous sums to develop, can be defeated by small businesses that apply basic, modern security controls.

Conversely, businesses with poor cyber hygiene are routinely compromised by automated attacks that indiscriminately scan the internet for weak settings, unpatched devices, and reused passwords.

You are not too small to be attacked, but you are small enough to defend effectively.

2. Expect Attacks You Have Never Seen Before

Many modern attacks are zero-day threats, which are novel, unseen malware that exploit vulnerabilities not yet identified or patched. AI has made it easier to generate these attacks at scale, and traditional signature-based antivirus alone is no longer sufficient to protect yourself against them.

Cyber Centre of Excellence for Local Public Services

Today, protection must sit directly on laptops and mobile devices. Modern endpoint security tools detect all suspicious behaviour, not just known malware. Some of this capability is already included in tools many businesses own, such as Microsoft Defender, but it **must** be enabled, configured, and kept updated to be effective.

Assume attackers will try something new. Every laptop and phone must be able to defend itself.

3. Attackers Look for the Easiest Way In

Most successful breaches still exploit simple weaknesses, including:

- Default router names and passwords
- Poorly secured home networks used for work
- Smart TVs, printers, CCTV, and other devices that were never designed with security in mind
- Reused passwords and lack of MFA
- Unpatched laptops and phones

Attackers will target any weaknesses they can find. If your business laptop shares a network with family devices, smart home systems, or entertainment equipment, those devices will become indirect entry points.

Remove the obvious weaknesses and attackers move on.

4. Secure the Basics First (This Stops Most Attacks)

Change Default Router Settings

Routers often ship with predictable names and passwords that attackers already know. Changing these dramatically reduces risk.

Actions:

- Change the Wi-Fi name
- Change the router admin password
- Use a strong, unique password
- Disable remote management unless absolutely necessary

Keep Systems Updated

Automatic updates close known vulnerabilities that attackers routinely exploit. This applies to laptops, phones, routers, and smart devices.

Protect Every Laptop and Mobile Device

Every device that can access business data must have modern endpoint protection capable of blocking unseen malware. This includes both laptops and smartphones.

Separate Risky Devices from Business Systems

Home networks are now business networks. Smart TVs, printers, heating systems, and family devices should not share the same network as business laptops.

Actions:

- Enable a guest network on your router
- Use a device such as Eero to create separate home and work networks
- Put business devices on one network
- Put smart devices and family devices on another

If a device can access your data, it must be protected and ideally isolated.

5. Invest in User Training

Human error remains the single biggest cybersecurity risk. Affordable, NCSC-assured training can significantly reduce incidents caused by phishing, unsafe downloads, and simple mistakes.

Technology cannot compensate for untrained users.

6. Don’t Ignore Physical Security

Cyber security includes physical access. A lost laptop, an unlocked office, or an unattended device can compromise sensitive data just as easily as a digital attack.

Cybersecurity does not stop at the keyboard.

7. Regularly Test Yourself and Your Suppliers

Security degrades over time unless actively maintained. Both your own controls and those of your suppliers should be reviewed and tested regularly. Contact the CCoE to help with this at enquiries@ccoe.org.uk.

Cyber resilience is a continuous process, not a one-off project.

Cyber Centre of Excellence
for Local Public Services

8. Essential Tools for Small and Micro-Businesses

These tools provide strong, affordable protection aligned with the controls above:

OSP Cyber Academy	NCSC-assured training for staff
Eero	simple network segmentation for home and office
1Password	password management and dark-web monitoring
Incogni	removal from data broker sites
NordVPN	Secures communications, especially on public Wi-Fi
FSecure	smartphone protection
AppGuard	advanced Windows protection proven to stop zero-day attacks, even offline

9. A 30-Day Action Plan for Small Businesses

Week 1

- Change router credentials □
- Enable MFA on all accounts □
- Install a password manager □
- Deploy protection on laptops and phones □

Week 2

- Separate home and work networks □
- Check for leaked credentials □
- Enable automatic updates everywhere □

Week 3

- Review online accounts □
- Confirm backups are working and recoverable □

Week 4

- Create a simple incident response plan □

If you would like help with this, Eastbourne Chamber has teamed up with the Cyber Centre of Excellence and Southern IT to help you make these changes.

For further information on cyber tools and services that might help your organisation please email: **enquiries@ccoe.org.uk**

Developed by the Cyber Centre of Excellence (CCoE).

Cyber Centre of Excellence
for Local Public Services