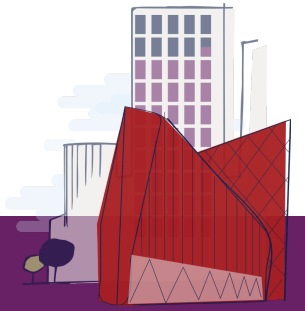
National Cyber Security Centre

Cyber Security: SME's

Partners in Procurement – Supplying the Public Sector



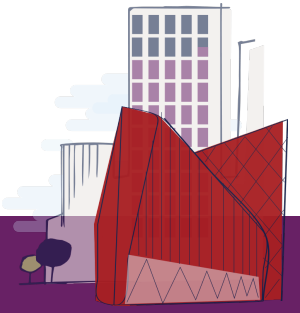
National Cyber Security Centre
a part of GCHQ

Supply Chain Security

How to gain and maintain control of your supply chain

1. **Understand the Risks**
2. **Establish Control**
3. **Check your arrangements**
4. **Continuous Improvement**

https://www.ncsc.gov.uk/guidance/supply-chain-security

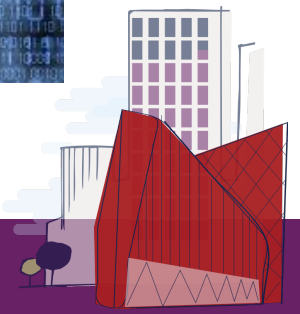


National Cyber Security Centre
a part of GCHQ

Why do we care about SME's?

- Vital component of UK economy
- Cyber attackers go after small businesses because they represent a low risk
- Small Businesses are vulnerable to untargeted attacks.
- Small Businesses do not have the time, money or resources that big businesses have to protect themselves
- 47% of all UK businesses identified at least one breach or attack in the last year

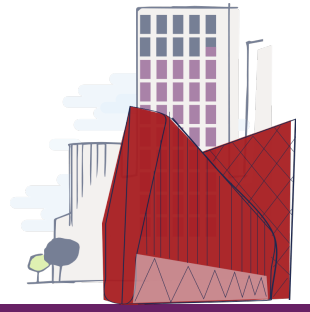
National Cyber Security Centre



National Cyber Security Centre
a part of GCHQ

Who commits Cyber Crime?

- Script kiddies
- Hacker Groups
- State Sponsored
- Insider Threat



National Cyber Security Centre
a part of GCHQ

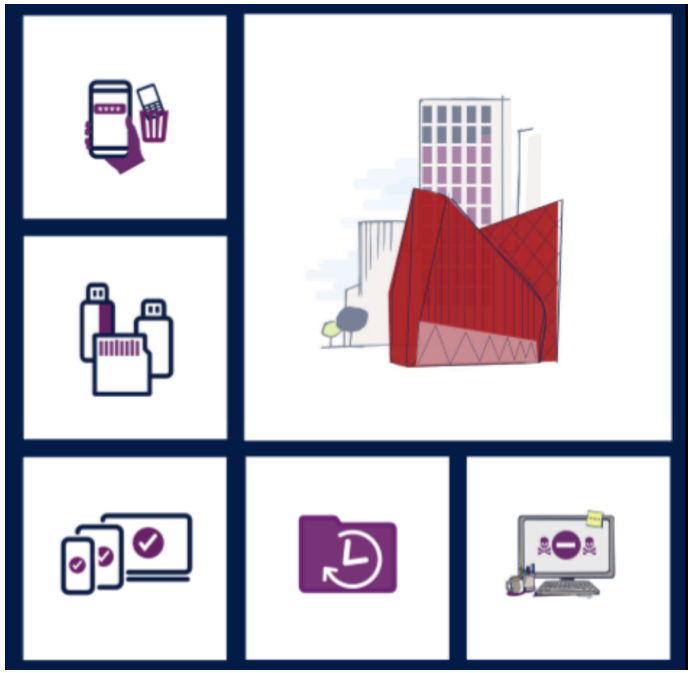
SME Top Threats

Phishing Attacks

Ransomware

DDOS

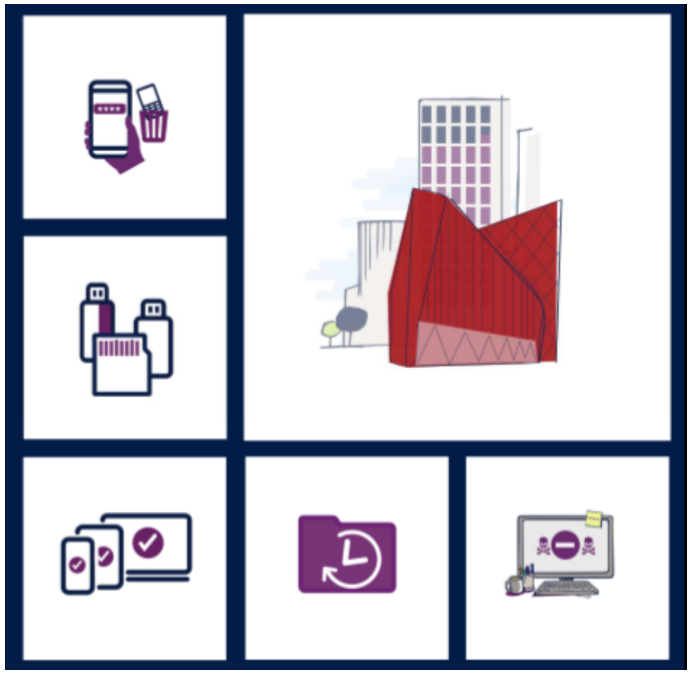
Insider Threat



National Cyber Security Centre
a part of GCHQ

What are we doing to help?

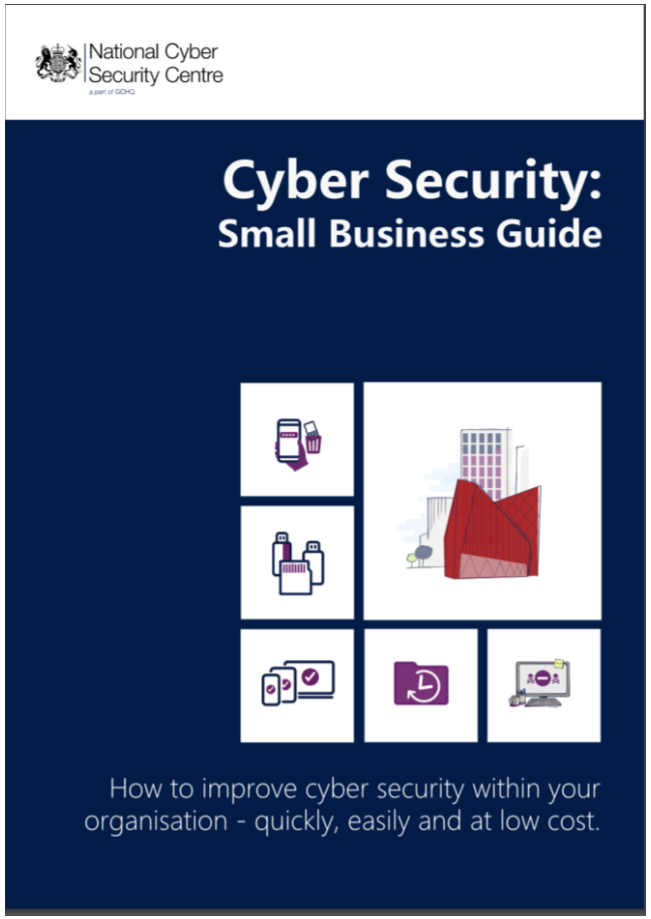
The Small Business Guide



https://www.ncsc.gov.uk/smallbusiness

National Cyber Security Centre
a part of GCHQ

The Small Business Guide



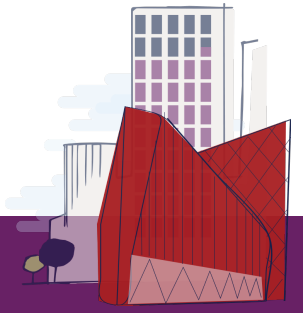
The SBG contains advice that is easy to understand and costs little to implement. Following the 5 steps will significantly increase protection from the most common types of cyber crime.

National Cyber Security Centre
a part of GCHQ

The Small Business Guide

5 simple, free or low cost steps

Backing up your data
Protecting your charity from malware
Keeping your smartphones (and tablets) safe
Passwords!!
Avoiding phishing attacks



National Cyber Security Centre
a part of GCHQ

Small Business Guide Actions List

Policy actions

These actions should be carried out by staff responsible for determining the overall cyber security policy.

- ☐ Identify and record essential data for regular backups.
- ☐ Create a password policy.
- ☐ Decide what access controls your users need so they can access only the information and systems required for their job role.
- ☐ Decide what staff need access to USB drives
- ☐ Sign up to threat alerts and read cyber local advice e.g. briefing sheets/threat reports from www.actionfraud.police.uk/signup.
- ☐ Create an inventory of approved USB drives and their issued owners, and review whether the ownership is necessary periodically.

Technical actions

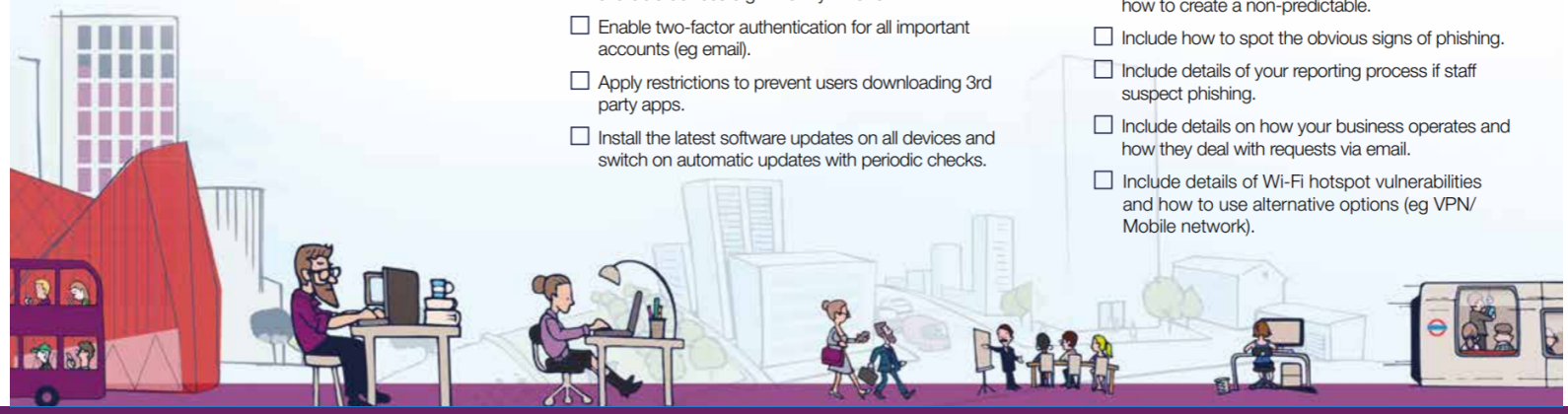
These actions should be carried out by technical staff responsible for the setup and configuration of devices, networks and software.

- ☐ Switch on your Firewall.
- ☐ Install and turn on Anti-virus software.
- ☐ Block access to physical ports for staff who do not need them.
- ☐ Consider making a password manager available to your staff to secure their passwords. Review the star ratings before choosing one from an app store.
- ☐ Ensure data is being backed up to a backup platform e.g. portable hard drive and/or the cloud.
- ☐ Set automated back-up periods relevant to the needs of the business.
- ☐ Switch on password protection for all available devices. Change default passwords on all internet-enabled devices as per password policy.
- ☐ Install and turn on tracking applications for all available devices e.g. Find my iPhone.
- ☐ Enable two-factor authentication for all important accounts (eg email).
- ☐ Apply restrictions to prevent users downloading 3rd party apps.
- ☐ Install the latest software updates on all devices and switch on automatic updates with periodic checks.
- ☐ Ensure all applications on devices are up to date and automatic updates have been set to download as soon as they are released. Schedule regular manual checks on updates.
- ☐ Set up encryption on all office equipment. Use products such as Bitlocker for Windows using a Trusted Platform Module (TPM) with a PIN, or FileVault (on mac OS).

Training and awareness actions

These actions should be carried out by staff responsible for implementing staff training and awareness.

- ☐ Provide secure physical storage (eg a locked cupboard) for your staff to write down and store passwords.
- ☐ Create a Cyber Security training plan that you can use for all staff.
- ☐ Include details of your 'Password' policy explaining how to create a non-predictable.
- ☐ Include how to spot the obvious signs of phishing.
- ☐ Include details of your reporting process if staff suspect phishing.
- ☐ Include details on how your business operates and how they deal with requests via email.
- ☐ Include details of Wi-Fi hotspot vulnerabilities and how to use alternative options (eg VPN/ Mobile network).



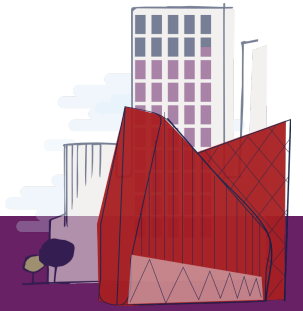
National Cyber Security Centre
a part of GCHQ

Future Plans in Development

GDPR Security Outcomes for SME's

"EXERCISE IN A BOX"

Small Business Guide to Response & Recovery



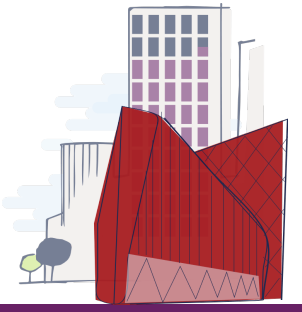
National Cyber Security Centre
a part of GCHQ

Post Incident

Reporting a cyber attack:

CSP

CYBER SECURITY INFORMATION SHARING PARTNERSHIP



National Cyber Security Centre
a part of GCHQ

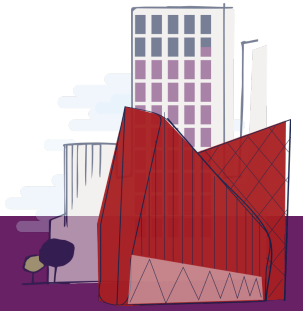
SME Engagement Team

We would love to hear from you!

- Feedback from you on our products and guidance

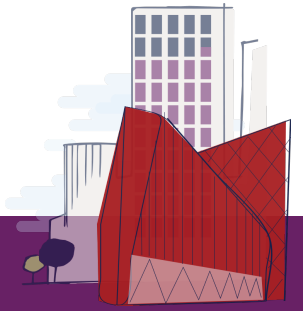
- Case Studies from SME cyber victims

Email Victoria.S2@ncsc.gov.uk



National Cyber Security Centre
a part of GCHQ

Download the guidance at:

https://www.ncsc.gov.uk/smallbusiness

Follow us @NCSC