

CYBER SECURITY AWARENESS MONTH

SMEs

Strong cyber foundations

- › The Cyber context
- › Building strong foundations
 - › Cyber Action Toolkit
 - › Cyber Essentials
 - › Early Warning
- › Adoption of Passkeys
- › How to support Cyber Security Awareness Month
- › Assets
- › Suggested copy



Throughout October, the National Cyber Security Centre will support Cyber Security Awareness Month by encouraging practical, expert guidance to help UK businesses strengthen their cyber resilience and bolster their defences.

This year's international theme, Don't Make It Easy For Them, focuses on making life harder for cyber criminals. The NCSC's supporting theme, Strong cyber foundations, focuses on the simple steps organisations can take to reduce risk and strengthen resilience.

For SMEs, strong foundations mean adopting core cyber security behaviours and recognised protections before progressing towards greater resilience.

We're encouraging organisations to:

- › Adopt passkeys where possible
- › Take practical action through the Cyber Action Toolkit
- › Work towards Cyber Essentials certification
- › Strengthen resilience through services such as Early Warning and Assured Services

We invite you to help amplify this campaign through your existing channels and networks..

CYBER SECURITY AWARENESS MONTH



National Cyber
Security Centre
a part of GCHQ

STRONG
CYBER
FOUNDATIONS

Why strong foundations matter

- Nearly half (46%) of small businesses experienced a cyber breach or attack the last 12 months. AI is making it easier and cheaper for cyber criminals to target organisations of all sizes, increasing the speed and scale of attacks. Getting the cyber foundations right remains one of the most effective ways to protect your business.
- Phishing attacks remained the most prevalent type of breach or attack by far (experienced by 38% of businesses).
- The proportion of businesses holding Cyber Essentials has increased rising from 3% in 2024/25 to 5% in 2025/2026.
- Despite improvements in some cyber hygiene measures last year, several resilience indicators declined. The proportion of businesses undertaking cyber security risk assessments fell from 48% to 41%.
- Many organisations still do not use multi-factor authentication with adoption of two-factor authentication remaining relatively low at 47% of businesses.

How you can protect your business

NCSC tools & services

The Cyber Action Toolkit

For sole traders, micro-businesses and small organisations, the Cyber Action Toolkit can act as the starting point on the cyber resilience journey. It helps organisations build the habits and protections that underpin Cyber Essentials certification.

Just like you'd install a lock on your shop door, this toolkit helps you secure your business with straightforward actions tailored to your size and situation.

Advice from the NCSC's experts, is turned into simple, achievable steps, which guide you through building stronger cyber protection at your own pace, with built-in features that recognise your progress – providing a starting point to cyber security and a pathway towards Cyber Essentials certification.



NCSC tools & services

Cyber Essentials:

www.ncsc.gov.uk/cyberessentials

Cyber Essentials is a UK government-backed certification that proves your organisation is protected against the most common cyber threats.

Implementing just **five key controls** reduces risk, builds protection and gives stakeholders verified assurance that your organisation prioritises cyber security and meets the UK minimum standard for cyber security.

Cyber essentials should be promoted and implemented through supply chains, to reduce the cyber risk and be cyber mature.

Just over one in ten businesses said they reviewed the risks posed by their immediate suppliers (15%) and under one in ten were looking at their wider supply chain (6%)¹.

NCSC tools & services

Early Warning

www.ncsc.gov.uk/section/active-cyber-defence/early-warning

For many organisations, the cost of network monitoring is prohibitive, and the specialist skills it requires often aren't available in-house. Early Warning is a free service designed to warn organisations of potential cyber attacks on their network, as soon as possible, potentially giving invaluable time to detect and stop a cyber incident before it escalates.

Once strong foundations are in place, organisations can strengthen resilience further through services such as Early Warning, helping identify issues before they become incidents.

Adoption of Passkeys

The NCSC has been encouraging the adoption of passkeys as a safer, simpler and more resilient alternative to traditional passwords. Passkeys help protect against common threats such as phishing, password reuse and weak passwords.

- As more online services begin supporting passkeys, SMEs have an opportunity to strengthen account security whilst making sign-in easier for staff and customers.
- While adoption is increasing, many organisations still rely heavily on passwords. Wider use of passkeys can help reduce common security risks and improve cyber resilience over time.
- This Cyber Month, we encourage organisations to explore passkeys as part of building strong cyber foundations alongside Cyber Action Toolkit, Cyber Essentials and other NCSC guidance.

Passkey logins are up to 8 times faster than signing in with username, password and 2SV code.

How you can support Cyber Security Awareness Month

Encourage action

Help SMEs take the next step on their cyber resilience journey.

Whether that's adopting passkeys, using the Cyber Action Toolkit, working towards Cyber Essentials or signing up for Early Warning

Signpost

Use your channels and networks to share relevant NCSC guidance, products and services that can help organisations build strong cyber foundations.

Social media

Share or comment on the NCSC's content. Use the suggested copy and hashtags provided in this pack.

Tag NCSC and use the hashtag:

#CyberMonth2026

Assets

[Click here to download all assets](#)

Assets within the pack

- Social statics in 1x1 9x16, 16x9
- Email signature

Planned Cyber Month Content themes:

w/c 5th – Passkeys & Cyber Governance for Boards
w/c 12th – Early Warning & Cyber Essentials
w/c 19th – Cyber Essentials & Cyber Assessment Framework
w/c 26th – Cyber Action Toolkit



You can find us on: [LinkedIn](#), [X \(Twitter\)](#), [Instagram](#), [Bluesky](#), [Facebook](#), [Threads](#)



Suggested Copy

Cyber threats are evolving, but so are the ways to protect against them. This #CyberMonth2026, explore @NCSC's guidance to help your organisation stay secure.

Learn how your organisation can improve its cyber resilience all #CyberMonth2026 with tools and advice shared by @ncsc throughout October

Cyber security is everyone's responsibility. This #CyberMonth2026, @NCSC is sharing tools and tips to help organisations and individuals build resilience together.

Wondering how to boost your organisation's cyber resilience? This #CyberMonth2026, @NCSC is sharing expert tips and tools all October long.



Thank You

For terms and conditions, please refer to the NCSC website:
[Terms & conditions - NCSC.GOV.UK](https://www.ncsc.gov.uk/terms-conditions)