NCSC: Leave passwords in the past – passkeys are the future

Passkeys are the more secure and user-friendly login method and should be the default authentication option for consumers.

- GCHQ's National Cyber Security Centre (NCSC) heralds a new era of secure sign in with passkeys now ready for mass adoption
- Passwords are no longer resilient enough for the contemporary world, cyber experts say in new report published on Day Two of CYBERUK conference in Glasgow
- Consumers encouraged to migrate to passkeys where possible to unlock simpler and safer digital lifestyle

Passkeys should now be consumers' first choice of login across all digital services, the UK government's technical authority on cyber security has announced today (Thursday).

Overhauling decades of security practice, the National Cyber Security Centre – a part of GCHQ – has taken the decision to no longer recommend individuals use passwords where passkeys are available because passwords lack the relative resilience to modern cyber threats.

Passkeys are a newer method for logging into online accounts which do much of the heavy lifting for users, only requiring user approval rather than needing to input a password. This makes passkeys quicker and easier to use and harder for cyber attackers to compromise.

A new technical report, published today on Day Two of CYBERUK – the UK government's flagship cyber security event in Glasgow, shows that passkeys are at least as secure as, and generally more secure than, pairing the strongest password with two-step verification (2SV).

The majority of cyber harms to individuals start with criminals stealing or compromising login details, making the adoption of passkeys a huge leap in boosting the UK's resilience to phishing attacks.

A number of popular online service providers already support passkeys, including Google, eBay and PayPal – and new data from Google shows the UK already lead global adoption of passkeys, with just over 50% of active Google services users in the UK having one registered.

The NCSC stopped short of endorsing the adoption of passkeys last year due to some key implementation challenges. However, progress within industry means they can now be recommended to the public as the more secure and user-friendly login method and to businesses as the default authentication option to offer consumers.

> *Adopting passkeys wherever you can is a strong step towards a safer, simpler login experience and I am pleased that we can now support uptake.*
>
> *The headaches that remembering passwords have caused us for decades no longer need to be a part of logging in where users migrate to passkeys – they are a user-friendly alternative which provide stronger overall resilience.*
>
> *As we aim to accelerate the UK's cyber defences at scale, moving to passkeys is something all of us can do to improve the security of everyday digital services and be prepared for modern and future cyber threats.*
>
> Jonathon Ellison, Director for National Resilience, NCSC

Where a particular service does not support passkeys, the NCSC's advice to consumers is to use a password manager to create stronger passwords and keep using two-step verification.

Making passkeys the default authentication recommendation is a critical step towards revolutionising the way individuals use and access their online identities.

The key benefits include:

- **Easy to use:**
  Fast, frictionless passkey logins can be completed up to eight times faster than signing in with a username, password and two-step verification code.
- **Harder to compromise:**
  Passkeys are highly resistant to phishing attacks and cannot be intercepted, reused or guessed like passwords can.
- **Reduced password fatigue:**
  Users no longer need to meet additional requirements, such as creating complex passwords – or even remembering them at all. This prevents weak points and patterns developing across a user's online presence.
- **Security that pays off:**
  Safety and savings can go hand in hand for online service providers that make passkeys available for customers, replacing SMS-based verification systems which incur additional costs.

Last year, the UK government announced it would roll out passkey technology for its digital services as an alternative to the current SMS-based verification system, offering a more secure and cost-effective solution that could save several million pounds annually.

PUBLISHED

23 April 2026

WRITTEN FOR

Cyber security professionals Large organisations Public sector Self employed & sole traders Small & medium sized organisations You & your family

NEWS TYPE

General news