

NCSC now recommends passkeys over passwords wherever they are available



The UK's NCSC no longer recommends passwords where passkeys are offered, and advises businesses to make passkeys the default sign-in option for consumers. Its new report finds them at least as secure as a strong password with two-step verification.

- The NCSC, part of GCHQ, now recommends passkeys as individuals' first choice of login wherever a service supports them.
- A new technical report finds passkeys at least as secure as, and generally more secure than, a strong password paired with two-step verification.
- Businesses are advised to offer passkeys as the default authentication option to consumers.
- Where a service lacks passkey support, consumers should use a password manager and keep two-step verification on.

- The NCSC held back from endorsing passkeys last year because of implementation challenges, which industry progress has since addressed.

The UK National Cyber Security Centre (NCSC), part of GCHQ, has announced that passkeys should now be the first-choice login for individuals across digital services. It no longer recommends passwords where a passkey is available, citing their weaker resilience against modern threats.

What the NCSC found

A technical report published at the CYBERUK conference concludes that passkeys are at least as secure as, and generally more secure than, pairing the strongest password with two-step verification. The NCSC notes that most cyber harms to individuals begin with stolen or compromised login details, and that passkeys are highly resistant to phishing and cannot be intercepted, reused or guessed.

The NCSC did not endorse passkeys last year because of implementation challenges. Industry progress now allows it to recommend them to the public, and to businesses as the default authentication option for consumers.

Practical points

The NCSC also lists usability gains, including logins up to eight times faster than a username, password and verification code, and less password fatigue. For service providers, it points to savings from replacing SMS-based verification, which carries extra cost. Where a service does not support passkeys, its advice is to use a password manager and keep two-step verification.

The guidance is aimed at consumer authentication. Institutions in the Kingdom can treat it as a useful reference point when reviewing their own customer-facing sign-in options, while assessing fit against their regulatory obligations.

What to do now

1. Review which customer-facing and workforce applications already support passkeys (FIDO2/WebAuthn).
2. Assess offering passkeys as a default or preferred sign-in option for customers, alongside existing controls.
3. Check passkey adoption against applicable NCA and SAMA authentication requirements before changing policy.
4. Evaluate the cost and risk of SMS-based verification as a candidate for replacement.
5. For services without passkey support, encourage password managers and keep multi-factor authentication enabled.