Passkeys: the promise of a simpler and safer alternative to passwords

The merits of choosing passkeys over passwords to help keep your online accounts more secure, and explaining how the technology promises to do this

James L

Today, using online services such as messaging, shopping, travel, social media, media streaming and government services almost always means having to set up and manage *yet another* account and password. At the same time, we're seeing more and more attempts by cyber criminals to take over online accounts for their own gain – often at your expense.

Keeping these account passwords out of the hands of cyber criminals can be overwhelming. Fortunately, there is technology that promises to make this easier, by using **credential managers** and **passkeys** to do much of the heavy lifting for you.

What's the problem with passwords?

You probably know all too well the personal pains of having to create, recall and enter passwords so I won't repeat them here. When it comes to cyber attacks against online accounts, the main reasons why passwords are a pain are:

- **Passwords can be guessed:** Being told to think up and remember so many passwords means people (understandably) often create weak – and therefore more predictable – passwords. This means a cyber criminal has a higher-than-we'd-like chance to *guess* someone's password.
- **Passwords can be stolen:** Being asked to enter (or paste) passwords so often and in so many places has made people less cautious when being asked to sign in to *yet another* site. By going phishing, a cyber criminal can *steal* someone's password by successfully tricking them into entering their password into a look-alike site.

- **Passwords can be reused:** Services storing people's passwords insecurely allow cyber criminals to discover people's passwords, meaning they can not only sign in to someone's account in that service, but also any other service where that person has *reused* the same password.

What's being done about this?

Two big things.

Firstly, improving the use of passwords where we aren't quite ready to get rid of them yet, including encouraging the use of a password manager and enabling 2-step verification.

Secondly, removing the need for a password in the first place – creating a 'passwordless' account sign-in process. You may have already come across some options for passwordless account sign-in – such as social login, magic links and email or text-based one-time passwords (or 'OTP'). It's in this area where another option is emerging as a popular choice around the world thanks to their ideal blend of usability, privacy and security: **passkeys**.

What are passkeys?

Passkeys are created, saved, stored and managed for you on your trusted device(s) – such as your smartphone, tablet or computer. This is done by your chosen **credential manager**. This will most likely be the default one built in to your device – such as Apple Passwords, Google Password Manager, Samsung Pass or Windows Hello – unless you have specifically chosen to install and use another one.

This credential manager is responsible for protecting your passkeys and only allowing a passkey to be used once you've proven to it that you're really you trying to use it. When you want to use a passkey to access an account, it will often look like you are 'just' using your PIN, fingerprint or face to unlock the

account. While there is a lot more security going on behind the scenes, they really are that easy to use.

As part of managing your passkeys most popular credential managers will also:

- securely back up new passkeys for their safety in case you lose all your devices
- copy (or 'sync') them to other devices you have so you don't have to create a new passkey on each one

Where passkeys are offered, you can set one up for an existing account (look in the account security or privacy settings) or right from the beginning when creating a new account.

How do passkeys work?

Passkey technology is based on a unique pair of virtual keys that your device creates for you. These keys are related to but different from each other – you can think of them as 'siblings'. In this sibling pair there is:

1. Your *passkey*.

This is kept secret for you by your chosen **credential manager** on your device(s), such as your smartphone and computer.

2. Its *verifier*.

This is intentionally given over to the online service which will use it only as a means to verify you to your account.

The important difference to passwords here is that **both unique parts of the sibling pair are needed to sign in to an account** – unlike passwords where it is the same 'identical twin' that is shared between both sides.

If you want a more detailed look 'under the hood' at how passkeys work to protect your account better than a password, then you can read more about this

in the expanded section below.

An 'under the hood' look at how the passkey registration and sign-in work Hide

Much like passwords, there are two stages to the use of passkeys to access an online account:

- **Registration:** where you add a new passkey-verifier pair to your account (either during creation of a new account or adding one to your existing account).
- **Sign-in:** where the passkey is used to prove you are the person that is allowed to access that account.

Registering a passkey for an account
When you register a passkey for an account in an online service, your device creates a new, unique pair of keys specifically for that account.

- The *passkey* (and other important information about your account, including your username) is saved to the credential manager that you've chosen to trust on your device(s).
- The *verifier* part is sent by your device to the online service, which saves it for later use whenever you go to sign in to your account using its sibling passkey.

Notice the important differences to passwords here are that:

- Your device creates an account-unique passkey and saves it to your credential manager for you, so you don't have to worry about this.
- Your device shares the accompanying verifier (not your passkey) with the online service.

Signing in to your account using a passkey
When you go to sign in to an online service, your device will:

- Receive a ‘challenge’ created by the online service in response to your request to sign in.
- Take the website address you are trying to sign in to from the browser or app you’re using.
- Ask your credential manager to show you a list of passkeys you have for that website for you to choose from.
- Prompt you to prove that you're really you, using something you already have like a PIN or your fingerprint or face.

Once you’ve chosen the account that you want to sign in to from that list:

- Your device sends back the ‘challenge’ it got from the online service with proof that you have a passkey for that account in your credential manager – and does this without having to reveal or share the passkey itself (by using public key cryptography).
- The online service will use that passkey’s verifier on the ‘challenge’ returned by your device to check the proof that you have the passkey.

Notice the important differences to passwords here are that:

- Your device and credential manager work together to only show you passkeys that you have for the service you’re signing in to, so cyber attacks using look-alike websites simply don’t work on passkeys.
- The passkey itself is never sent to the online service you’re signing in to – only a message that proves you have the passkey – so the passkey can’t be cloned.

Basically, passkeys are easier to use and more secure than passwords

The technology behind passkeys might be complicated (for good reason), but using them shouldn't be.

Setting up your account with a passkey is easier as your chosen credential manager does much of the heavy lifting for you, which means you don't have to:

- think up or worry about yet another username and password
- type in your password twice to confirm you entered - or pasted - it correctly first time
- deal with annoying password complexity rules

Then, once your account is set up, signing in to it using a passkey is also easy as you can rely on your chosen credential manager to help you through the process. This means you don't have to:

- remember the username you registered to that online service with
- type in or paste your username and password as your credential manager automatically presents you with a choice of relevant accounts to pick from

Passkeys are worth your time to keep your online accounts more secure than passwords because:

- the keys are created by your chosen credential manager so they can be much more complex and random than anything created by a human – making it near impossible for an attacker to *guess* the key
- they can only be used with the matching service they were created for – so attackers can't *steal* one using phishing attacks and fake websites
- if a cyber criminal manages to hack into an online service and get your verifier key, they won't have everything they need to get into your account – and they won't have anything to *reuse* on your accounts in other sites and services

---

Want to know more?

Hopefully you'll now have a grasp on what passkeys are and why they matter for you and your cyber security. All that said, while passkeys *promise* a universal and seamless experience, we have found that there are still some 'rough edges' that need smoothing out before passkeys can replace passwords everywhere for UK citizens. To find out what we think of the current state of passkeys and where we think they still need some work, take a look at our other blog Passkeys: they're not perfect but they're getting better.

James L
Senior Security Researcher

WRITTEN BY

James L
Senior Security Researcher

PUBLISHED

15 January 2025

PART OF BLOG

Inside the NCSC