Passkeys: What They Are and Why They Matter

A Wey Valley Radio guide to safer logins — for the station, and for you

VERSION 1.0 · JUNE 2026

The short version

Passwords are no longer good enough. The UK's own cyber security authority now says so, and the technology that replaces them — **passkeys** — is already built into the phone and computer you use every day. Wey Valley Radio recommends that everyone involved with the station switches to passkeys wherever they can, and — importantly — that you set up **more than one way** to sign in, so you're never locked out.

This guide explains what a passkey is and why it matters. A companion guide, *How to Use Passkeys*, walks you through the actual setup step by step.

What is a passkey?

A passkey is a modern replacement for the password. Instead of typing a secret string of characters, your device proves who you are using cryptography — the same kind of maths that secures online banking. You confirm it's really you with something you already use: your **fingerprint, face, or device PIN**.

When you create a passkey for a website, your device generates a unique pair of keys. One half (the *private* key) never leaves your device. The other half (the *public* key) is handed to the website. When you log in, the website sends a challenge, your device signs it with the private key, and the website checks the signature. **No password is ever sent**, which means there's nothing to steal in a data breach and nothing to be tricked out of by a fake login page.

That last point is the big one: passkeys are **phishing-resistant by design**. Even if you click a convincing fake email and land on a counterfeit site, there's no password to hand over.

Why this matters now

This isn't a fringe idea or a tech fad. In April 2026 the **National Cyber Security Centre (NCSC)** — part of GCHQ — said it was overhauling decades of security practice to recommend passkeys, where available, as the most secure way to protect your accounts. The NCSC believes passkeys are less vulnerable to hacks and to human error than passwords, and its director for national resilience, Jonathan Ellison, described them as a user-friendly alternative with stronger overall resilience.

Platforms most of us already use — Apple, Google, Microsoft, X — now support them. The government has also adopted passkeys across its own digital services.

The honest caveat, which the experts in the BBC piece make plainly, is that passkeys are **"not a silver bullet."** Their main weakness is exactly the one this guide keeps returning to: if you lose the device that holds a passkey — and you've set up no other way in — getting back into your account can be difficult. That's not a reason to avoid passkeys; it's the reason to set up more than one.

Further reading: *Passkeys: What are they and why are they more secure?* by Liv McMahon, BBC News, 24 April 2026 — a clear, five-minute, non-technical introduction: bbc.co.uk/news/articles/cq8wnzly5j5o.

WVR's advice: don't rely on just one passkey

The single most important point in this guide is this:

> **Set up more than one way to sign in.**

A passkey is brilliant right up until the moment you lose access to the *one device* that holds it. The fix is not to avoid passkeys — it's to have a backup. We recommend a layered approach, building up from what you already own:

1. Start with what's already built in (free). If you're on Windows, your PC already has Windows Hello (a PIN, fingerprint, or face login). If you're on Apple, your iPhone, iPad, and Mac already store and sync passkeys through iCloud. These cost nothing and are likely already half set up. This is your everyday method.

2. Add a physical passkey if you can (recommended for important accounts). A small USB/NFC hardware key — a YubiKey or Google Titan, typically **£25–£60** — gives you the strongest possible protection and a reliable backup that works even if your phone is lost or broken. For high-value accounts (your main email, the station's accounts, banking), this is well worth the cost. Many security professionals carry one as their primary key and keep a second as a spare.

3. Use a password manager if you aren't already (Bitwarden or 1Password). If you'd rather not buy hardware, or you want your passkeys to follow you across every device automatically, a password manager does exactly that. It also tidies up your remaining old-fashioned passwords in the same place. See the pricing below.

The ideal setup combines at least two of these — for example, **Windows Hello or Apple as your daily login, plus a hardware key kept safely as backup**, or **a password manager synced across your devices plus a hardware key for the accounts that really matter.**

Password manager pricing

Both of these can store and sync passkeys, fill them in for you, and look after your old passwords too. Both set their list prices in US dollars; the pound figures below are converted at the current rate (about £0.75 to the dollar, June 2026), so treat them as a guide and confirm the exact amount at checkout — it will vary a little with the exchange rate and any card fees.

Bitwarden

Open-source, independently audited, and the best free tier in the business.

Plan	Annual price	Monthly (billed yearly)	Covers
Free	£0	—	One person, unlimited devices — **includes passkey storage**
Premium	~£15/yr	~£1.25/mo	Adds built-in authenticator, file attachments, emergency access
Families	~£36/yr	~£3/mo	Up to 6 people

Bitwarden's **free** plan is unusually generous: unlimited passwords across unlimited devices, and it can store and fill passkeys too — so for most people it's all you need, at no cost. The paid tiers add extras like a built-in authenticator app and emergency access. Being open-source and audited, it's a popular choice for the privacy- and budget-conscious.

1Password

(Prices rose at the March 2026 renewal — these are the current rates.)

Plan	Annual price	Month-to-month	Covers
Individual	~£36/yr	~£3.70/mo	One person, unlimited devices
Families	~£54/yr	~£5.95/mo	Up to 5 people

Paying annually works out cheaper than monthly, and there's a 14-day free trial. 1Password is widely regarded as the most polished option, particularly across mixed Windows/Apple households.

Other managers (LastPass, Dashlane and similar) also handle passkeys and work in much the same way. We'd lean towards Bitwarden or 1Password — in LastPass's case partly because of the significant data breach it suffered in 2022 — but any reputable manager is far safer than reusing passwords.

This protects you, not just the station

It's easy to think of this as an admin task for Wey Valley Radio. It isn't. The same passkey you set up for a station account is the same technology that protects **your** email, **your** online shopping, **your** banking, and **your** social media. Every account you move off passwords is one that can't be phished, can't be guessed, and can't be exposed in someone else's data breach.

Setting up passkeys for the station is a perfect excuse to do the same for the accounts that matter most in your own life. The skills carry over completely — once you've done it once, you've done it everywhere.

The bottom line

Any passkey is dramatically safer than any password — the UK's national cyber security authority now says as much. Use the methods already built into your devices, add a physical key for the accounts that matter, and lean on Bitwarden or 1Password if you'd like everything to sync automatically. Above all, **set up more than one** so you're never locked out.

Pick whatever fits your life, and you're already ahead of the vast majority of people online — at the station and at home.

Questions, or want a hand getting set up? Get in touch with the WVR team. The step-by-step instructions are in the companion guide, How to Use Passkeys.