Kensington®

Forget Your Password

The most secure log-in is at your fingertips.

Your Employees are the Biggest Threat to Your Data Security

Data breaches are on the rise. 8.5 billion data breaches are estimated to have occurred in 2019[1], up 70% on 2018.[2]

Hacking (using exploits to gain access to privileged information) and phishing (posing as a trustworthy source so that confidential data is surrendered) are the most common cyberattacks used to cause data breaches. **80% of hacking-related breaches are caused by compromised, weak and reused passwords.**[3]

'Secure' passwords - using upper case, lower case, numbers and symbols - are very forgettable. Considering the average business user has 191 passwords[4], they are very real challenge to manage.

Instead of relying solely on user names and passwords, Multi-Factor Authentication (MFA) creates an additional layer of security. **Requiring an additional factor to grant access, biometric authentication is the most secure level of MFA.**

MFA can be seamlessly implemented into user workflows with Windows Hello supporting biometric log-in and passwordless access to online services. The FIDO Alliance have created standards to maximise compatibility for devices.

Kensington VeriMark™ USB Fingerprint Key

- ☑ Biometric log-in
- ☑ Supports MFA
- ☑ Windows Hello
- ☑ FIDO U2F Certified

Kensington®

It’s Time to Forget Your Password

Single-factor authentication - in other words, a password that requires no additional verification - is seen by hackers as the path of least resistance. When a phishing campaign or replay attack successfully harvests a password, it allows for even more information to be hijacked when access to the device is compromised.

Passwords, even strong ones, are no longer enough to protect sensitive accounts and assets from hacking and phishing attacks.

There is a close relationship between password-only security and data breaches, as both perpetuate a vicious cycle of costly information theft.

Your Passwords Aren't Safe Enough

Without additional security measures, passwords are vulnerable to routine theft and interception. **Two-factor authentication** (or **multifactor authentication**) should be part of any modern set of authentication protocols.

By requiring an extra piece of information (or factor) in addition to a password, or two pieces of unique information without any password at all, 2FA/MFA avoids the known complexities and shortcomings of password-oriented log-ins.

Unique biometric credentials, such as fingerprints, are superior to traditional SMS texts and security questions, which can be intercepted without the user even knowing. Authentication technology has evolved with the introduction of biometric solutions such as Microsoft's Windows Hello log-in[5], compatible with **Kensington's VeriMark™ Fingerprint Key.**

Why 2FA and MFA?

The fundamental flaw of single-factor password security is that if an unauthorised party has the correct log-in, they have access to the password-protected account. **It doesn't matter whether they attained the password by theft, a systematic dictionary attack or fortunate guessing: the resulting risk is the same.**

Second and multifactor authentication changes the authentication model for the better in two distinct ways:

- Requiring verification of another credential after successful password entry.
- Permitting log-in exclusively through a more secure passwordless mechanism.

In either case, the authentication solution will attempt to verify a user's identity by **requesting something they know, have or can be identified by.** The possibilities range from a one-time password sent via SMS or generated in an authenticator app, to something significantly stronger such as a hardware or fingerprint key. The latter two provide greater security because they are not vulnerable to interception or phishing.

The Benefits of Biometrics for 2FA, MFA and Passwordless Log-Ins

Biometrics offer a unique combination of convenience and security, as they are:

- **Easy to scan, verify and associate with a specific identity.**
- **Based on credentials that are difficult to duplicate or steal.**
- **Stored or transferred through specialised hardware, to prevent remote access or theft.**

Biometric authentication can deliver more than just a better log-in experience for end users.

Biometrics allow for a passwordless log-in that reduces the password reset burden on the IT Help Desk. Each password reset is estimated to cost more than £50[6] - and more than 40% of users require 50+ resets per year.[7]

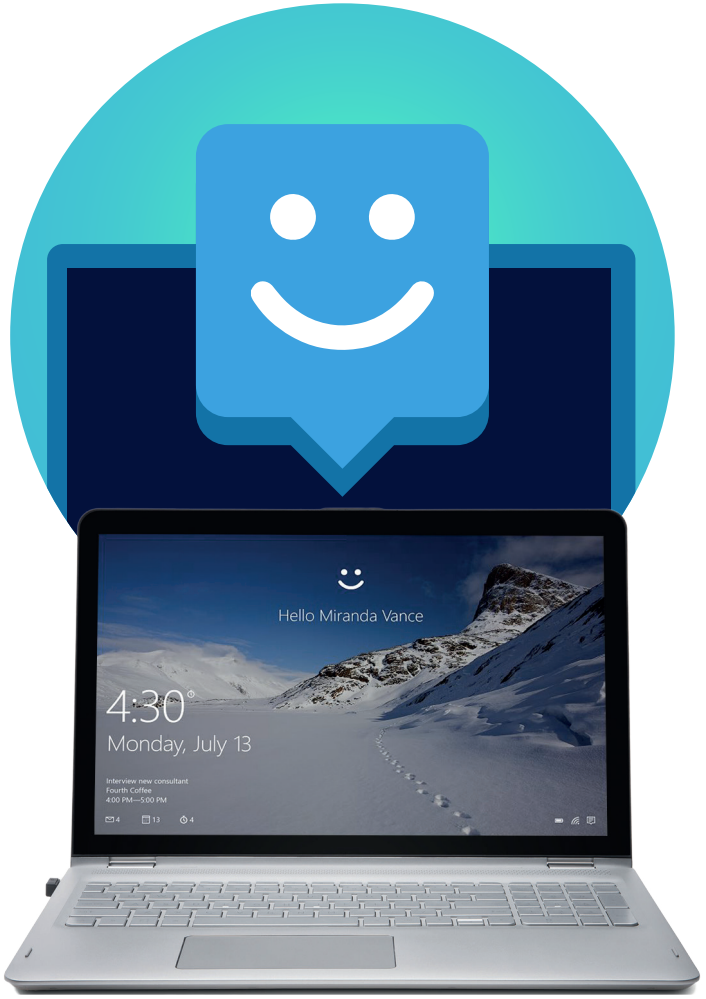
In an organisation of 1000 users, that adds up to £1 million per year in lost time and productivity.

Windows Hello Supports Instant Biometric Log-In

Windows Hello, which is a standard feature of Windows 10, supports instant biometric log-in. These biometric options include facial recognition, iris scanning and fingerprint reading, **the latter via FIDO U2F-certified hardware such as the Kensington VeriMark™ Fingerprint Key.**

Windows Hello eliminates the inconvenience of creating and remembering complex passwords. Even more importantly, it avoids the common loopholes in password-based security, such as exposing credentials via phishing.

The log-in experience for Windows Hello is very straightforward. Successful biometric authentication unlocks access to a supported Windows device.



What is FIDO?

The **Fast IDentity Online (FIDO) Alliance** was established to set standards for both 2FA/MFA and password-free authentication.

FIDO Universal Second Factor (U2F) is an open standard, defining specifications for 2FA using a robust and tamper-proof non-password second factor. Since it is standardised, FIDO U2F has broad compatibility with popular online services, including Gmail, Facebook, Github, Dropbox and many others.

Biometric fingerprint and hardware keys using USB, NFC or Bluetooth technologies are the typical additional factors for services utilising U2F.

fido™ ALLIANCE

VeriMark™ - the 1st Fingerprint Security Key from Kensington that Ensures Strong, Streamlined 2FA

VeriMark™ works with both Windows Hello and FIDO U2F authentication to provide a secure and seamless way to log into Windows 7, 8.1 and Windows 10 as well as to enable 2FA on important accounts.

The VeriMark™ Fingerprint Key offers best-in-class biometric performance within a practical, compact and standards-compliant package.

False rejection (3%) and false acceptance (0.002%) rates that exceed industry standards by leveraging TLS1.2/AES256 encryption and Anti-Spoofing Protection (ASP) technology.

VeriMark™ is the perfect solution for individuals who require biometric authentication that works with current or legacy Windows operating systems, while also supporting U2F authentication for cloud-based service and software providers such as Facebook, Google, GitHub, Dropbox and more.

Kensington VeriMark™ Fingerprint Key

- **Advanced fingerprint technology** combines superior biometric performance and 360° readability with anti-spoofing protection, while exceeding industry standards for False Rejection Rate (3%) and False Acceptance Rate (0.002%).
- **Universal integration** provides scalable, out-of-the-box access for Windows computers and platforms, including biometric log-in for Windows Hello™.
- **FIDO U2F Certified** to ensure seamless interoperability and meet 2nd-factor security key log-on requirements for cloud-based service and software providers, including Google, Dropbox, GitHub and Facebook.
- **Compact design** easily attaches to a standard keyring for convenient portability.

Part No. K67977WW

For more information, samples or deal pricing:


www.kensington.com/forget-your-password


contact@kensington.com

Sources

1. Risk Based Security's Q3 2019 Data Breach QuickView Report
2. darkreading.com/threat-intelligence/2018-was-second-most-active-year-for-data-breaches/d/d-id/1333875
3. Verizon 2019 Data Breach Investigations Report
4. securitymagazine.com/articles/88475-average-business-user-has-191-passwords
5. symantec.com/content/en/uk/enterprise/other_resources/b-is-your-data-safe-security-non-compliance-infographic-21330416-UK.pdf
6. infosecurity-magazine.com/opinions/how-much-passwords-cost
7. plan-net.co.uk/blog/password-reset-processes