yubico

Securing shared workstations against modern cyber threats with phishing-resistant MFA

Legacy authentication is putting your organization at risk

The very nature of shared workstations make them low-hanging targets for cyber criminals and insider attacks, amplifying risks associated with devices, user access, and authentication.

Multi-factor authentication (MFA) can be a strong first-line of defense to protect users using shared workstations and devices against modern cyber threats, however not all forms of MFA are created equal. Legacy authentication such as usernames and passwords can be easily hacked, and mobile-based authentication such as SMS, OTP codes, and push notifications are highly susceptible to modern phishing attacks, malware, SIM swaps, and man-in-the-middle (MiTM) attacks. In addition to security, it's also important to consider usability, portability, and scalability of authentication solutions. Poor user experiences, low portability, and lack of scalability can result in MFA gaps, low user adoption, and an increased risk of a breach.

Shared kiosks

Shared kiosks often support multiple users in a single shift, increasing the prevalence of insecure practices around password sharing to attempt to cut down on logout/login time.

Mobile-restricted

Shared workstations and devices across mobile-restricted environments call for authentication that is highly secure, compliant to industry regulations, and simple to use.

Grab-and-go

As no user is tied to a particular device in this scenario, it is important to have controls that quickly and simply grant access to only those applications and services associated with the specific user credentials.

Point of Sale (POS) terminals

Special attention must be paid to speed and ease of authentication across POS terminals, avoiding potential account lockouts, and most importantly, ensuring the security of customer and payment information compliant with PCI DSS standards.

Key considerations to secure shared workstation environments

While considering authentication solutions for shared workstation environments, in addition to how effective the solution is in protecting against external cyberattacks and insider threats, organizations should also consider how the solution affects user productivity (account lockouts, log in times), how reliable the solution is across varied environments and use cases, external variables which may negatively impact performance, such as cell signal and batteries, and what the long-term total cost of ownership is.

Security

How do you make sure the user logging into the device is the legitimate person?

Efficiency

How do you make sure the user is able to seamlessly authenticate against multiple devices?

Reliability

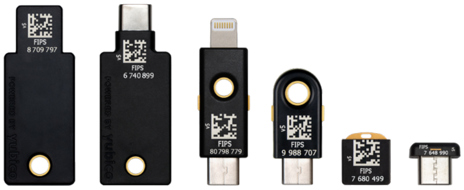
How do you ensure consistent authentication that always works, even in tough environments with varying degrees of connection?

Cost

How do you reduce the number of authentication-related support tickets?

The YubiKey 5 Series

From left to right: YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano and YubiKey 5C Nano



The YubiKey 5 FIPS Series

From left to right: YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS and YubiKey 5C Nano FIPS

Securing shared workstations with the YubiKey

Yubico offers the YubiKey, a hardware security key in a portable USB and nano form factor that is ideal for shared workstation environments. The YubiKey provides strong phishing-resistant two-factor, multi-factor, and passwordless authentication at scale, with the hardware authenticator protecting the private secrets on a secure element that cannot be easily exfiltrated. The YubiKey is the only solution that is proven to stop 100% of account takeovers in independent research.[1]

With the YubiKey, users can securely and easily authenticate to more than 700 applications and services across a variety of devices, with a simple tap or touch—no software installation, battery, or cellular connection is required. The YubiKey uses modern authentication protocols such as FIDO U2F and FIDO2 open authentication standards to help eliminate phishing-driven credential attacks. YubiKeys also supports SmartCard, OTP, and OpenPGP protocols, enabling the use of a single security key across a variety of modern and legacy systems.

	Username & password	Mobile-based authenticators	YubiKey
Security	Low, easily hacked	Medium, 10-50% account takeover rates[2]	High, 0% account takeover rate[3]
Efficiency	Password fatigue, account lockouts	Users that can't, won't, don't use mobile MFA	Tap-and-go experience. 4x faster to login than OTP[4]
Reliability	Prone to human error	Reliant on device battery and cellular network Not suited to mobile-restricted environments	Robust build, does not rely on cellular network
Cost	No up-front cost High IT support cost High potential risk	$1,840 is the true cost of enterprise mobility per owned device[5]	Low cost compared to mobile MFA, and 92% reduction in support tickets[6]

[1] Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019), https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

[2-4] Ibid

[5] Wander: Uncovering the true costs of enterprise mobility https://www.clevermobile.it/risorse/file/wandera/tcowhitepaper.pdf

[6] https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

About Yubico As the inventor of the YubiKey, Yubico makes secure login easy. As a leader in setting global standards for secure access to computers, mobile devices, and more, Yubico is also a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards. For more information, please visit: **www.yubico.com.**

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (toll free)
650-285-0088