EBOOK

Not all MFA is created equal

How modern MFA is more secure than SMS or mobile authentication apps

yubico

Legacy MFA such as SMS, OTP and push notification apps don't stop modern cyber threats.

Phishing attacks are on the rise, but not all forms of multi-factor authentication (MFA) are phishing-resistant. Older forms of MFA have been proven to be broken repeatedly as these methods are easily bypassed by attackers using phishing, malware, ransomware, SIM swaps, and attacker-in-the-middle attacks.

> "Any form of MFA is better than just a username and password, but most MFA can still be phished. It didn't take long to realize we needed stronger authentication for all employees that couldn't be phished."

Daniel Jacobson
Director of IT, Datadog

Learn more yubi.co/datadog

Risk of account takeovers
350,000 hijacking attemps

- 0% FIDO security key (YubiKey)
- 10% On-device prompt
- 24% SMS code
- 21% Secondary email
- 50% Phone number

Results of YubiKey deployment versus OTP phone app

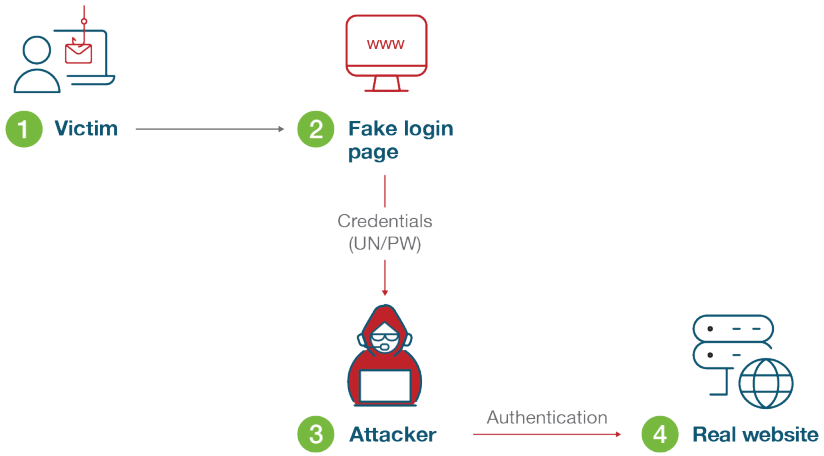
- 0 Account takeovers
- 4x Faster to login
- 92% Support reduction
- 0 Account lockouts
- 50m+ In ROI
- Google Research

Security Keys: Practical Cryptographic Second Factors for the Modern Web

yubico

Let's take a look at an example of a phishing attack that's able to bypass SMS and other software-based MFA.

Anatomy of a phishing attack



Step 1

- In the upper left hand corner we have our victim. Let's say that their name is Joe.
- Joe is sent a fake url by an attacker via email or a social post.

Step 2

- Joe clicks on the link which directs them to a fake website, which looks like the real website.
- On this fake website, Joe enters their credentials (UN/PW) thinking they're logging into the real website.

Step 3

- The attacker through the fake login page gathers credentials.

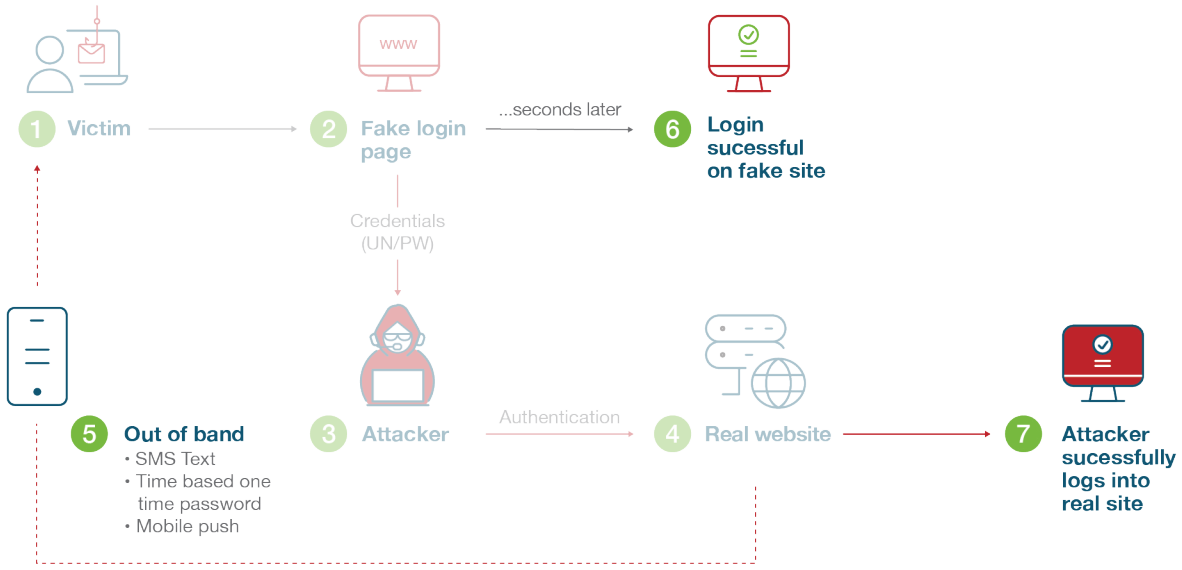
Step 4

- The attacker then submits the credentials to the real client web portal/login page/website (real server).

yubico

Let's take a look at an example of a phishing attack that's able to bypass SMS and other software-based MFA.

Anatomy of a phishing attack



Step 5

- But even if there is 2FA or MFA in place such as SMS, Joe's account can still be breached.
- The real website triggers the SMS code which is sent to Joe's phone.

Step 6

- Seconds later, Joe enters this code into the fake website, and is able to login there.

Step 7

- The attacker now grabs this SMS string that Joe has entered, and enters it into the real website, successfully logging in.
- The attacker can even take this one step further.
- The attacker can update the password on Joe's account and mobile number, locking Joe out completely.

yubico

Why and how modern phishing-resistant MFA stops account takeovers

Modern, phishing-resistant MFA, offered only by FIDO or Smart Card/PIV protocols, have been proven to stop account takeovers in their tracks. Hardware security keys, such as the YubiKey, support multiple authentication protocols including FIDO U2F, FIDO2, and Smart Card/PIV, making them truly phishing-resistant and delivering peace of mind. YubiKeys are purpose-built for security and support device-bound passkeys, ensuring compliance to Authenticator Assurance Level 3 (AAL3) standards.

Wondering why it's worth it to carry one more thing? Don't let the hardware form factor fool you! The YubiKey is a powerful next gen solution that will protect your online digital identity and stop modern cyber threats and account takeovers in their tracks.

fido™ ALLIANCE | simpler stronger authentication

In close collaboration with the Internet thought leaders, Yubico designed and created a set of new authentication capabilities that stop phishing and man-in-the-middle attacks at scale and these capabilities became the foundation of the FIDO/WebAuthn standards.

"A security key is the 'Gold Standard' for authentication, something you physically have. For me, the YubiKey was the only choice. I didn't look elsewhere."

Brent Deterding
CISO, Afni

Learn more yubi.co/afni

How does the magic of the YubiKey work?

Hardware with strong crypto

- Any software downloaded on a computer or phone is vulnerable for malware and hackers.
- Besides smart cards most authentication schemes rely on centralized servers with stored credentials that can be breached.
- With the YubiKey, security is significantly enhanced by storing encryption secrets on a separate secure chip, with no connection to the internet, and using strong public key cryptography where only the public key is stored on the server.

Origin bound keys

- Once a user registers a YubiKey to a service it is bound to that specific URL and the registered credential cannot be used to login to a fake website, making the YubiKey an effective defense against phishing attacks.

User presence

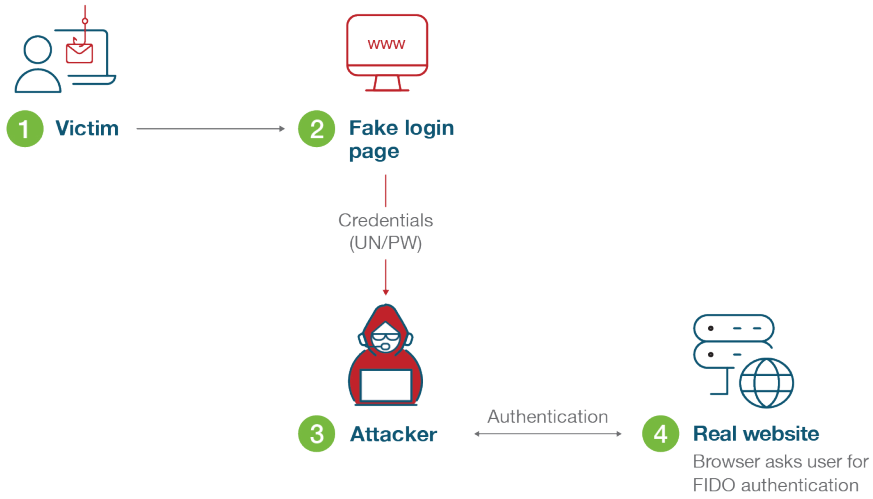
- Many authentication solutions expose vulnerabilities through remote attacks after the device is authenticated.
- The touch sensor on the YubiKey verifies that the user is a real human and the authentication is done with real intent. It also verifies that the authentication is not triggered remotely by an attacker or trojan.

Many apps, no shared secrets

- And finally, YubiKeys authenticate through the FIDO open standard, enabling access to thousands of applications and services, providing high security and privacy at scale, across both your work and personal life.

This is what would have happened if Joe had phishing-resistant MFA...

Stop account takeovers with modern, phishing-resistant MFA



Step 1

- Attacker sends Joe an email pointing to a fake website/login page.

Step 2

- Joe submits credentials (UN/PW).

Step 3

- The attacker through the fake login page gathers credentials and submits it to a real client web portal/login page/website (real server).

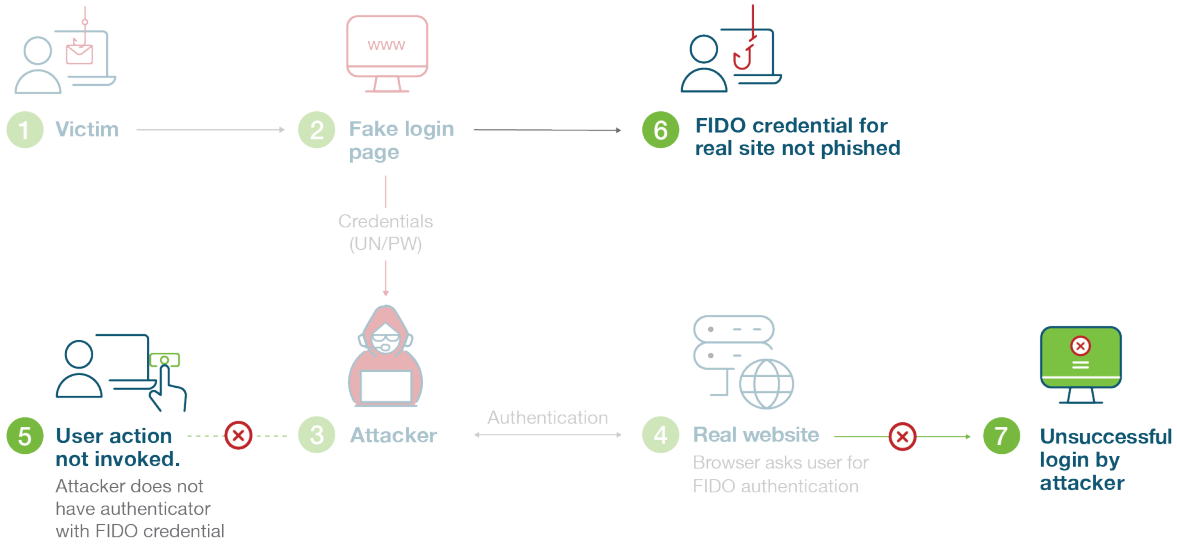
Step 4

- Real client web portal invokes MFA (FIDO)... meaning the browser asks for FIDO authentication.
- Joe needs to use a security key (instead of sending an SMS, or use a mobile authentication app).

yubico

This is what would have happened if Joe had phishing-resistant MFA...

Stop account takeovers with modern, phishing-resistant MFA



Step 5

- Joe inserts YubiKey (or uses some close proximity/inline method... NFC, BLE, USB).

Step 6

- Real website and FIDO security key has a secret handshake so when a user inserts FIDO security key, the security key understands that a fake website is asking for info.
- Does not allow the user/ authentication process to continue and the phishing attack is thwarted!
- FIDO authentication fails on real website because there is a trusted relationship between FIDO key and the real website.

Step 7

- The attacker is unable to login to Joe's account and their account remains secure.

yubico

The bottomline: Even if the user is fooled, **the YubiKey is never fooled!**

How to get started on your journey to phishing-resistant MFA at scale

Plan

Ensure readiness by clarifying use case cases and user populations

Validate

Confirm the process with a small group of users before broader rollout

Integrate

Ensure key apps and services are YubiKey-ready

Launch

Distribute keys to users with turnkey delivery services or channel partners

Adopt

Drive adoption with best practice training and support

Measure

Report on security and business value impact

Think adopting hardware security keys is hard? **Think again, Yubico has you covered.** Modern enterprises are pivoting to security as a subscription across the globe. With cost efficiencies, predictable spending, flexible YubiKey upgrades, and turnkey delivery to corporate and residential addresses YubiEnterprise Subscription can help you accelerate your journey towards modern authentication and rapid protection for all your users.

yubico

Contact us
yubi.co/contact

Learn more
yubi.co/bpg-mfa

About Yubico

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, a hardware security key that is the gold standard in phishing-resistant multi-factor authentication (MFA). Yubico's solutions offer organizations and users deployment expertise and operational flexibility as YubiKeys work across hundreds of consumer and enterprise applications and services.

Yubico is a creator and core contributor to the FIDO2/passkey, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering modern, hardware-based passkey authentication security at scale to customers in over 160 countries.

For more information, please visit: www.yubico.com.

yubico