THE TREND OF AUTHENTICATION

FIDO2 + Biometric Security Key = The Solid Passwordless Option

AUTHENTREND

JUNE 2021

A small leak will sink a great ship.

— Benjamin Franklin

Passwords Aren’t Enough to Protect Your Data

AUTHENTREND

JUNE 2021

54% of consumers use 5 or fewer passwords for all of their accounts.

TeleSign Consumer Account Security Report

1. 123456
2. 123456789
3. password
4. qwerty
5. iloveu

NordPass's most common passwords list

80%

of account vulnerabilities were due to weak or stolen passwords

-Verizon 2019 Data Breach Investigations Report

On average, it costs an enterprise $70 for a single password reset.

- Forrester Research, January 2018

AUTHENTREND

JUNE 2021

Set up 2-factor authentication?

AUTHENTREND

JUNE 2021

Adopting either 2nd-factor authentication can improve security,

BUT...

SMS

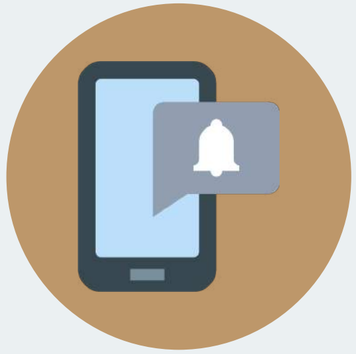
- **Coverage issues**
- **Delay**
- **Phishable**

Backup Codes

- **Saving required**
- **Phishable**

OTP/ TOTP

- **Shared Secret Key**
- **Phishable**



Mobile Push

- **Internet required**
- **Phishable**

Security Key

Phishing-resistant

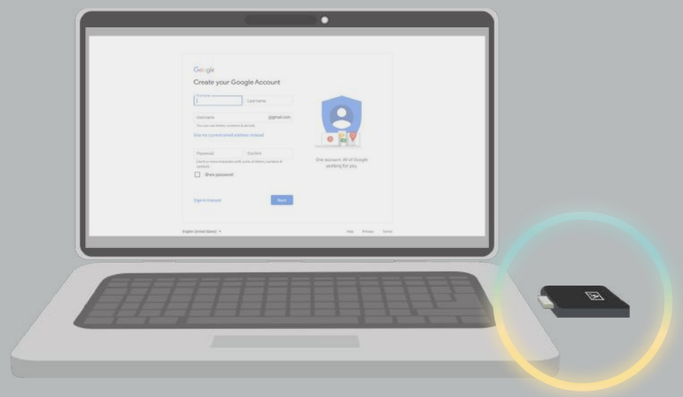
Level of Assurance

Time to authenticate

- Google Cloud

Google has not had any of its 85,000+ employees phished on their work-related accounts since 2017, when it began requiring all employees to use physical **Security Keys** in place of passwords and one-time codes.

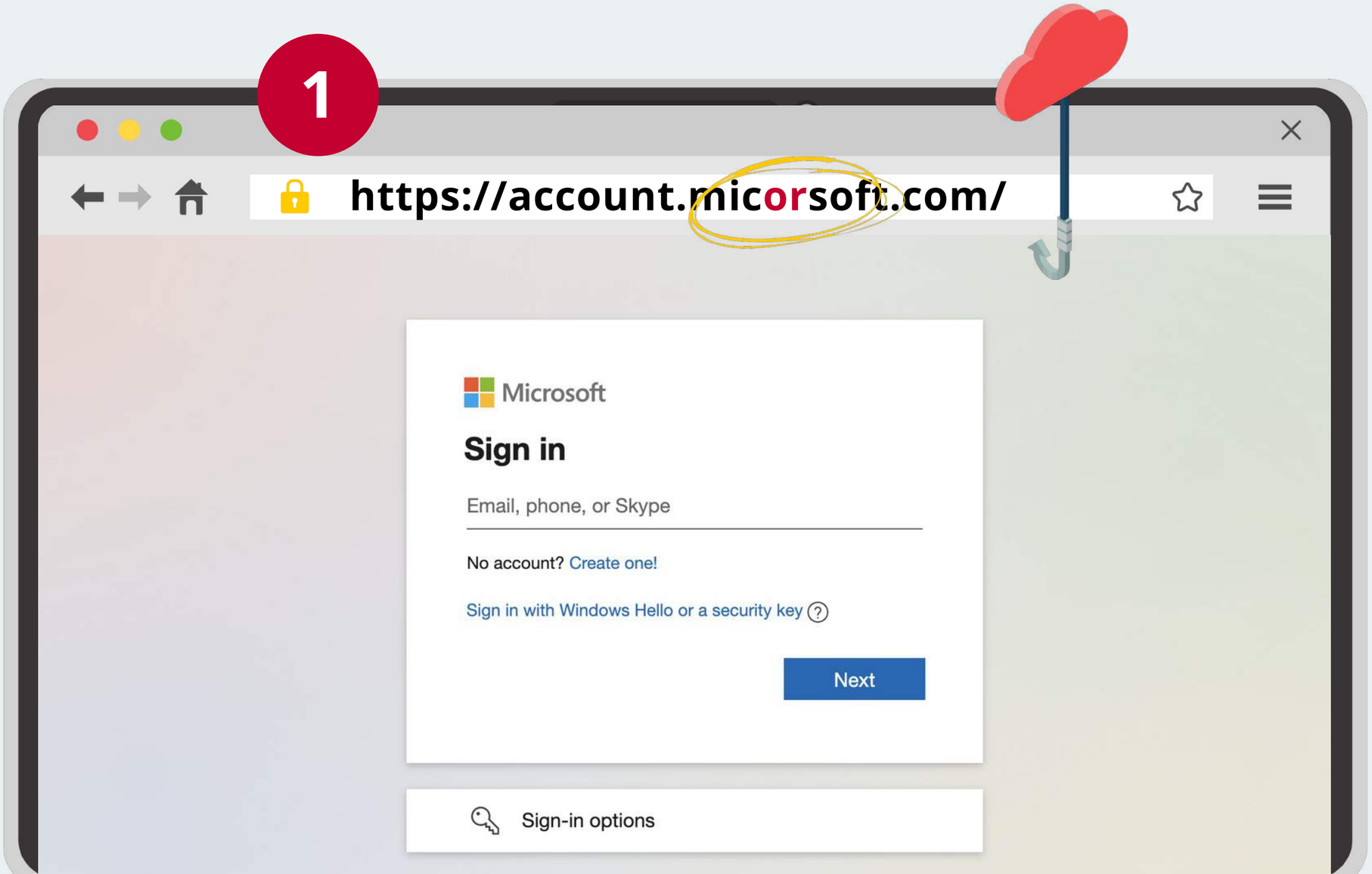
- KrebsOnSecurity



AUTHENTREND

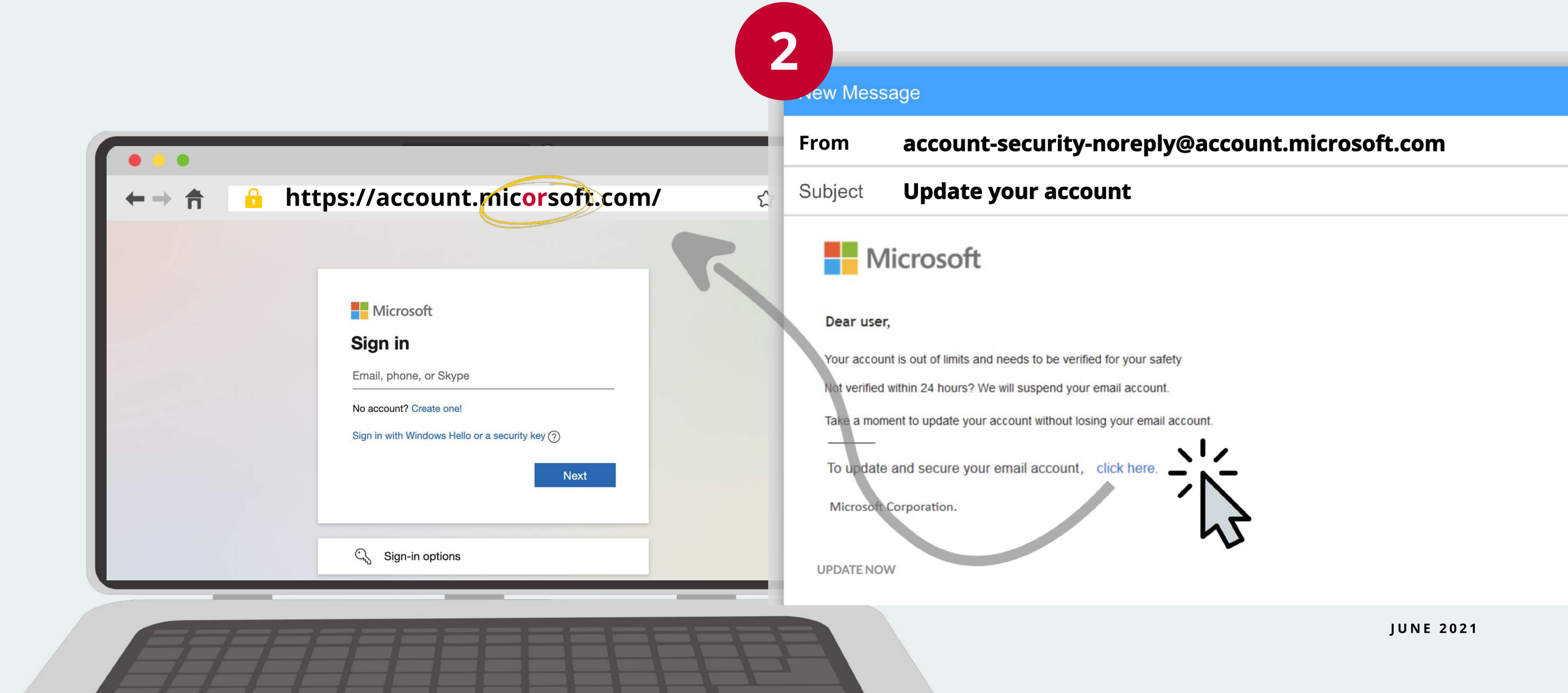
JUNE 2021

Phishing Attacks are Easier than you think!

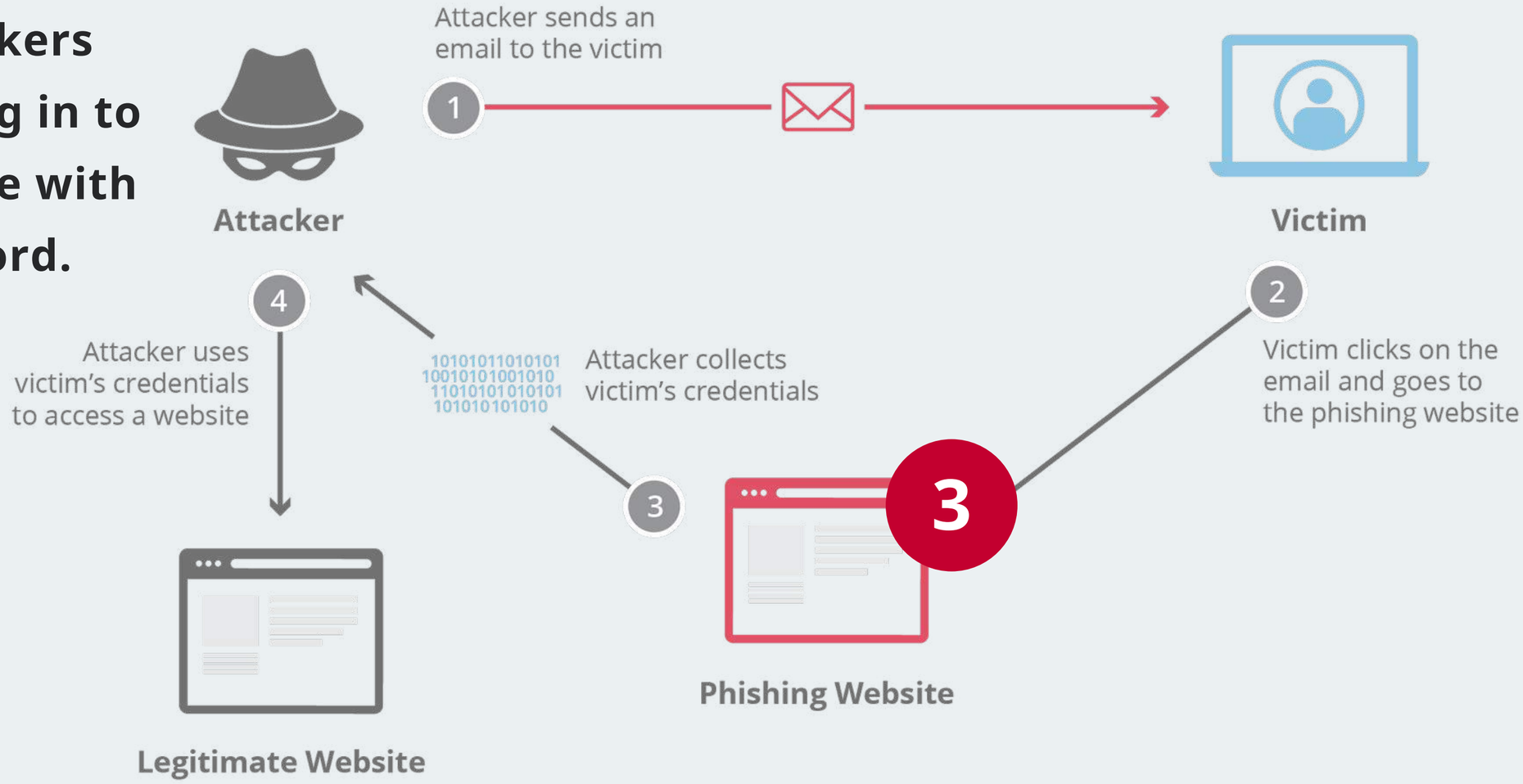


JUNE 2021

Phishing Attacks are Easier than you think!

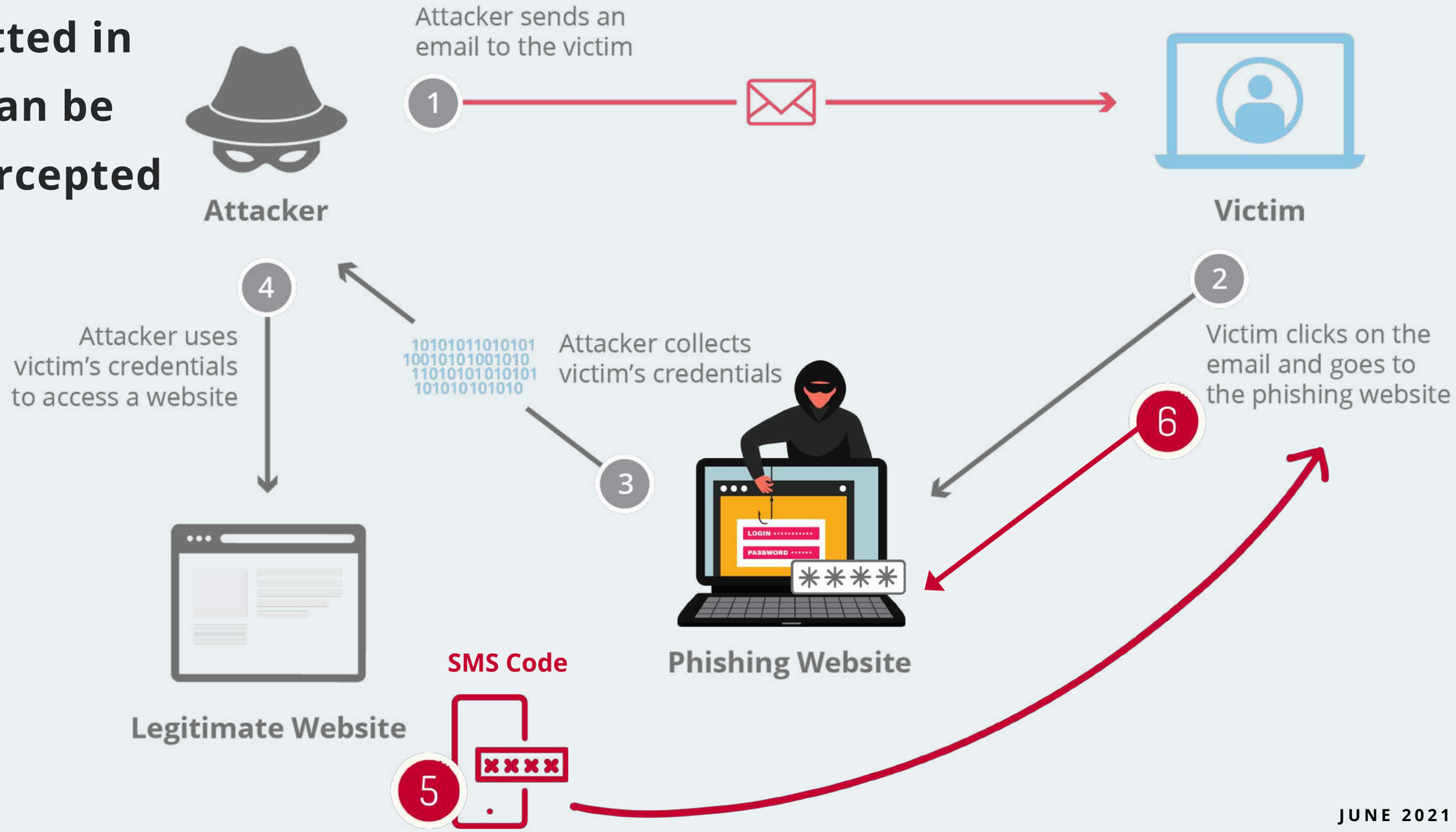


Once you enter your credential on the fake site, attackers immediately log in to the real website with your ID/Password.

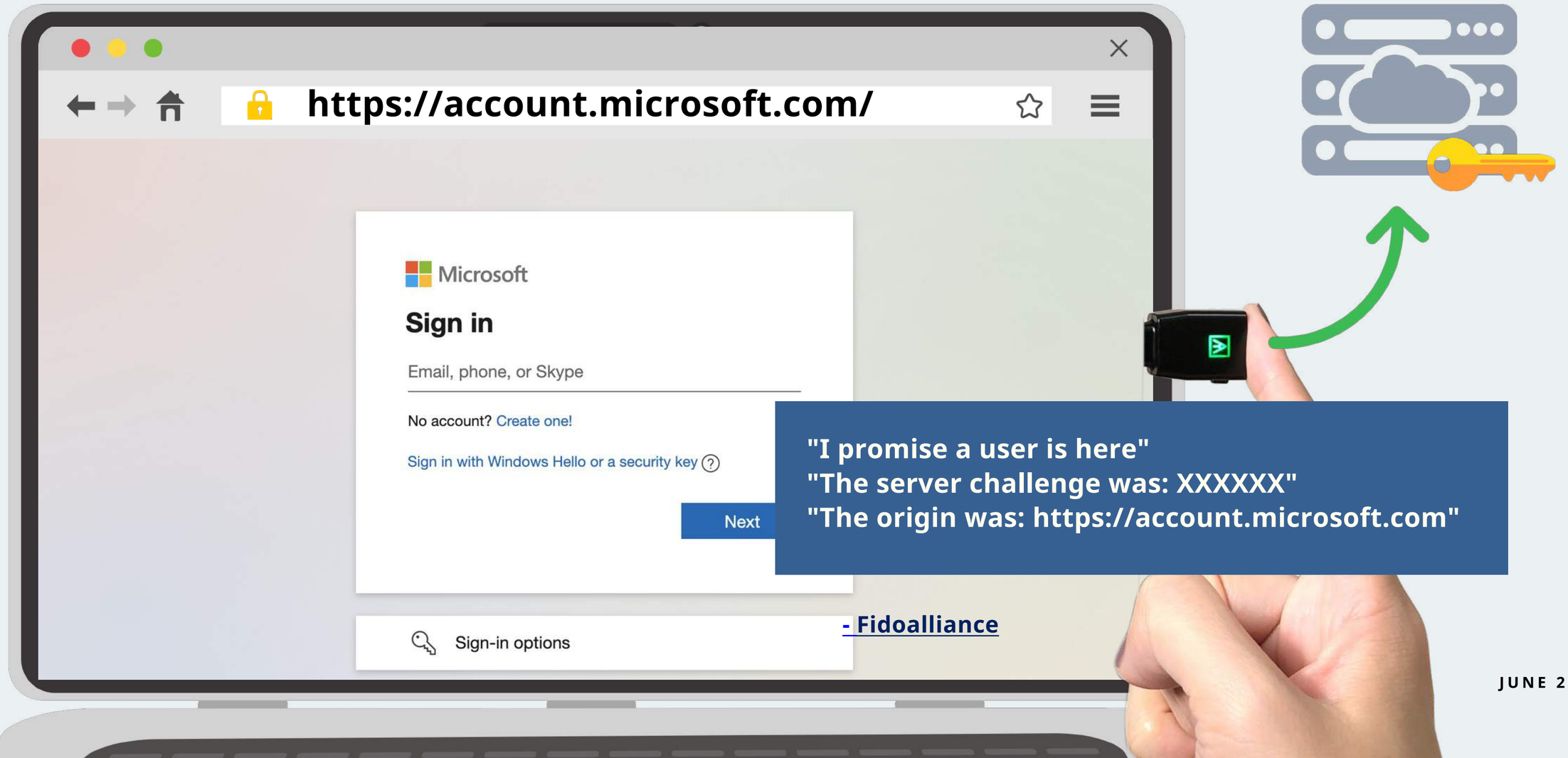


What about SMS Code?

SMS is transmitted in cleartext and can be also easily intercepted by attackers

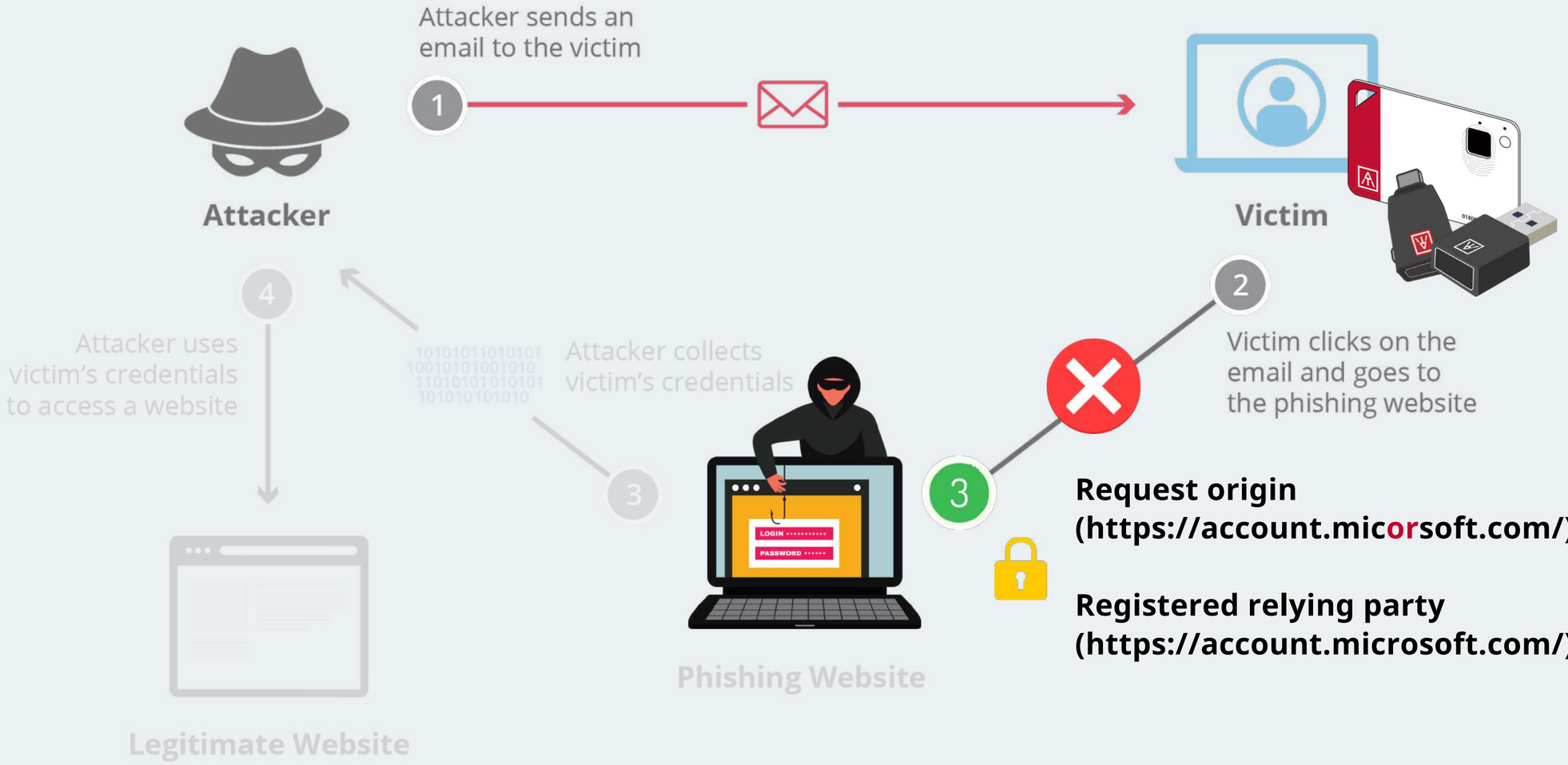


What About A Physical Security Key?



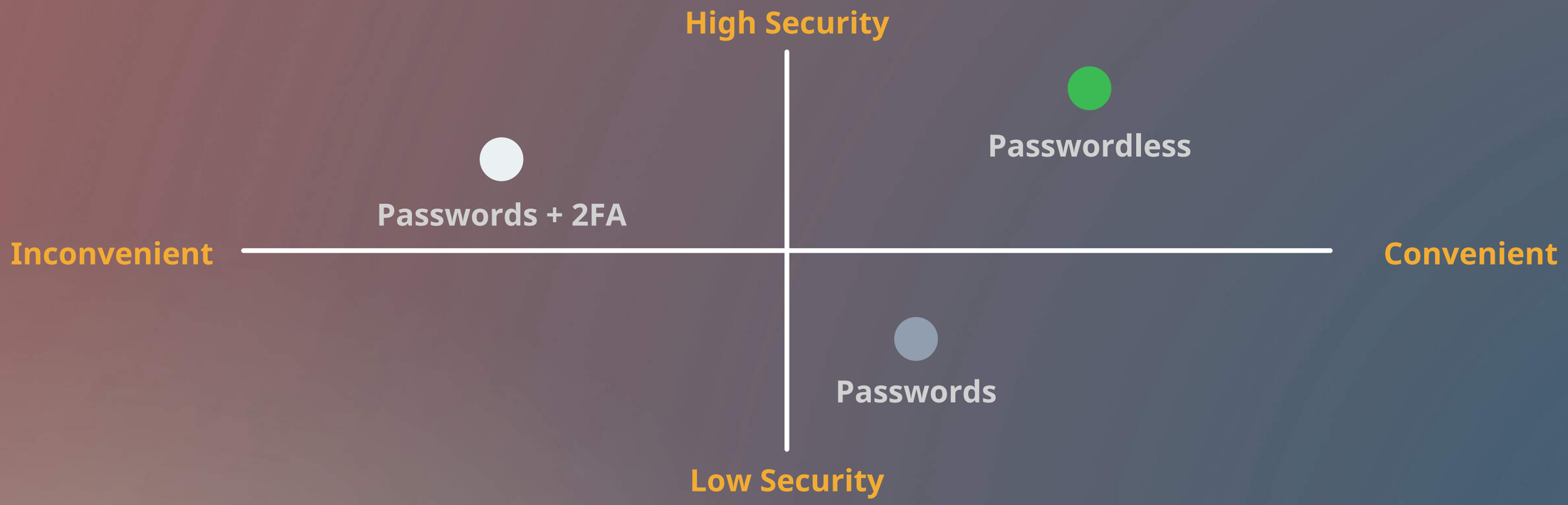
[- Fidoalliance]

How Security Key Prevents Phishing Attacks



It's not enough...

2FA gives us stronger, safer password protection for your accounts, but it's a waste of time.



That's where FIDO2 and WebAuthn play a role.

A better standard offers an extra layer of security
by allowing users to authenticate their devices without using a password.

- Microsoft

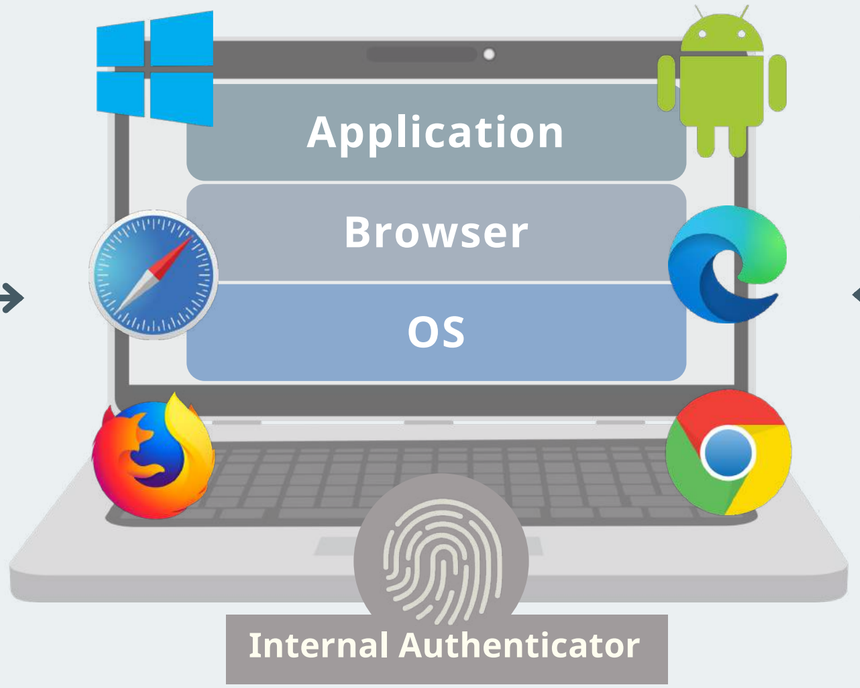
FIDO2: The New Passwordless Standard

External Authenticator

CTAP

fido™

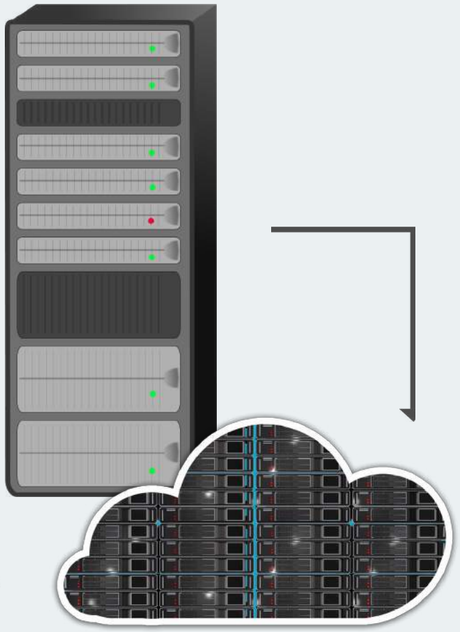
Platform/Client



WebAuthn

W3C

Relying Party (RP)



FIDO Server

Metadata

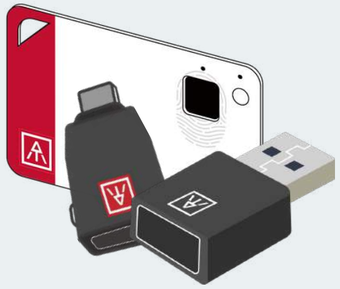
AUTHENTREND

- Fidoalliance

JUNE 2021

+ Biometric = Truly Passwordless

Fingerprint-enable Security Key



PIN-only Security Key

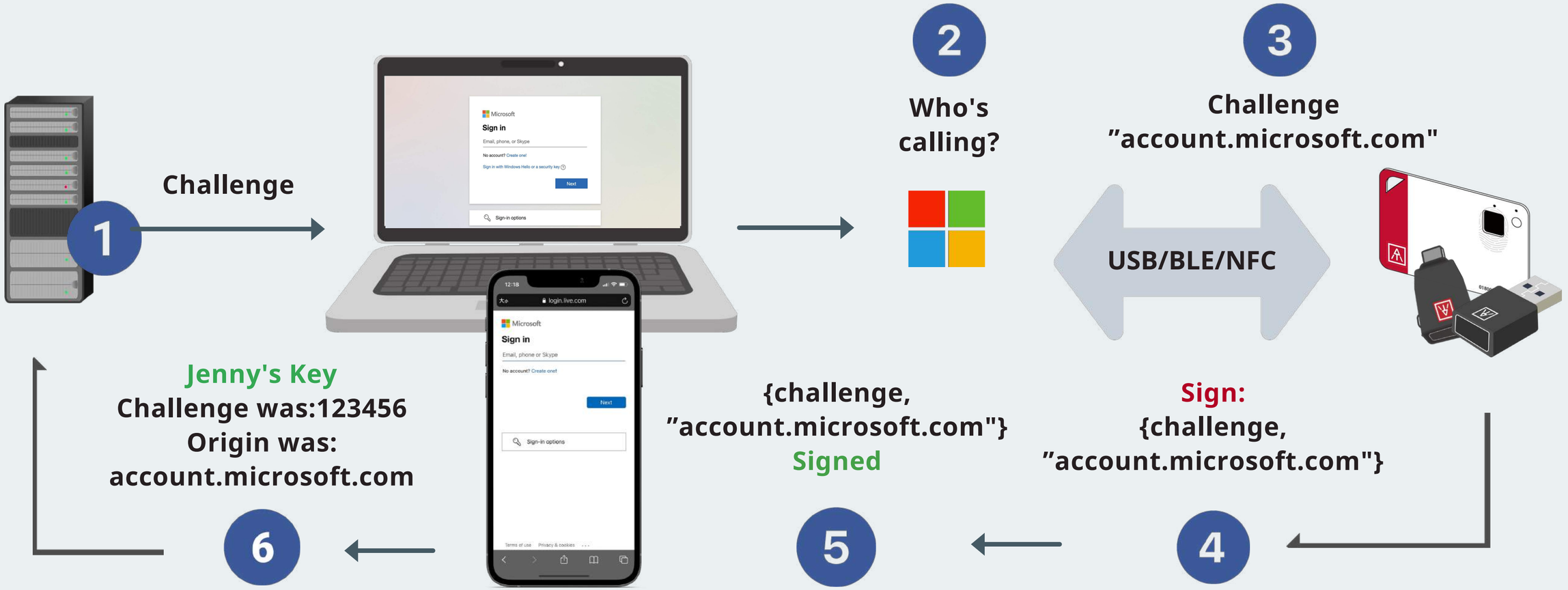
Fingerprint-enable Security Key		PIN-only Security Key
Truly Passwordless	User Verification	PIN + Touch
< 1s	Time to Authenticate	> 3s (Depends on PIN length)
Using just a fingerprint match	User Experience	A strong PIN is difficult to remember
No one can guess the fingerprint The enrolled fingerprint template is stored and biometrically matched in a specialized secure element to protect it from digital and physical attacks.	Security Consideration	**PIN is still guessable!** • It's risky to type the PIN on an unknown device. • Losing the key by accident will pose a security risk. • Easily profiled when entering PIN codes in public places.

Individual User Journey

AUTHENTREND

JUNE 2021

How FIDO2 Security Key Works?



- Google

Where people can use the FIDO2 ATKey

For Business

AUTHENTREND

JUNE 2021

Passwordless+Biometric MFA Options on Azure

User's Device

Windows 10
Pro laptop or desktop

ANY DEVICE has a web browser

(BYO or enterprise Windows OS, mobile devices, virtual desktops, thin clients, etc.)

Passwordless Authentication

Device Bound:
PC / Desktop

Biometric Match-on-device

Device Bound:
Microsoft Authenticator App

Biometric Match-on-device

CROSS-DEVICE
+ FIDO2 Security Key

Biometric Match-on-chip

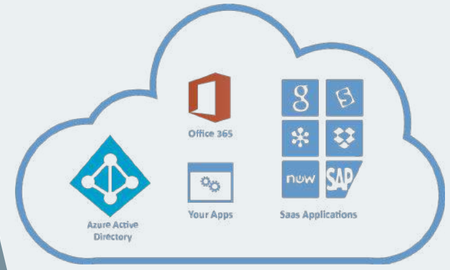
Identity Provider

Microsoft Active Directory

Azure AD Connect

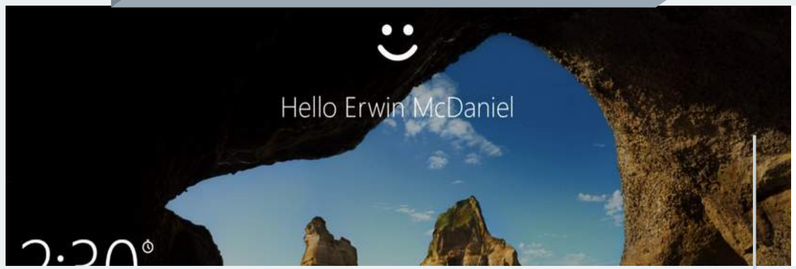
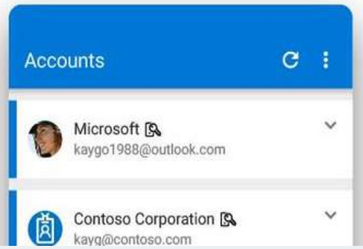
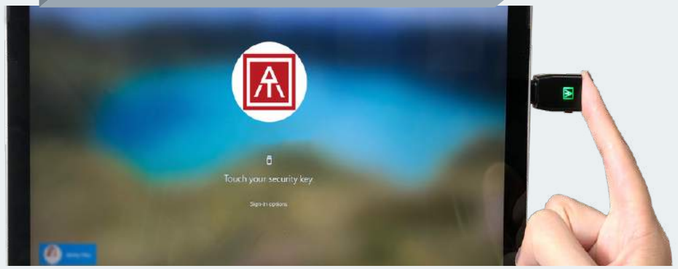
Microsoft Azure Active Directory

Access Application



Anything protected with Azure AD-
Physical devices,
SaaS web apps,
virtual apps,
virtual desktops, etc.

Comparing Microsoft Passwordless Methods

	Windows Hello for Business	Microsoft Authenticator	Fingerprint Security Key
			
Pre-Pequisite	Windows 10, version 1511 or later Azure Active Directory	Microsoft Authenticator App Phone (iOS and Android 6.0 or above devices)	Windows 10, version 1809 or later Azure Active Directory
Security Assurance	Device Bound: Anyone with the PIN of the device can log in directly	Out of Band: Fraud is still possible from remote to control the user	**Cross-device : Only near-field authentication between key and devices**
Device Requirements /Applicability	• Relies on devices with built-in Trusted Platform Module (TPM) • Windows Hello for Business compatible hardware, and **only works with Windows 10-based devices.**	• Can be used to Azure AD-join a Windows 10-based devices (since Windows 10 1909), non-Windows devices (Mac, Linux, Android, iOS, web browser, etc) and non-managed devices (aka BYOD). • **A device can only be registered in a single tenant.**	• **Places with poor network communication** • **Non-managed Windows devices or not place any company-related information on their personal devices.** • **Works with all major Operating Systems.**
Restrictions	• The maximum number of supported Windows Hello for Business enrollments on a single Windows device is **10**. • Needs to be enrolled for each Windows 10-based device individually.	• **Must back up the Authenticator App when switching a new phone device** or no longer work on the new device. • Requires colleagues to use their personal device for corporate purposes.	• Microsoft-validated security key, Such as the entire series of ATKey security keys. • Require a logistical process to deploy.

FIDO2 Security Key Scenarios

HIGH-TECH MANUFACTURERS

For places where mobiles are not feasible or where Internet connectivity is poor

PRIVILEGED ACCESS

Safeguard privileged user accounts and lower the risk of attacks

REMOTE ACCESS

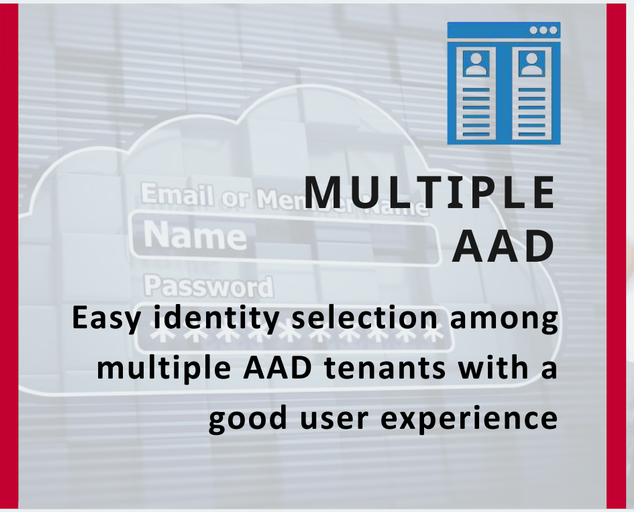
Securely work anywhere and help IT leaders manage workforces more securely

THIRD-PARTY CONTROL

Safely work with outside experts, consultants, and other third-party vendor

SHARED WORKSPACE

In an environment with shared devices or kiosk, users can sign in more quickly



MULTIPLE AAD

Easy identity selection among multiple AAD tenants with a good user experience

OFFICE EMPLOYEES

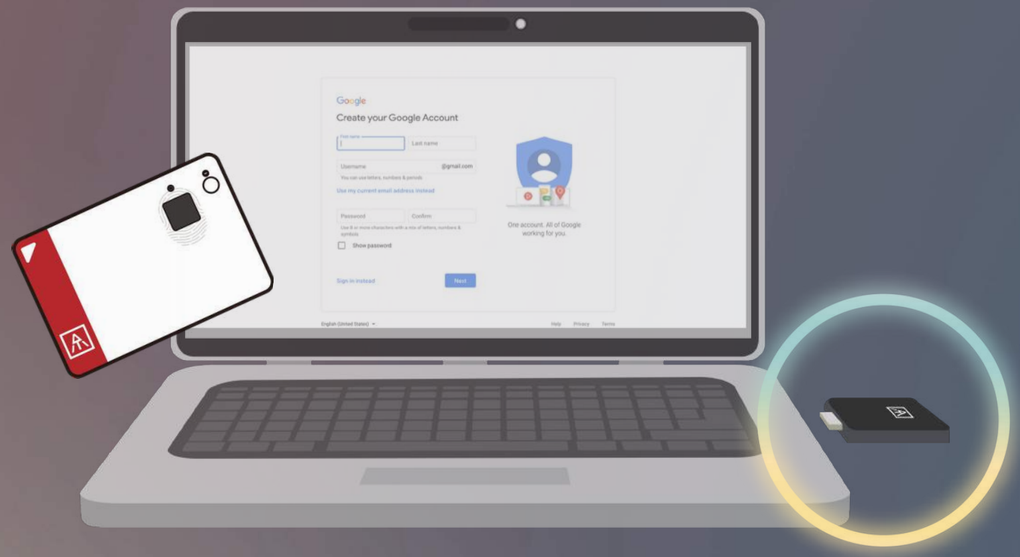
Combined with office scenarios, one security key or card for multiple uses

HIGHLY SECURE SENSITIVE ACCESS

Remotely have simple, highly secure access to the most sensitive data

THE TREND OF AUTHENTICATION

Raise your Security Standards Today with ATKey



www.authentrend.com

AUTHENTREND

JUNE 2021