MEETUP URK

FIDO2
&
Azure Active Directory

Gepresenteerd door:

Jan Bakker

MEETUP URK

https://janbakker.tech

https://www.linkedin.com/in/jan-bakker/

https://twitter.com/janbakker_

Jan Bakker

Azure Content Hero

Agenda

- The problem with passwords
- What is FIDO?
- Passwordless, why is it better?
- Usecases
- FIDO2 security keys
- Demo 1 - How to set it up in your tenant?
- Demo 2 - End-user experience
- A gift from FEITIAN
- Q&A

MEETUP URK

THE PROBLEM WITH PASSWORDS

MEETUP URK

Fernando Corbató


Welcome02
Summer2020
password#
1234567

90+


73%

Shared secret

Beste J.,

Bij VakantieVeilingen doen we er alles aan om het bieden zo leuk en veilig mogelijk te maken. Uit onze systemen is helaas naar voren gekomen dat er mogelijk door iemand anders is geprobeerd in te loggen op jouw account.

Bij deze inlogpogingen wordt gebruikt gemaakt van zogenaamde “credential stuffing”. Hierbij misbruiken derden elders onbevoegd verkregen inloggegevens en proberen daarmee in te loggen. Veel mensen gebruiken altijd dezelfde combinatie van e-mailadres en wachtwoord voor verschillende sites. Als een onbevoegde derde dan op één of andere manier deze wachtwoorden in zijn bezit krijgt, dan kunnen ze proberen of ze toevallig op een andere site met dezelfde gegevens kunnen inloggen en dat is bij jouw account ook gebeurd.

Het is daarom helaas mogelijk dat de inlogpoging bij VakantieVeilingen gelukt is en dat informatie over jou, waaronder gegevens die je hebt opgegeven in je account, toegankelijk zijn geweest voor iemand anders dan jezelf.

Het gaat om de door jou ingevulde voor- en achternaam, adresgegevens, telefoonnummer, geboortedatum, e-mailadres en als je die bij ons hebt opgegeven ook je IBAN. Er zijn vanuit jouw account geen verdachte transacties op ons platform waargenomen.

Om er zeker van te zijn dat niemand meer bij je gegevens kan, hebben we je wachtwoord gereset. Je moet dan voordat je weer kunt inloggen, eerst een nieuw wachtwoord kiezen. Dat kan via onderstaande link. Let erop dat je kiest voor een uniek en sterk wachtwoord dat je niet gebruikt op andere websites. Daarnaast blijven wij continu andere technische en organisatorische maatregelen nemen om de ongeautoriseerde inlogpogingen van derden tegen te houden.

Je wachtwoord wijzigen

Wij hebben dit incident gemeld bij de Autoriteit Persoonsgegevens. Voor eventuele verdere vragen kun je het beste mailen naar wachtwoordreset@emesa.nl of contact opnemen met de klantenservice.

Wees de komende tijd extra alert op fraude en identiteitsdiefstal. Kijk voor meer info op https://www.fraudehelpdesk.nl.

Bedankt voor je begrip. We zien je graag weer terug op onze website!


MY PASSWORD
12345678

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address

pwned?

Generate secure, unique passwords for every account

Learn more at 1Password.com

Why 1Password?

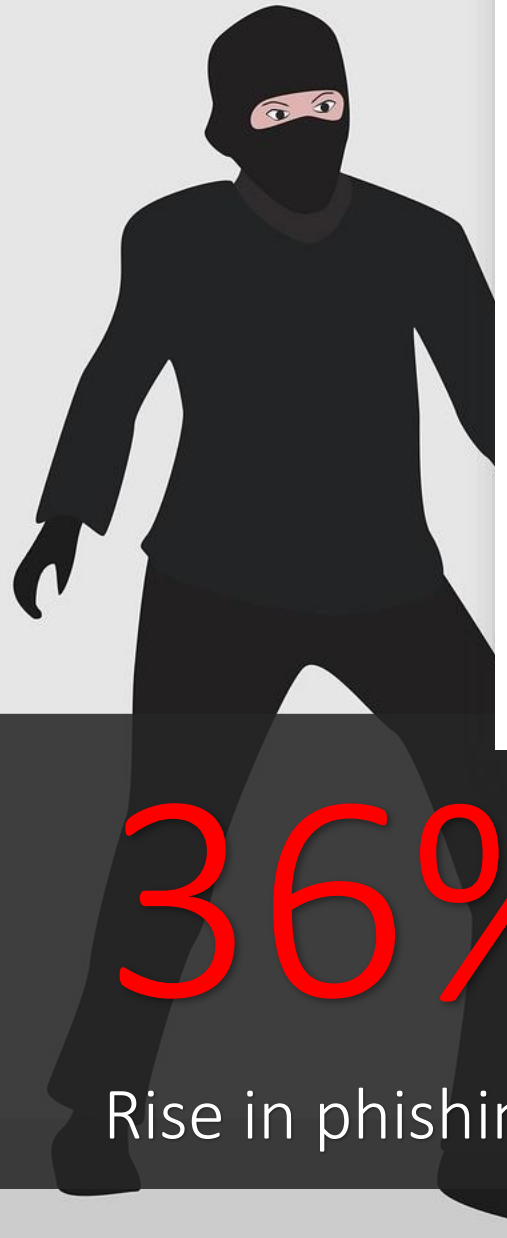
81%


€60

2.3B

2017


ALEXANDER
ZOEY
CAMERON
LAKE
MATTHEW
RILEY
NATHAN
BENJAMIN
CLAIRE
BRYAN
BROOKE
ISABELLA
GIOVANNI
OLIVIA
ETHAN
AVA
WYATT
COOPER
NOAH
HENRY
KEVIN
TAYLOR
EMILY
LUCAS
LIAM
CONNOR
EMMA
CHRISTOPHER
JORDAN
BRANDON
ANNA
JACKSON
KHLOE
ANGEL
ABIGAIL
MICHAEL
LUKE
JACOB
OLIVER
AYDEN
CARLOS
JOSIAH
KAYLEE
CARTER
MACKENZIE



Twitter Support @TwitterSupport · Jul 31, 2020

Replying to @TwitterSupport

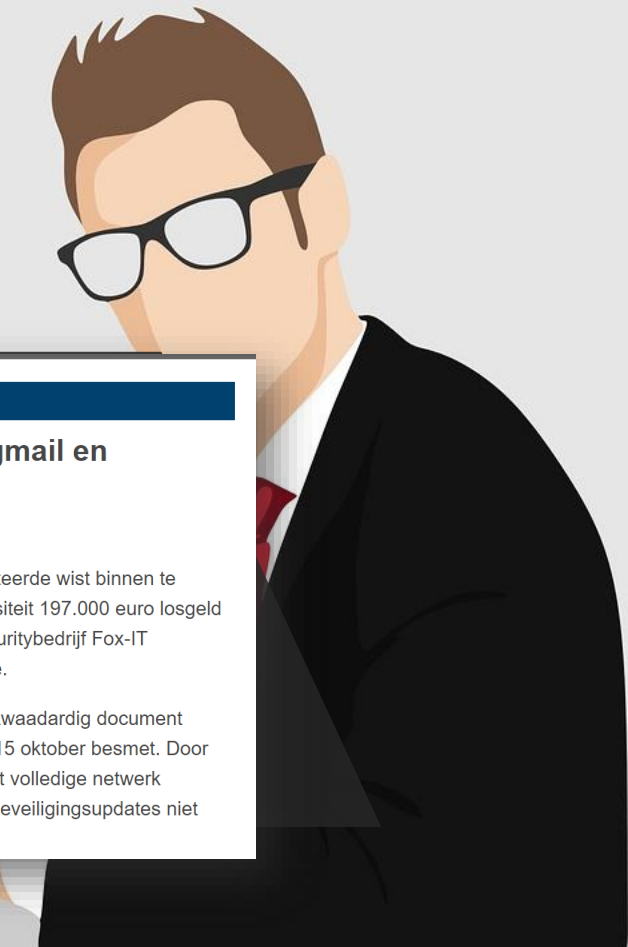
The attack on July 15, 2020, targeted a small number of employees through a phone spear phishing attack. This attack relied on a significant and concerted attempt to mislead certain employees and exploit human vulnerabilities to gain access to our internal systems.

Twitter Support
@TwitterSupport

By obtaining employee credentials, they were able to target specific employees who had access to our account support tools. They then targeted 130 Twitter accounts - Tweeting from 45, accessing the DM inbox of 36, and downloading the Twitter Data of 7.

2:49 AM · Jul 31, 2020

416 233 people are Tweeting about this



Nieuws

Universiteit Maastricht werd besmet via phishingmail en verouderde software

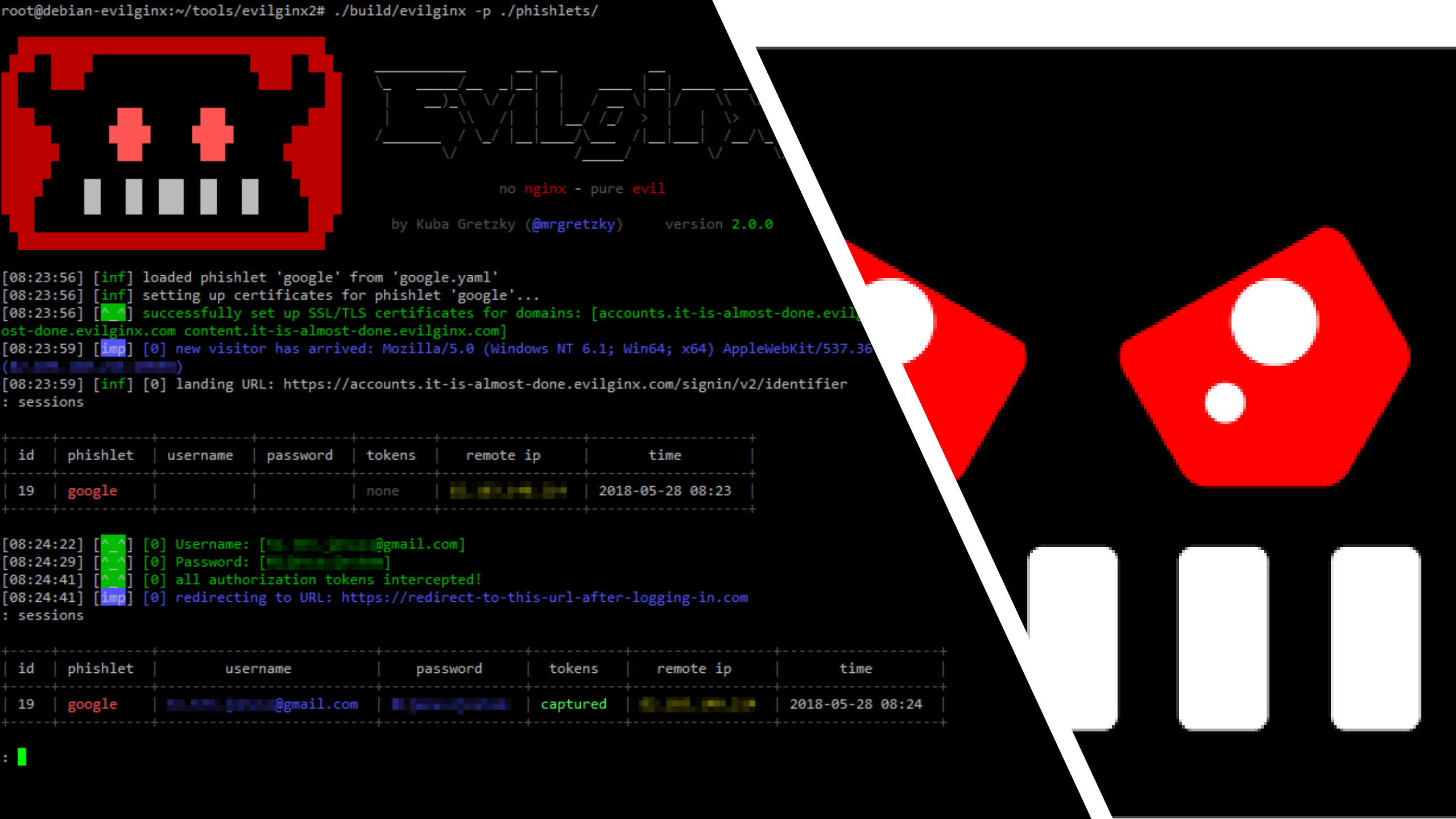
woensdag 5 februari 2020, 14:34 door **Redactie**, 66 **reacties**
Laatst bijgewerkt: 05-02-2020, 15:59

De aanvaller die systemen van de Universiteit Maastricht met ransomware infecteerde wist binnen te komen via een phishingmail en verouderde software. Daarnaast heeft de universiteit 197.000 euro losgeld betaald dat de aanvaller vroeg voor het ontsleutelen van bestanden. Dat lieten de universiteit en securitybedrijf Fox-IT vandaag weten tijdens een **symposium** over de ransomware-aanval dat de universiteit organiseerde.

De aanvaller verstuurde op 15 en 16 oktober e-mails met het onderwerp "Documents" die naar een kwaadardig document linkten. Via dit document, waarvan hieronder een screenshot is te zien, werd het eerste systeem op 15 oktober besmet. Door een ongepatcht besturingssysteem op twee servers kon de aanvaller vervolgens op 21 november het volledige netwerk compromitteren en zich lateraal door het netwerk bewegen. Op deze twee servers waren bepaalde beveiligingsupdates niet doorgevoerd. Om welke verouderd besturingssysteem het ging is niet gemeld.

36%

Rise in phishing attacks in 201



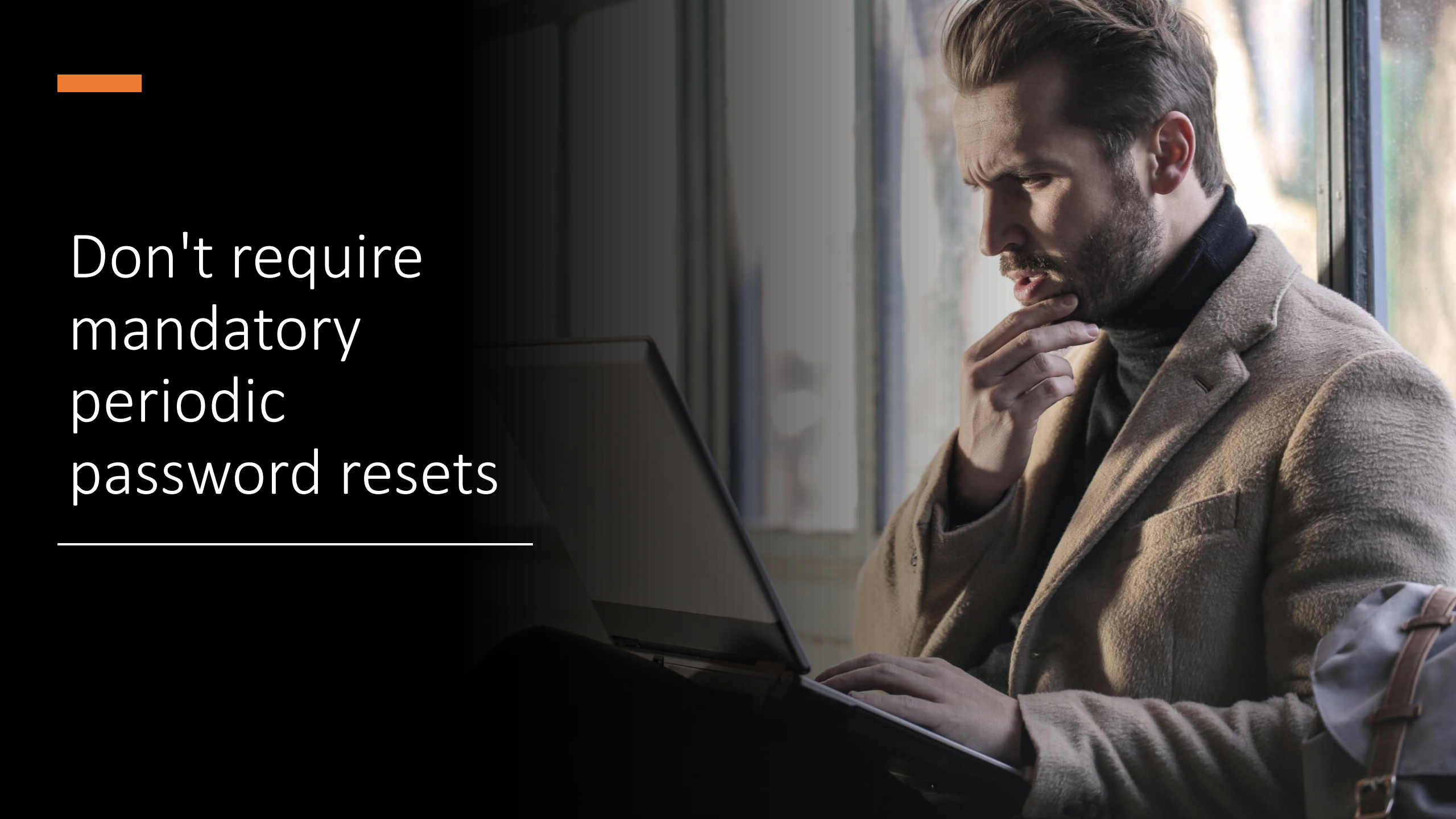
```
root@debian-evilginx:~/tools/evilginx2# ./build/evilginx -p ./phishlets/

                                               no nginx - pure evil

                                    by Kuba Gretzky (@mrgretzky)     version 2.0.0

[08:23:56] [inf] loaded phishlet 'google' from 'google.yaml'
[08:23:56] [inf] setting up certificates for phishlet 'google'...
[08:23:56] [^_^] successfully set up SSL/TLS certificates for domains: [accounts.it-is-almost-done.evil
ost-done.evilginx.com content.it-is-almost-done.evilginx.com]
[08:23:59] [imp] [0] new visitor has arrived: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
([redacted])
[08:23:59] [inf] [0] landing URL: https://accounts.it-is-almost-done.evilginx.com/signin/v2/identifier
: sessions

+-----+-----------+----------+----------+--------+-----------------+------------------+
| id  | phishlet  | username | password | tokens |    remote ip    |       time       |
+-----+-----------+----------+----------+--------+-----------------+------------------+
| 19  | google    |          |          | none   | [redacted]      | 2018-05-28 08:23 |
+-----+-----------+----------+----------+--------+-----------------+------------------+

[08:24:22] [^_^] [0] Username: [[redacted]@gmail.com]
[08:24:29] [^_^] [0] Password: [[redacted]]
[08:24:41] [^_^] [0] all authorization tokens intercepted!
[08:24:41] [imp] [0] redirecting to URL: https://redirect-to-this-url-after-logging-in.com
: sessions

+-----+-----------+-------------------------+----------------+----------+-----------------+------------------+
| id  | phishlet  |         username        |    password    | tokens   |    remote ip    |       time       |
+-----+-----------+-------------------------+----------------+----------+-----------------+------------------+
| 19  | google    | [redacted]@gmail.com    | [redacted]     | captured | [redacted]      | 2018-05-28 08:24 |
+-----+-----------+-------------------------+----------------+----------+-----------------+------------------+

:
```

Ease The Pain

Use **Passphrases** Instead of Passwords

Turn on **MFA**

Don't require mandatory periodic password resets



Educate & test your users

Easy on password complexity requirements

A = @
S = $
L = 1
E = 3

Þassword1!

Ban common passwords

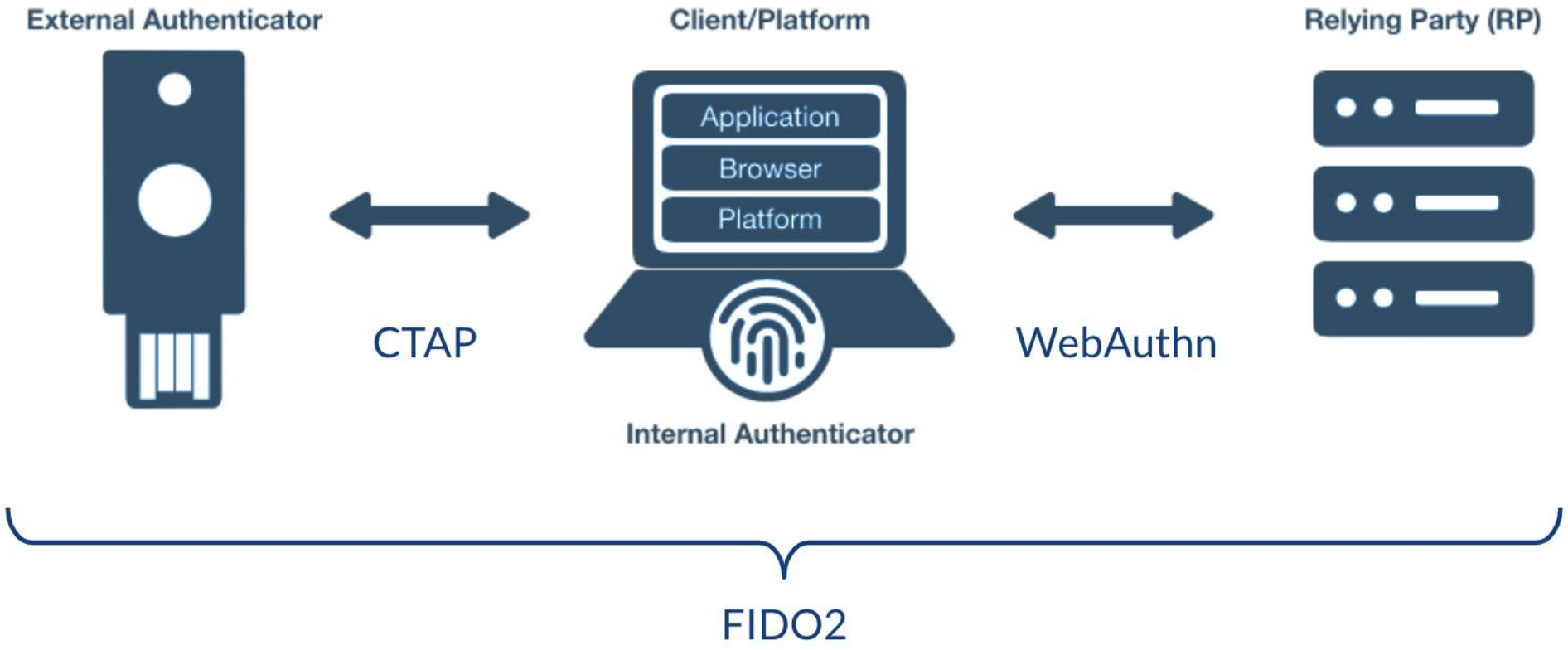
WHAT IS FIDO?

fido™ ALLIANCE

simpler
stronger
authentication

*Founded in **2012***

FIDO2: WebAuthn & CTAP



MEETUP URK

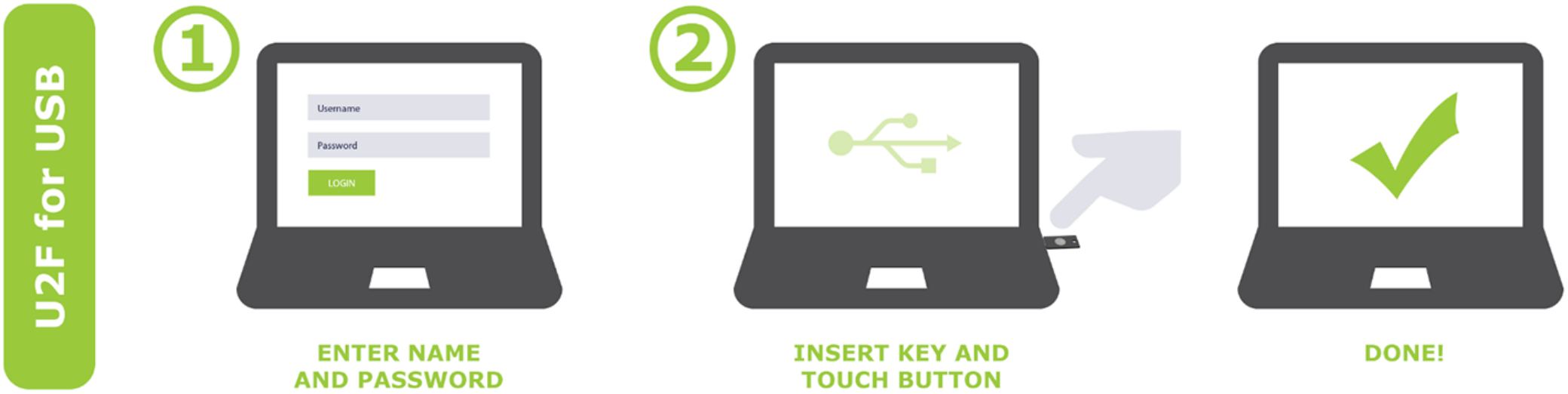
PUBLIC KEY CRYPTOGRAPHY

3 User unlocks private key when logging in

1 Registration generates a private key and public key

2 Public key is entered for the web service

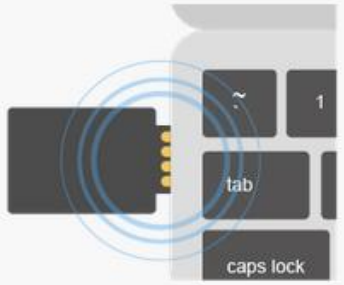
MEETUP URK



Universal 2nd Factor (U2F)

Google

2-Step Verification



Insert your Security Key

Use a verification code instead

Don't ask for my Security Key again on this computer

aws

Sign in using MFA

Your account is secured by multi-factor authentication (MFA) using U2F Security Key. Learn more

Insert your U2F security key into your USB port, and then tap the button or gold disk.

Waiting for security key

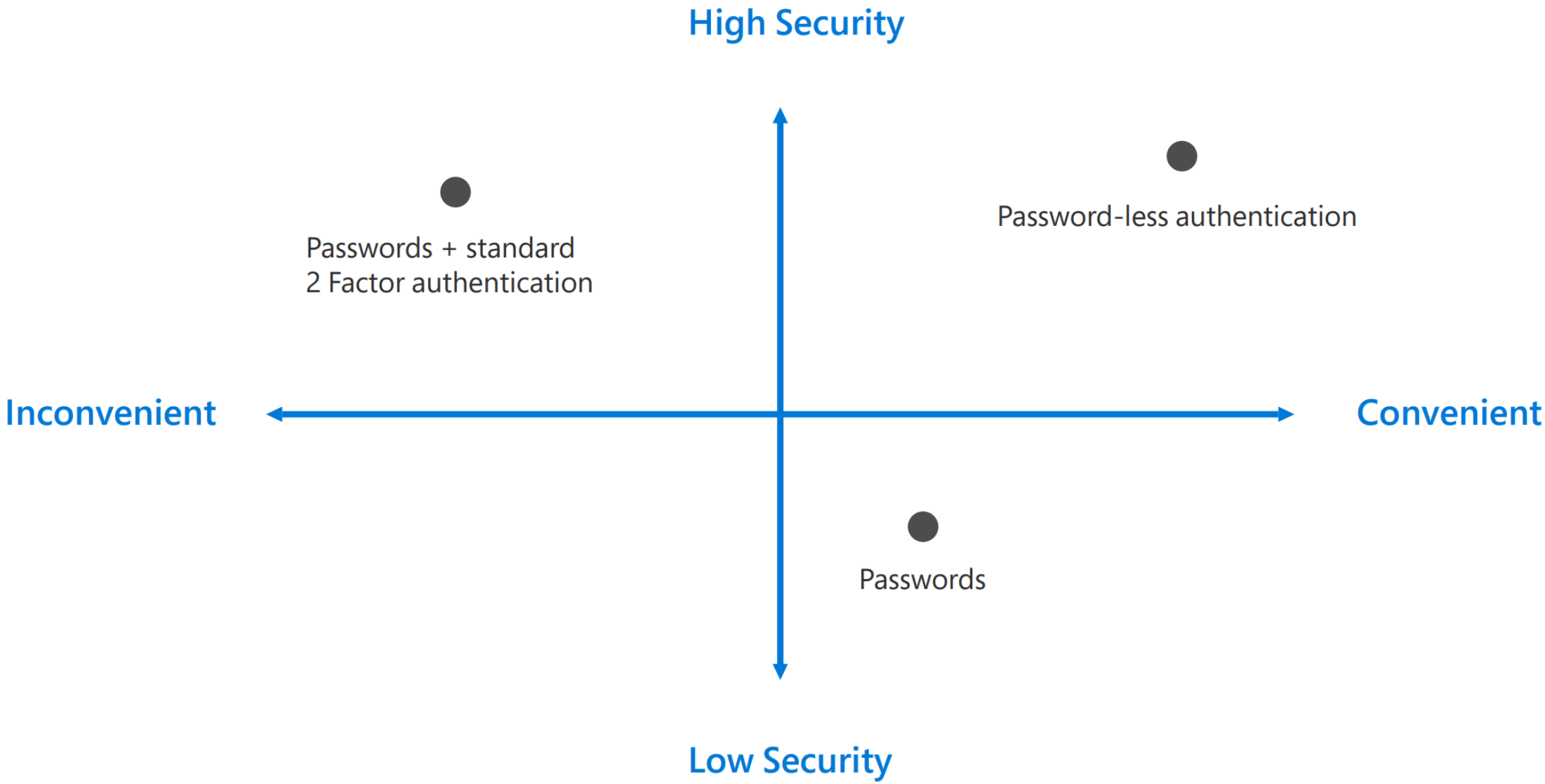
Troubleshoot MFA

Cancel

Universal 2nd Factor (U2F)

PASSWORDLESS

2015


High Security
Password-less authentication
Passwords + standard
2 Factor authentication
Inconvenient
Convenient
Passwords
Low Security

What is passwordless?

High security, convenient methods of strong authentication

Windows Hello

Microsoft Authenticator

FIDO2 Security Keys

No need to create passwords
No need to remember passwords
No need to change passwords
No need to reset passwords
No need to protect passwords

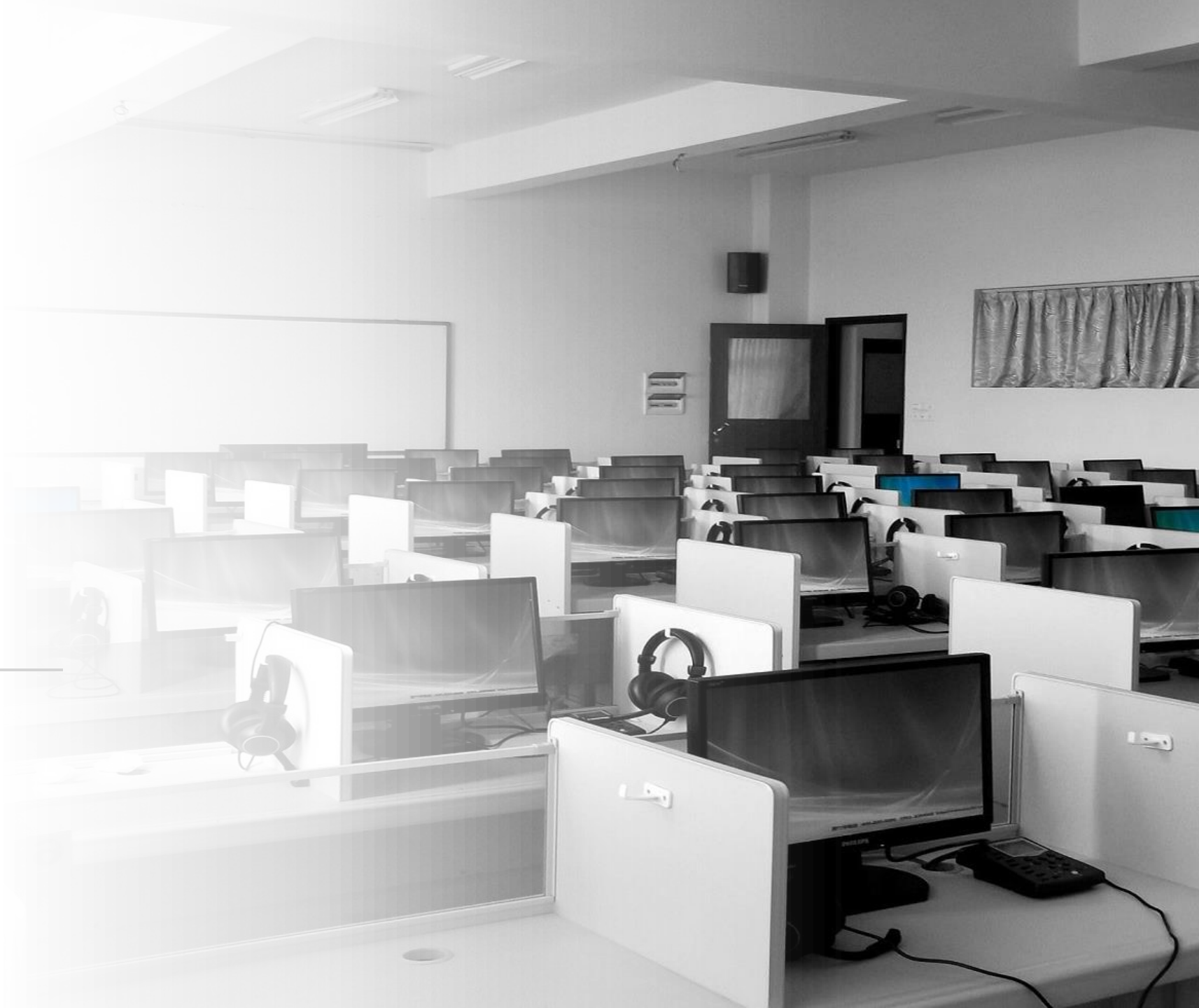
BENEFITS

- Open standards
- Works with most devices
- Supported Natively Across Browsers and Platforms
- Mitigate Data Breaches
- One key can be used for different services
- True passwordless with use of biometrics
- Biometrics (hash) stored on the device itself


USECASES

USERS WITHOUT CORPORATE PHONE & “REFUSERS”

SHARED DEVICES



HIGH-SECURE ENVIRONMENTS

DEVICES WITHOUT TPM

MULTIPLE DEVICES OR ACCOUNTS

VIP USERS


DEMO

USB-A
USB-C
NFC
BLE
Biometric
Lightning

BioPass FIDO2 Manager

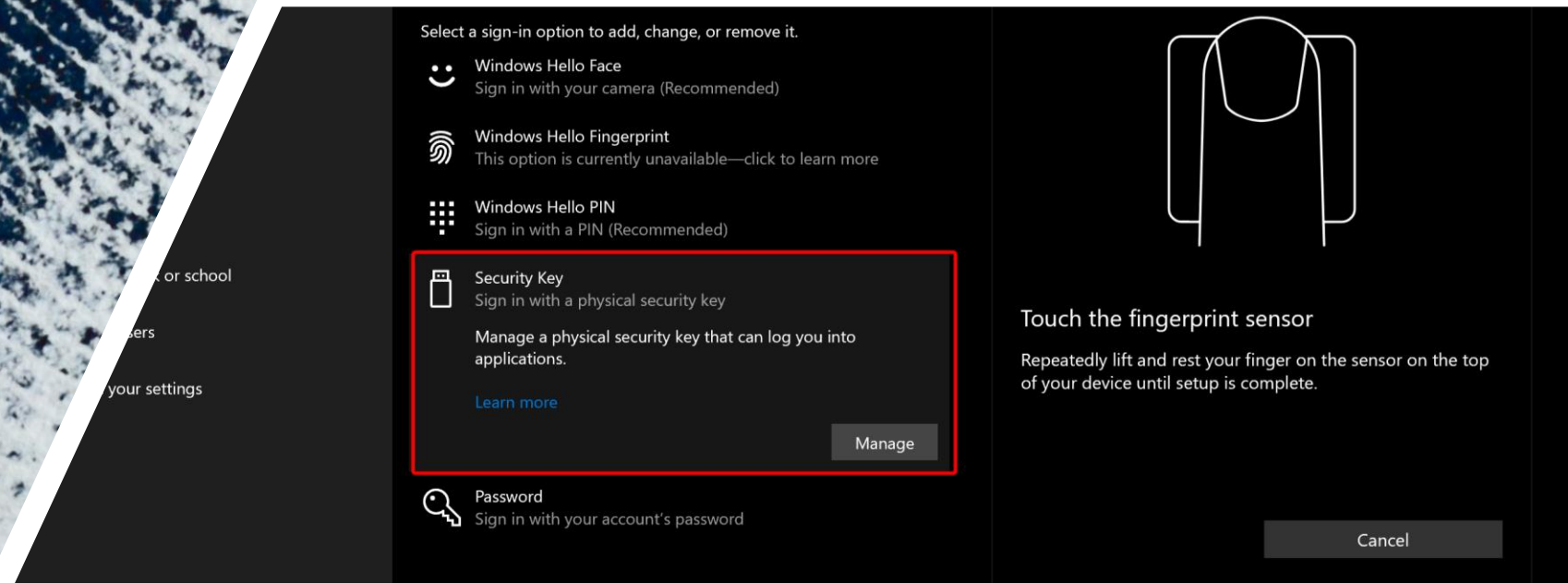
Feitian Technologies Co., Ltd. • Hulpprogramma's en hulpmiddelen

♡ Verlanglijstje

With this application you can enroll your fingerprints to Feitian BioPass FIDO device(fingerprints) afterwards. You will setup the BioPass FIDO2 device as t passwordless logon to Windows 10 RS4 and other services with your Azure

3 PEGI

PEGI 3



FIDO Platform/Browser Support

Updated 6/29/2020

Now support FIDO U2F multi-factor authentication at:

Microsoft Azure

Home Azure Portal Feedback Forums

How can we improve Azure Active Directory?

← Azure Active Directory

166
votes

Vote

Provide support for YubiKey / FIDO as the MFA

Many other services (Google Apps, Facebook etc) now allow this and would be great to have in Azure AD.

https://www.yubico.com/about/background/fido/

Ian McDonald shared this idea · April 04, 2017 · Flag idea as inappropriate...

ADMIN

PLANNED · **Azure AD Team** (Product Manager, Microsoft Azure) responded · July 25, 2020

Azure AD now supports FIDO2 security keys in public preview. We're working on allowing them to be used as a second factor as well (today they are used only first in sequence, but they satisfy MFA).

Show previous admin responses (1)

Now support FIDO2 Passwordless authentication at:

FEITIAN
WE BUILD SECURITY

FEITIAN Epass K9B


ORIGINAL TASTE
Coke
Nutrition Facts
Calories 140