Multi-Factor Authentication

And its common misconception.

About

Tijme Gommers

- Product Lead / Red Teamer / Developer
- Works at Northwave Security
- Lives in the Netherlands
- Author of open-source software
  Kernel Mii, Raivo OTP, WikiRaider
- Socials username is @tijme
  Twitter, GitHub, LinkedIn

Our corporate accounts can't be hacked, we use strong passwords *and MFA*.

- Chief Information Security Officer -

Multi-Factor Authentication (MFA)

It comes in many factors, according to Microsoft categorized as below.

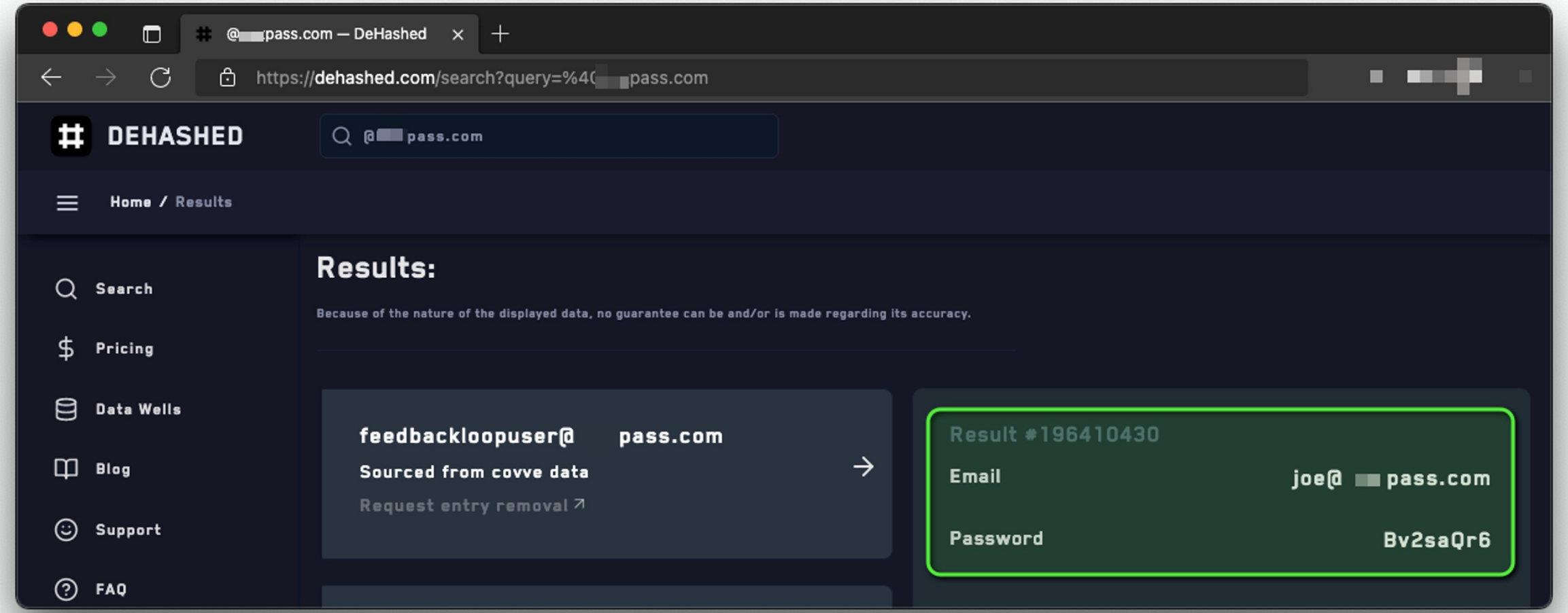
Bad	Good	Better	Best
password	*password and …*	*password and …*	*paswordless*
• 123456 • Welcome01 • Summer2022! • Winter2022! • September2022! • Coffee02	SMS 	Raivo  Push 	Certificates   Biometrics 

Our corporate accounts can’t be hacked, we use strong passwords *and MFA*.

- Chief Information Security Officer -

Password without MFA

Vulnerable to data breaches.



Multi-Factor Authentication (MFA)

It comes in many factors, according to Microsoft categorized as below.

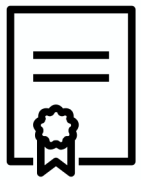
Bad	Good	Better	Best
password	*password and …*	*password and …*	*paswordless*

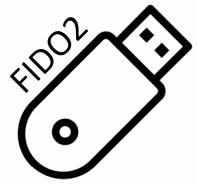
SMS

Raivo

Push

Certificates

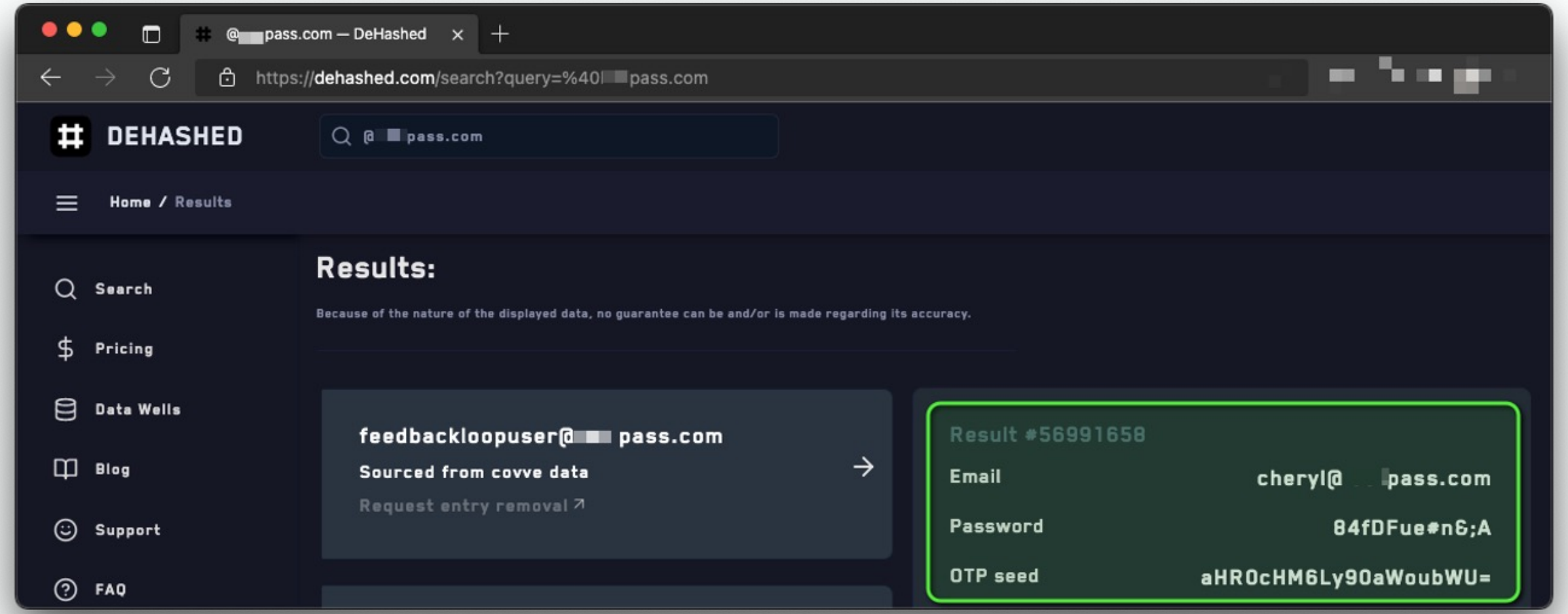




Biometrics

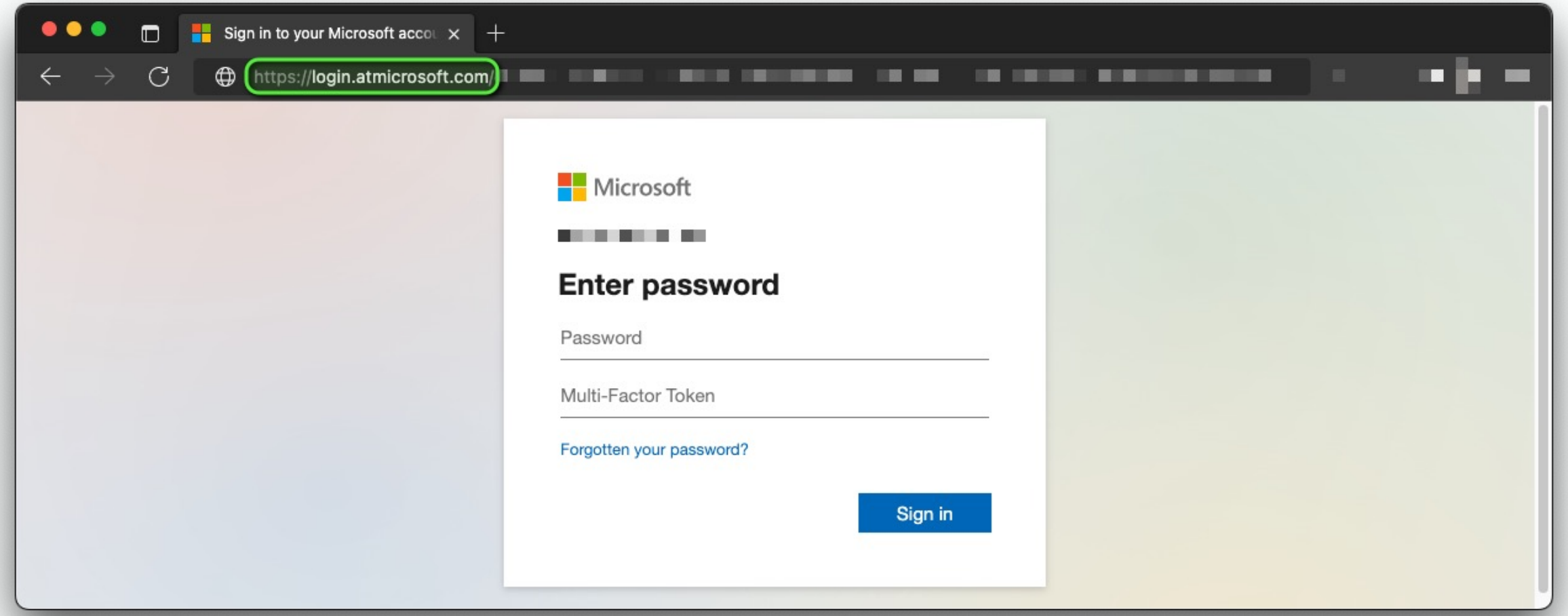
Password with SMS MFA

Vulnerable to data breaches.



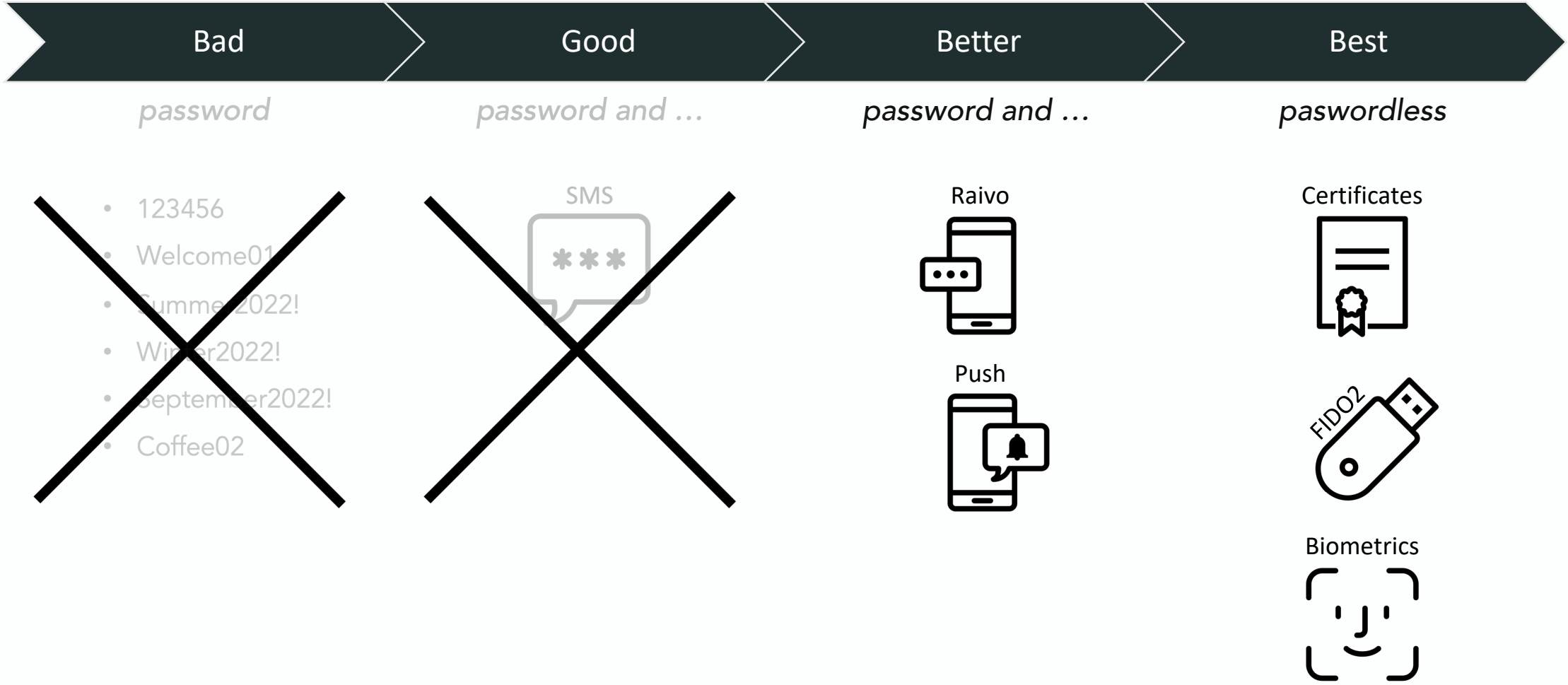
Password with SMS MFA

Vulnerable to password & token phishing.



Multi-Factor Authentication (MFA)

It comes in many factors, according to Microsoft categorized as below.



Password with push MFA

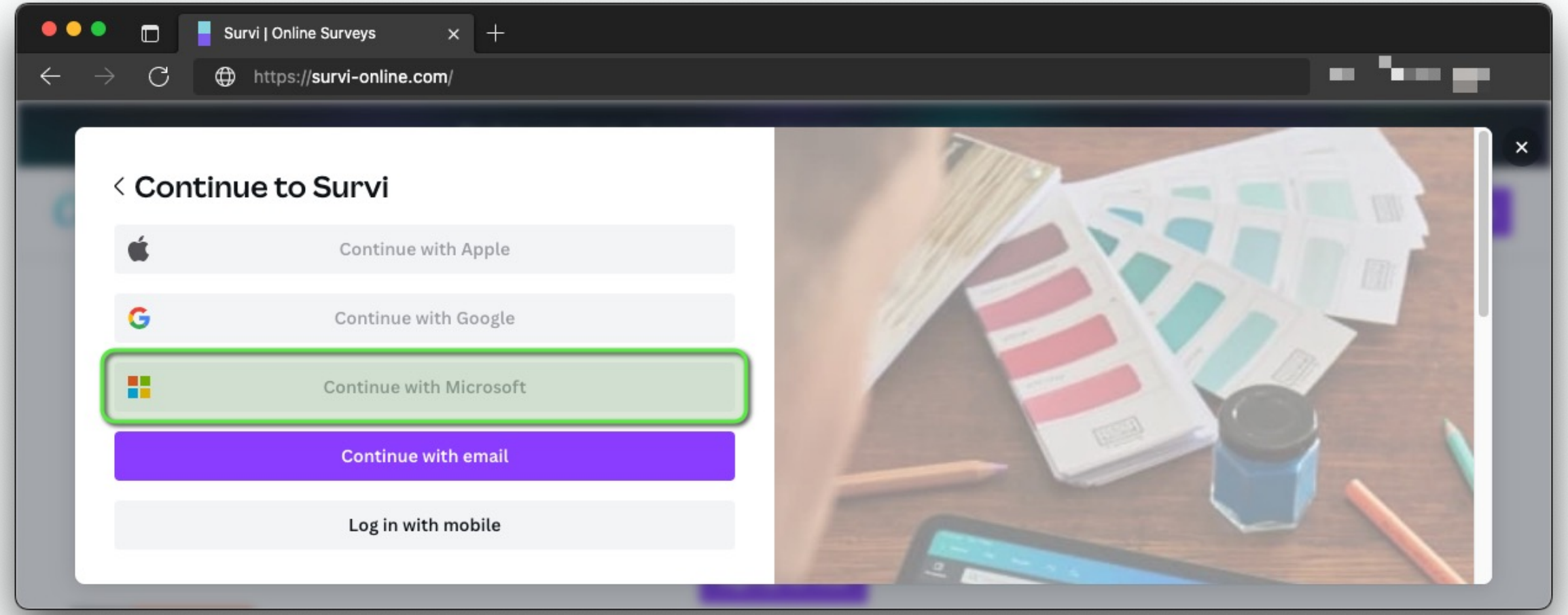
Vulnerable to password spraying.


```
$ spray365.py spray -ep plans/password.plan --lockout 2

[2022-05-09 13:25:11 - INFO]: Processing execution plan 'plans/pass
[2022-05-09 13:25:11 - INFO]: Identified 521  credentials in the provided execution p
[2022-05-09 13:25:11 - INFO]: Password spraying will take at least 31790 seconds
[2022-05-09 13:25:11 - INFO]: Lockout threshold is set to 2 accounts
[2022-05-09 13:25:11 - INFO]: Starting to spray credentials
[2022-05-09 13:25:12 - SPRAY 001/521]: b.jong / January2022! (Failed: Invalid credentials)
[2022-05-09 13:25:17 - SPRAY 002/521]: a.wijkerd / January2022! (Failed: Invalid credentials)
[2022-05-09 13:25:23 - SPRAY 003/521]: a.moos / January2022! (Failed: Invalid credentials)
[2022-05-09 13:25:28 - SPRAY 004/521]: a.baan / January2022! (Failed: Invalid credentials)
[2022-05-09 13:25:33 - SPRAY 005/521]: a.rovert / January2022! (Success: Valid credentials)
[2022-05-09 13:25:39 - SPRAY 006/521]: a.gaanders / January2022! (Failed: Invalid credentials)
[2022-05-09 13:25:44 - SPRAY 007/521]: a.bol / January2022! (Failed: Invalid credentials)
[2022-05-09 13:25:49 - SPRAY 008/521]: aa.romoes / January2022! (Failed: Invalid credentials)
[2022-05-09 13:25:55 - SPRAY 009/521]: ab.timons / January2022! (Partial Success: Account locked)
[2022-05-09 13:26:00 - SPRAY 010/521]: b.kuijpers / January2022! (Failed: Invalid credentials)
[2022-05-09 13:26:05 - SPRAY 011/521]: ac.langestraat / January2022! (Failed: Invalid credentials)
```

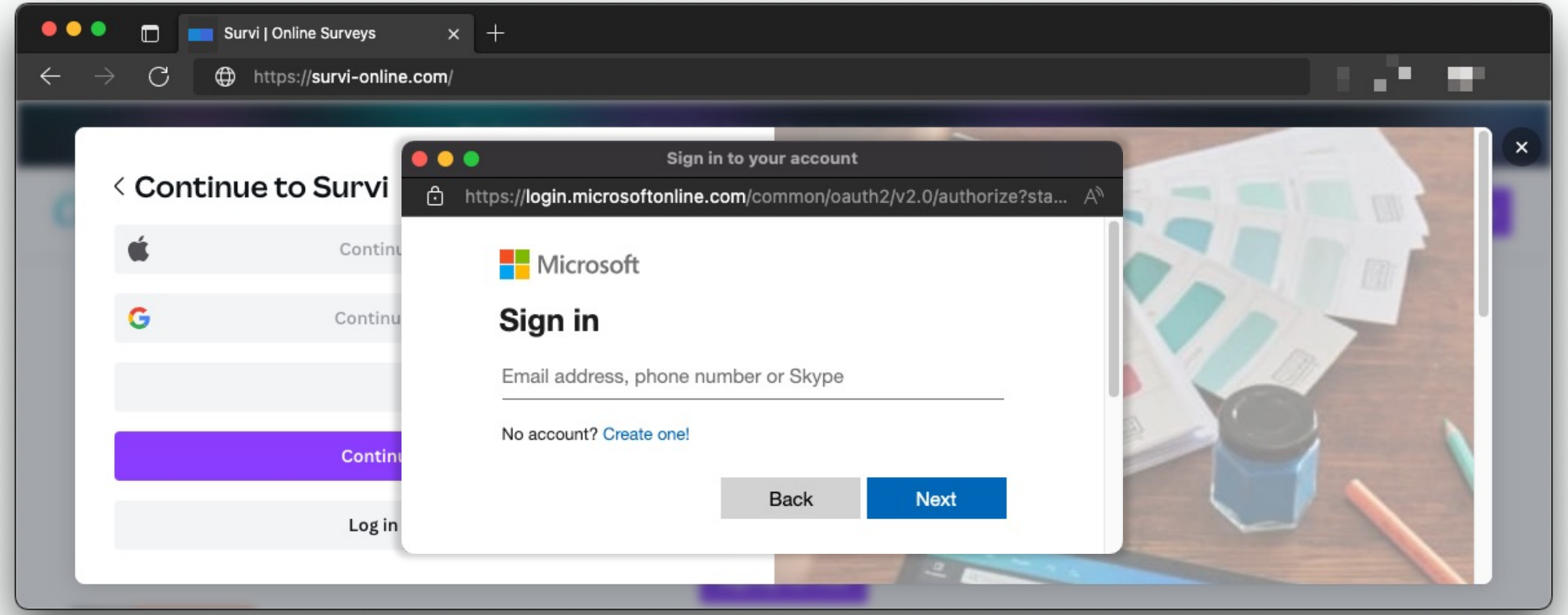
Password with push MFA

Vulnerable to (BITB) proxy phishing.



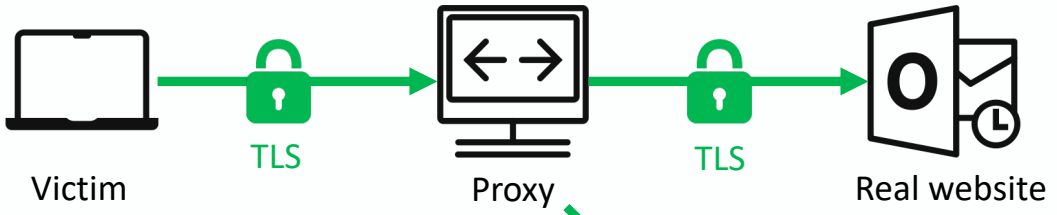
Password with push MFA

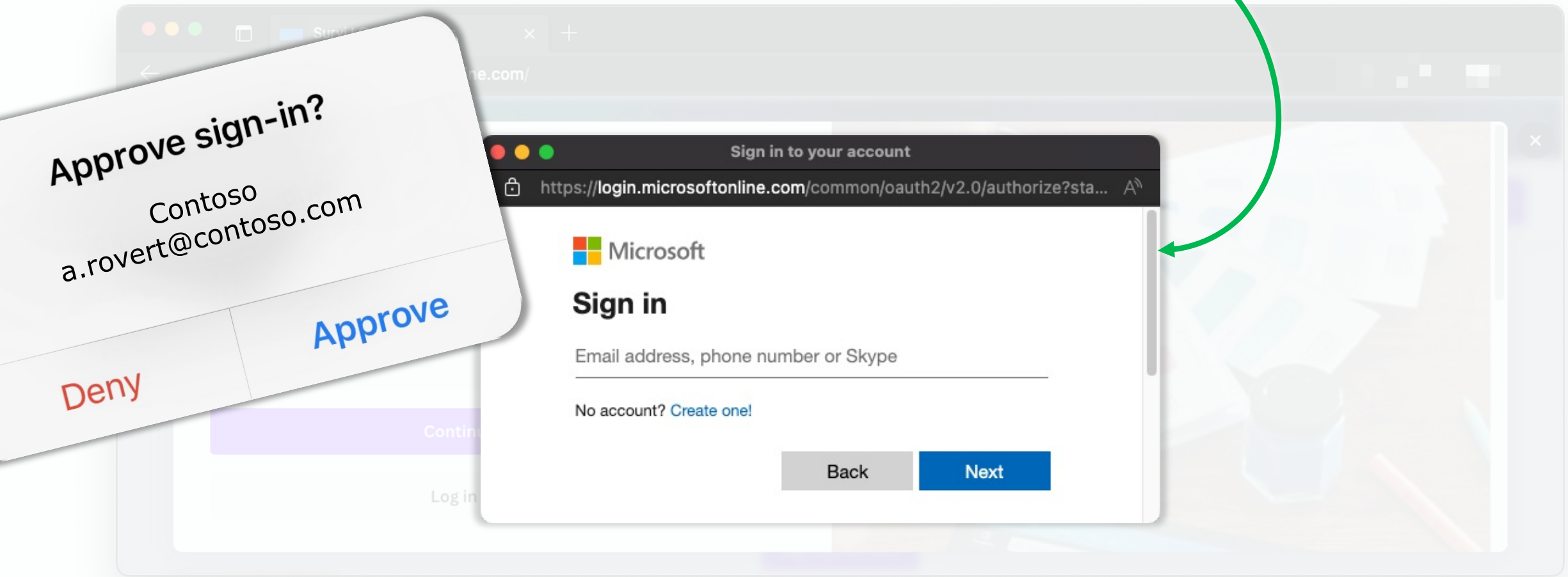
Vulnerable to (BITB) proxy phishing.



Password with push MFA

Vulnerable to (BITB) proxy phishing.





Passwordless MFA

It comes in many factors.

Bad → Good → Better → Best

password | *password and …* | *password and …* | *paswordless*

- 123456
- Welcome01
- Summer2022!
- Winter2022!
- September2022!
- Coffee02

SMS

Push

Certificates

FIDO2

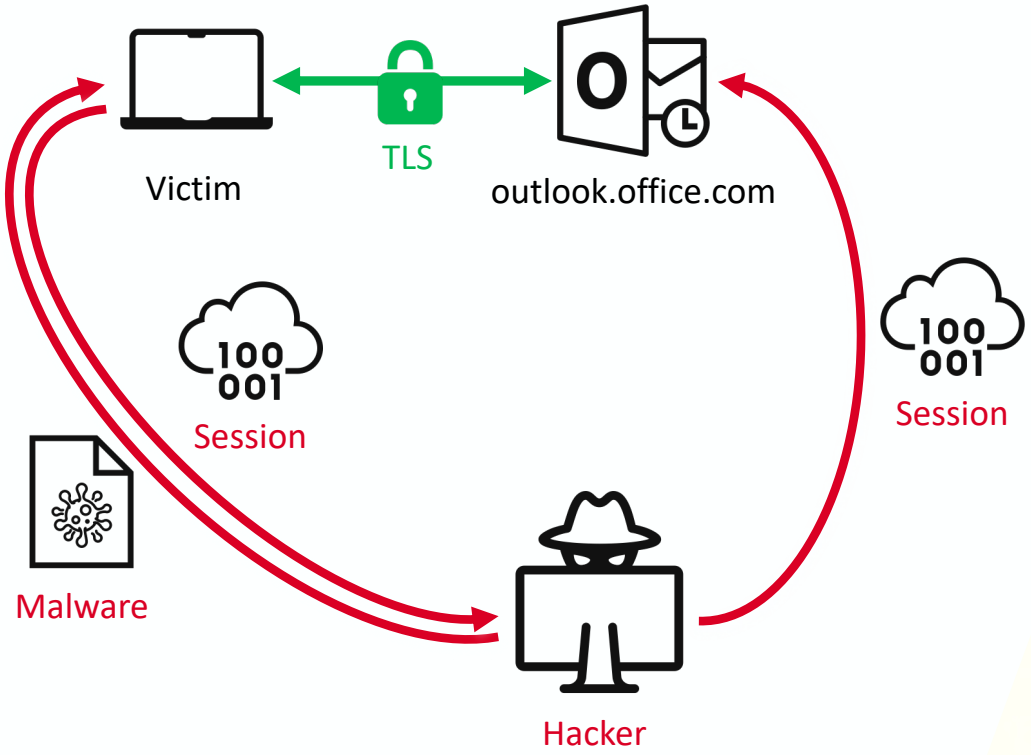
Biometrics

So, if we go passwordless our corporate accounts can’t be abused?

- Chief Information Security Officer -

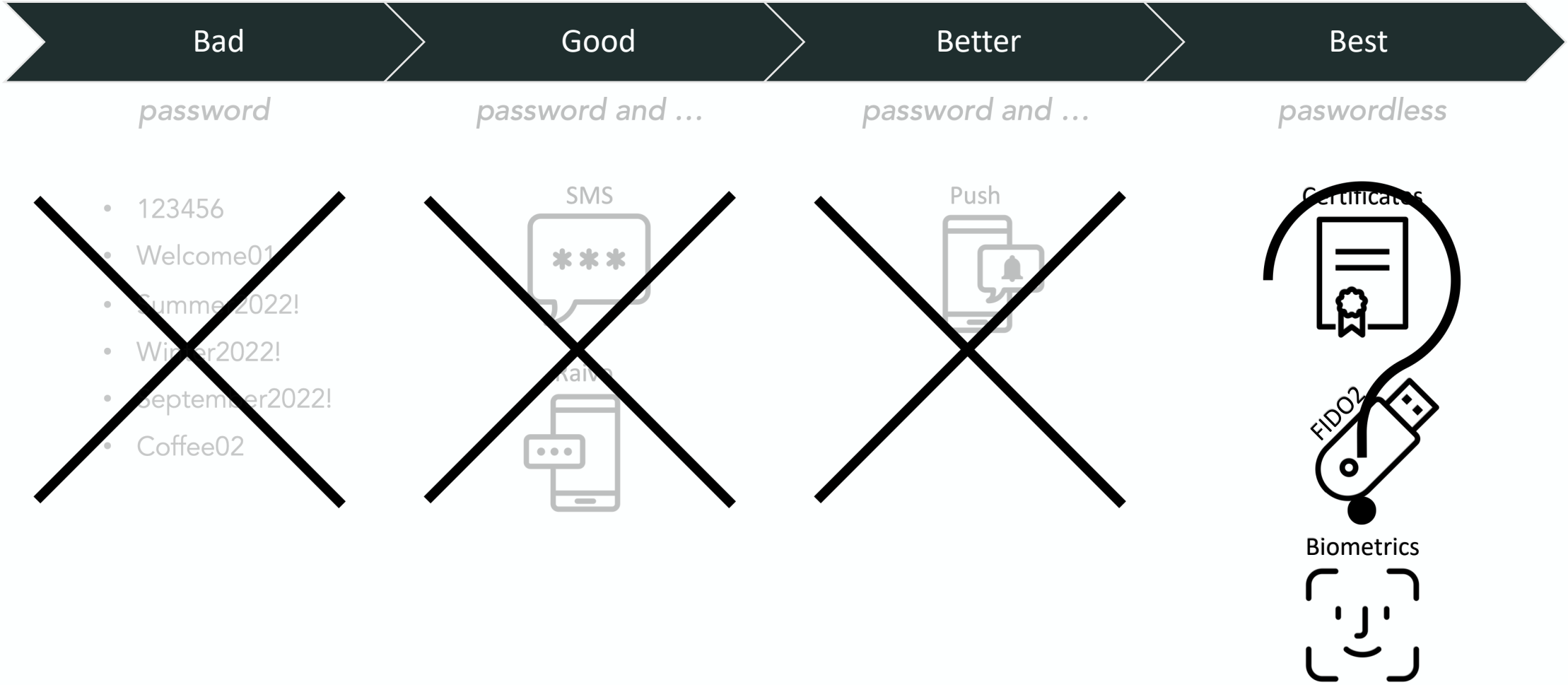
Passwordless

Let’s put it to the test!



Multi-Factor Authentication (MFA)

It comes in many factors.



Passwordless authentication is not the holy grail, but it's the best we have!

- Chief Information Security Officer -


Multi-Factor
Authentication
And its common misconception.
twitter.com/tijme
github.com/tijme
linkedin.com/in/tijme