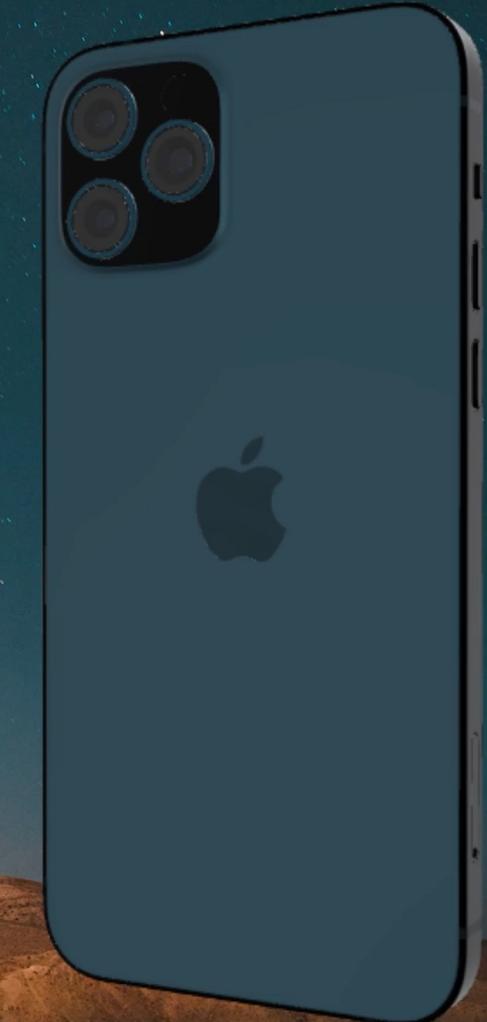


Multi-Factor Authentication

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](#)

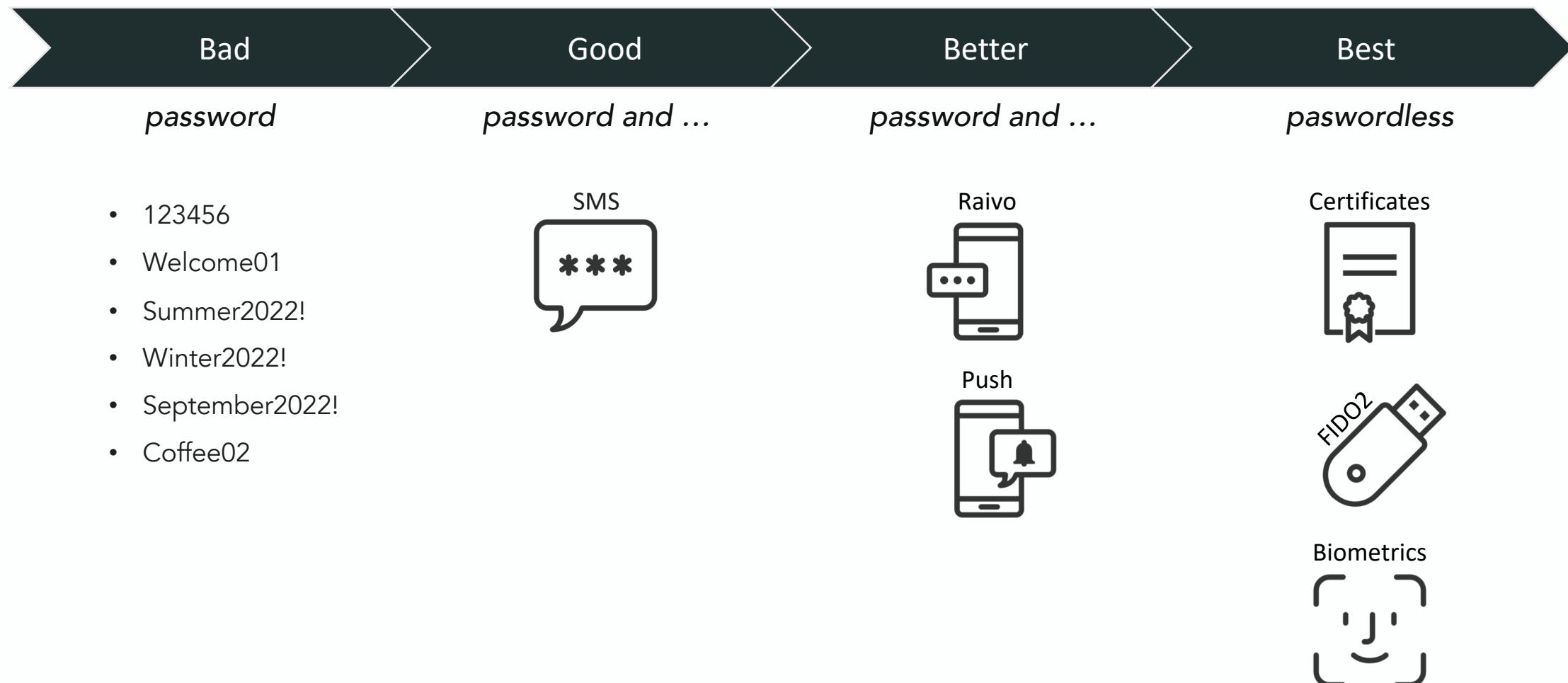


**Our corporate accounts can't
be hacked, we use strong
passwords and MFA.**

- Chief Information Security Officer -

Multi-Factor Authentication (MFA)

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



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

- Chief Information Security Officer -

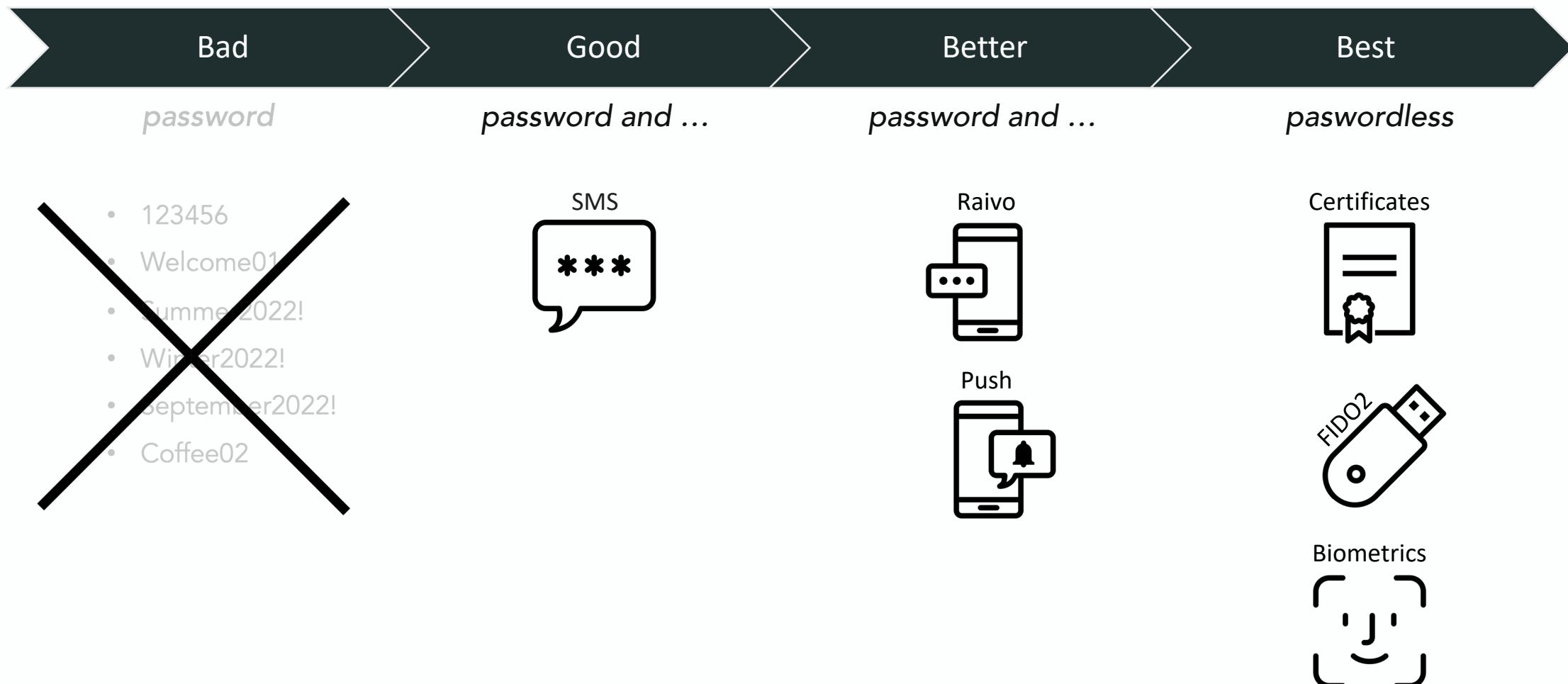
Password without MFA

Vulnerable to data breaches.

The screenshot shows a web browser window with a dark theme. The address bar displays the URL [https://dehashed.com/search?query=%40\[REDACTED\]pass.com](https://dehashed.com/search?query=%40[REDACTED]pass.com). The main content area is titled "DEHASHED" with a magnifying glass icon. Below it, there's a navigation menu with "Home / Results". On the left, there's a sidebar with links for "Search", "Pricing", "Data Wells", "Blog", "Support", and "FAQ". The main content area has a heading "Results:" and a sub-heading "Because of the nature of the displayed data, no guarantee can be and/or is made regarding its accuracy.". Two results are shown in cards. The first card, which is gray, contains the email "feedbackloopuser@[REDACTED]pass.com", a note "Sourced from covve data", and a link "Request entry removal". An arrow points from this card to the second card. The second card, which is green, is highlighted with a green border. It contains the text "Result #196410430", "Email joe@[REDACTED]pass.com", and "Password Bv2saQr6".

Multi-Factor Authentication (MFA)

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



Password with SMS MFA

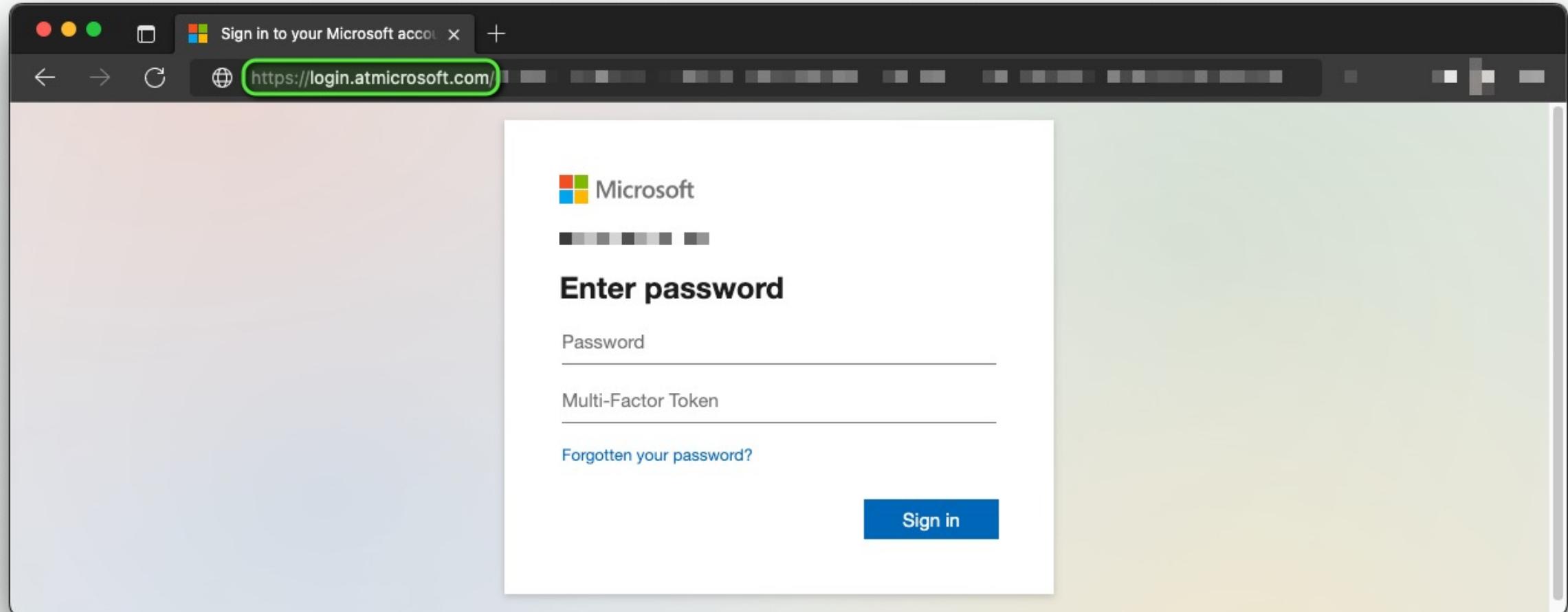
Vulnerable to data breaches.

The screenshot shows a web browser window with the title bar "# @ pass.com – DeHashed". The URL in the address bar is <https://dehashed.com/search?query=%40 pass.com>. The main content area is titled "DEHASHED" with a search bar containing "@ pass.com". On the left, there's a sidebar with links: Home / Results, Search, Pricing, Data Wells, Blog, Support, and FAQ. The main content area has a heading "Results:" and a note: "Because of the nature of the displayed data, no guarantee can be and/or is made regarding its accuracy." Below this, there are two main result cards. The first card, for "feedbackloopuser@ pass.com", includes links to "Sourced from covve data" and "Request entry removal". An arrow points from this card to the second card. The second card, highlighted with a green border, contains the following information:

Result #56991658	
Email	cheryl@ pass.com
Password	84fDFue*n6;A
OTP seed	aHROcHM6Ly90aWoubWU=

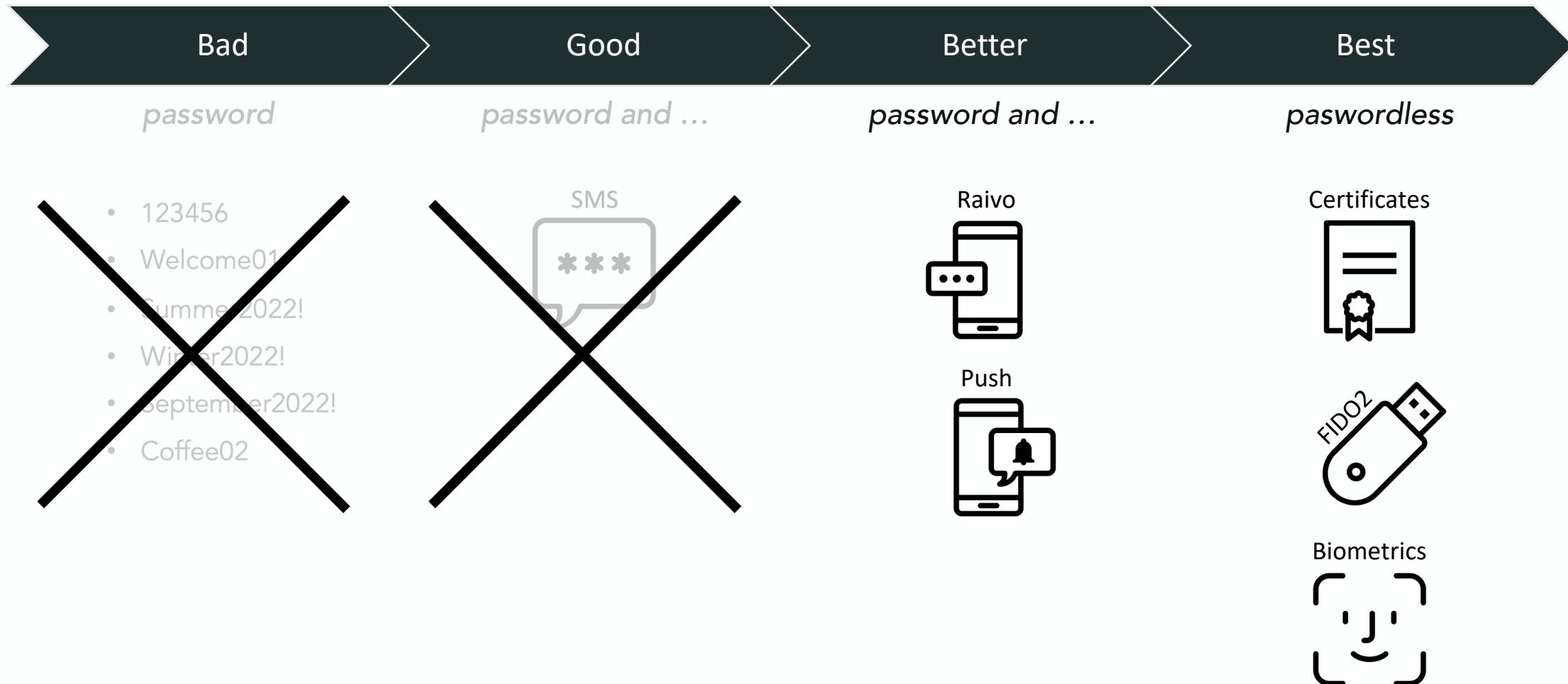
Password with SMS MFA

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/password.plan'  
[2022-05-09 13:25:11 - INFO]: Identified 521 credentials in the provided execution plan.  
[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)
```

Approve sign-in?

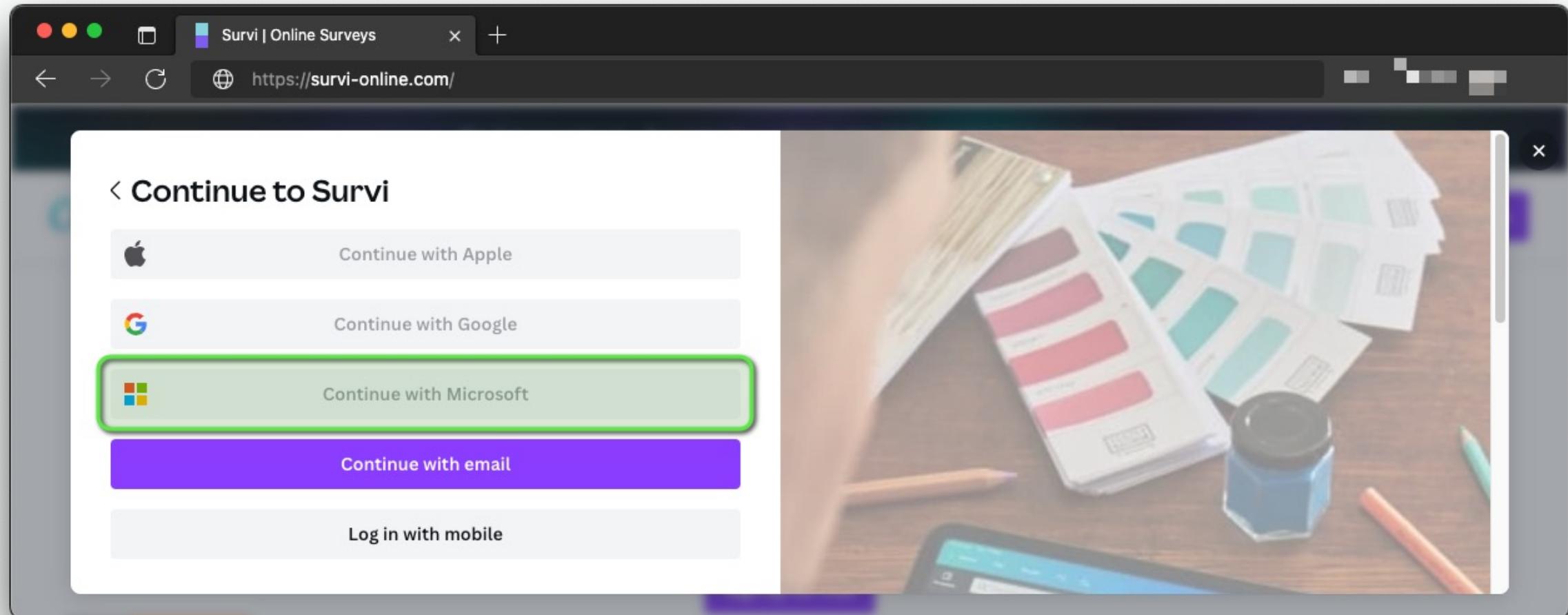
Contoso
a.rovert@contoso.com

Deny

Approve

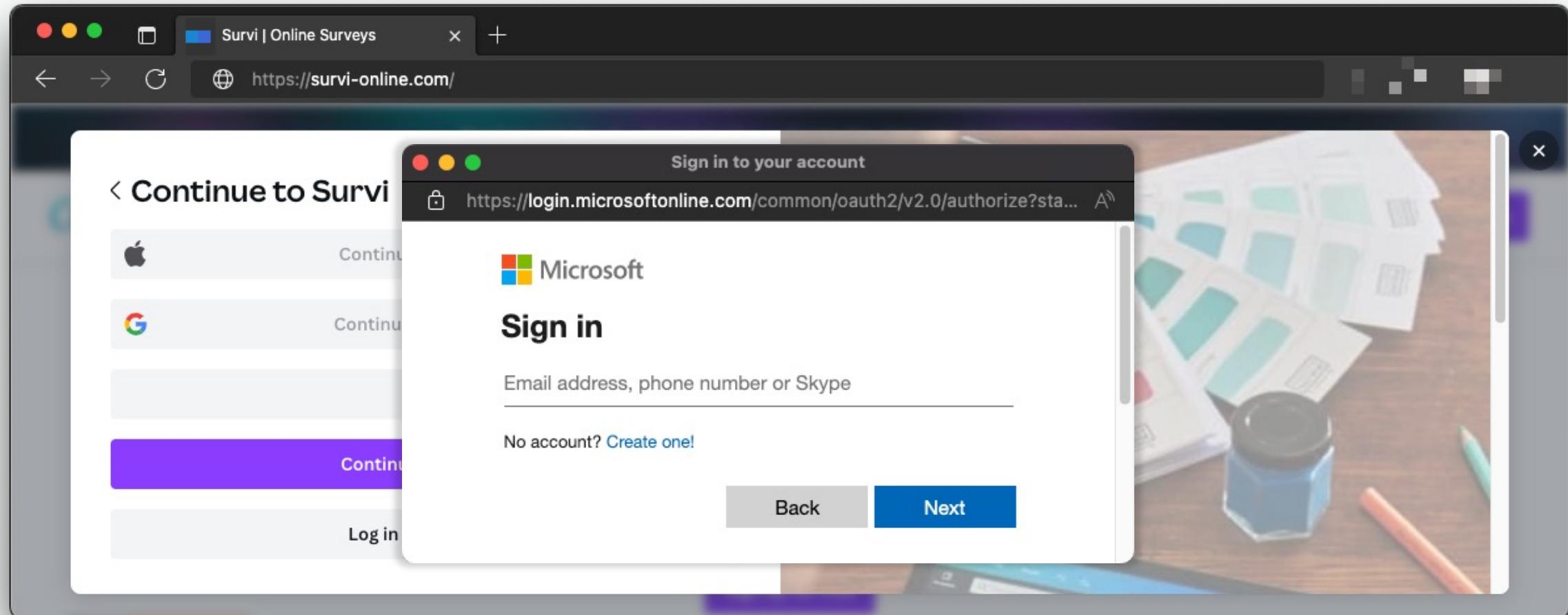
Password with push MFA

Vulnerable to (BITB) proxy phishing.



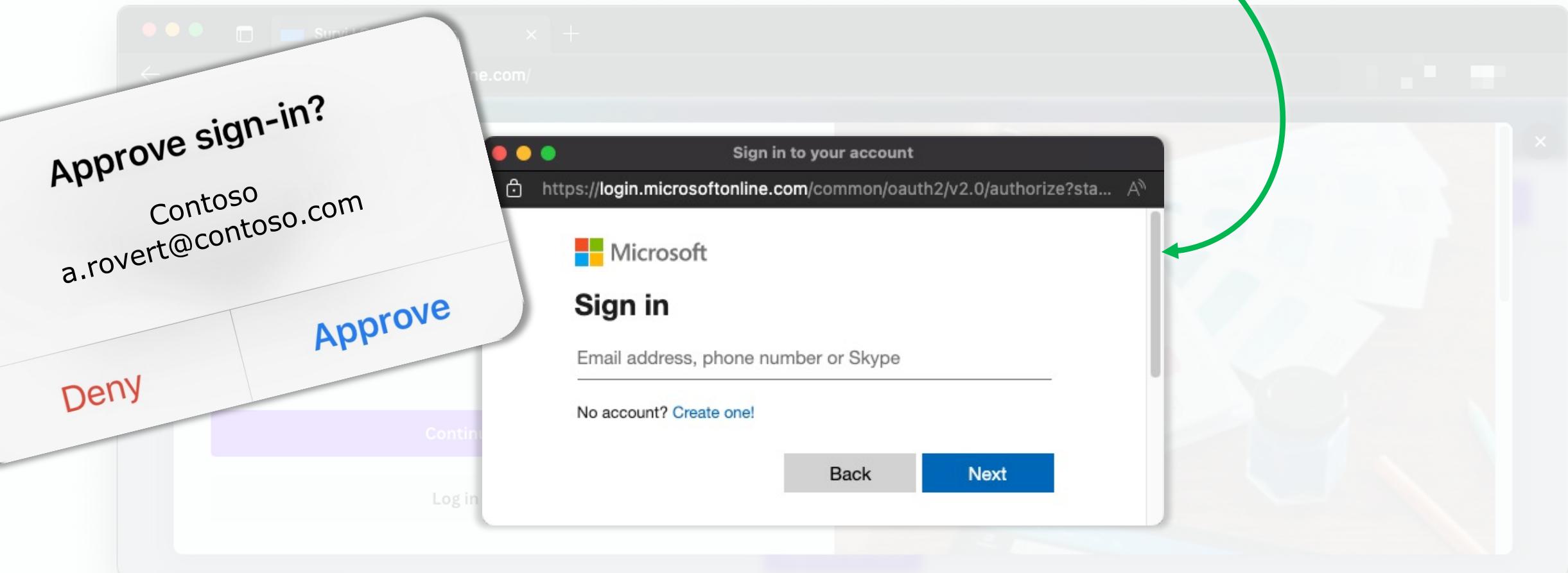
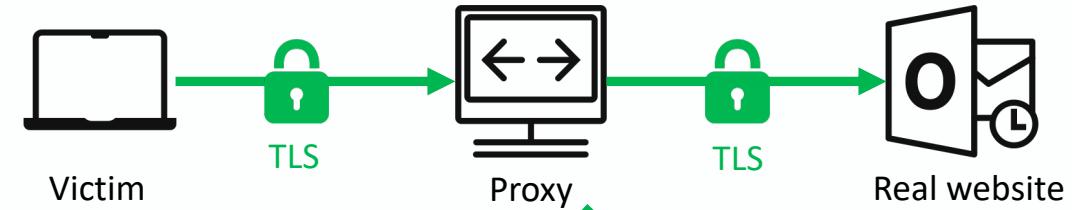
Password with push MFA

Vulnerable to (BITB) proxy phishing.



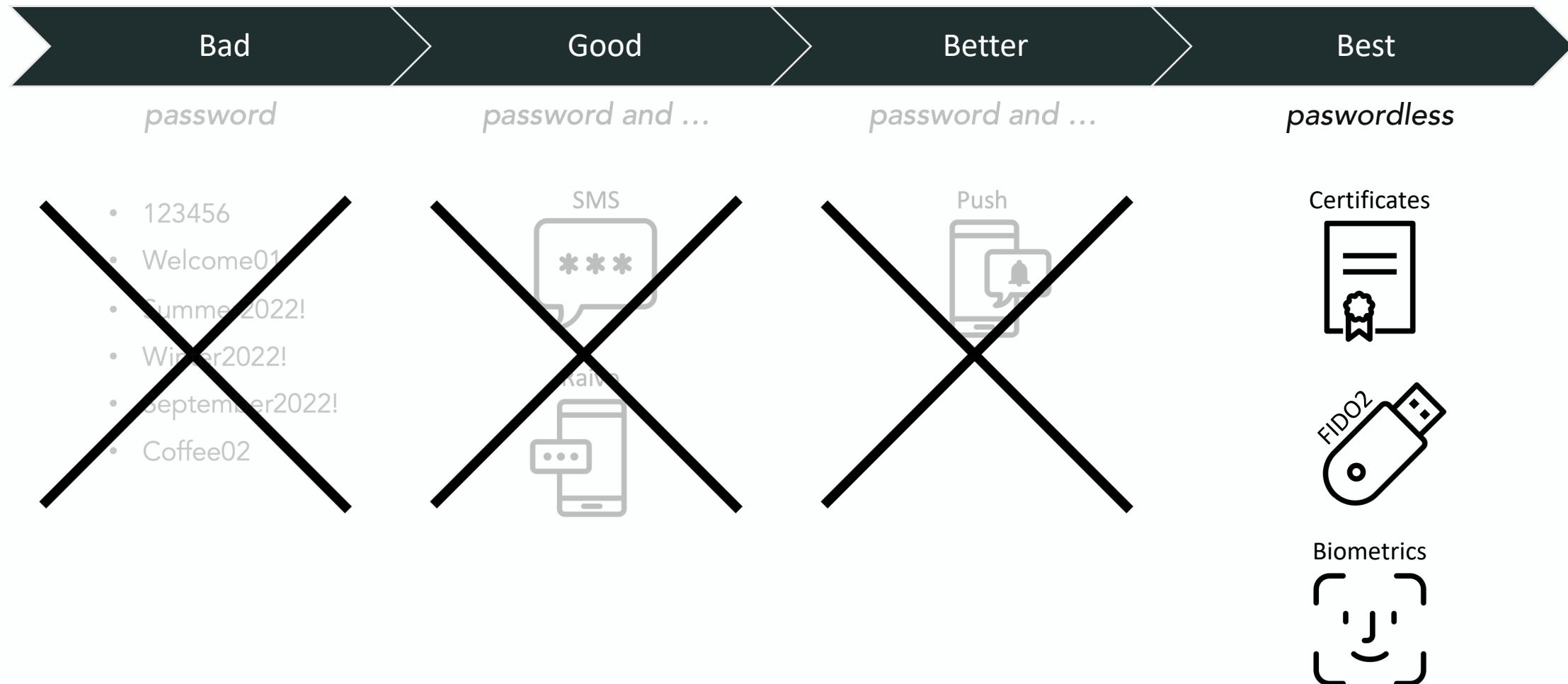
Password with push MFA

Vulnerable to (BITB) proxy phishing.



Passwordless MFA

It comes in many factors.

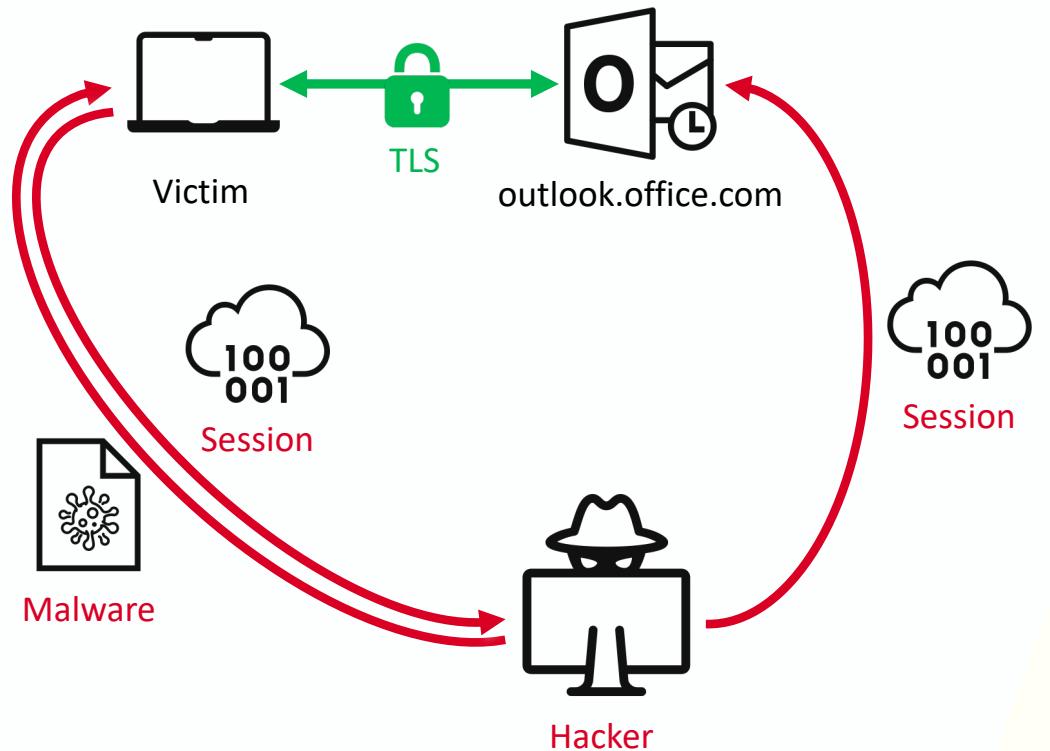


**So, if we go passwordless
our corporate accounts
can't be abused?**

- Chief Information Security Officer -

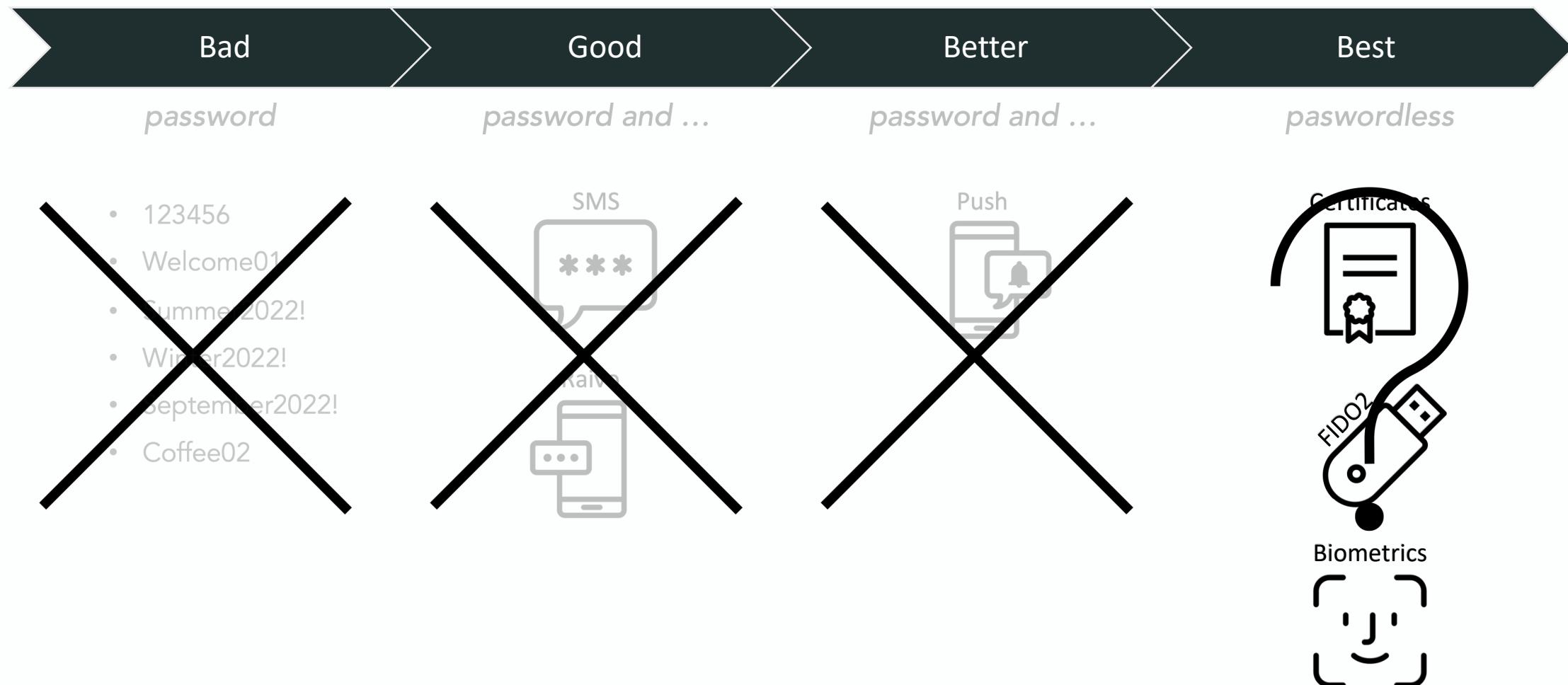
Passwordless

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

