ETH Zürich

Carleton UNIVERSITY

Is Real-time Phishing Eliminated with FIDO?

Social Engineering Downgrade Attacks against FIDO Protocols

Enis Ulqinaku, Hala Assal, AbdelRahman Abdou, Sonia Chiasson, and Srdjan Capkun

Phishing Trend: attackers adapt continuously

Passwords: weak, reuse, leakage, keyloggers, phishing,...

sms

2FA

Two factor authentication

‘00: Collect credentials, exploit later.

Cheap & Scalable

fido ALLIANCE simpler stronger authentication

‘10: Real-time phishing to bypass 2FA.

Cheap* & Scalable

‘20: Real-time phishing against FIDO?

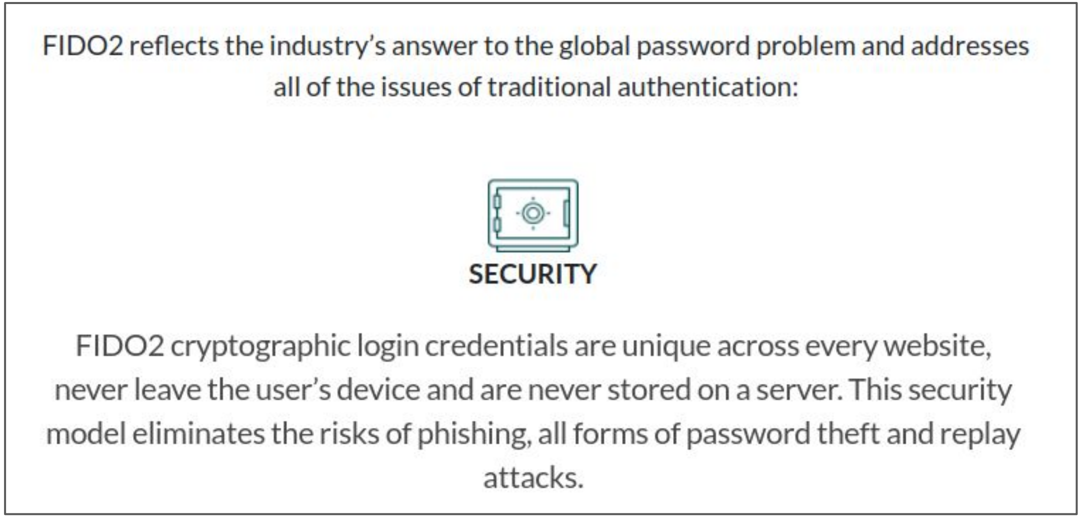
Cheap & Scalable?

* Automated tools similar to Evilginx reduce manual efforts to mount real-time phishing.

FIDO: Motivation

Goals:

- Secure Authentication
    - Privacy preserving.
- Easy to use
- Scalable



FIDO2 reflects the industry's answer to the global password problem and addresses all of the issues of traditional authentication:

SECURITY

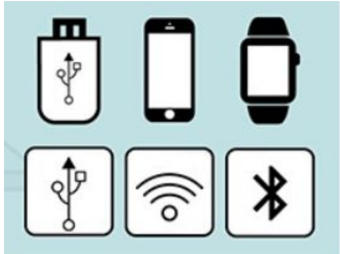
FIDO2 cryptographic login credentials are unique across every website, never leave the user's device and are never stored on a server. This security model eliminates the risks of phishing, all forms of password theft and replay attacks.

https://fidoalliance.org/fido2

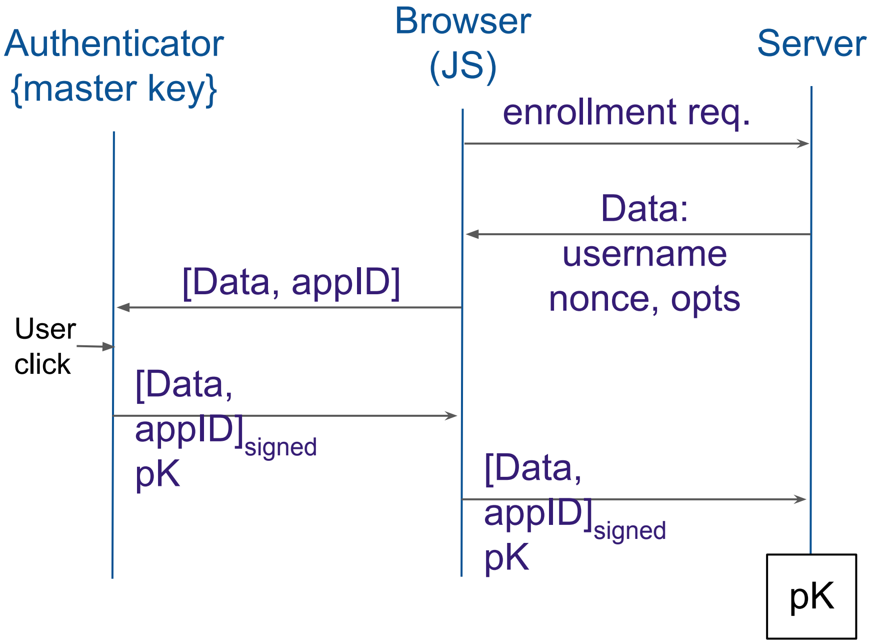
FIDO Overview

Trusted:

- FIDO servers.
- Client software (host).
  - WebAuthn & CTAP
- Authenticators (security keys).

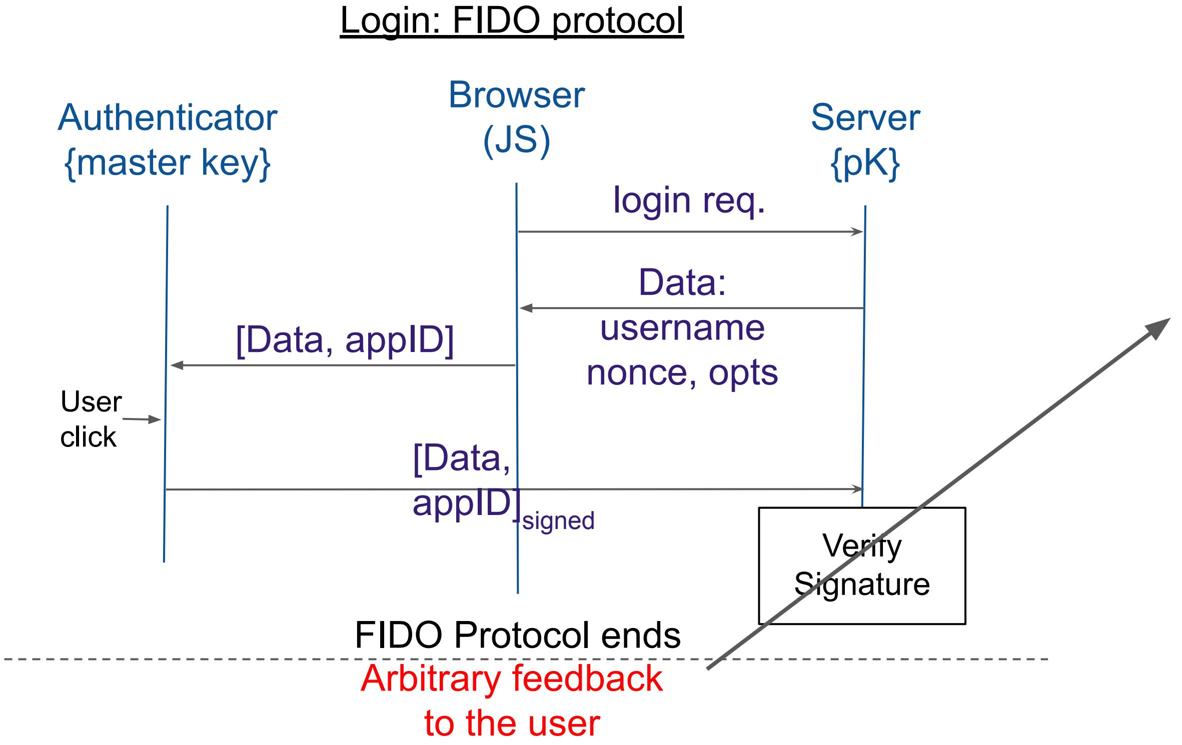


FIDO Enrollment



Images from https://fidoalliance.org

Weakness 1: No (secure) feedback to the user



The **lack of secure feedback** allows an attacker to render the usual **success message** for FIDO step, thus potentially giving **a false sense of security** to the victim!

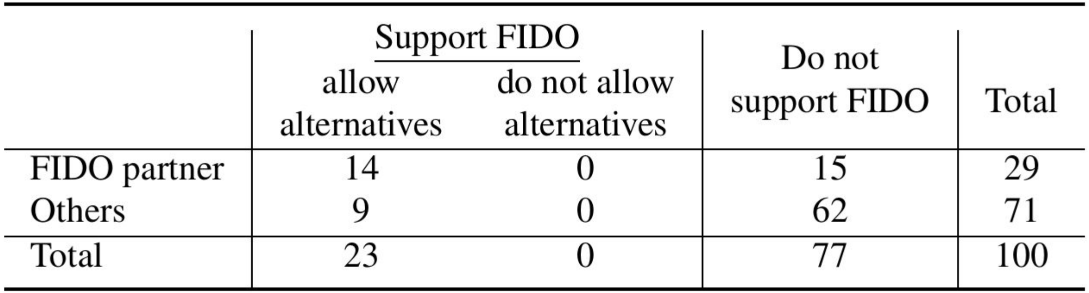
Weakness 2: Recovery and fallbacks

- FIDO: [security and usability] vs availability.
- Secure recovery at scale is difficult.
- Common practice: weaker 2FA
  - SMS / e-mails
  - OTP
  - Prompts
  - ...

Vulnerable to phishing

Intuition: FIDO & other 2FAs

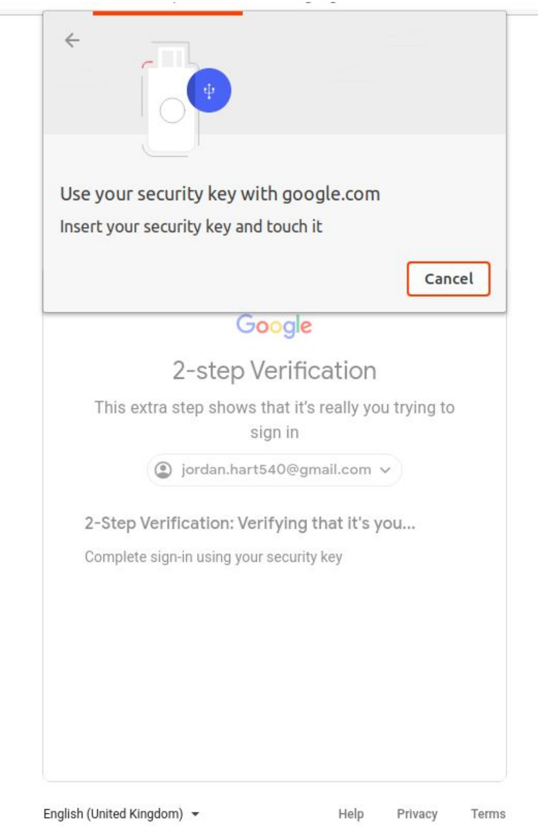
Alexa Top-100:



	Support FIDO		Do not support FIDO	Total
	allow alternatives	do not allow alternatives		
FIDO partner	14	0	15	29
Others	9	0	62	71
Total	23	0	77	100

- Does FIDO eliminate phishing?
- Is FIDO enough to secure a user account?
- What is the security of FIDO + other 2FAs?

Browser: FIDO prompt & OTP



Use your security key with google.com

Insert your security key and touch it

Cancel

Google

2-step Verification

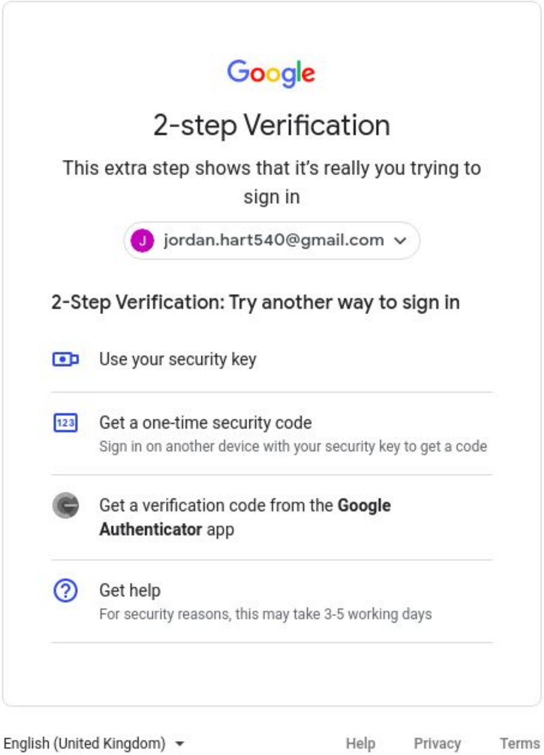
This extra step shows that it's really you trying to sign in

jordan.hart540@gmail.com

2-Step Verification: Verifying that it's you...

Complete sign-in using your security key

English (United Kingdom) Help Privacy Terms



Google

2-step Verification

This extra step shows that it's really you trying to sign in

jordan.hart540@gmail.com

2-Step Verification: Try another way to sign in

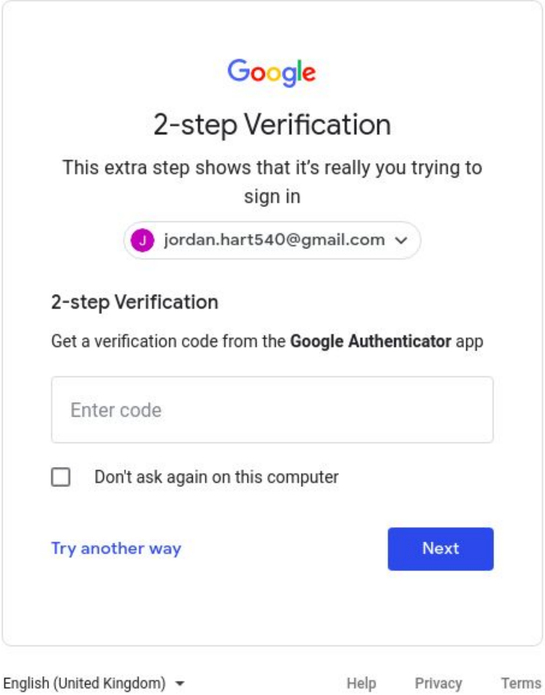
Use your security key

Get a one-time security code
Sign in on another device with your security key to get a code

Get a verification code from the **Google Authenticator** app

Get help
For security reasons, this may take 3-5 working days

English (United Kingdom) Help Privacy Terms



Google

2-step Verification

This extra step shows that it's really you trying to sign in

jordan.hart540@gmail.com

2-step Verification

Get a verification code from the **Google Authenticator** app

Enter code

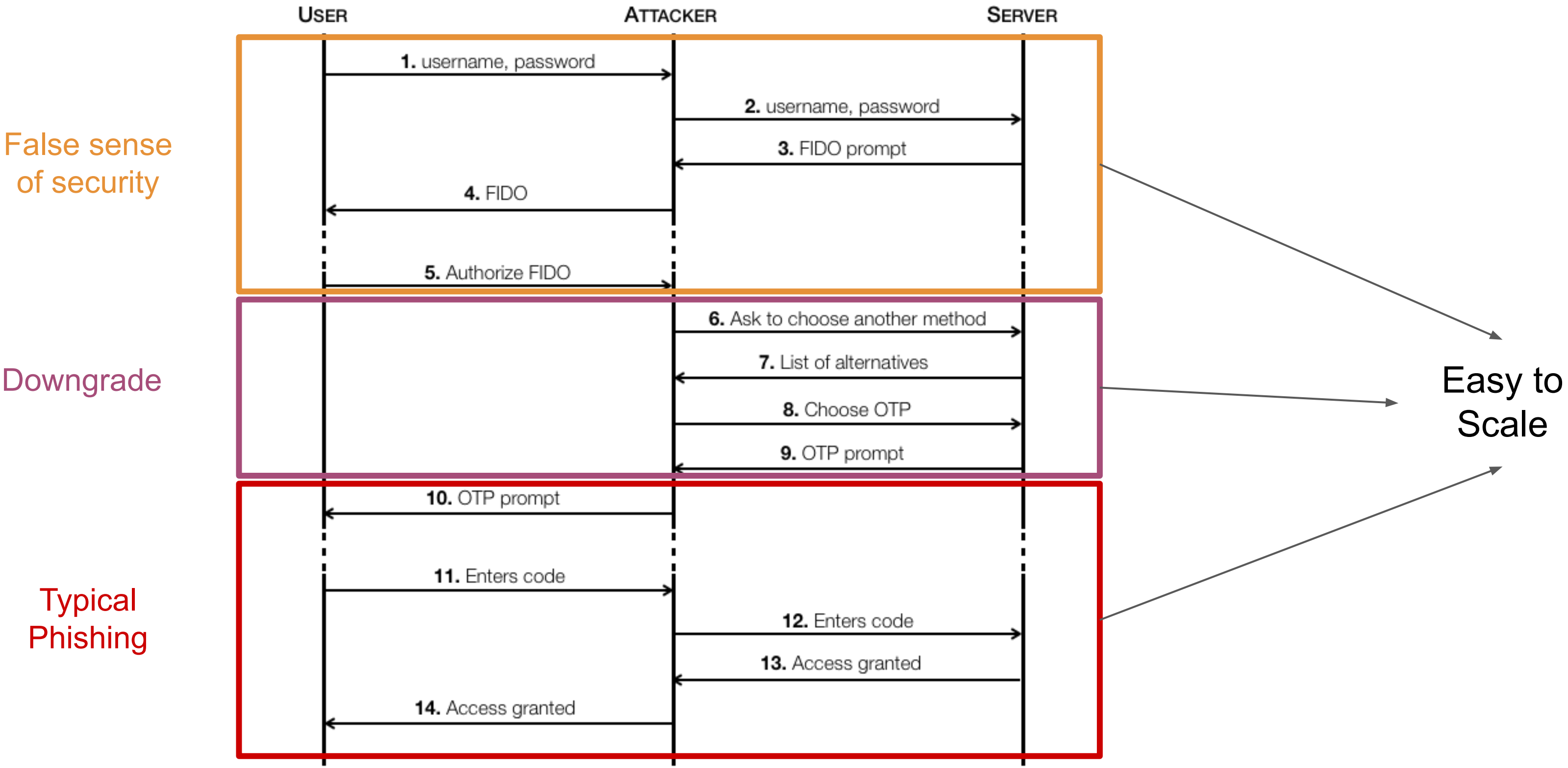
□ Don't ask again on this computer

Try another way Next

English (United Kingdom) Help Privacy Terms

Images from https://google.com

Attack Overview: user feedback + alternatives



USER | ATTACKER | SERVER

False sense of security

1. username, password
2. username, password
3. FIDO prompt
4. FIDO
5. Authorize FIDO

Downgrade

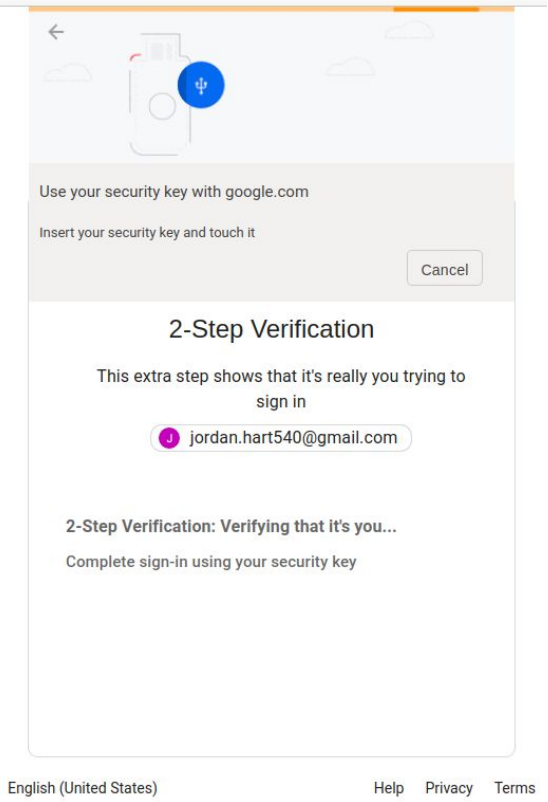
6. Ask to choose another method
7. List of alternatives
8. Choose OTP
9. OTP prompt

Typical Phishing

10. OTP prompt
11. Enters code
12. Enters code
13. Access granted
14. Access granted

Easy to Scale

Mimicry: FIDO prompt & OTP



Use your security key with google.com

Insert your security key and touch it

Cancel

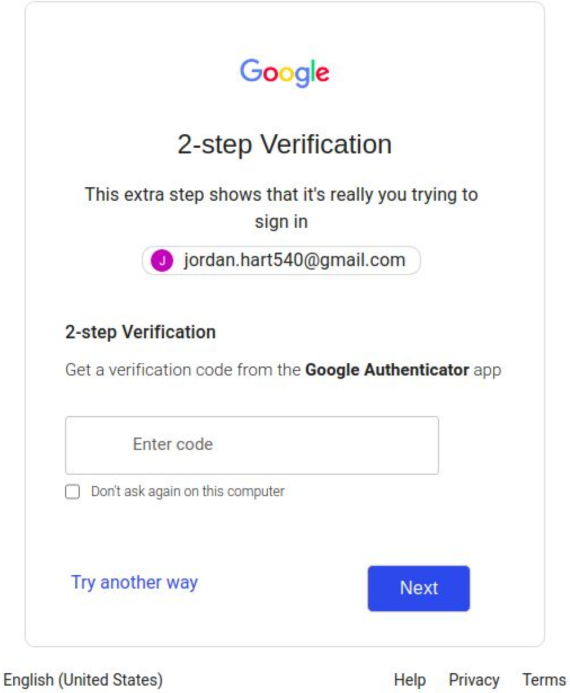
2-Step Verification

This extra step shows that it's really you trying to sign in

jordan.hart540@gmail.com

2-Step Verification: Verifying that it's you...

Complete sign-in using your security key



2-step Verification

This extra step shows that it's really you trying to sign in

jordan.hart540@gmail.com

2-step Verification

Get a verification code from the **Google Authenticator** app

Enter code

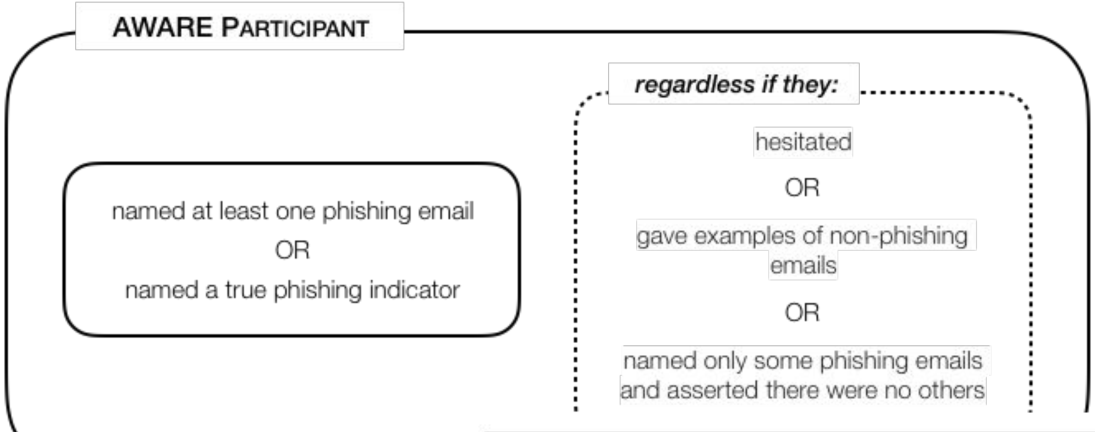
□ Don't ask again on this computer

Evaluation: User Study

- Study design: Role playing experiment + semi structured interview (~1 hour).
- Scenario: New employee in a tech company.
- 15 email: 4 phishing
- 51 participants
  - 25 in Zurich, 26 in Ottawa
  - Age: 18-64, mean: 29.9, median: 27

“If we told you that 50% of our participants access fake websites during their study sessions, do you think you are one of them? Why/Why not?”

Evaluation: Results

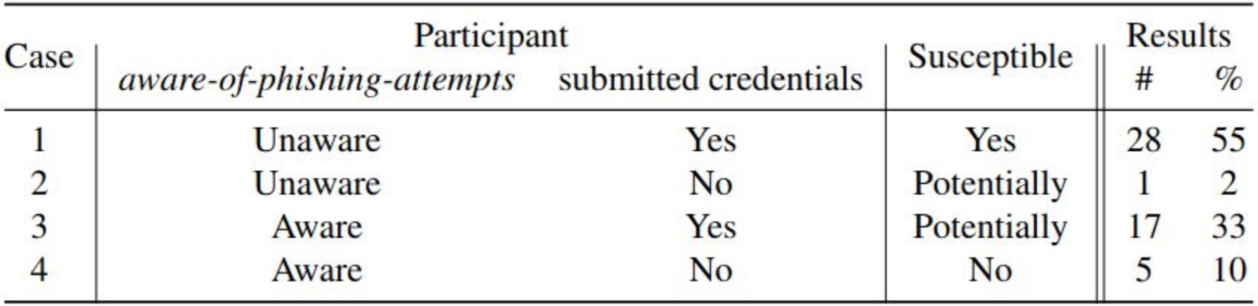


AWARE PARTICIPANT

named at least one phishing email
OR
named a true phishing indicator

regardless if they:

hesitated
OR
gave examples of non-phishing emails
OR
named only some phishing emails and asserted there were no others



Case	Participant		Susceptible	Results	
	aware-of-phishing-attempts	submitted credentials		#	%
1	Unaware	Yes	Yes	28	55
2	Unaware	No	Potentially	1	2
3	Aware	Yes	Potentially	17	33
4	Aware	No	No	5	10

User’s perceptions

Security of FIDO + OTP:

“I had to put in the information [OTP] as well and I felt secure: the company even took me to verify everything [using OTP + FIDO] to make sure that it was secured”

FIDO vs OTP security:

“If you have to use the authentication app on the phone, with the changing number always, it is really difficult for someone to hack your system to find this kind of information.”

Indicators:

“[...] if the website looks fine, I mean the front page, I am not suspicious”, “It’s the same because it looks the same up here [refers to logo section], and I would be trusting it’s fine”

Possible Countermeasures

- Disable Weaker Alternatives
    - Cons: Degradation on usability & availability. Scalable & Secure Recovery?
- Risk Based Authentication
    - Cons: Mimicry of user’s attributes/behaviour.
- Browser Hints
    - Cons: User habituation; User are vulnerable to social engineering; FIDO’ added value?
- Secure Login and Recovery Alternatives
    - Challenge: Scalability & availability.
- User Education
    - Plausible (yet somewhat ineffective) countermeasure.

Concluding Remarks

- Even with FIDO, users remain potentially vulnerable to real-time phishing that downgrades FIDO to weaker alternatives.
- Despite understanding how to use FIDO, users do not understand how FIDO protects them.
- Enabling only FIDO alternatives to FIDO is an effective countermeasure.
- Fallbacks & recovery schemes should prioritize security over usability.

Thank you

Danke
Merci
Faleminderit
Hvala