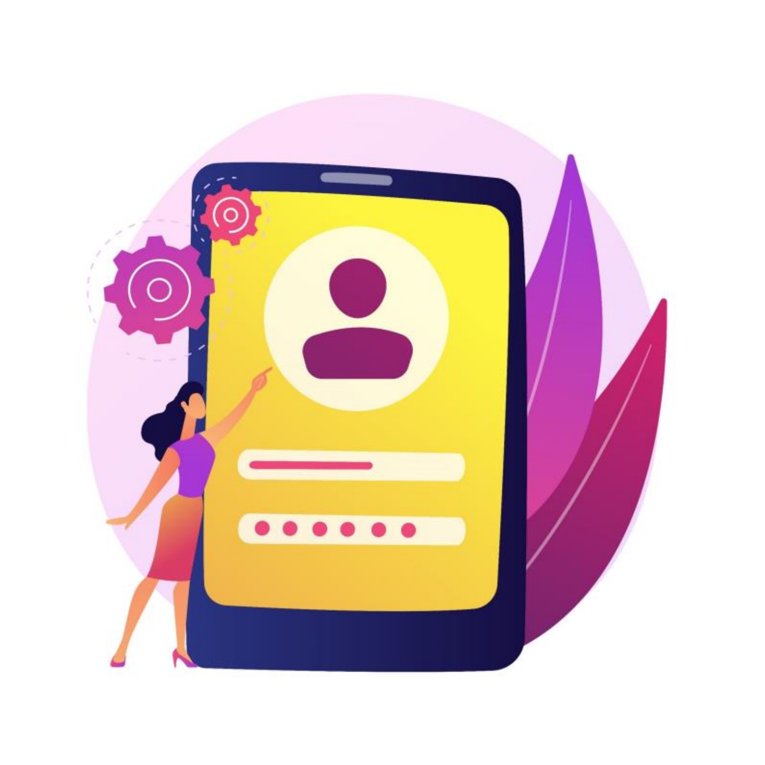
Multiple Factor Authentication

Presentation for the course
«Applied Cryptography» (prof. Ranise)

Leonardo Errati, UniTN
MSc Cryptography

1. User authentication
2. Simple authentication
3. Multi-Factor authentication
4. Security of MFA

User authentication



User authentication problem: an user accessing a resource claims to possess an identity, how to check?
- we need to transfer credentials
- only allow access to authorised users AND only to resources they are authorised to access

1. *Identification*
2. *Authentication*
3. *Authorisation*

Zurko, Simon (1996): *«mechanisms and models that are confusing to the user will be misused»*.

Example: passwords

we build *trust* (how?)

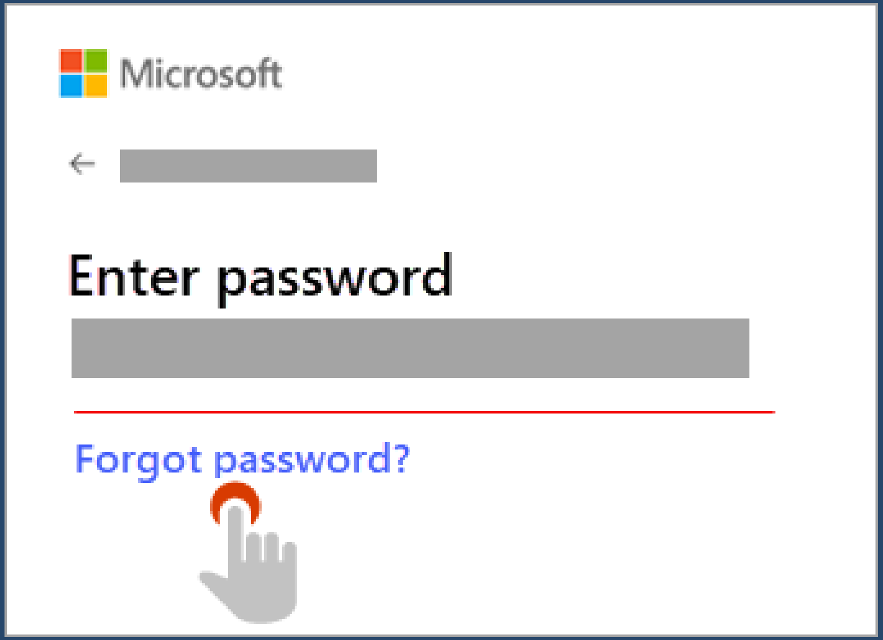
PASSWORDS: trust granted if you know something we agreed on before

PROS:

- only one exchange
- can be stored hashed

CONS:

- threat model outdated
- scaling



Microsoft

← [redacted]

Enter password

[redacted]

Forgot password?

Example: passwords

we build *trust* ***via EVIDENCE***

PASSWORDS: trust granted if you know something we agreed on before

PROS:
- only one exchange
- can be stored hashed

CONS:
- threat model outdated
- scaling
- **what if leaked?**

Example: passwords

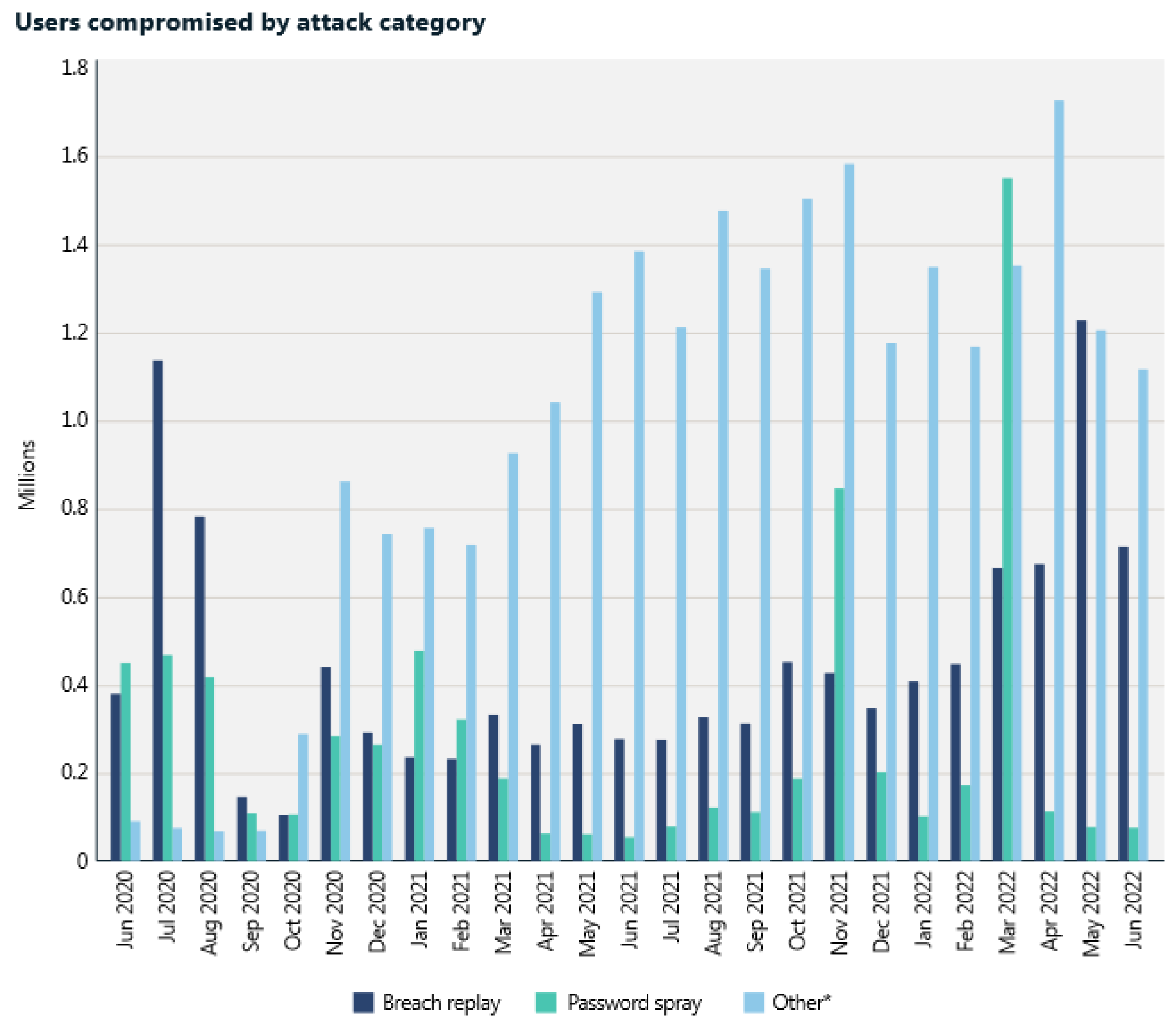
user auth → **simple auth** → MFA → security of MFA

REAL WORLD

Microsoft

Microsoft Digital Defense Report 2022

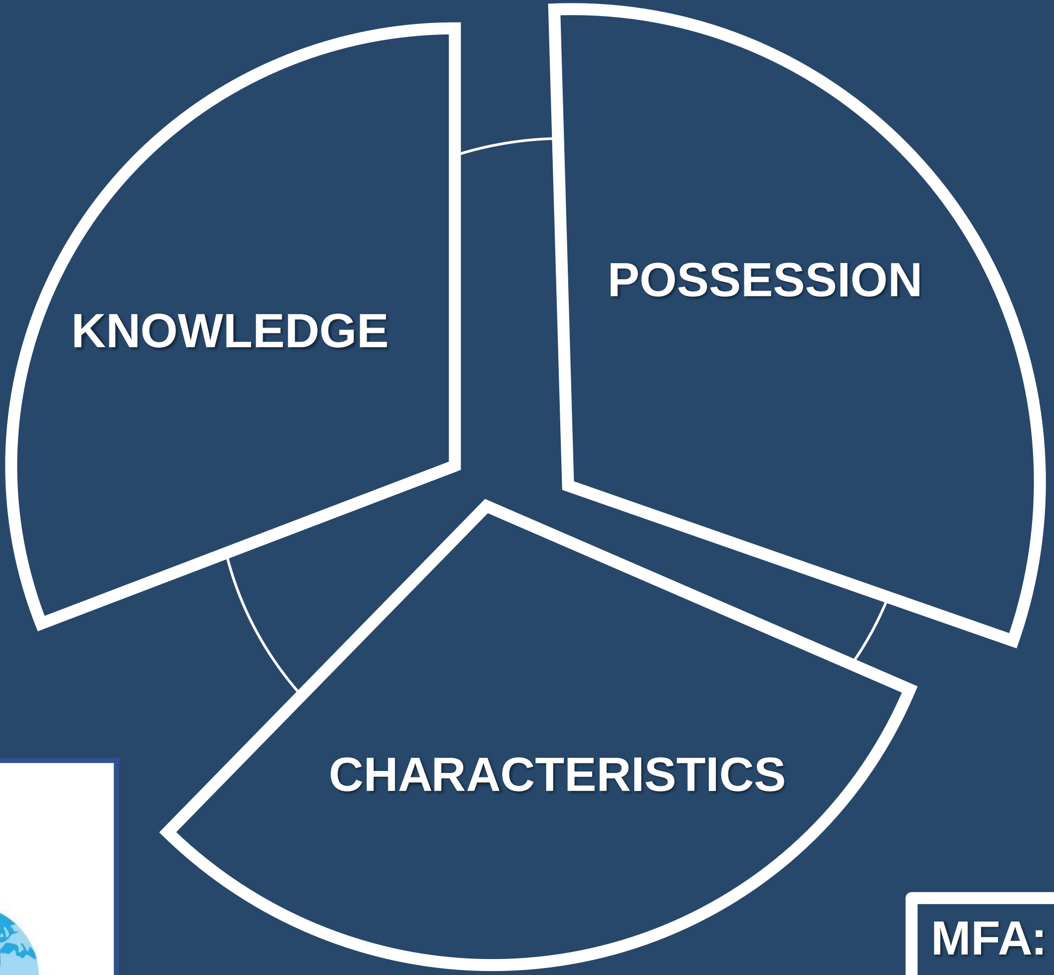
- 921 password attacks per second
- 70% more than 2021
- 20% use the same username and password for different platforms



Users compromised by attack category

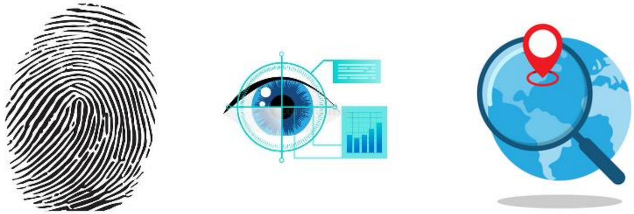
MFA

«something you know»



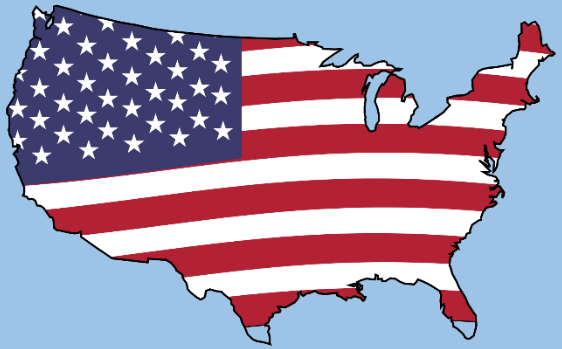
«something you have»

«something you are»



MFA: trust is granted with more than one factor

Regulation for MFA



USA

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

(NIST SP 800-63A,B,C)

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

(and more…)

EU

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

European Commission

(and more…)

- study of threat data
- recommendations
- regulations

Choosing factors

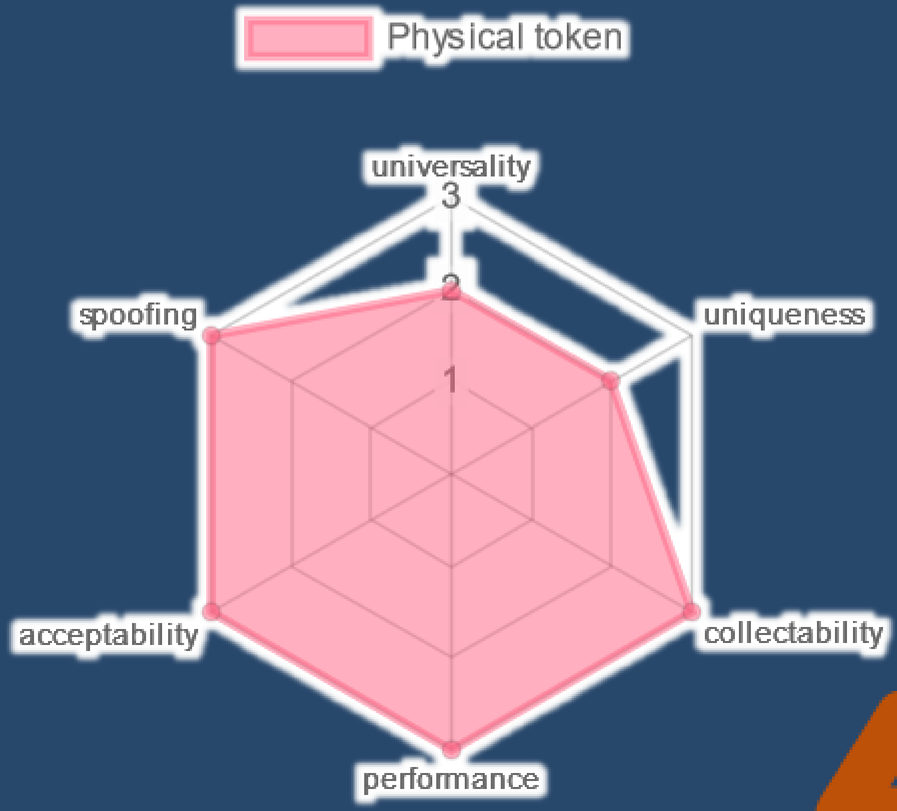
«OLD» STANDARD

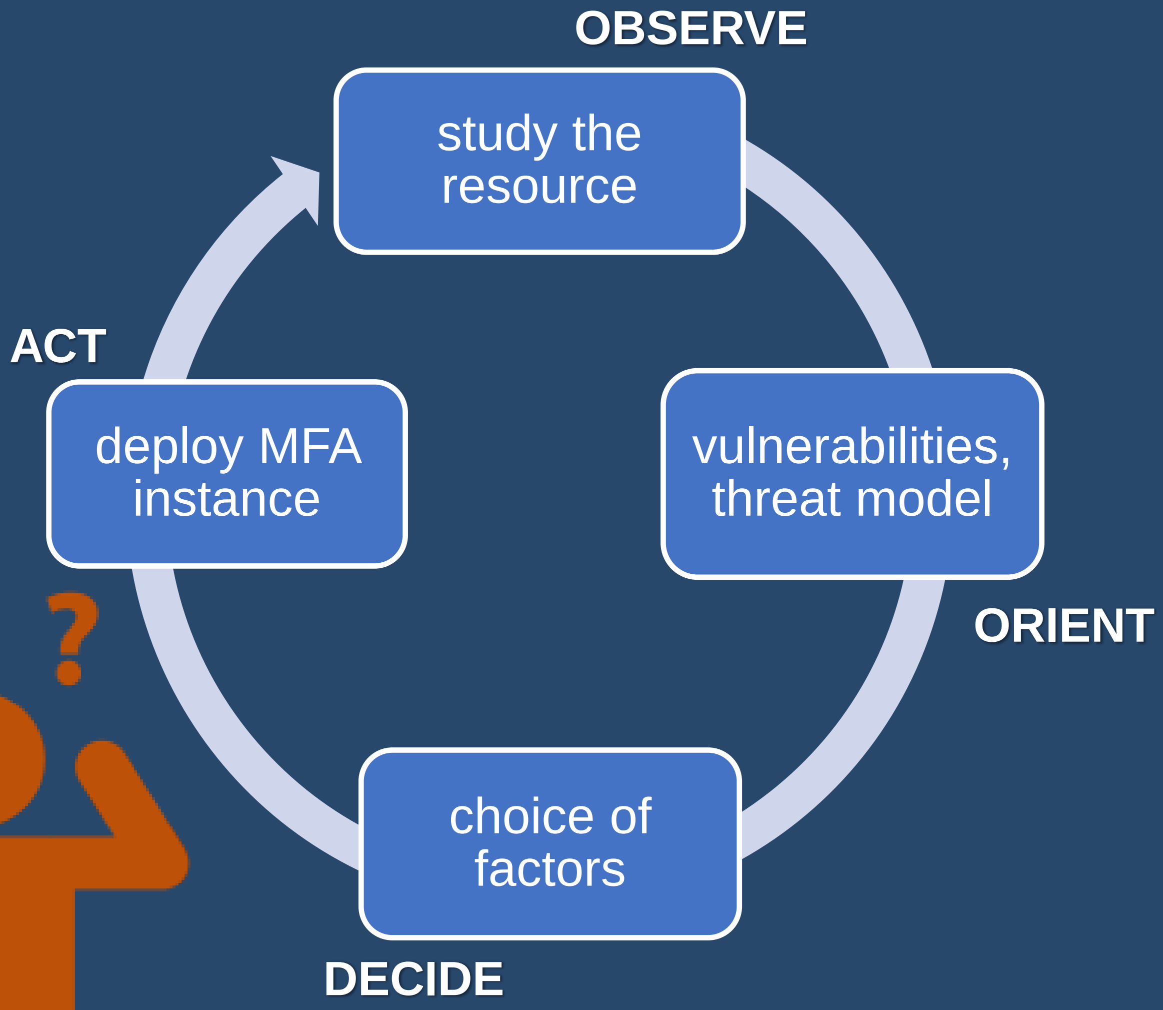
- built-in clock, hardcoded seed
- central server (RSA Authentication Manager)
- protection from replay attacks
- vulnerable to MITM attacks

«NEW» STANDARD *(U2F)*

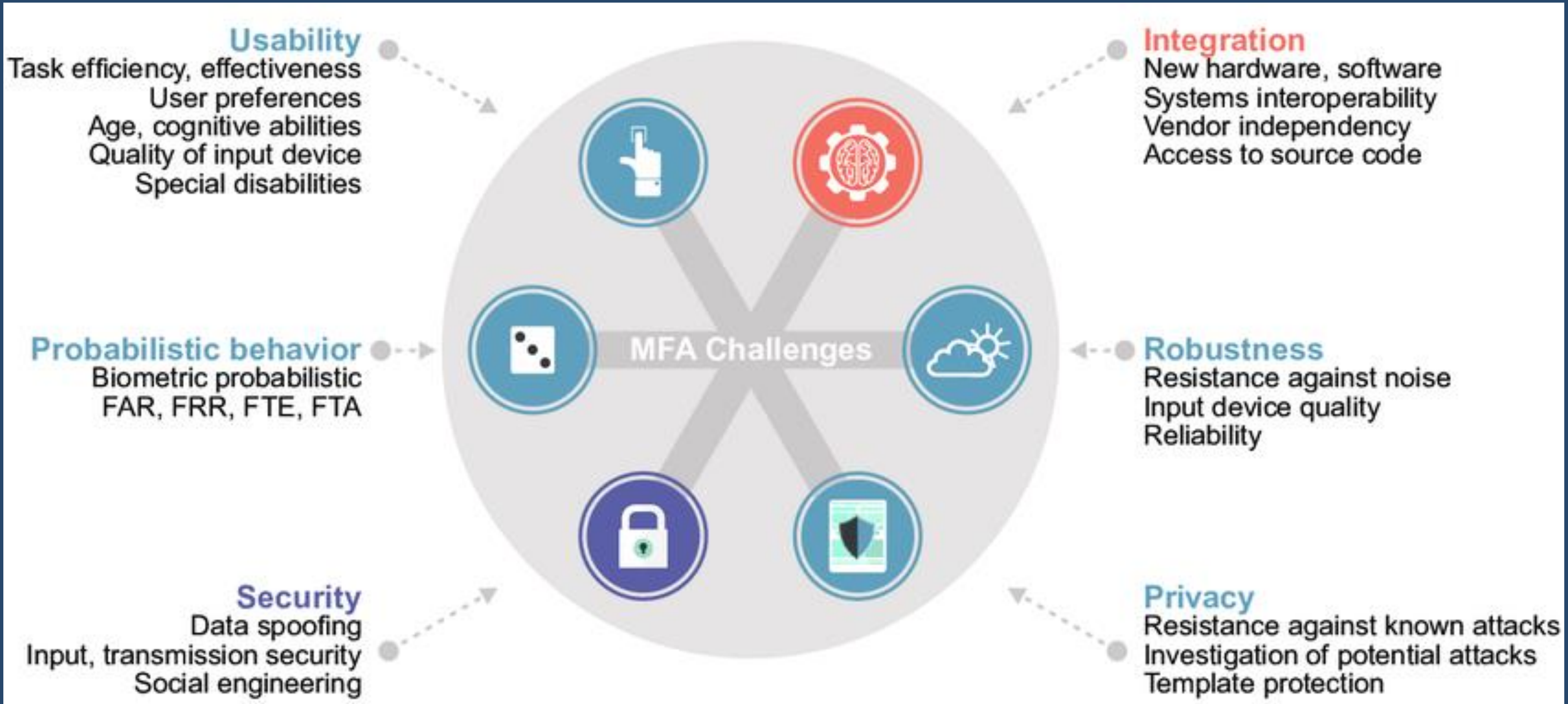
- USB (some also enable NFC)
- exploits HID protocol (no special software!)
- shared secret is NOT backed up
- challenge-response is signed (no MITM)

Choosing factors





Limits of MFA



Usability
Task efficiency, effectiveness
User preferences
Age, cognitive abilities
Quality of input device
Special disabilities

Integration
New hardware, software
Systems interoperability
Vendor independency
Access to source code

Probabilistic behavior
Biometric probabilistic
FAR, FRR, FTE, FTA

Robustness
Resistance against noise
Input device quality
Reliability

Security
Data spoofing
Input, transmission security
Social engineering

Privacy
Resistance against known attacks
Investigation of potential attacks
Template protection

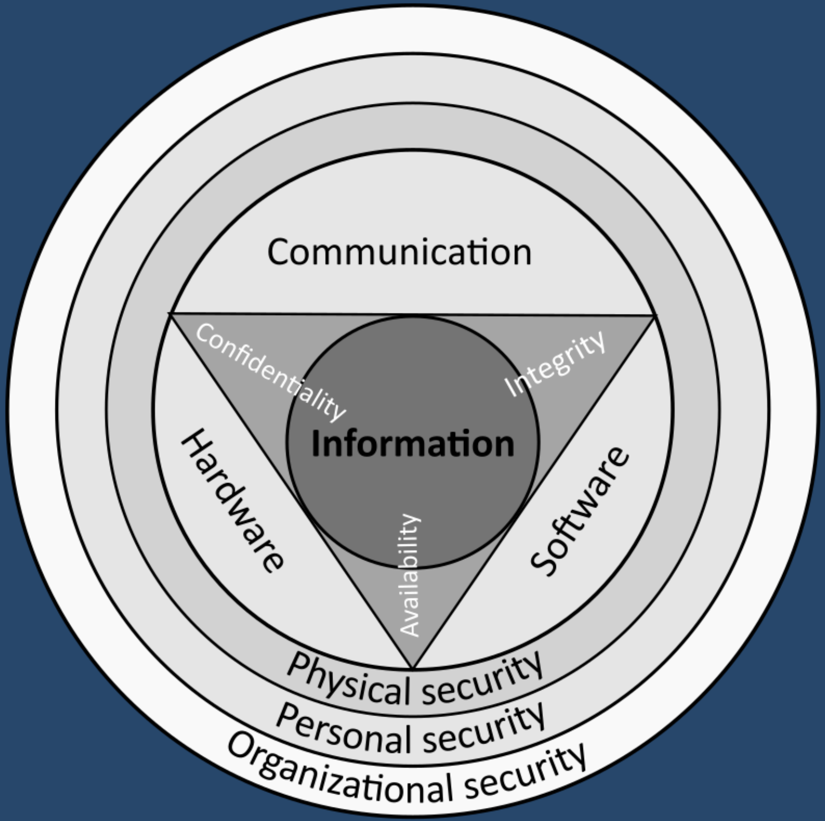
TAKE AWAYS

1. **User authentication problem**
   - the example of passwords: we build trust via evidence

2. **Multiple Factor Authentication (MFA)**
   - factors can be of various nature
   - in EU, ENISA provides guidelines and EU directives require it in some cases

3. **How do I implement MFA?**
   - what level of security does the organisation have?
   - is MFA easy to use in our context?
   - how much would it cost to implement it?

Information security

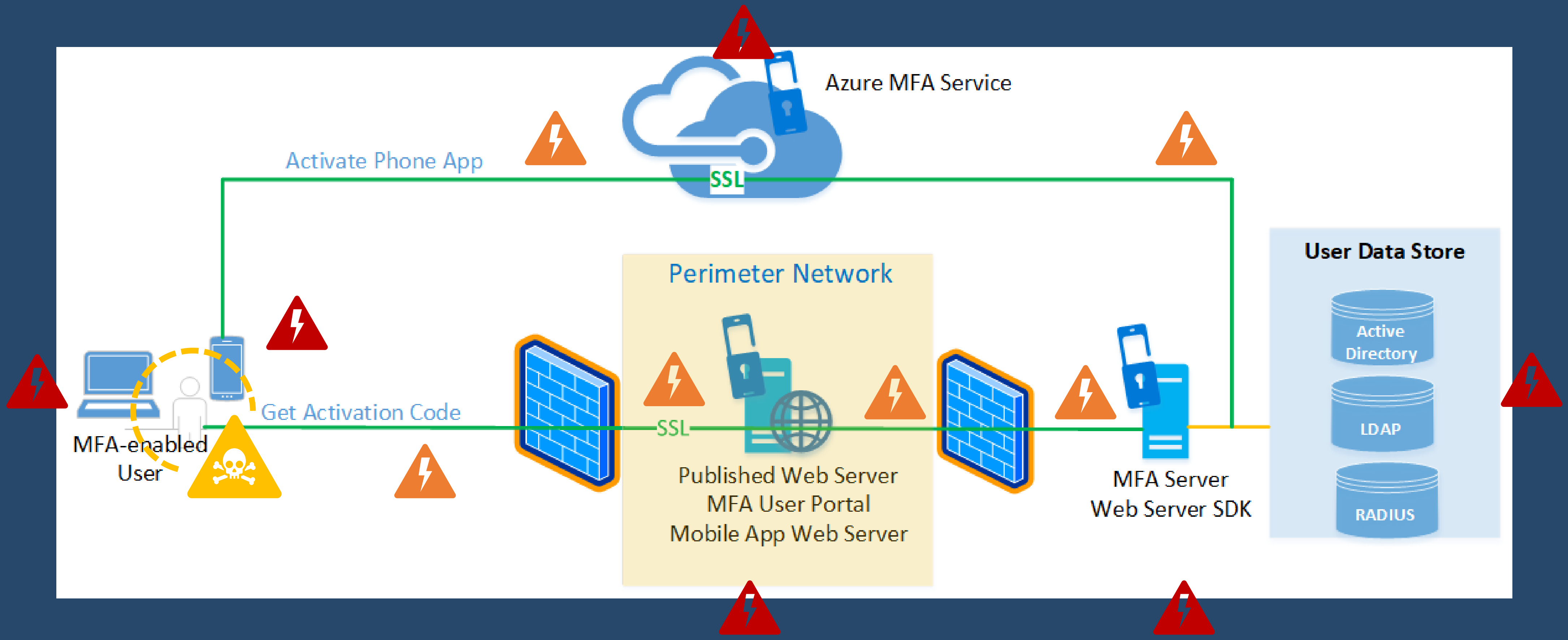


Information security:
Defined via its key attributes Confidentiality, Integrity, Availability.

User authentication is key in access control mechanisms.
A threat in AC mechanisms could hinder C, I and A.

What is our threat model?

Information security



Attacks can target **resources** or **data transmission**.
The most dangerous ones (easier to perform, more rewarding) target **users**.

ATTACK: side channel

user auth → simple auth → MFA → **security of MFA**

REAL WORLD

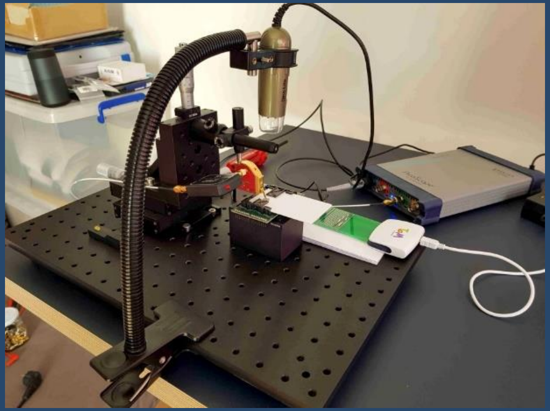
<u>physical token factors</u>

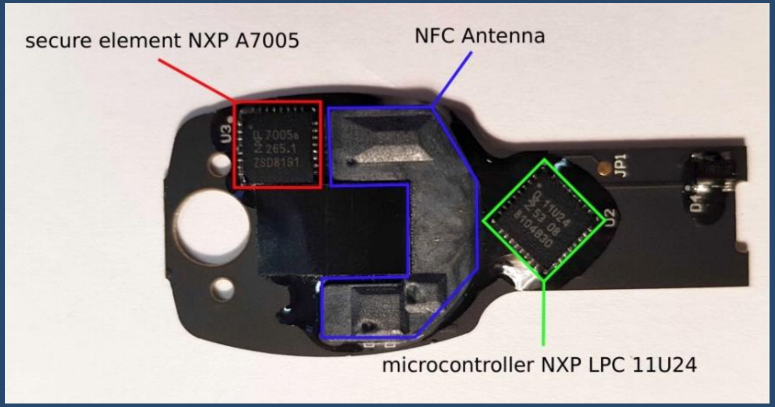
PROS:

- easy to use
- availability

CONS:

- cost and setup phase
- recent introduction (scarce support)





Google Titan Key

<u>Full reconstruction of ECDSA secret key</u> after 6000 operations of NXP A7005a microcontroller.

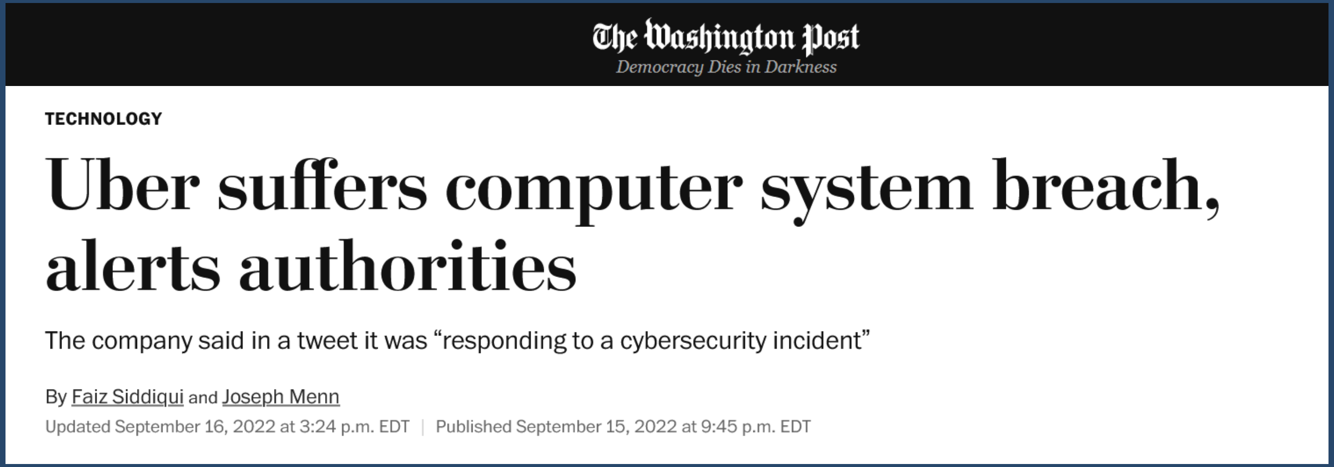
Implementation choices are important too.

Leonardo Errati (UniTN), MSc Cryptography

ATTACK: exhaustion

user auth → simple auth → MFA → **security of MFA**

REAL WORLD



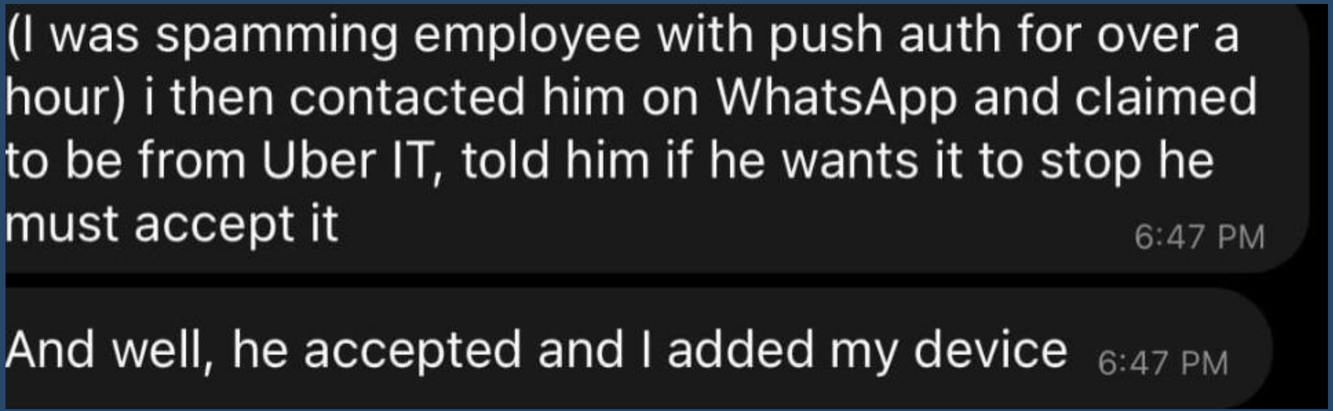
The Washington Post
Democracy Dies in Darkness

TECHNOLOGY

Uber suffers computer system breach, alerts authorities

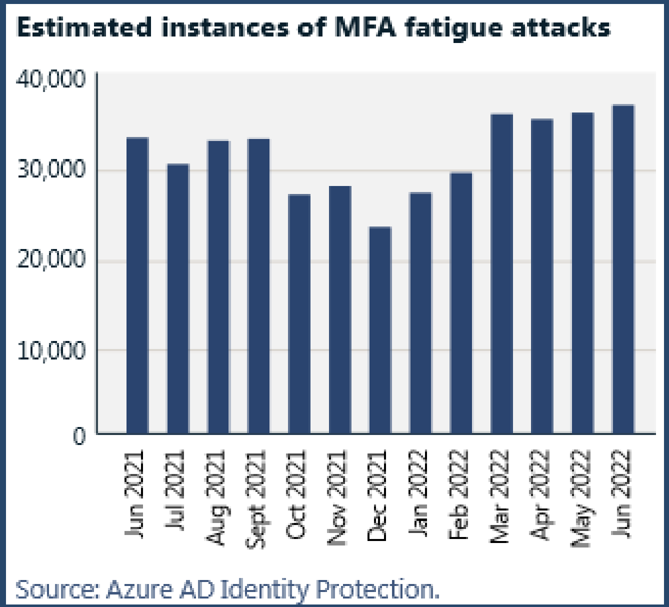
The company said in a tweet it was “responding to a cybersecurity incident”

By Faiz Siddiqui and Joseph Menn
Updated September 16, 2022 at 3:24 p.m. EDT | Published September 15, 2022 at 9:45 p.m. EDT



(I was spamming employee with push auth for over a hour) i then contacted him on WhatsApp and claimed to be from Uber IT, told him if he wants it to stop he must accept it 6:47 PM

And well, he accepted and I added my device 6:47 PM



Estimated instances of MFA fatigue attacks

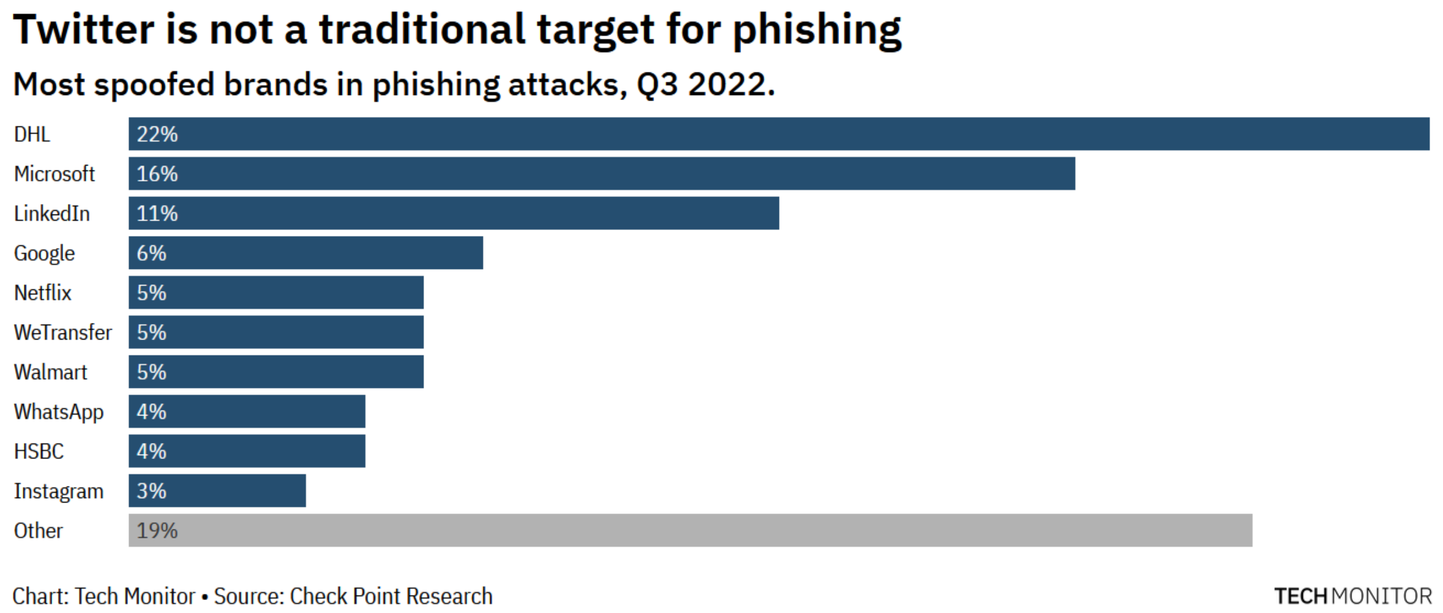
Source: Azure AD Identity Protection.

MFA exhaustion: send multiple MFA requests to the victim’s device, it could accept inadvertently or as a result of fatigue

Use Context Aware Authentication, limiting requests, etc.

REAL WORLD

Can’t hide behind MFA when users are the vulnerability.
Training and education are of paramount importance.

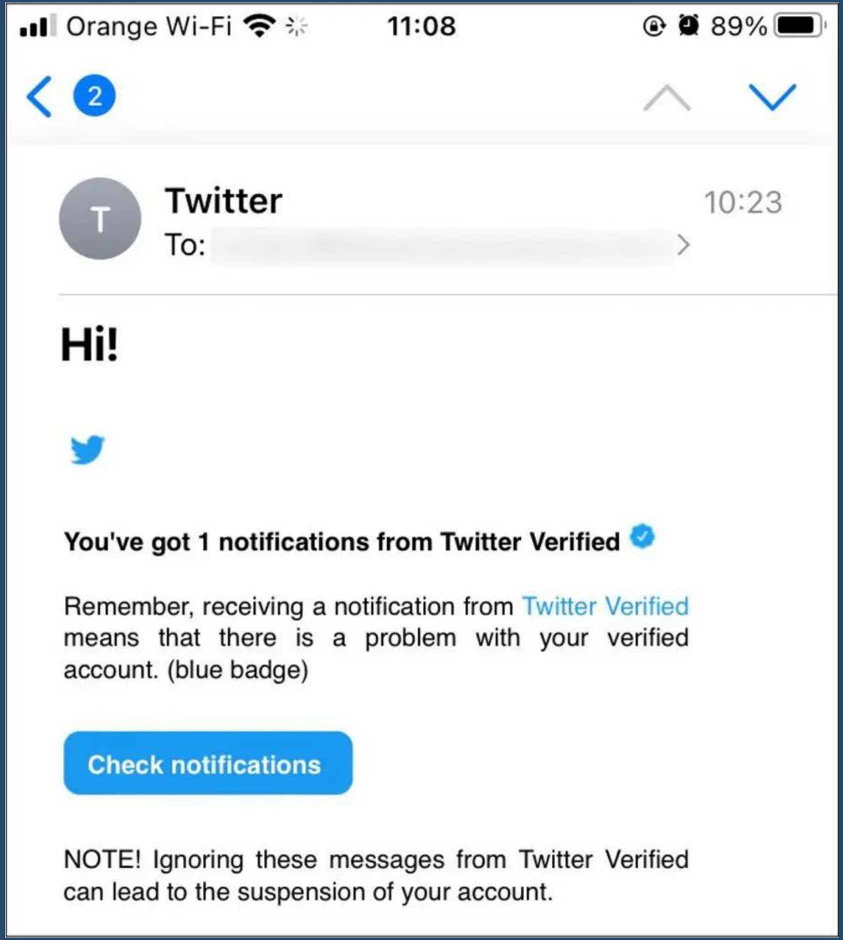


Twitter is not a traditional target for phishing

Most spoofed brands in phishing attacks, Q3 2022.

Chart: Tech Monitor • Source: Check Point Research

TECHMONITOR



Twitter
To: [redacted]
10:23

Hi!

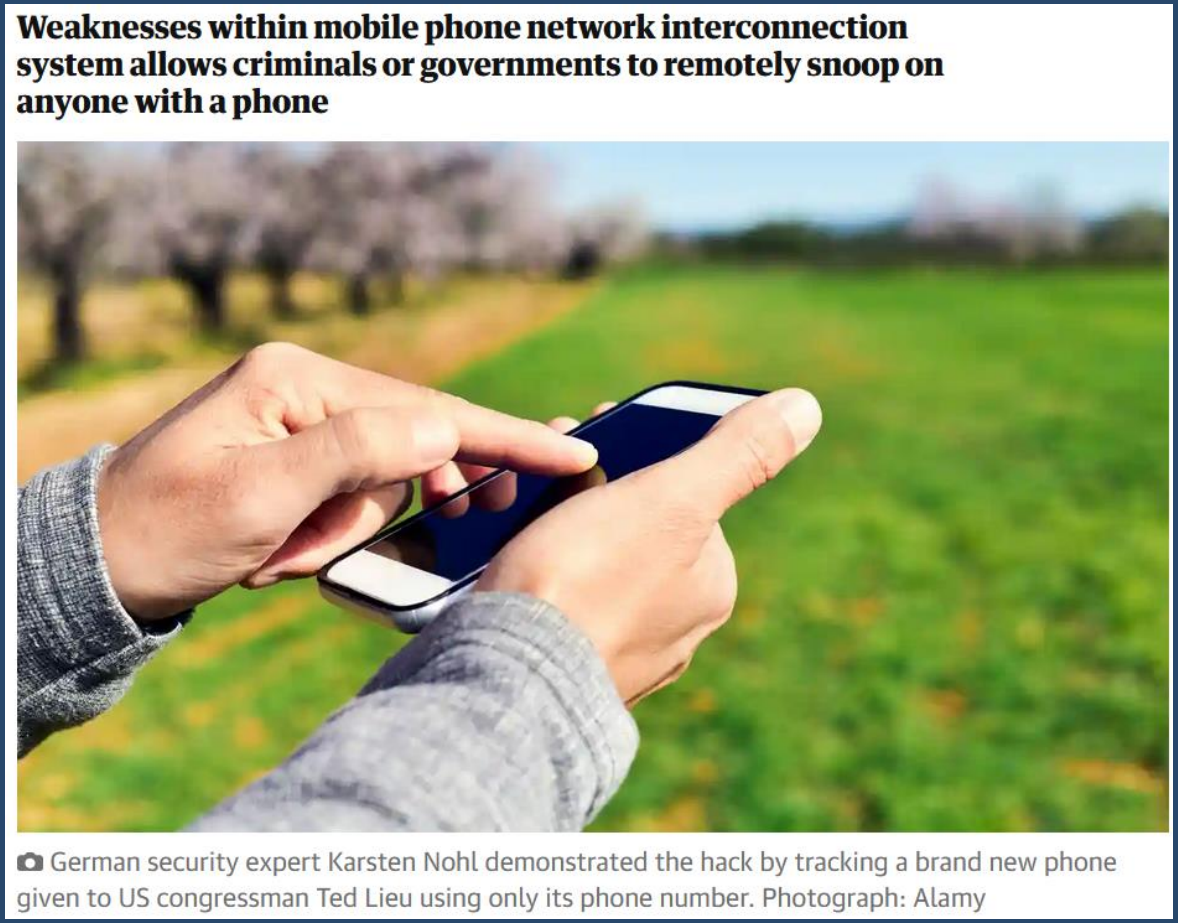
You've got 1 notifications from Twitter Verified

Remember, receiving a notification from Twitter Verified means that there is a problem with your verified account. (blue badge)

NOTE! Ignoring these messages from Twitter Verified can lead to the suspension of your account.

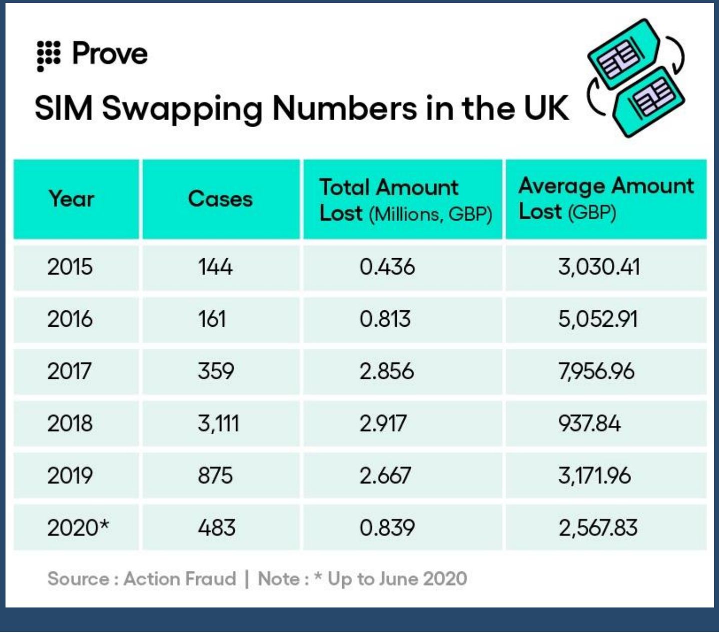
ATTACK: SMS factors

REAL WORLD



Weaknesses within mobile phone network interconnection system allows criminals or governments to remotely snoop on anyone with a phone

German security expert Karsten Nohl demonstrated the hack by tracking a brand new phone given to US congressman Ted Lieu using only its phone number. Photograph: Alamy



Prove

SIM Swapping Numbers in the UK

Year	Cases	Total Amount Lost (Millions, GBP)	Average Amount Lost (GBP)
2015	144	0.436	3,030.41
2016	161	0.813	5,052.91
2017	359	2.856	7,956.96
2018	3,111	2.917	937.84
2019	875	2.667	3,171.96
2020*	483	0.839	2,567.83

Source : Action Fraud | Note : * Up to June 2020

SMS-based factors

PROS:

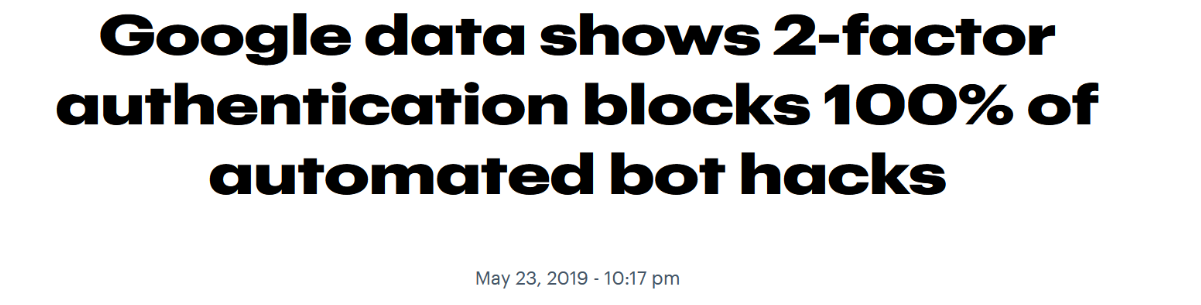
- software is relatively easy to create (w.r.t. apps)
- availability

CONS:

- only online, NO offline
- SIM swap attack
- **Signaling System 7 Vulnerability**

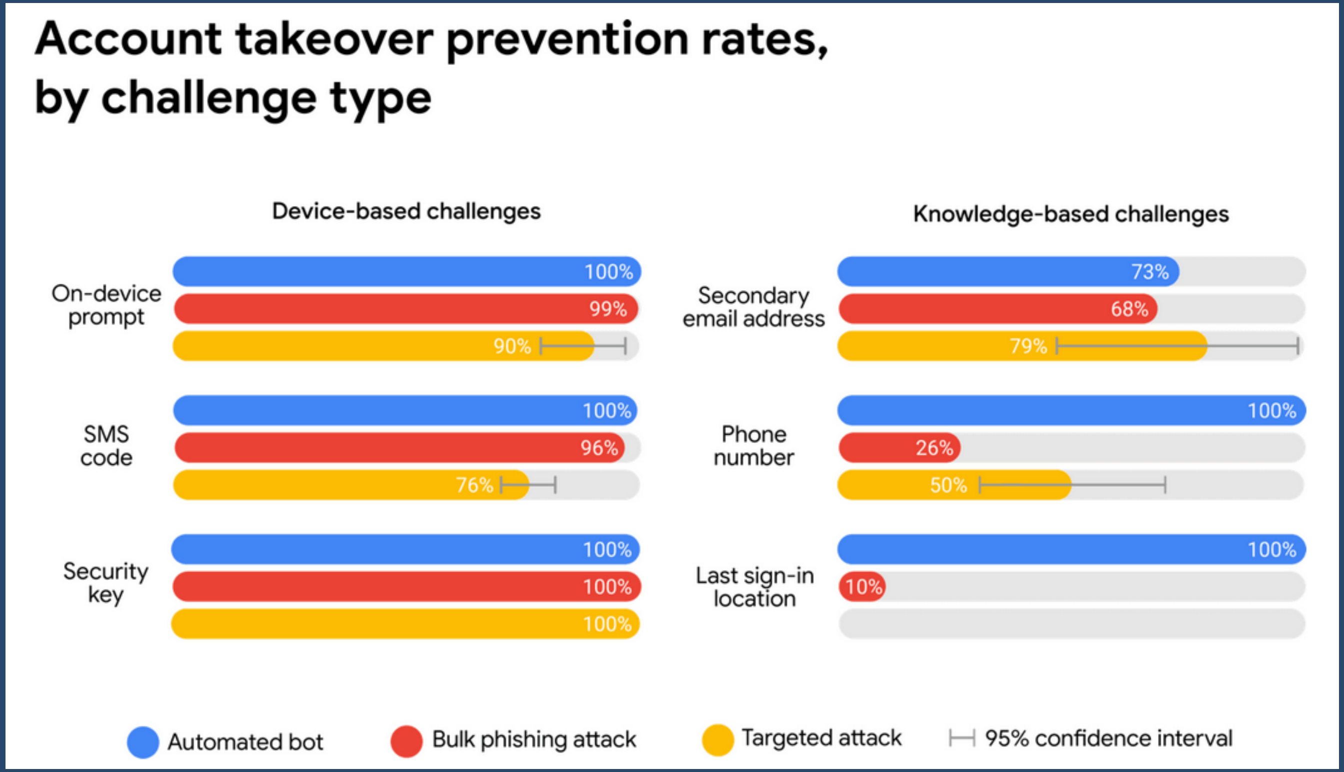
MFA in the wild

REAL WORLD



Google data shows 2-factor authentication blocks 100% of automated bot hacks

May 23, 2019 - 10:17 pm



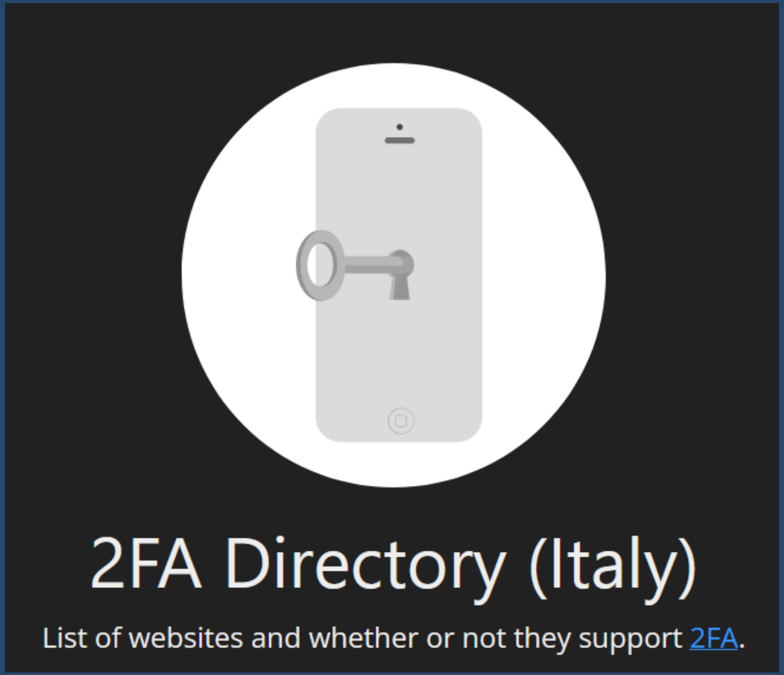
Account takeover prevention rates, by challenge type

Location: good but tamperable
SMS: still strong despite vulnerabilities
Security key: very strong, but there could be bias
Device prompt: users pay more attention

MFA in the wild

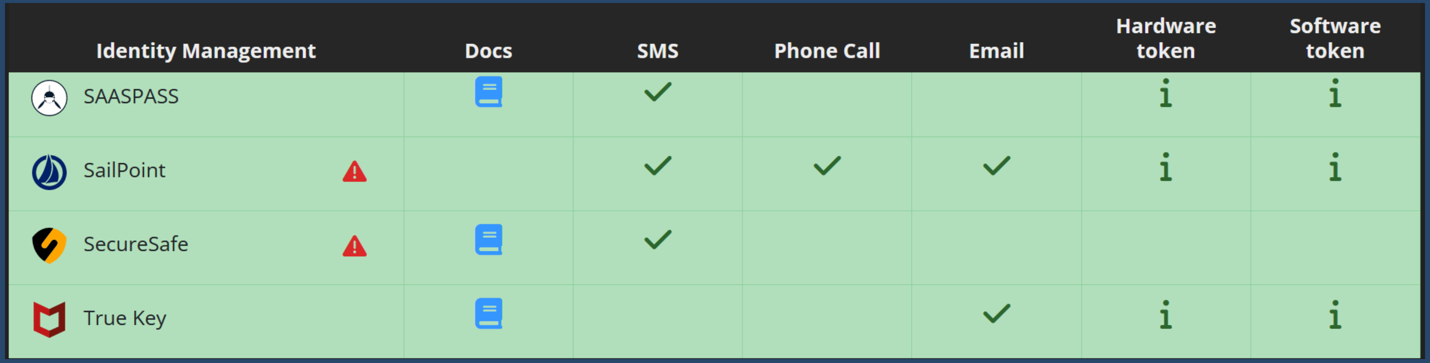
REAL WORLD

https://2fa.directory/it/

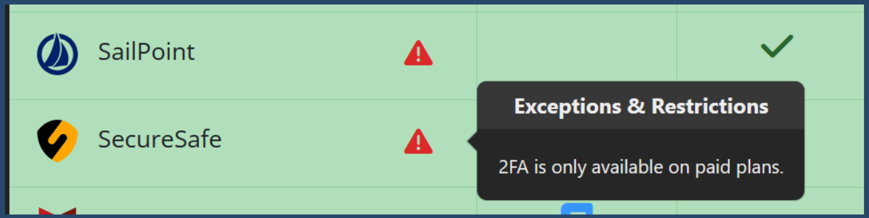


2FA Directory (Italy)

List of websites and whether or not they support 2FA.



Identity Management	Docs	SMS	Phone Call	Email	Hardware token	Software token
SAASPASS	📘	✓			i	i
SailPoint ⚠		✓	✓	✓	i	i
SecureSafe ⚠	📘	✓				
True Key	📘			✓	i	i



SailPoint ⚠		✓
SecureSafe ⚠		

Exceptions & Restrictions

2FA is only available on paid plans.

TAKE AWAYS

1. **Stronger is not better**
   - there are always trade-offs
   - don’t forget availability

2. **MFA is not invincible**
   - does not eliminate risk, but decreases it
   - does not protect everything

3. **Educate**
   - all users must be aware of good and bad practices
   - user input in design phase

Only in ancient legends:

One MFA to rule them all, One MFA to find them,
One MFA to bring them all, and in Security bind them,
In the Land of Access where Users lie.

Thank you for your attention.

Leonardo Errati (UniTN), MSc Cryptography
leonardo.errati@studenti.unitn.it

SOURCES

Authentication and passwords:

- https://www.techtarget.com/searchsecurity/definition/user-authentication
- https://www.cnbc.com/2022/11/21/why-microsofts-hack-data-means-you-may-need-new-login-passwords.html
- https://iteo.com/blog/post/identity-protection-multi-factor-authentication/
- https://www.zdnet.com/article/password-hacking-attacks-are-on-the-rise-heres-how-to-stop-your-accounts-from-being-stolen/

MFA definition and implementation:

- *ENISA Joint Publication - Enhanced Resilience (14 February 2022) & ENISA Threat Landscape 2022*
- *Microsoft Digital Defence Report 2022*
- *A method of risk assessment for Multi-Factor Authentication (Kim, Hong, 2011)*
- *A comprehensive study on multifactor authentication schemes (Abhishek, Roshan, Kimar, Ranjan, 2013)*
- https://www.bromba.com/knowhow/BiometricFailureRates.htm
- https://conetrix.com/blog/the-challenges-of-multifactor-authentication
- https://pages.nist.gov/800-63-3/
- https://en.wikipedia.org/wiki/Universal_2nd_Factor
- https://en.wikipedia.org/wiki/FIDO2_Project
- https://www.scmagazine.com/perspective/identity-and-access/three-questions-to-ask-when-setting-up-mfa%EF%BF%BC
- https://conetrix.com/blog/the-challenges-of-multifactor-authentication

SOURCES

Attacks part 1:

- *Multi-Factor Authentication: a survey (Ometov et al., 2018)*
- *Vulnerabilities of Multi-Factor Authentication in modern computer networks (Tolbert, Hess, Nascimento, 2021)*
- *Poster: user awareness of phishing and WebAuthn (Tran, Amft, Wermke, 2022)*
- *A usability study for five Two-Factor Authentication methods (Reese et al., Symposium of usable privacy and security, 2019)*
- *The great authentication fatigue and how to overcome it (Sasse, Steves, Krol, Chisnell, 2014)*
- *How mandatory second factor affects the authentication user experience (Abbott, Patil, 2020)*
- https://www.zdnet.com/article/new-side-channel-attack-can-recover-encryption-keys-from-google-titan-security-keys/
- https://arstechnica.com/information-technology/2021/01/hackers-can-clone-google-titan-2fa-keys-using-a-side-channel-in-nxp-chips/
- https://www.bleepingcomputer.com/news/security/uber-hacked-internal-systems-breached-and-vulnerability-reports-stolen/
- https://www.bleepingcomputer.com/news/security/mfa-fatigue-attacks-are-putting-your-organization-at-risk/

SOURCES

Attacks part 2:

- https://www.helpnetsecurity.com/2022/12/08/secret-double-octopus-mfa/
- https://www.tenfold-security.com/en/mfa-fatigue/
- https://www.cisa.gov/uscert/ncas/alerts/aa22-074a
- https://www.spiceworks.com/it-security/identity-access-management/articles/5-ways-hackers-can-get-around-your-mfa-solution/
- https://thenextweb.com/news/google-data-shows-2-factor-authentication-blocks-100-of-automated-bot-hacks
- https://www.avanan.com/blog/mfa-man-in-the-middle-and-you
- https://blog.knowbe4.com/many-ways-to-hack-mfa
- https://www.knowbe4.com/hubfs/12+_Ways_to_Hack_Two-Factor_Authentication-1.pdf
- https://www.theguardian.com/technology/2016/apr/18/phone-number-hacker-read-texts-listen-calls-track-you