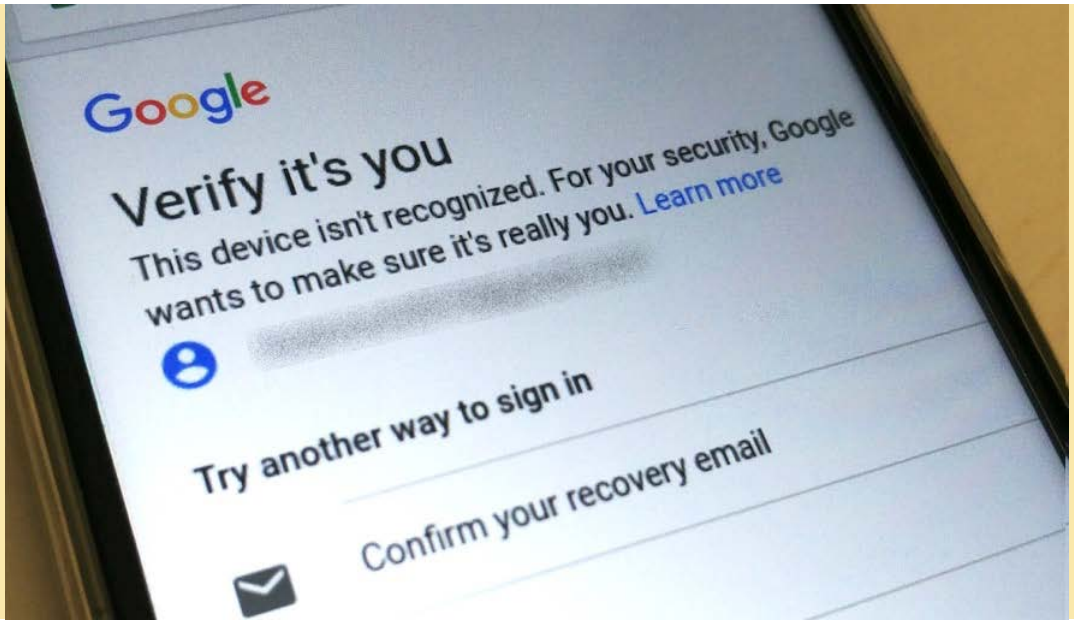
Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences

RUHR
UNIVERSITÄT
BOCHUM

RUB

UNC CHARLOTTE



Evaluation of Risk-based Re-Authentication Methods

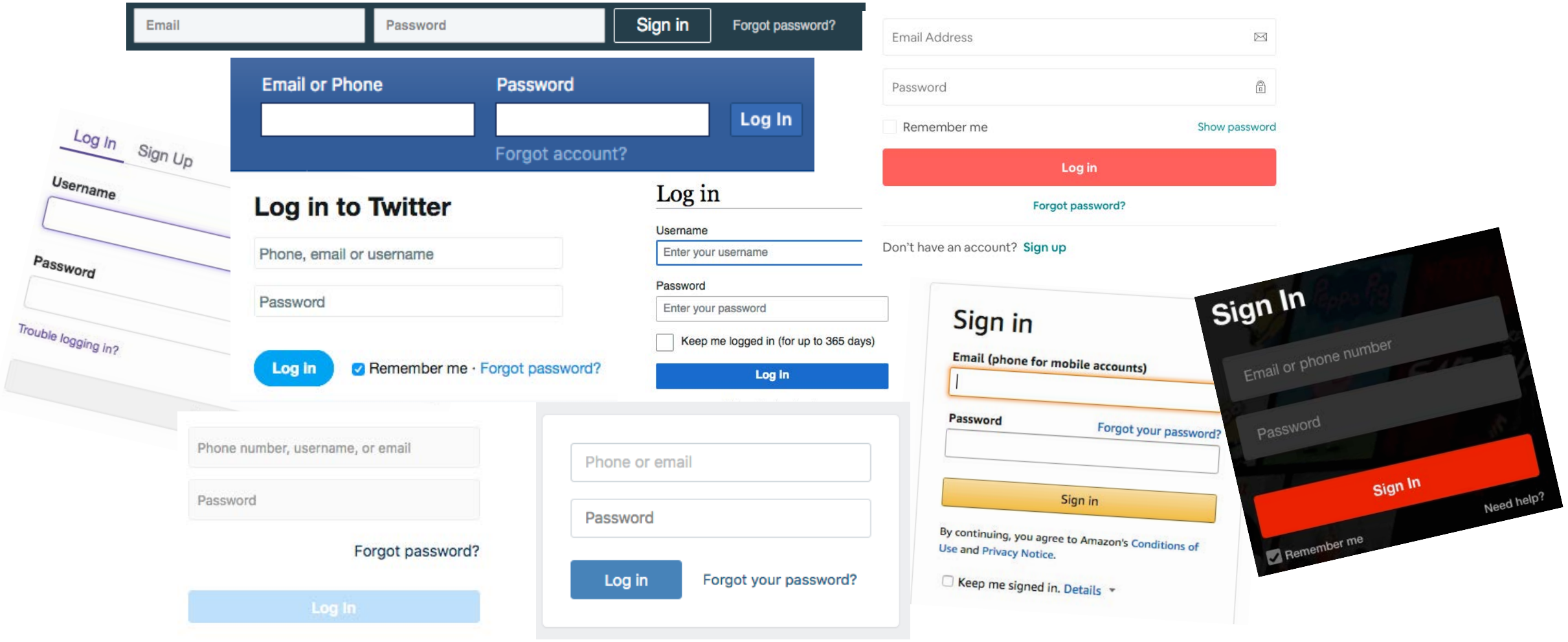
Stephan Wiefling*#, Tanvi Patil+, Markus Dürmuth#, Luigi Lo Iacono*

H-BRS University of Applied Sciences (*)

Ruhr University Bochum (#)

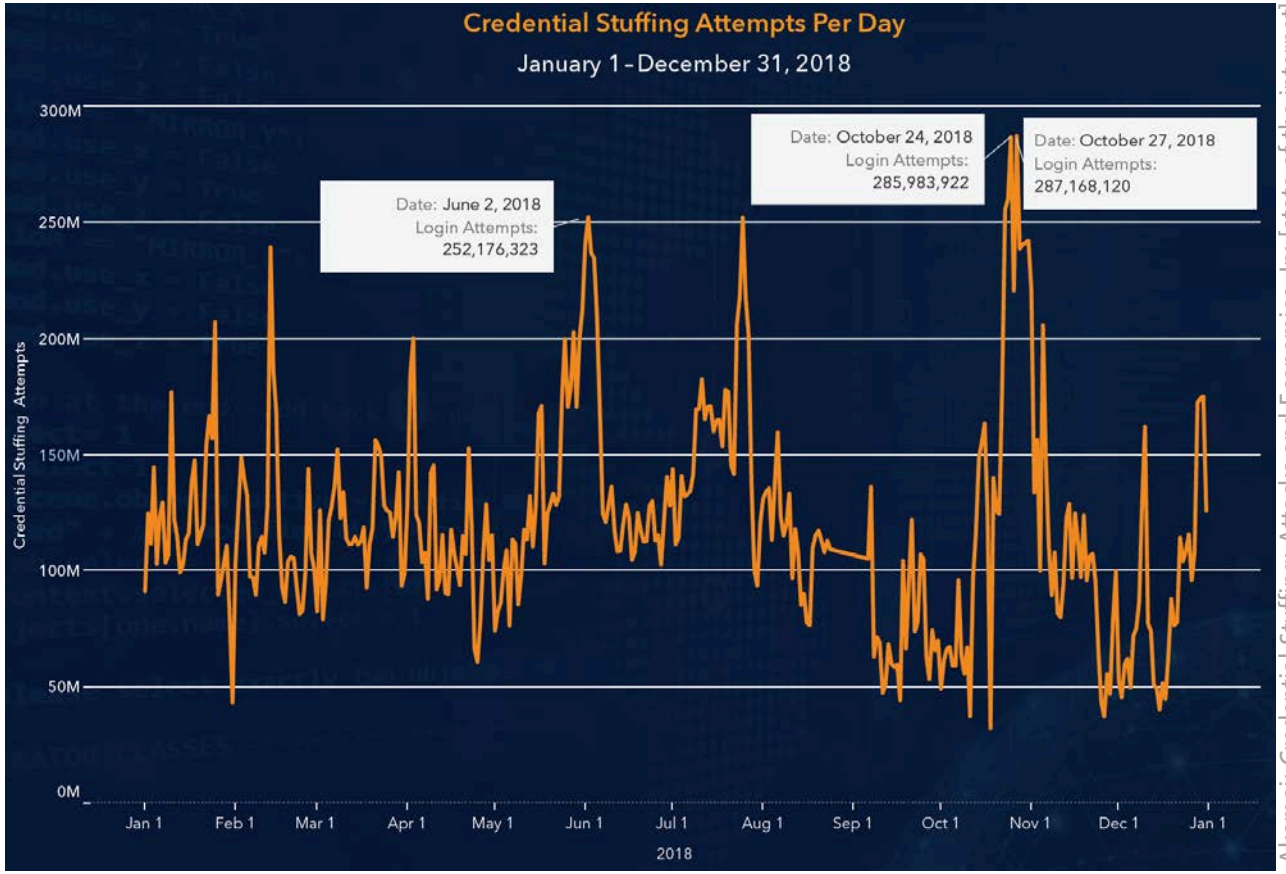
UNC Charlotte (+)

Maribor, Slovenia | IFIP SEC 2020


Email
Password
Sign in
Forgot password?
Email or Phone
Password
Log In
Forgot account?
Log In
Sign Up
Username
Password
Trouble logging in?
Log in to Twitter
Phone, email or username
Password
Log In
Remember me · Forgot password?
Log in
Username
Enter your username
Password
Enter your password
Keep me logged in (for up to 365 days)
Log in
Email Address
Password
Remember me
Show password
Log in
Forgot password?
Don't have an account? Sign up
Phone number, username, or email
Password
Forgot password?
Log In
Phone or email
Password
Log in
Forgot your password?
Sign in
Email (phone for mobile accounts)
Password
Forgot your password?
Sign in
By continuing, you agree to Amazon's Conditions of Use and Privacy Notice.
Keep me signed in. Details
Sign In
Email or phone number
Password
Sign In
Need help?
Remember me

Motivation

- Weaknesses in password-based authentication increase
- Large-scale password database leaks
  - Credential Stuffing
- Intelligent password guessing*
- Phishing



Akamai: Credential Stuffing: Attacks and Economies. In: [state of the internet] / security, vol. 5 (2019)

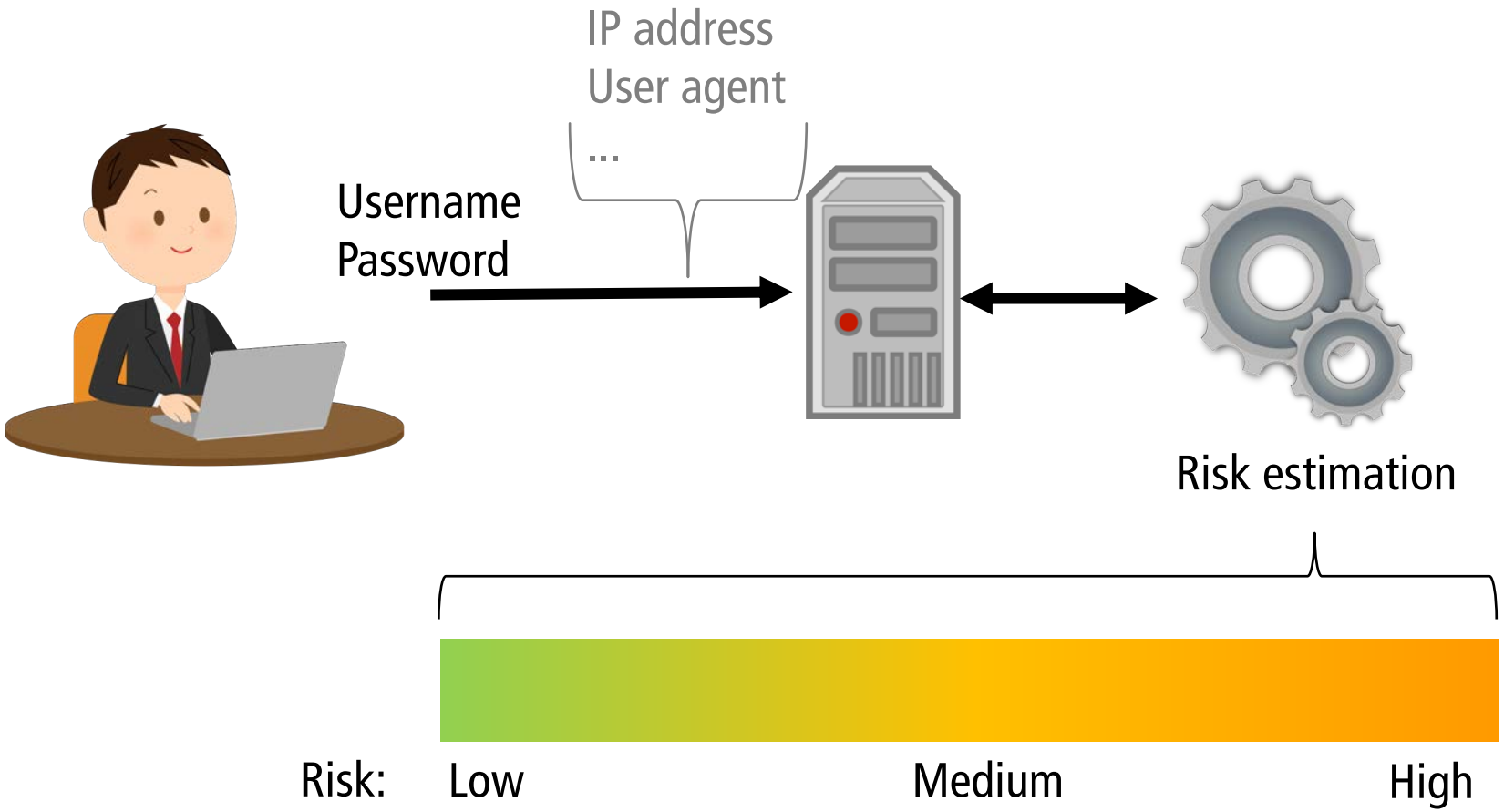
*D. Wang et al.: Targeted online password guessing: An underestimated threat. In CCS '16. ACM (2016)

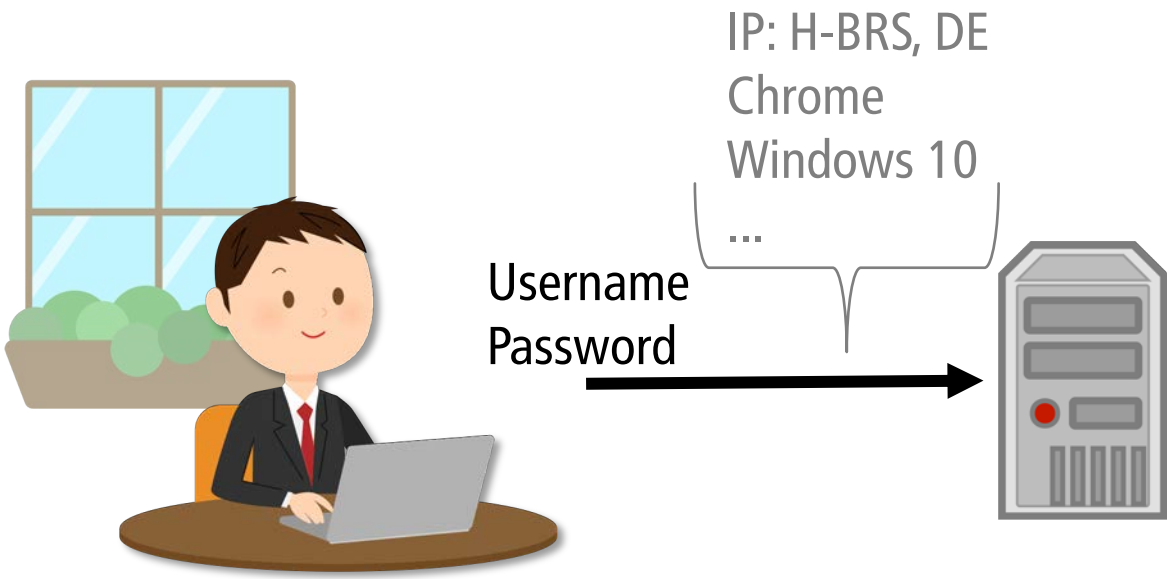
Motivation

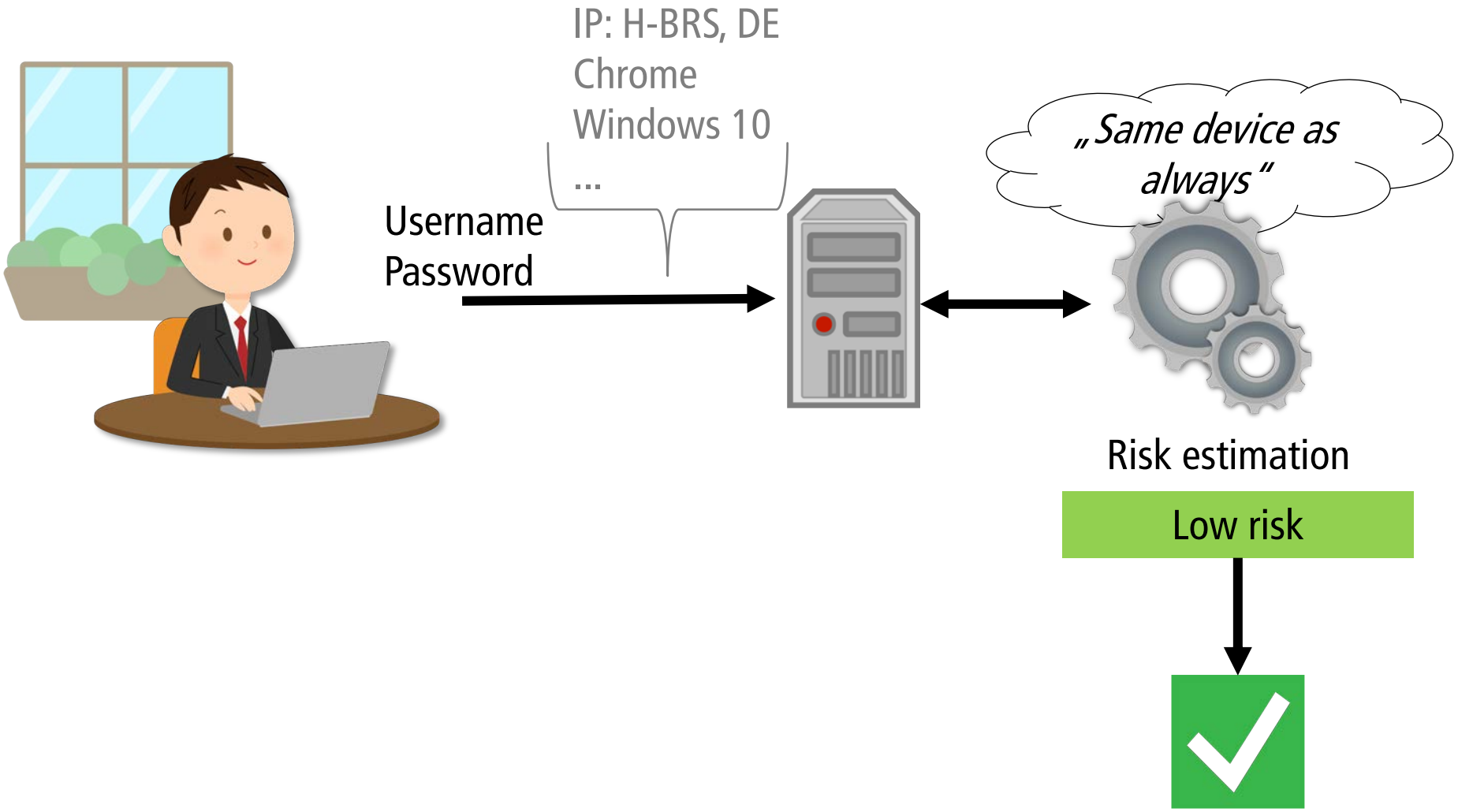
- 2FA is unpopular
- <10% of all Google accounts used 2FA in January 2018*

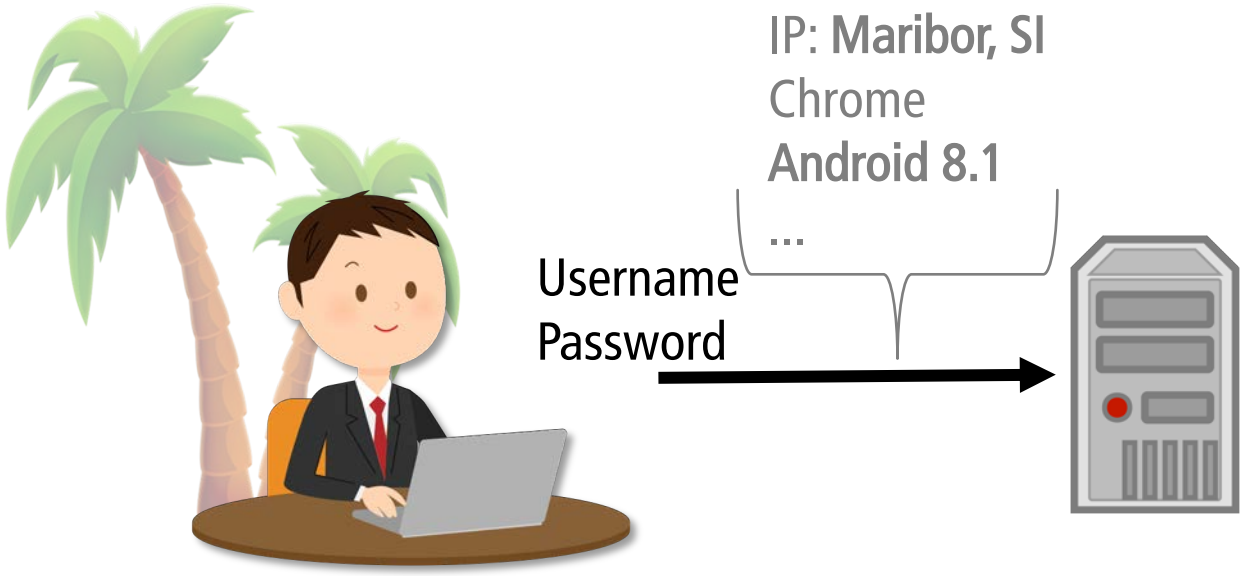
→ Using Risk-based Authentication
to increase account security
with minimal impact on user interaction

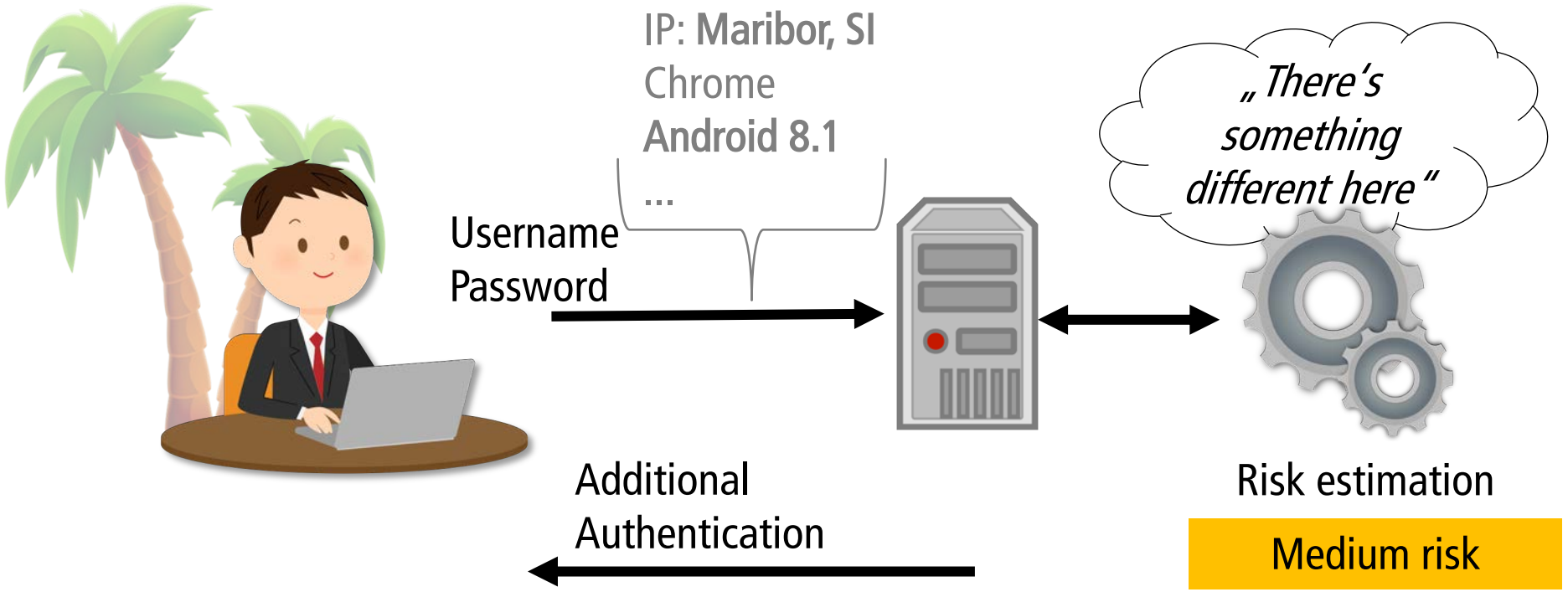
*Milka, G.: Anatomy of Account Takeover. In: Enigma 2018. USENIX (Jan 2018)


IP address
User agent
...
Username
Password
Risk estimation
Risk:
Low
Medium
High


IP: H-BRS, DE
Chrome
Windows 10
...
Username
Password

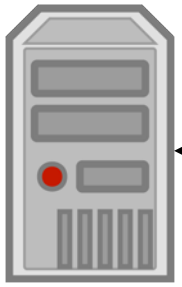

IP: H-BRS, DE
Chrome
Windows 10
...
Username
Password
„Same device as always“
Risk estimation
Low risk

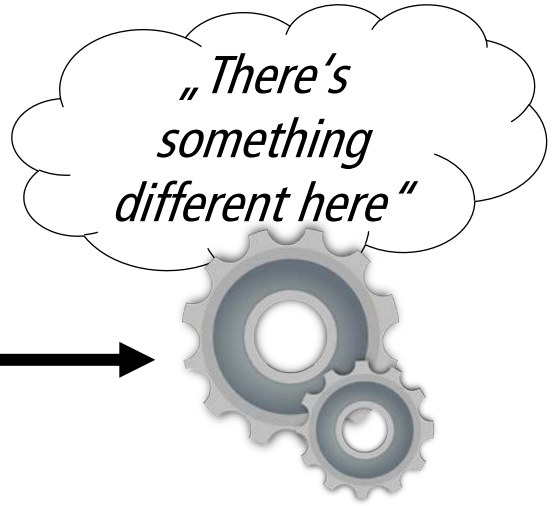

IP: Maribor, SI
Chrome
Android 8.1
...
Username
Password


IP: Maribor, SI
Chrome
Android 8.1
...
Username
Password
„ There's something different here "
Additional Authentication
Risk estimation
Medium risk

IP: **Maribor, SI**
Chrome
Android 8.1
...

Username
Password





Risk estimation

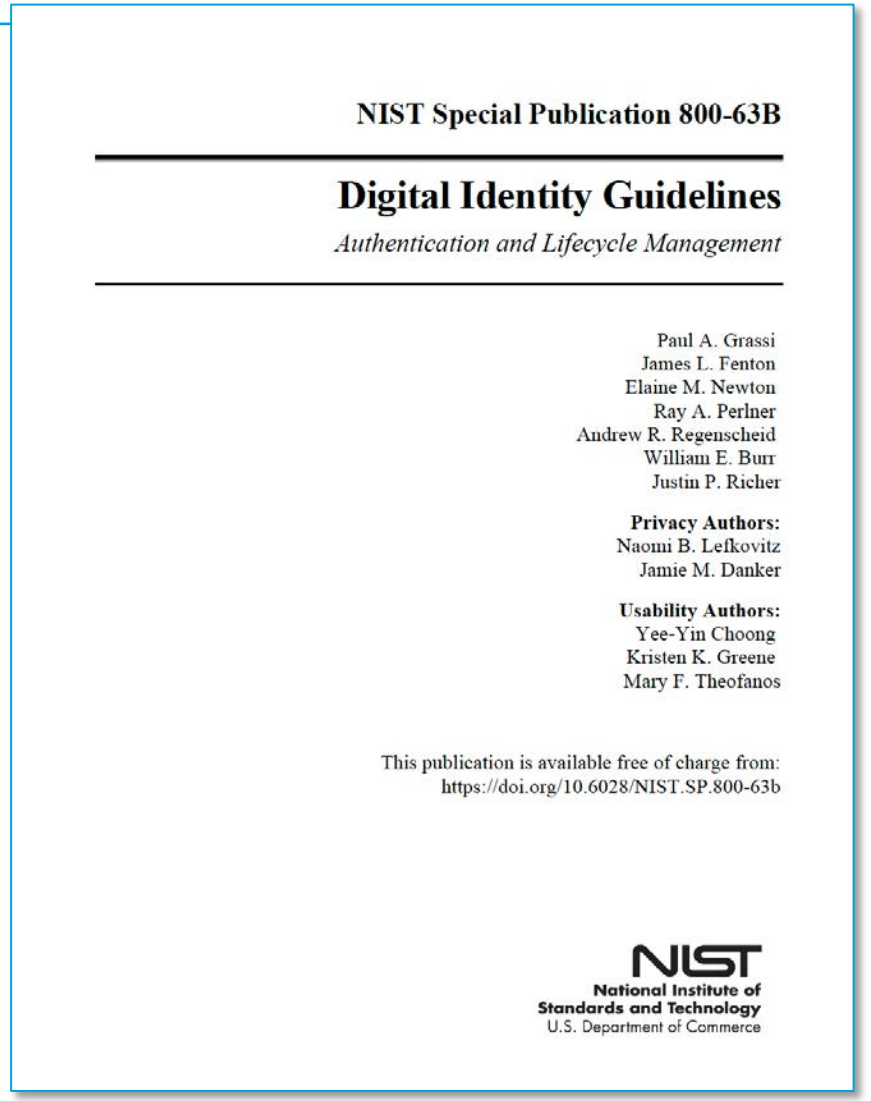
Medium risk

Additional Authentication

Proof for additional authentication

Risk-based Authentication

- Recommended by NIST digital identity guidelines[1]
- Used by large online services[2]
- More usable than comparable 2FA methods[3]



NIST Special Publication 800-63B

Digital Identity Guidelines

Authentication and Lifecycle Management

Paul A. Grassi
James L. Fenton
Elaine M. Newton
Ray A. Perlner
Andrew R. Regenscheid
William E. Burr
Justin P. Richer

Privacy Authors:
Naomi B. Lefkovitz
Jamie M. Danker

Usability Authors:
Yee-Yin Choong
Kristen K. Greene
Mary F. Theofanos

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63b

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

[1] Grassi et al.: Digital identity guidelines. Tech. Rep. NIST SP 800-63b (2017)
[2] Wiefling et al.: Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild. In: IFIP SEC '19. Springer (2019)
[3] Wiefling et al.: More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication. In: ACSAC '20. ACM (2020)

Current practice*

- Email verification
- Six digit code
  - Major impact on time exposure and usability
  - But not studied so far!

Service	Requested authentication factors
Amazon	▪ **Verification code** (**email***, text message)
Facebook	▪ Approve login on another computer ▪ Identify photos of friends ▪ Asking friends for help ▪ **Verification code** (text message)
GOG.com	▪ **Verification code** (**email**)*
Google	▪ Enter the city you usually sign in from ▪ **Verification code** (**email**, text message, app, phone call) ▪ Press confirmation button on second device
LinkedIn	▪ **Verification code** (**email**)*

*Wiefling et al.: Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild. In: IFIP SEC '19. Springer (2019)

Overview

- Study
- Results
- Conclusion

Overview

- Study
- Results
- Conclusion

Study Procedure

- 1. Registration
- 2. Login
- 3. Exit survey

Study Procedure

- 1. Registration
- **2. Login**
  - Re-Authentication requested
  - Method differed in each condition
- 3. Exit survey

Method 1: State of the Art (in use)

- Code-based method
- Code in email body

Your personal security code

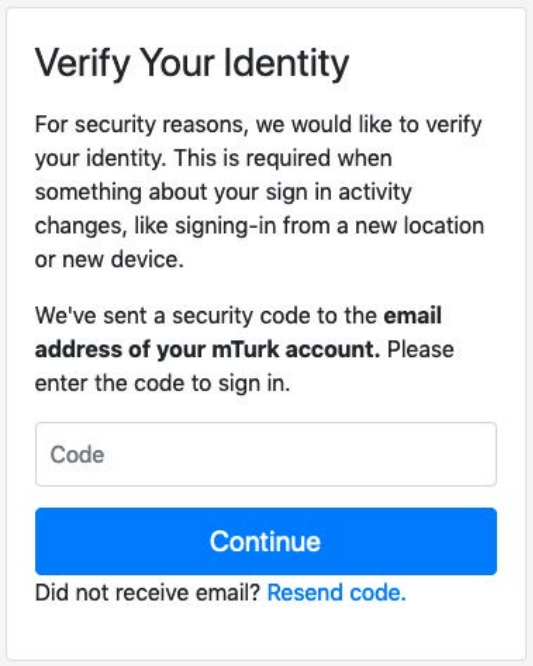
Dear [redacted] user,
Someone just tried to sign in to your [redacted] account.

If you were prompted for a security code, please enter the following to complete your sign in:

166832

If you were not prompted, please change your password immediately in the profile settings of cloust.de.

Thanks, the [redacted] Team



Method 2: Subject Line (new)

- Code-based method
- Code in email body **and subject line**

966601 is your personal security code

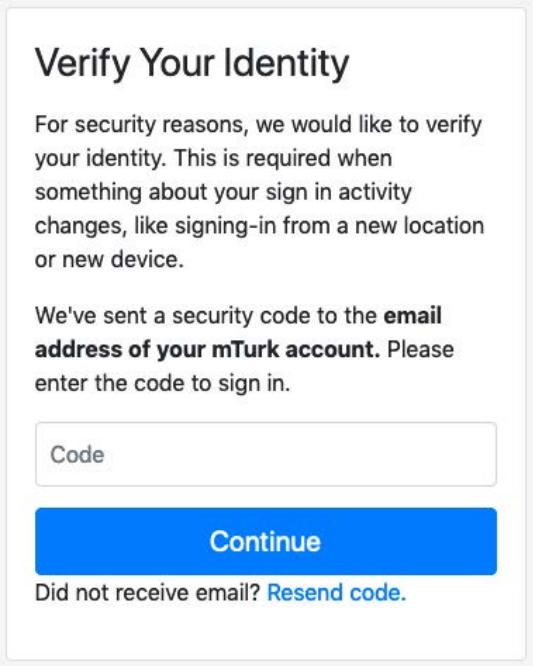
Dear [redacted] user,
Someone just tried to sign in to your [redacted] account.

If you were prompted for a security code, please enter the following to complete your sign in:

166832

If you were not prompted, please change your password immediately in the profile settings of cloust.de.

Thanks, the [redacted] Team



Method 3: Link (new)

- Link-based method
- Verification link in email body

Your personal confirmation link

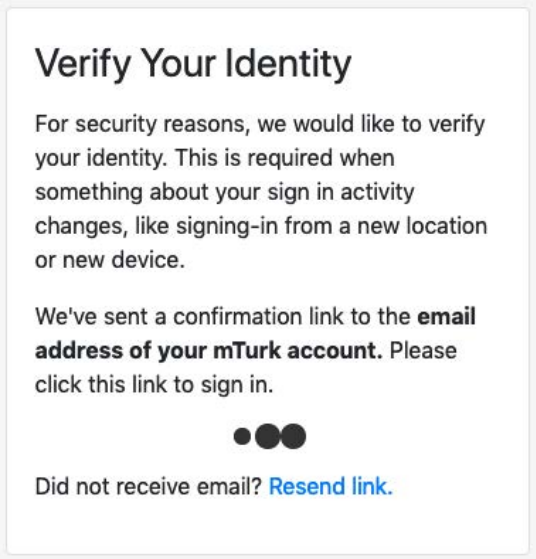
Dear [redacted] user,
Someone just tried to sign in to your [redacted] account.

If you were prompted to open a confirmation link, please click the link below to complete your sign in:

https://[redacted]/verify/vxno8ykjdyabx5zweuvoanqe42vgv0nj

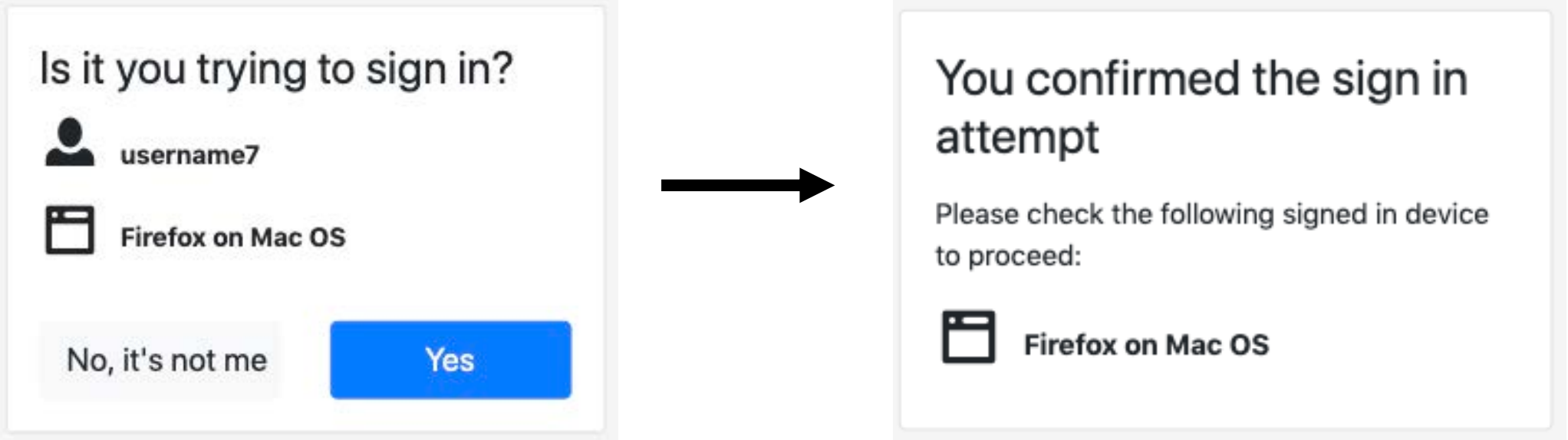
This link expires in 15 minutes.

If you were not prompted, please change your password immediately in the profile settings of cloust.de.
Thanks, the [redacted] Team



Method 3: Link (new)

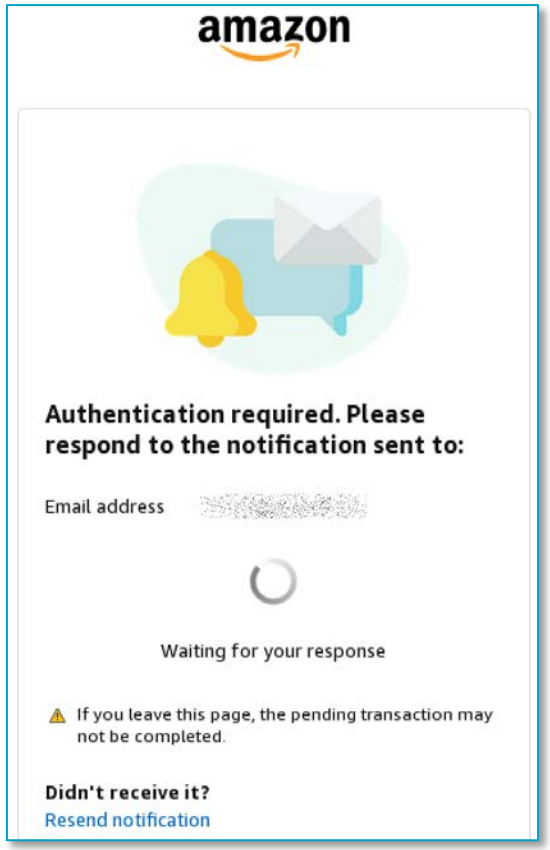
- Extra confirmation when confirmation device is different*

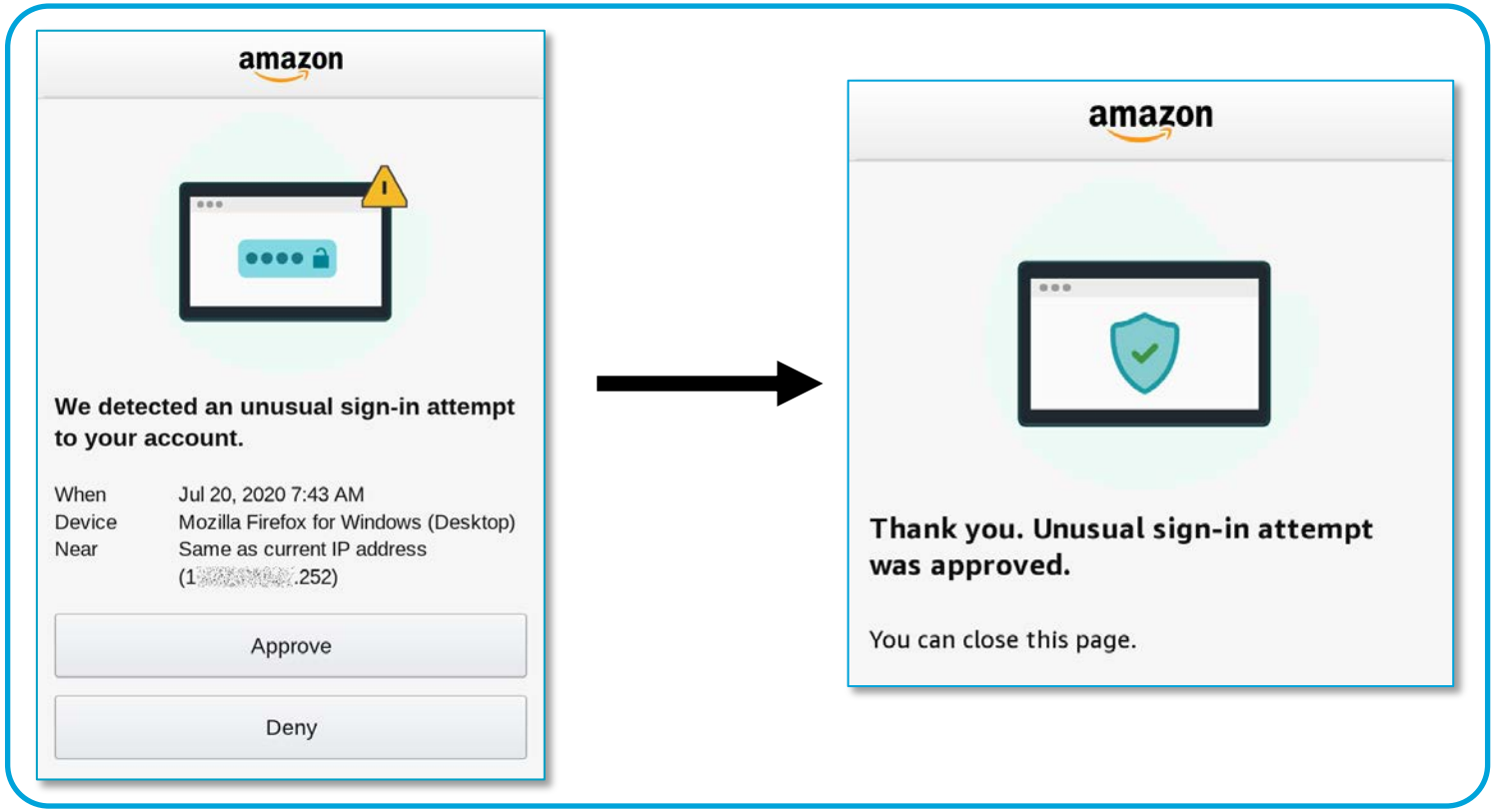


*Based on Google's Android device confirmation dialog

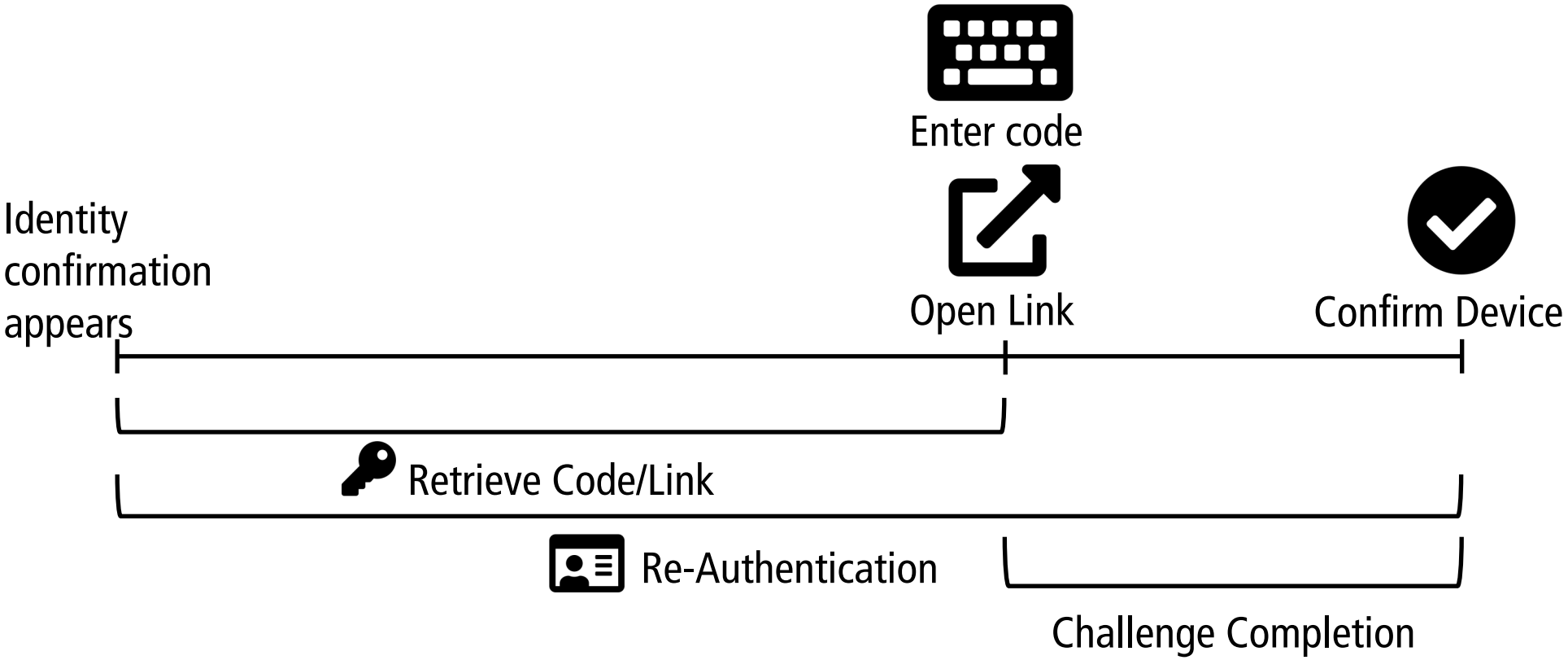
Method 3: Link (new)

- Amazon deployed method one year after our study

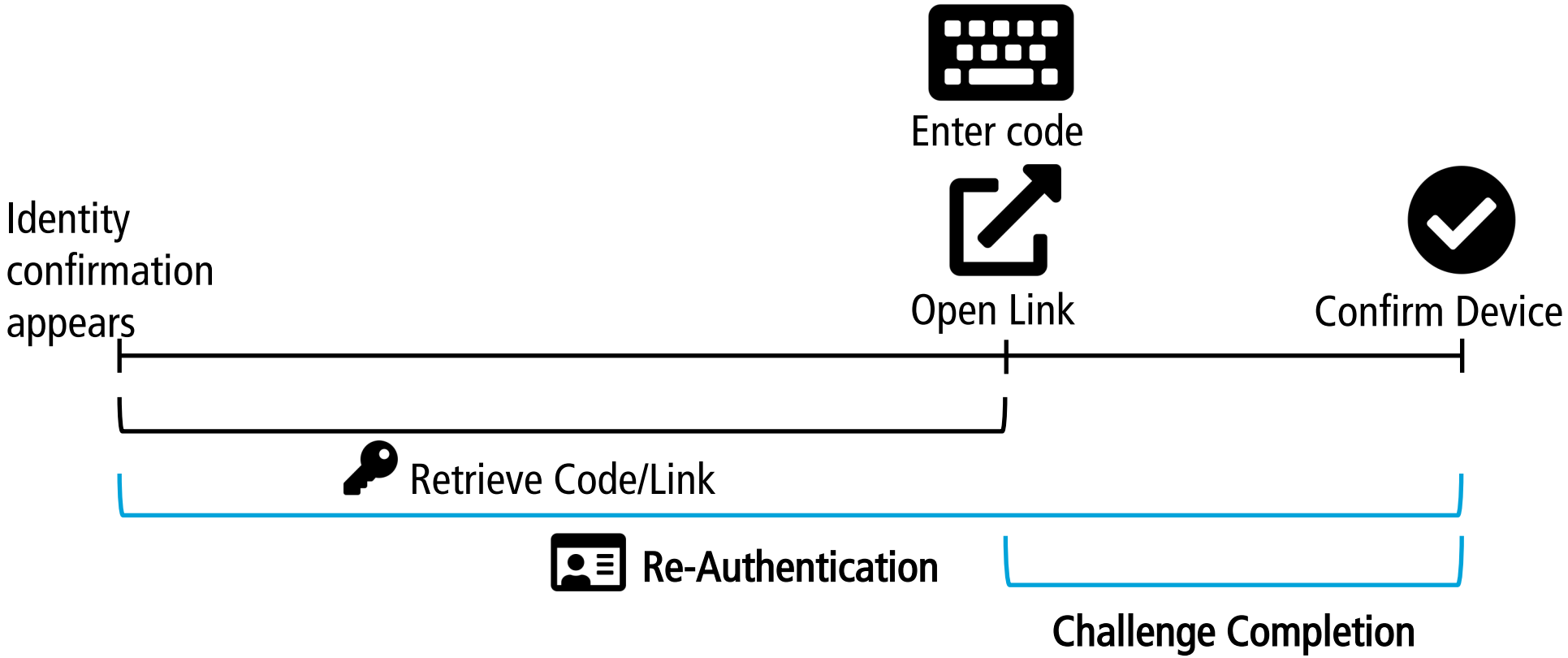




Timings: Measurement



Timings: Measurement



Study Procedure

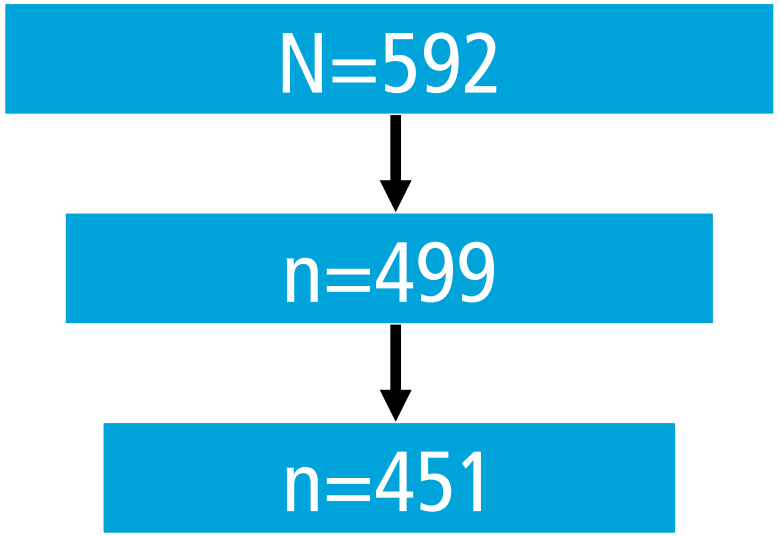
- 1. Registration
- 2. Login
- **3. Exit survey**

Overview

- Study
- **Results**
- Conclusion

Results: Demographics

- Recruited via MTurk

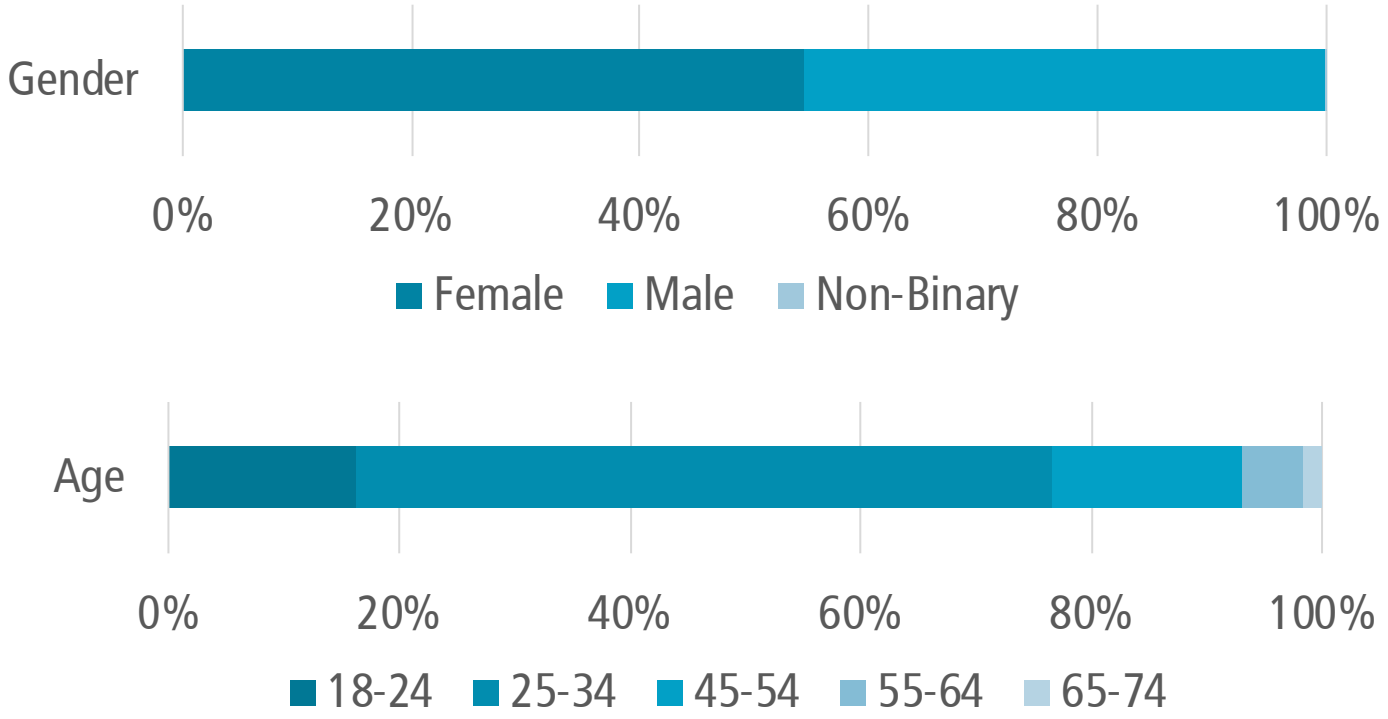


Participated

Completed

Passed tests → Taken for results

Results: Demographics (n=451)



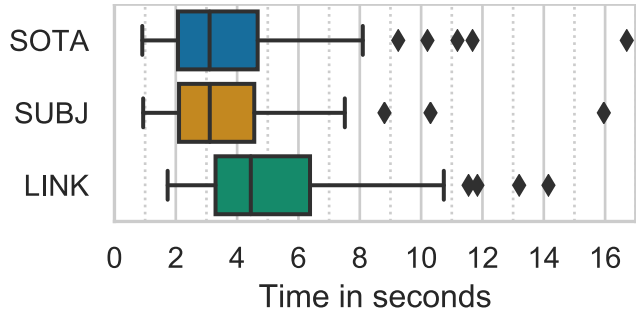
- Associate degree or higher (63%)
- No computer science background (74%)

Results: Timings

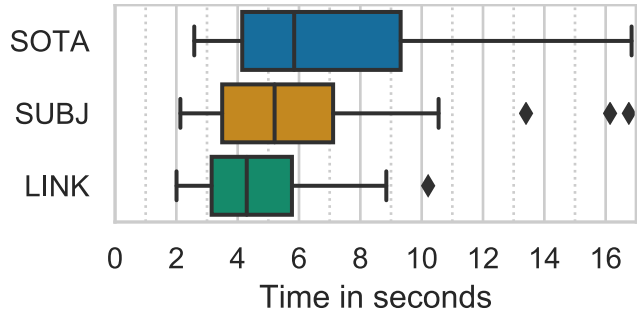
- Challenge completion time:
  - Median: 6 seconds
  - No significant differences between devices
- Re-Authentication time:
  - Median: 34 seconds

Results: Challenge Completion Time

- Faster in two cases (each $p<0.01$)
  - Code-based: Desktop PC for login + authentication
  - Link-based: Desktop PC for login, mobile device for authentication



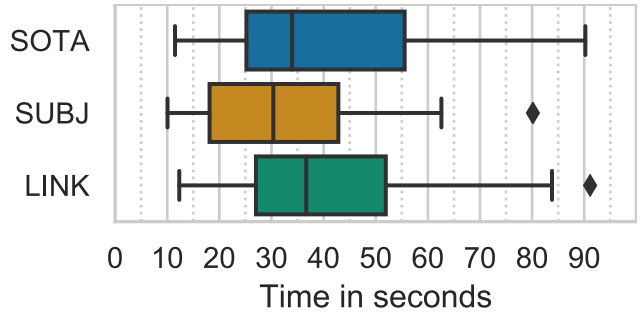
Desktop/Desktop



Desktop/Mobile

Results: Re-Authentication Time

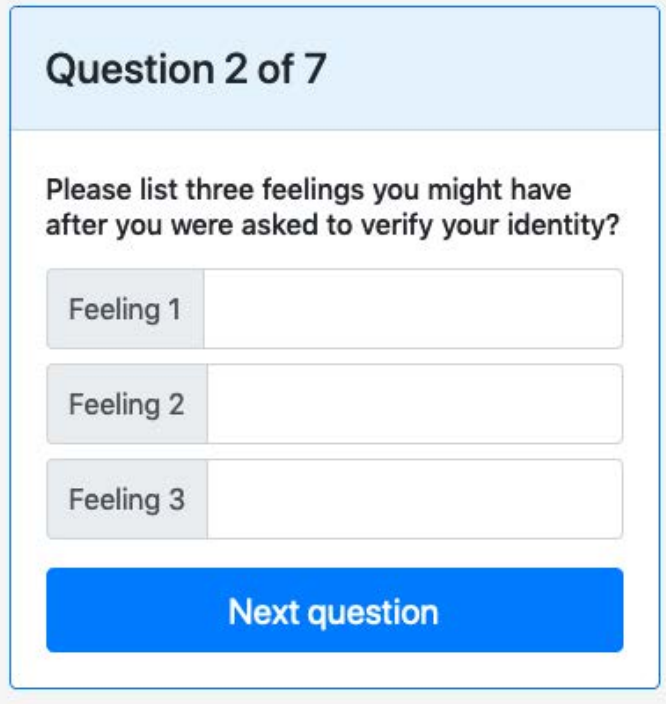
- Faster with code in subject line and body
  - Desktop PC for login + authentication (p=0.02)



Desktop/Desktop

Results: Feelings

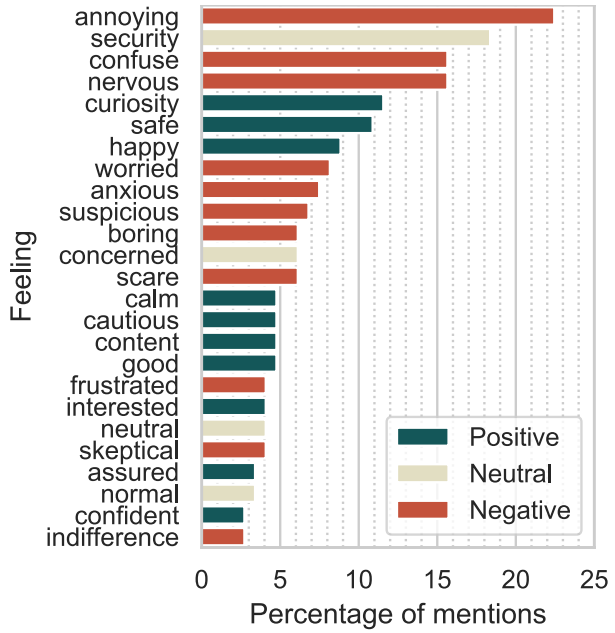
- Question in exit survey*



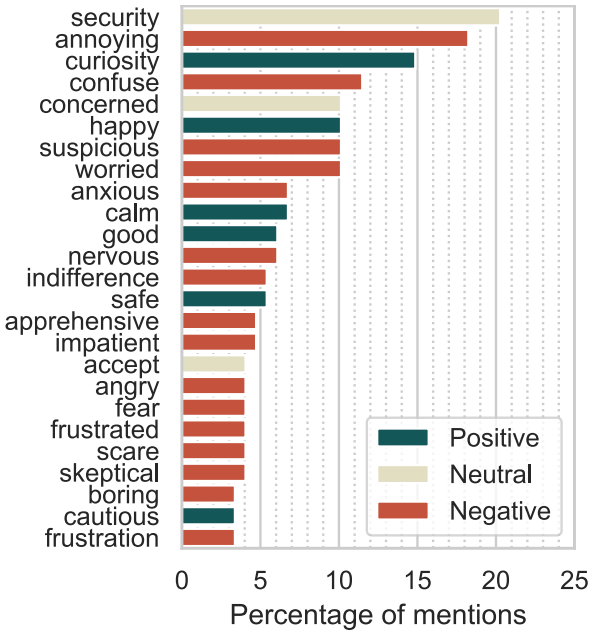
*Question similar to Golla et al. (CCS '18)

Results: Feelings

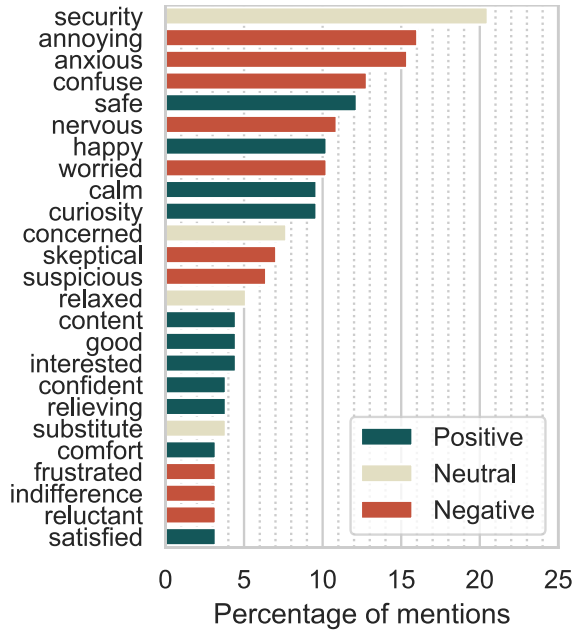
- Similar number of mentions in all conditions
- With three exceptions



State of the art (Code in body)



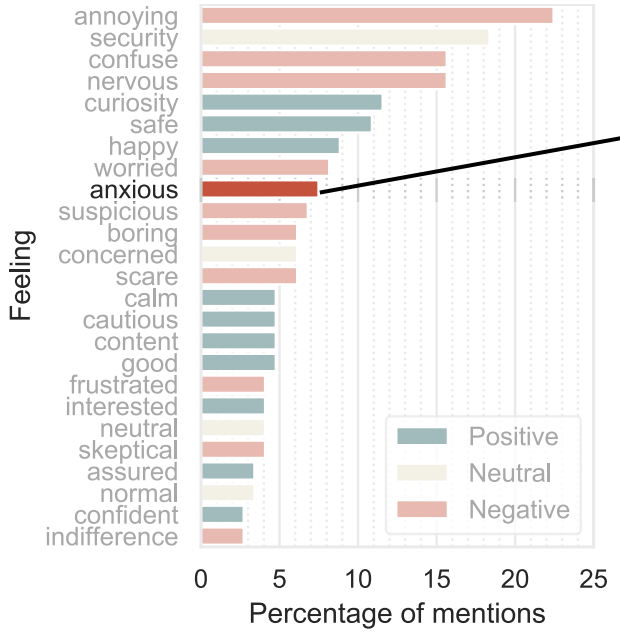
Code in body + subject line



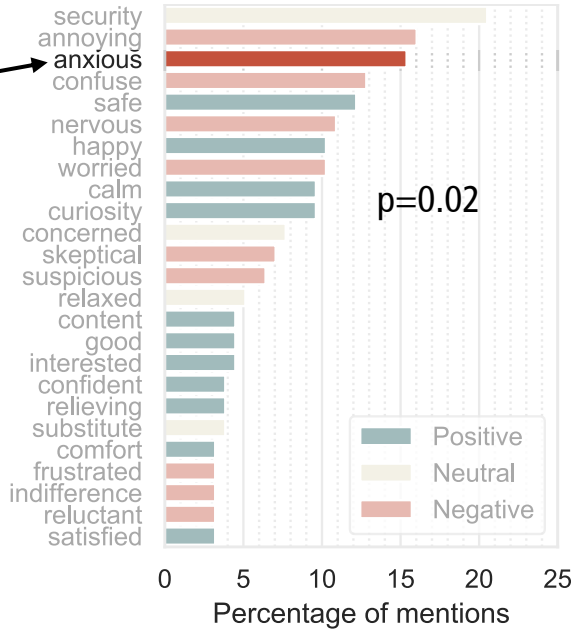
Link-based

Results: Feelings

- Link-based method made users significantly more anxious than code-based methods



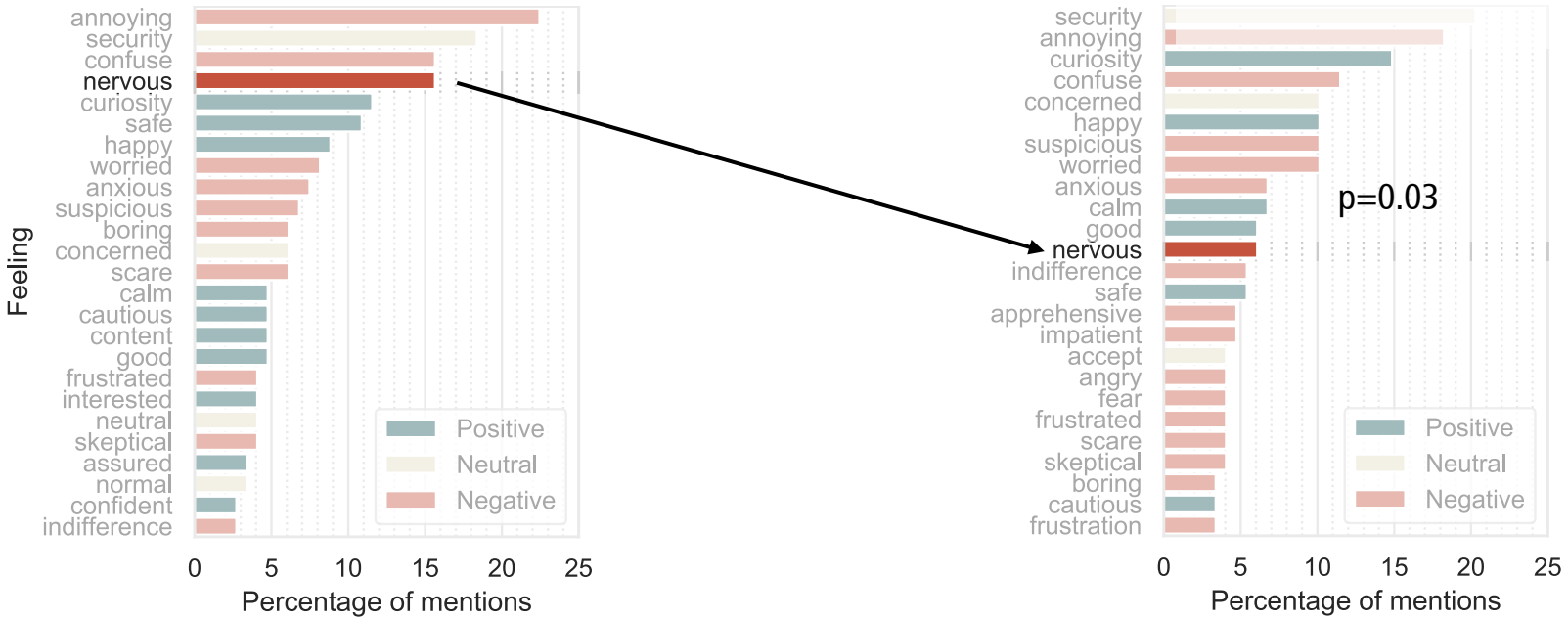
State of the art (Code in body)



Link-based

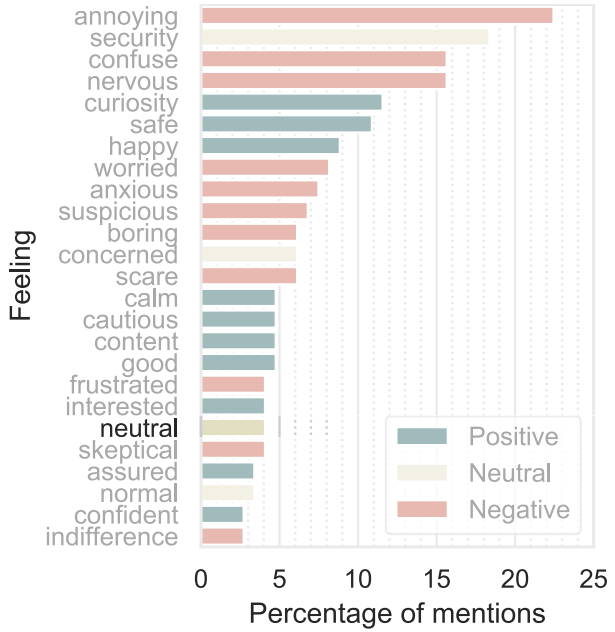
Results: Feelings

- Code in subject line and body made significantly less nervous



Results: Feelings

- Code in subject line significantly more neutral (p=0.04)



State of the art (Code in body)

State of the art	Code in body + subject line	Link-based
4.1%	0.7%	0.6%

Overview

- Study
- Results
- Conclusion

Conclusion

- Code in subject and body performed best
  - Faster re-authentication time
  - Significantly less nervous

→Not current RBA state of the art!

- Link-based method:
  - Re-authentication time did not improve
  - More anxious when perceived for first time

Thank you

riskbasedauthentication.org
das.h-brs.de

stephan.wiefling@h-brs.de

@swiefling