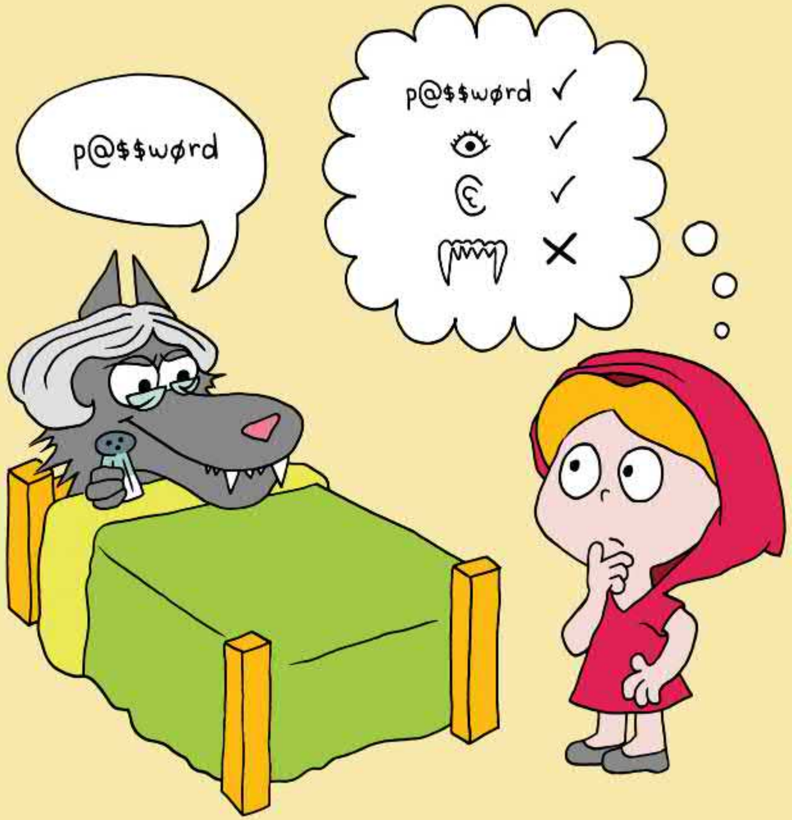
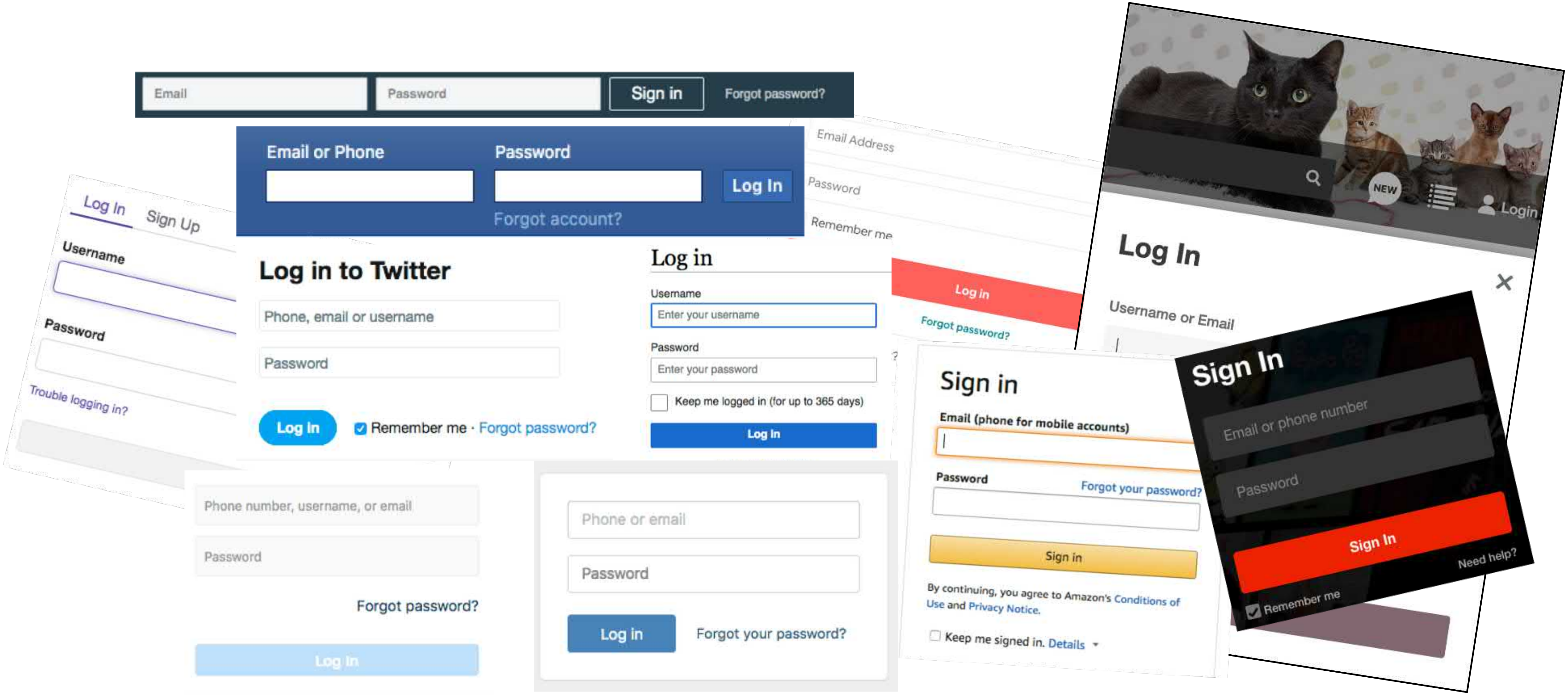
Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences

/DAS>
Data and Application Security Group



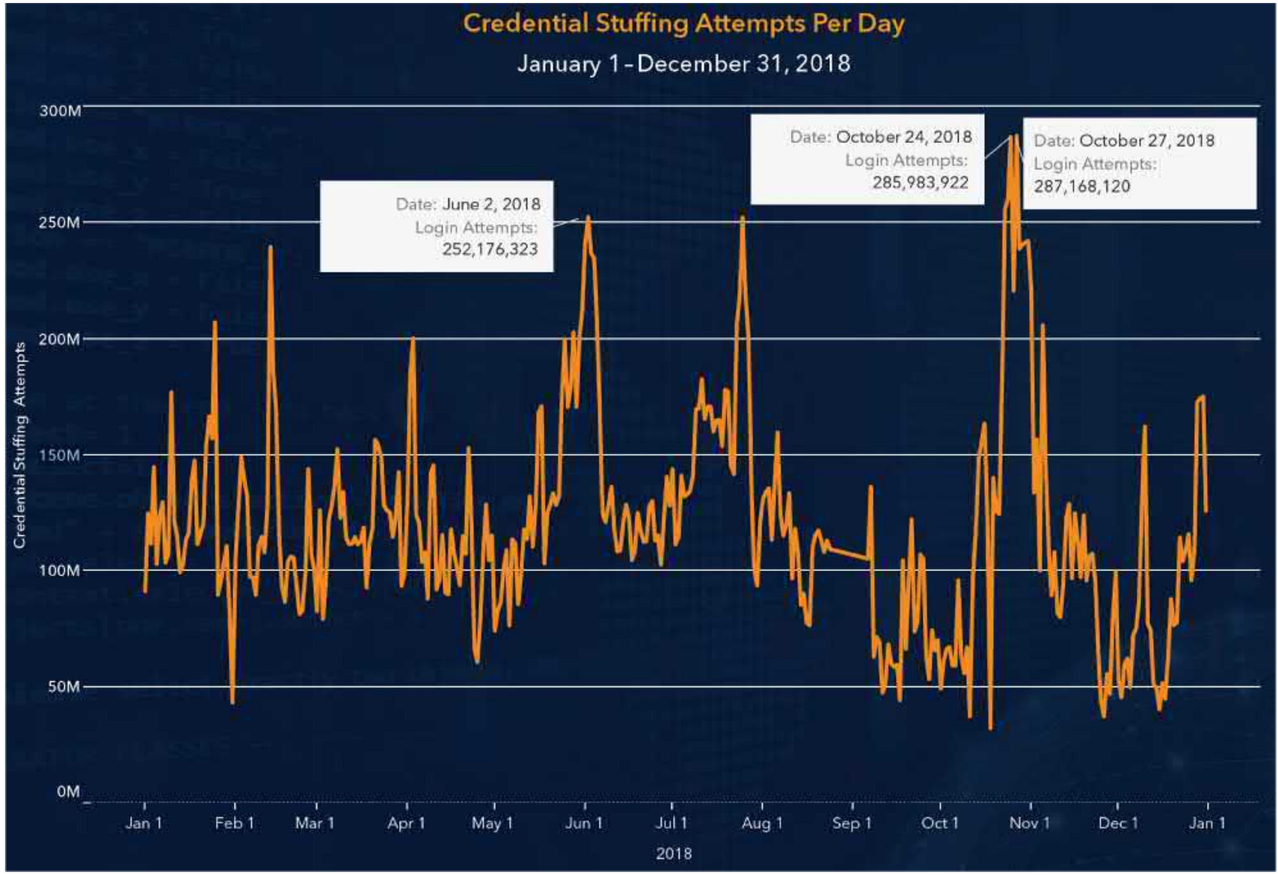
An Introduction to Risk-based Authentication

Luigi Lo Iacono – Data and Application Security Group
H-BRS University of Applied Sciences


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
Log in
Forgot password?
NEW
Login
Log In
Username or Email
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
☑ Remember me
Need help?
Phone number, username, or email
Password
Forgot password?
Log In
Phone or email
Password
Log in
Forgot your password?

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*

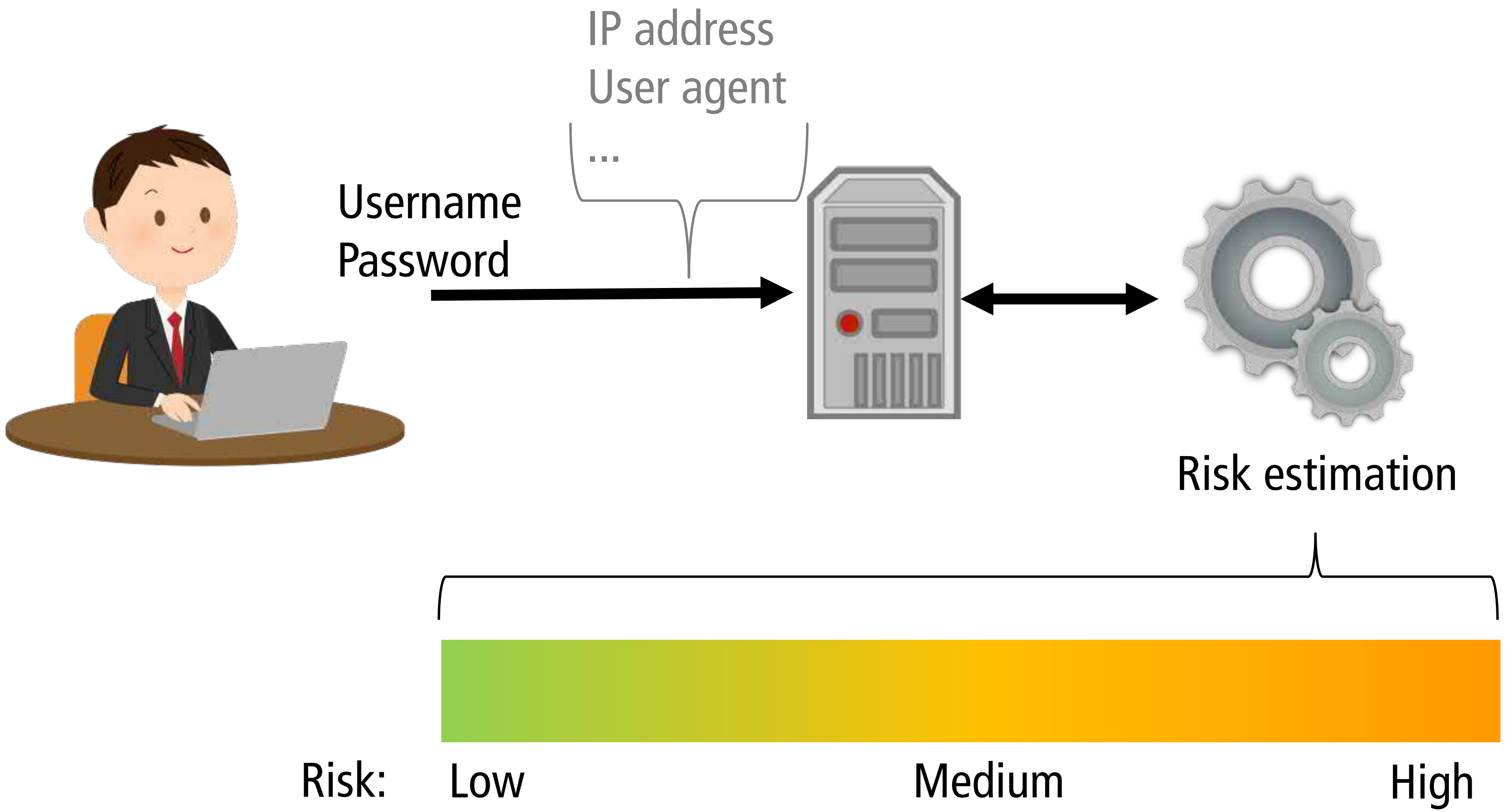
*Milka, G.: Anatomy of Account Takeover. In: Enigma 2018. USENIX (Jan 2018)

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)

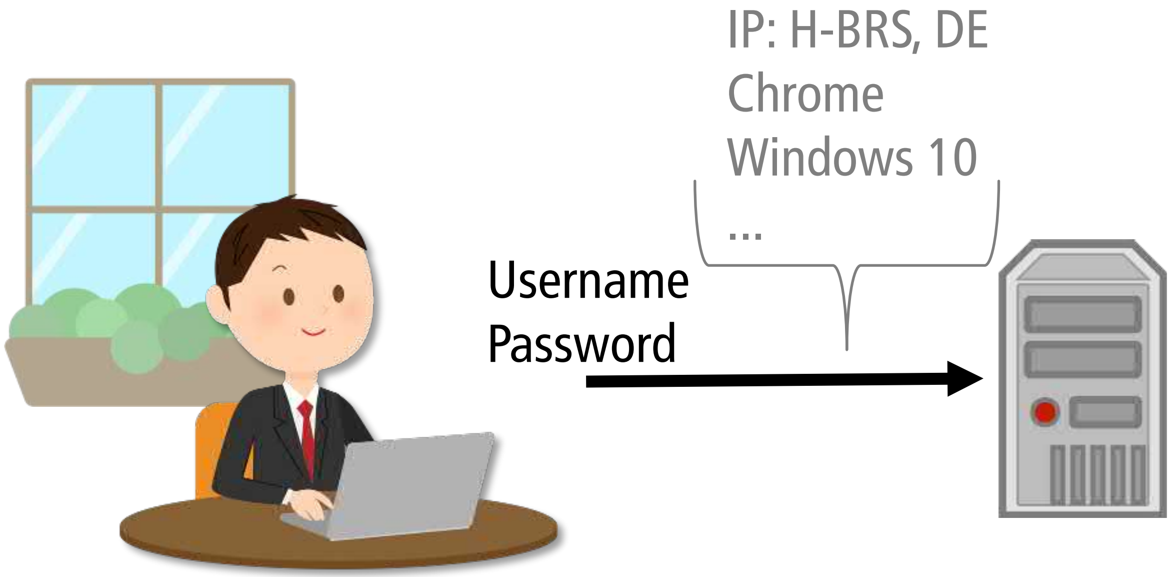


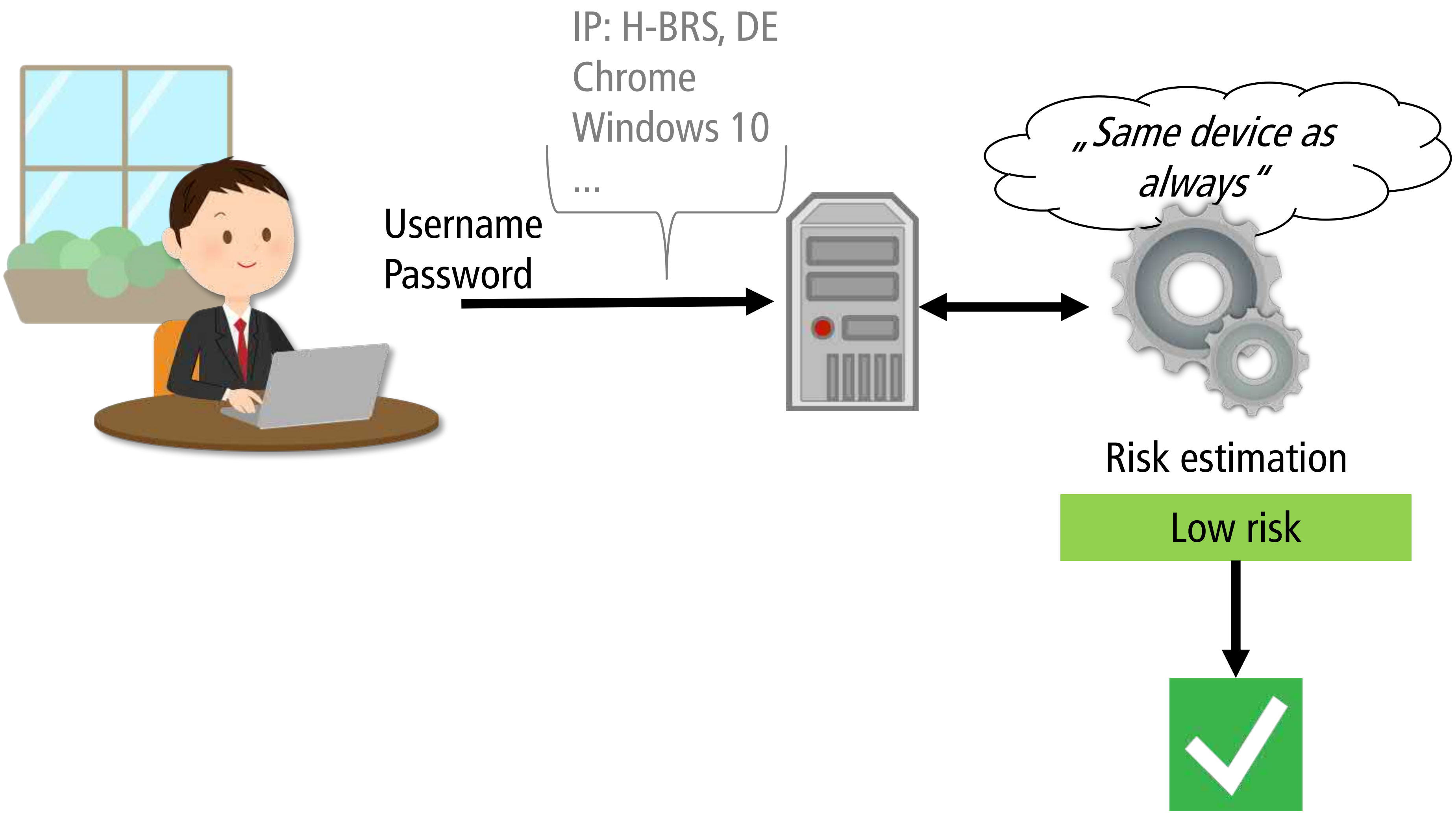
IP address
User agent
...

Username
Password

Risk estimation

Risk: Low Medium High


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



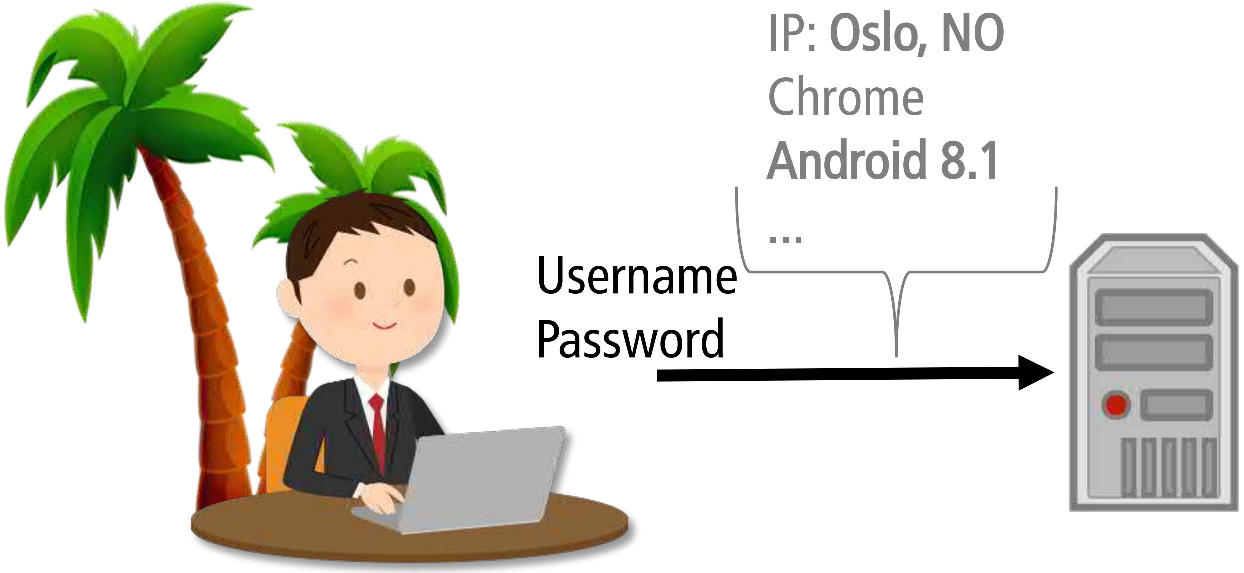
IP: H-BRS, DE
Chrome
Windows 10
...

Username
Password

„Same device as always"

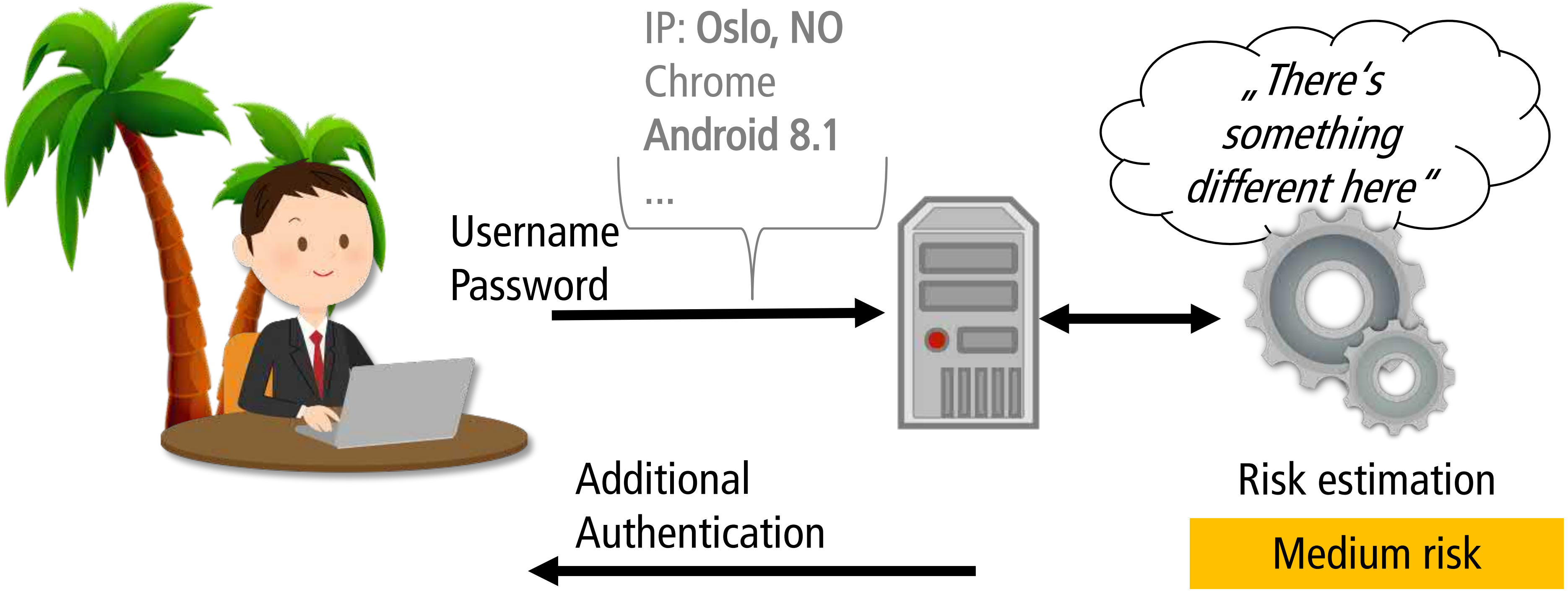
Risk estimation

Low risk



Username
Password

IP: Oslo, NO
Chrome
Android 8.1
...



IP: Oslo, NO
Chrome
Android 8.1
...

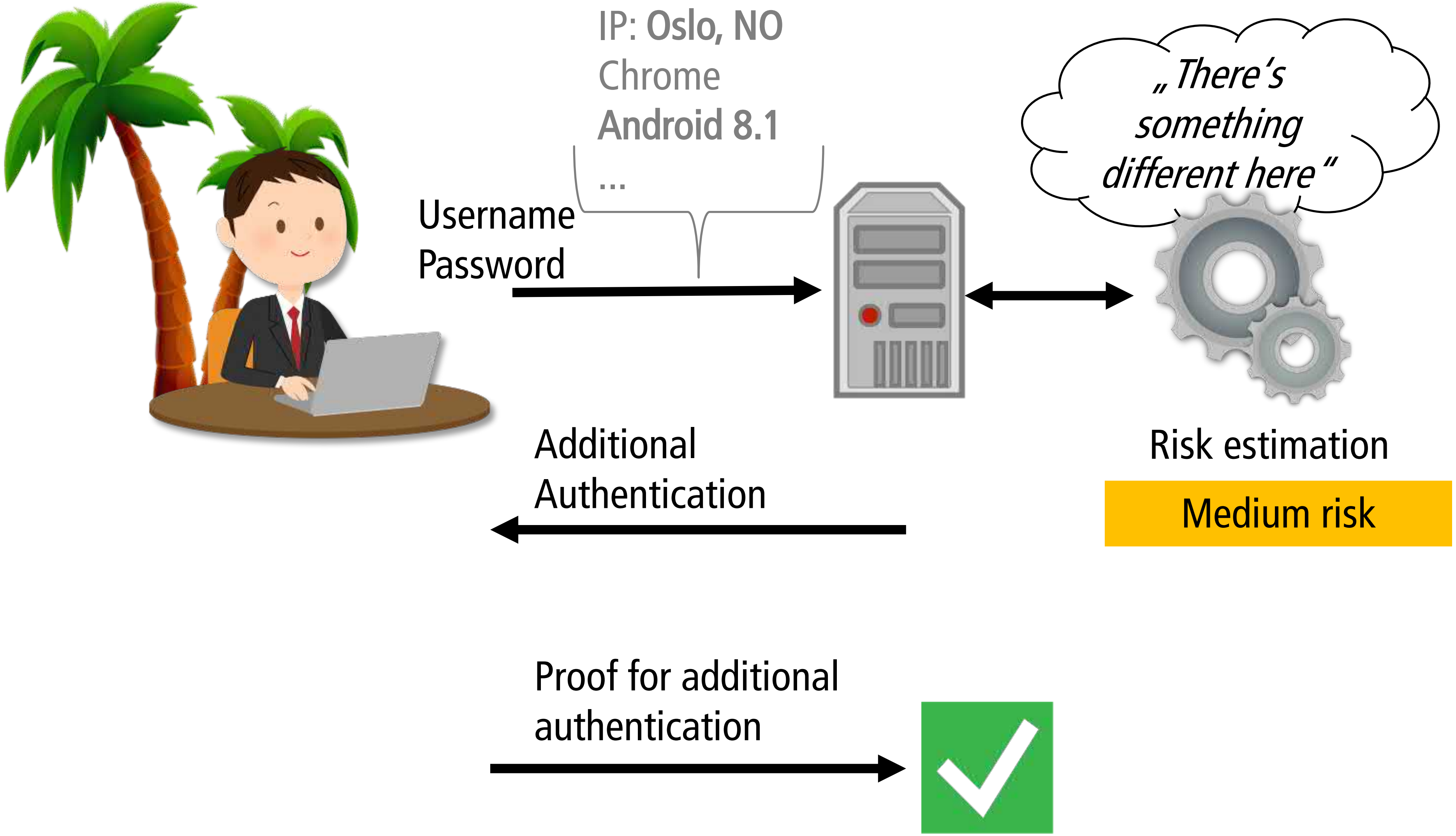
Username
Password

„There's something different here"

Risk estimation

Medium risk

Additional Authentication



IP: Oslo, NO
Chrome
Android 8.1
...

Username
Password

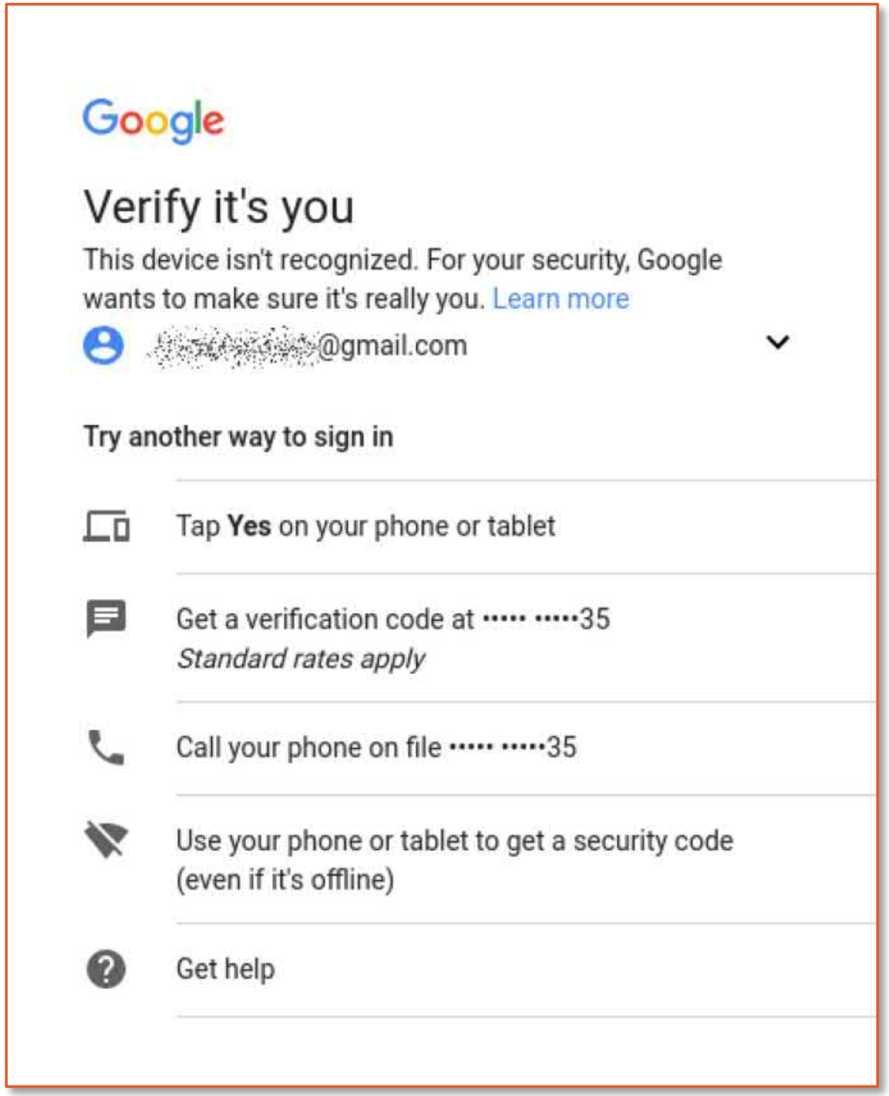
„There's something different here"

Risk estimation

Medium risk

Additional Authentication

Proof for additional authentication



Google

Verify it's you

This device isn't recognized. For your security, Google wants to make sure it's really you. Learn more

[redacted]@gmail.com

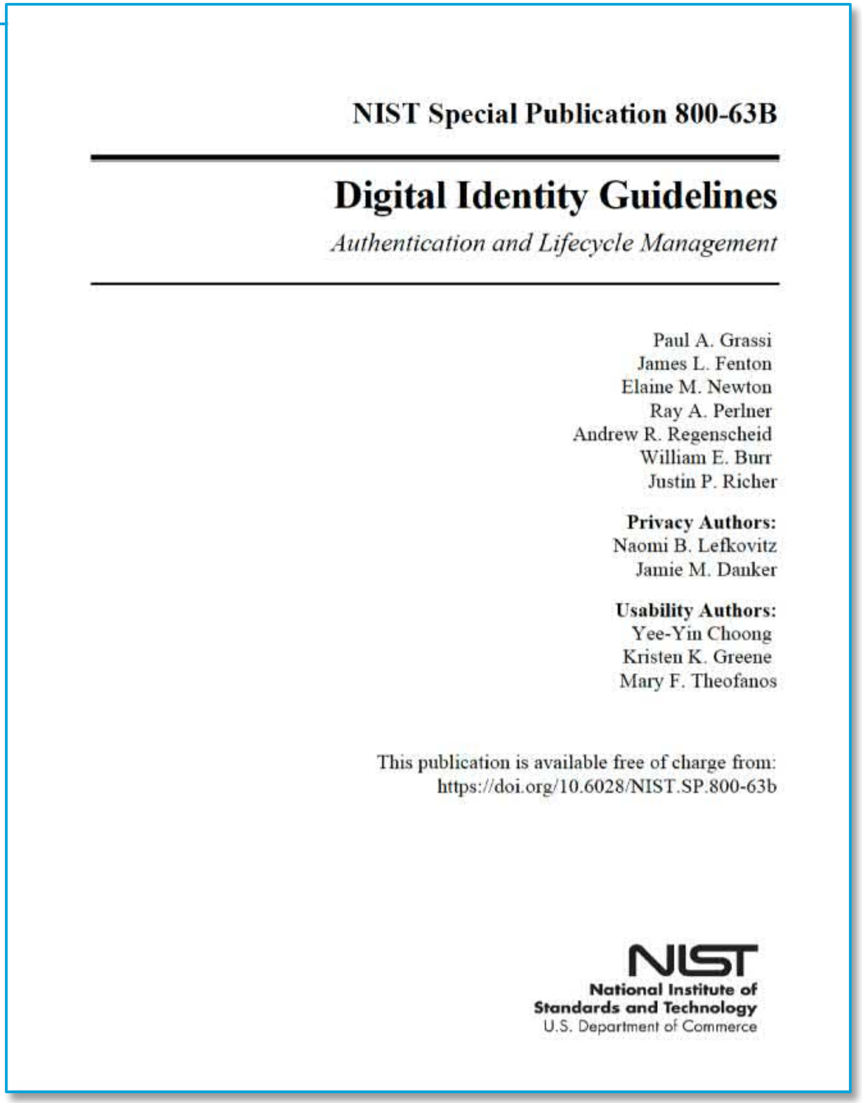
Try another way to sign in

- Tap **Yes** on your phone or tablet
- Get a verification code at ••••• •••••35
  Standard rates apply
- Call your phone on file ••••• •••••35
- Use your phone or tablet to get a security code (even if it's offline)
- Get help

Risk-based Authentication

- Recommended by NIST digital identity guidelines[1]
- Used by large online services[2]
  - But: Procedures not disclosed
  - Prevents widespread adoption

[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)



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

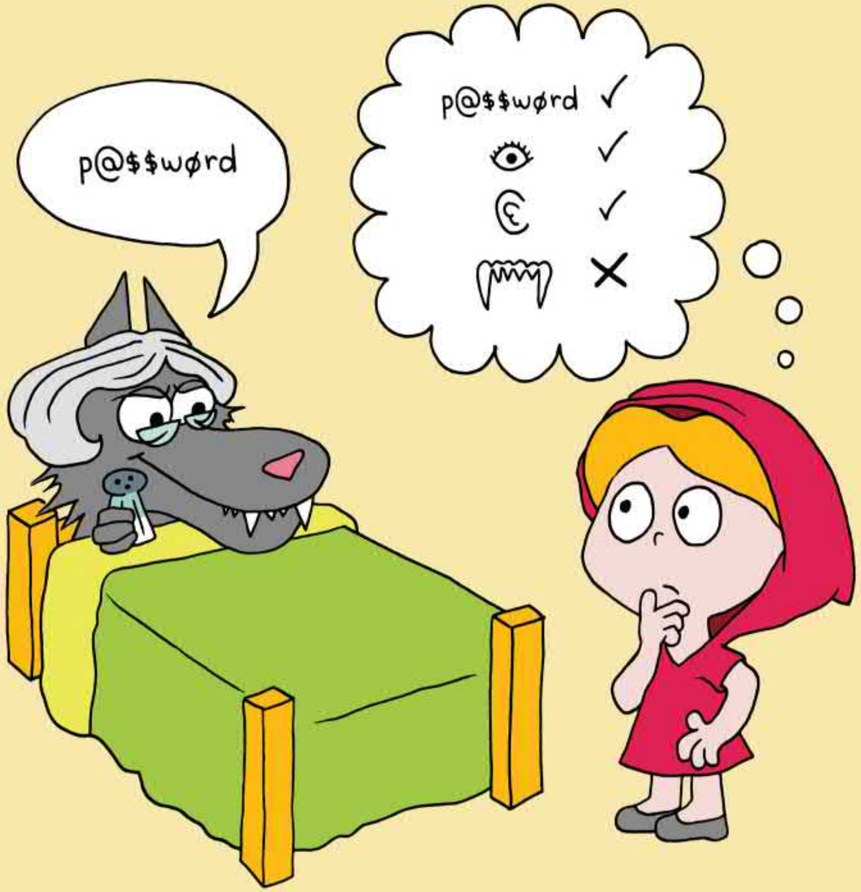


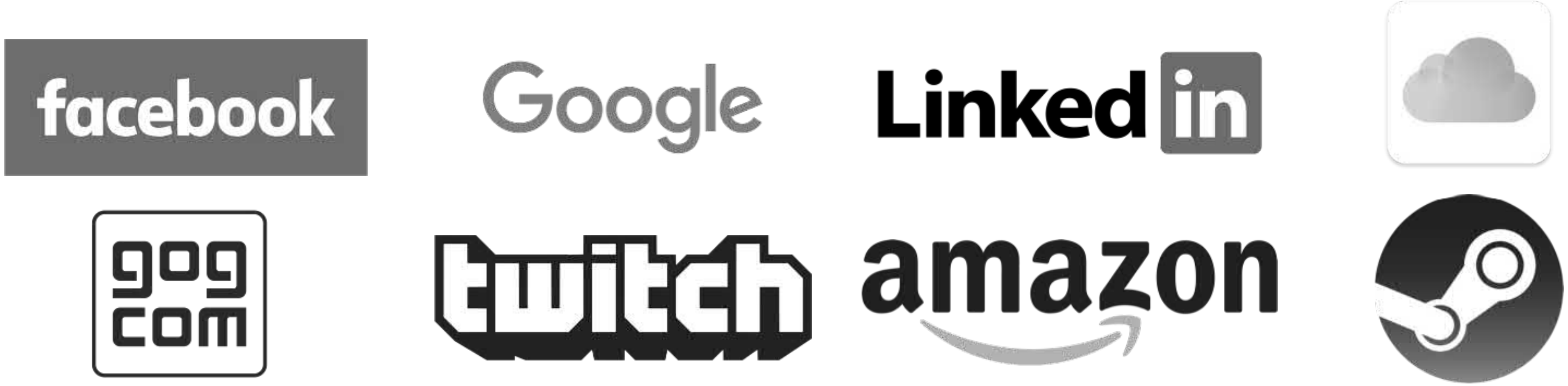
Image: Iwona Usakiewicz / Andrij Borys Associates
Bonneau et al.: Passwords and the evolution of imperfect authentication. Comm. ACM 58(7) (Jun 2015)

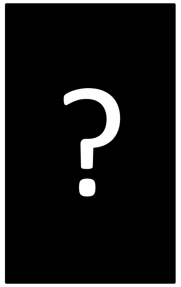
Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild

Stephan Wiefling, Luigi Lo Iacono – TH Köln – University of Applied Sciences
Markus Dürmuth – Ruhr University Bochum

RBA in the Wild

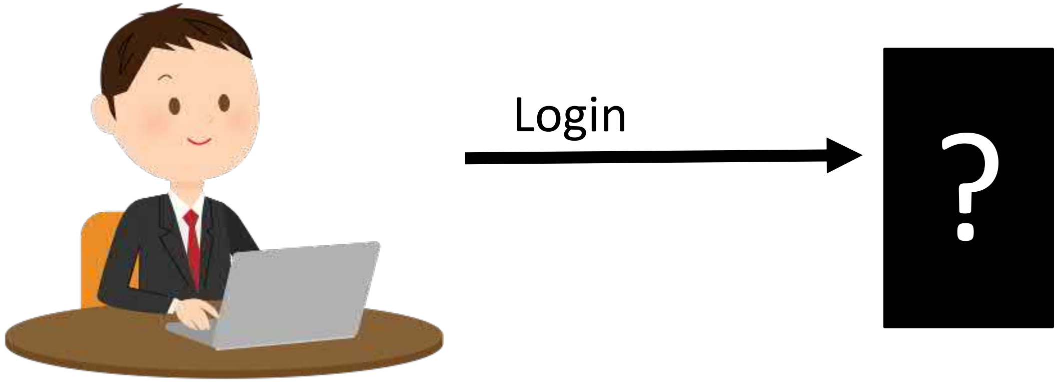
- Black-box tested eight popular online services



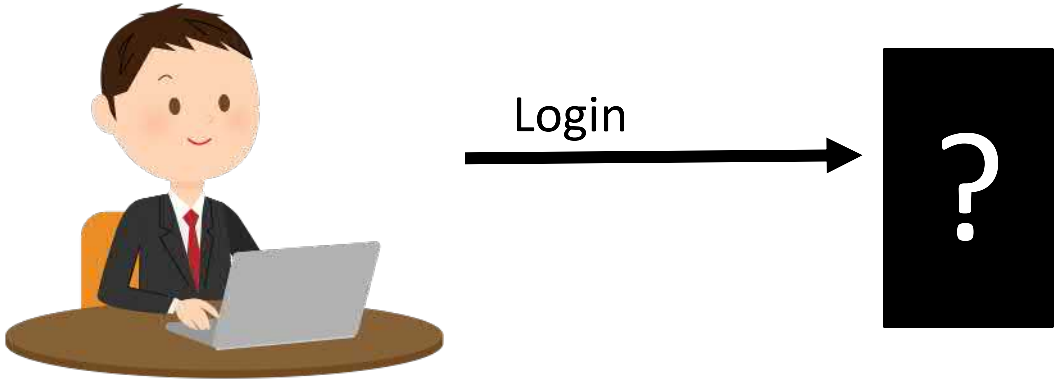


?

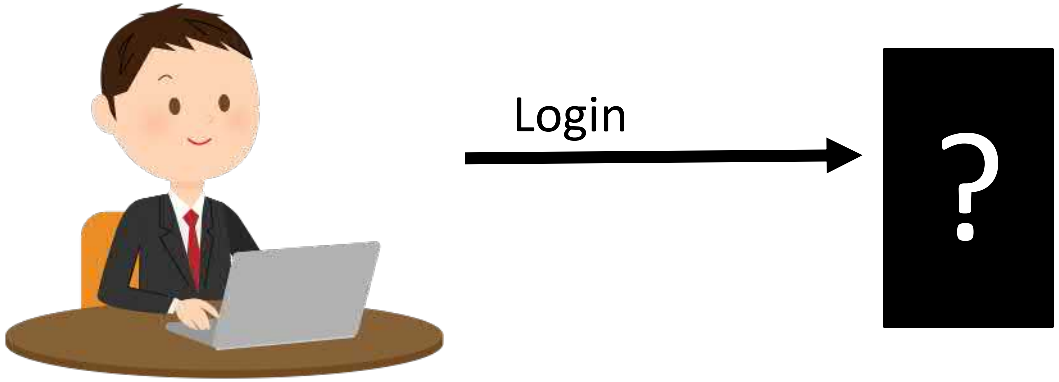
Login	IP address	User Agent	...



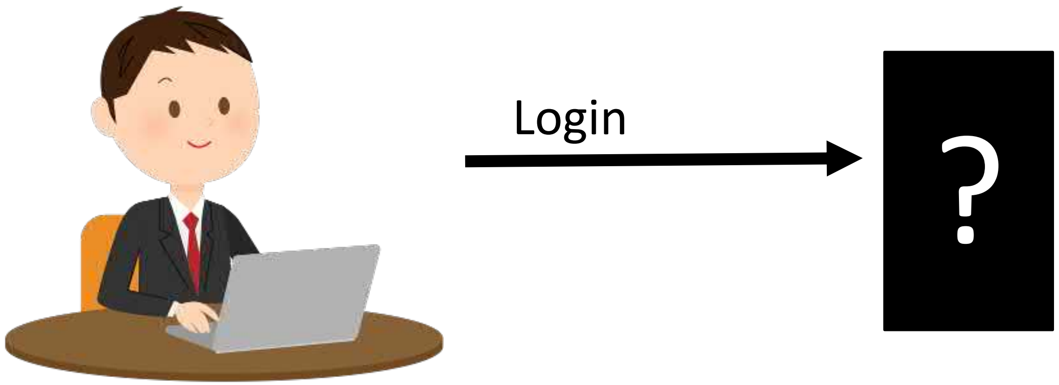
Login	IP address	User Agent	...
1	H-BRS	Chrome	...



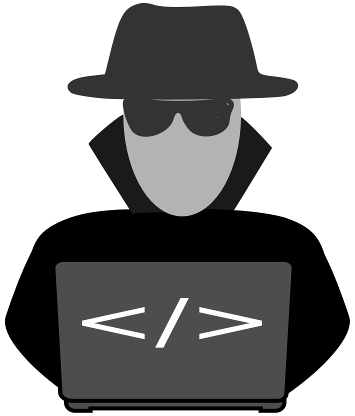
Login	IP address	User Agent	...
1	H-BRS	Chrome	...
2	H-BRS	Chrome	...

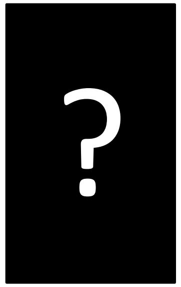


Login	IP address	User Agent	...
1	H-BRS	Chrome	...
2	H-BRS	Chrome	...
3	H-BRS	Chrome	...

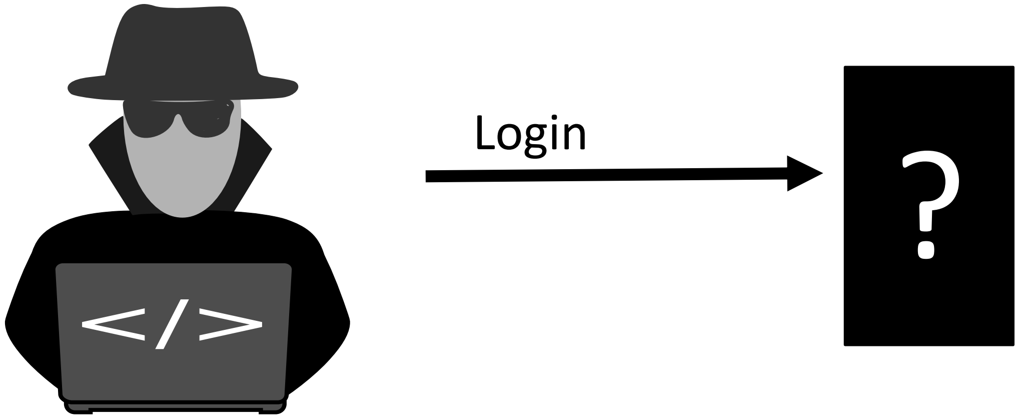


Login	IP address	User Agent	...
1	H-BRS	Chrome	...
2	H-BRS	Chrome	...
3	H-BRS	Chrome	...
...	...	...	....
20	H-BRS	Chrome	...

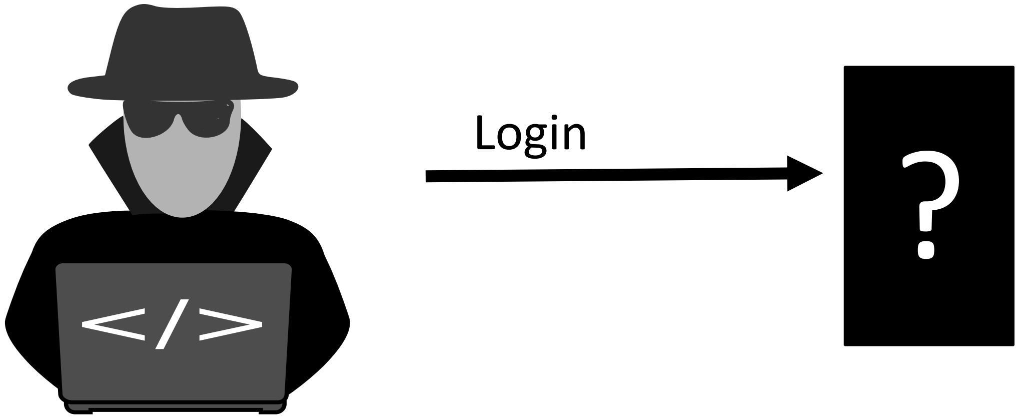




Login	IP address	User Agent	...
1	H-BRS	Chrome	...
2	H-BRS	Chrome	...
3	H-BRS	Chrome	...
...	...	...	....
20	H-BRS	Chrome	...



Login	IP address	User Agent	...
1	H-BRS	Chrome	...
2	H-BRS	Chrome	...
3	H-BRS	Chrome	...
...	...	...	....
20	H-BRS	Chrome	...
21	**Other Country**	Chrome	...



✅, 🟨 or ⛔?

Login	IP address	User Agent	...
1	H-BRS	Chrome	...
2	H-BRS	Chrome	...
3	H-BRS	Chrome	...
...	...	...	....
20	H-BRS	Chrome	...
21	**Other Country**	Chrome	...

It‘s not that easy…

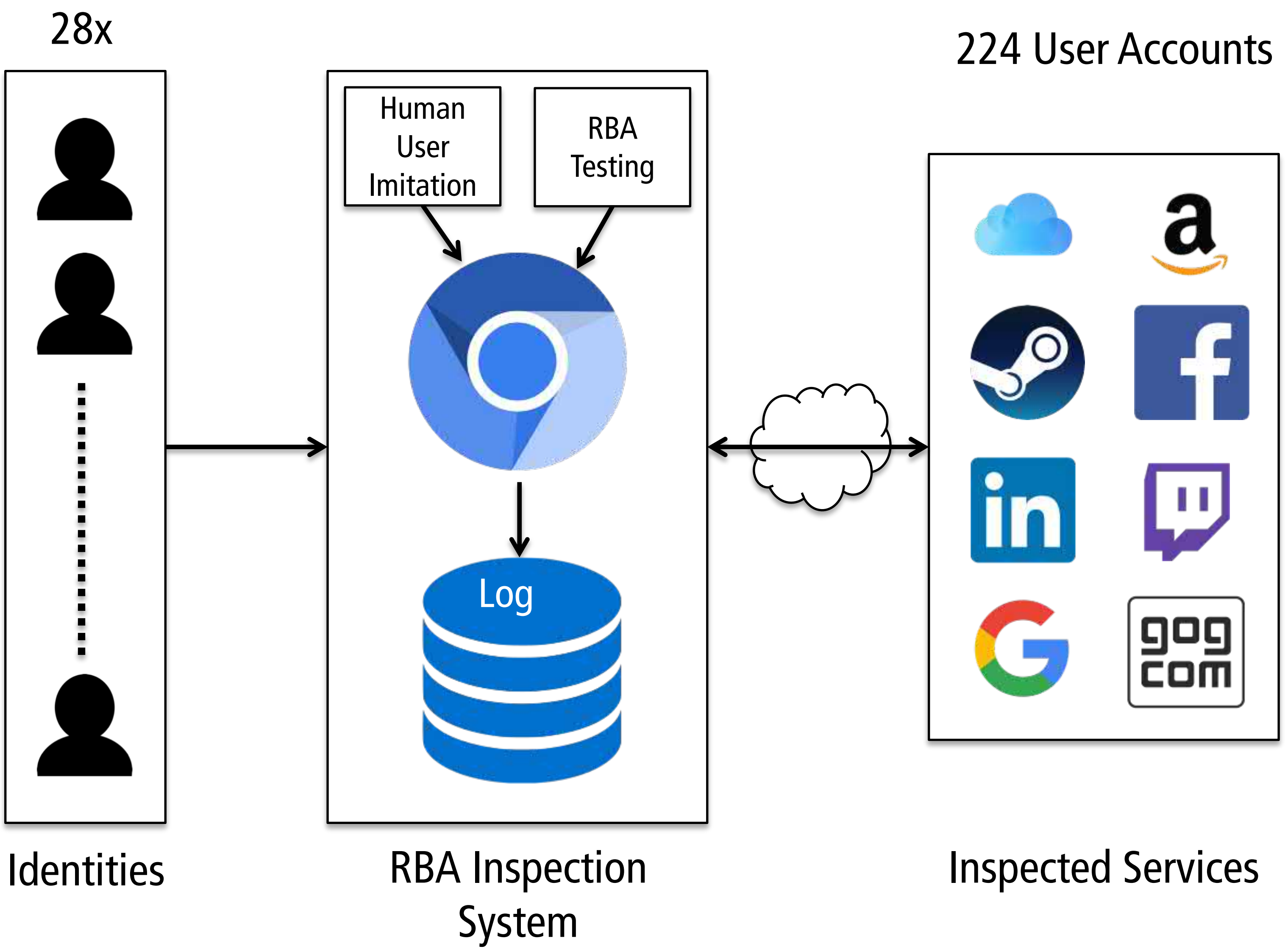
Login history influences risk score

Solution: Create many user accounts

It‘s not that easy...

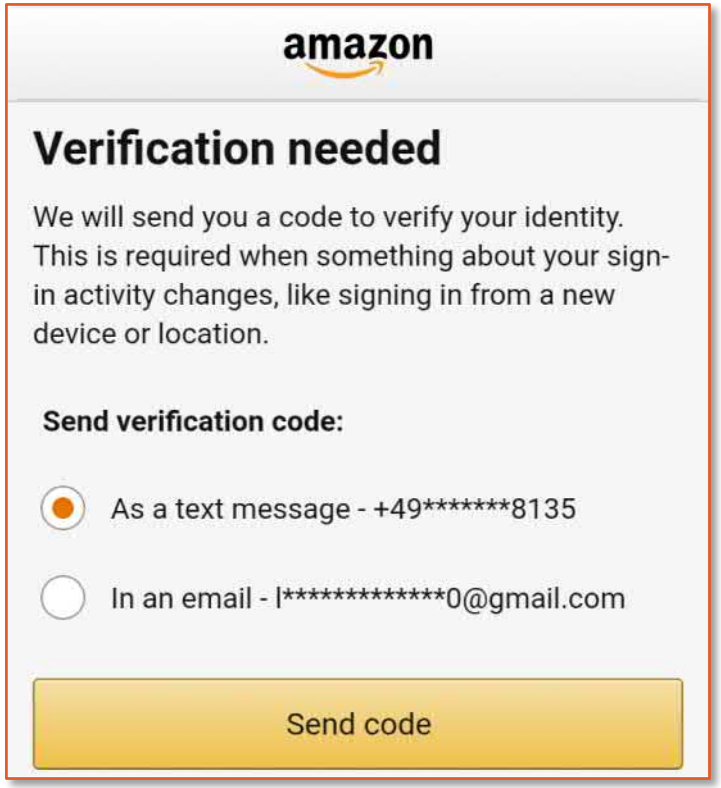
Automated testing influences result

Solution: Create human-like browsing behavior


28x
224 User Accounts
Human User Imitation
RBA Testing
Log
Identities
RBA Inspection System
Inspected Services

Results

Service	Used features and weightings
Amazon	IP address
GOG.com	IP address
Google	1. IP address 2. Time parameters 3. User agent string, display resolution
LinkedIn	1. IP address 2. User agent string, language, time parameters, display resolution



amazon

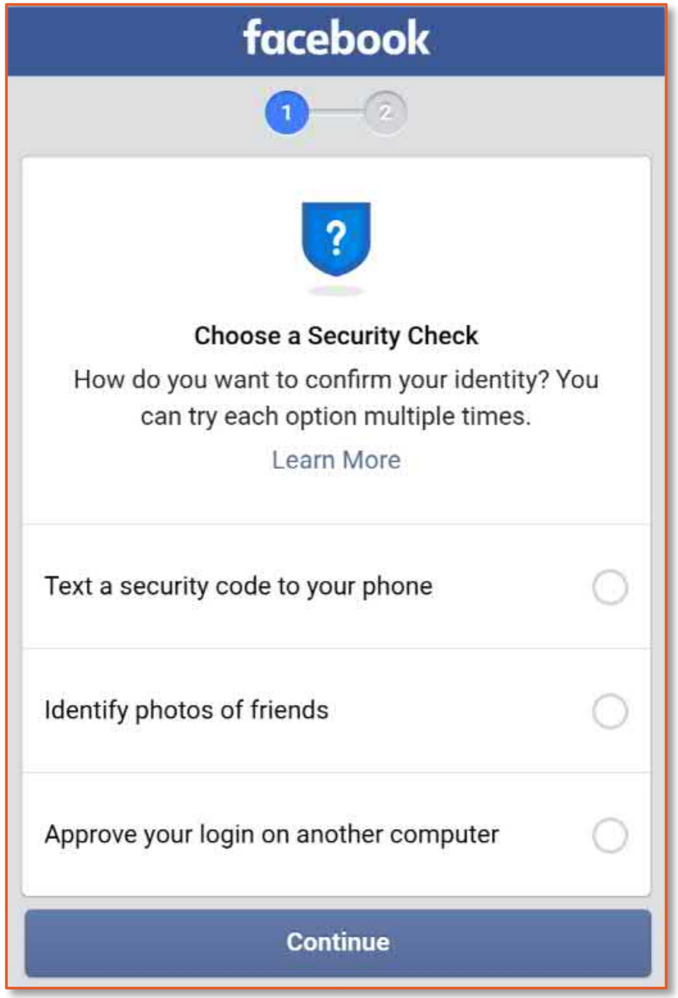
Verification needed

We will send you a code to verify your identity. This is required when something about your sign-in activity changes, like signing in from a new device or location.

Send verification code:

● As a text message - +49*******8135

○ In an email - l*************0@gmail.com



Choose a Security Check

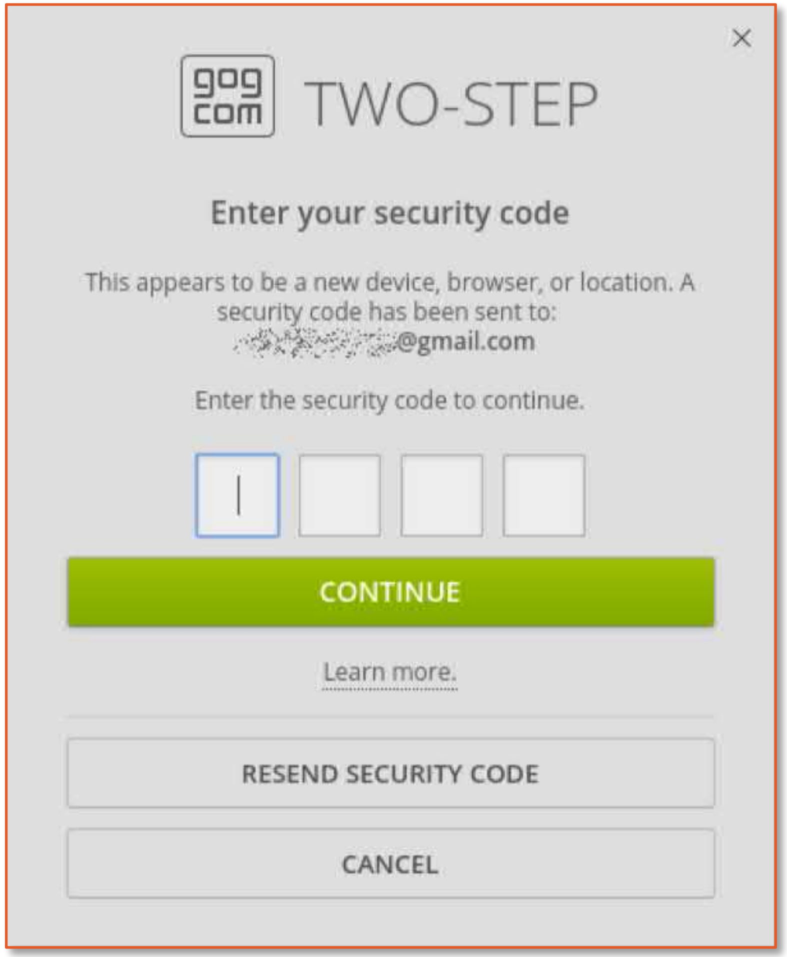
How do you want to confirm your identity? You can try each option multiple times.

Learn More

Text a security code to your phone ○

Identify photos of friends ○

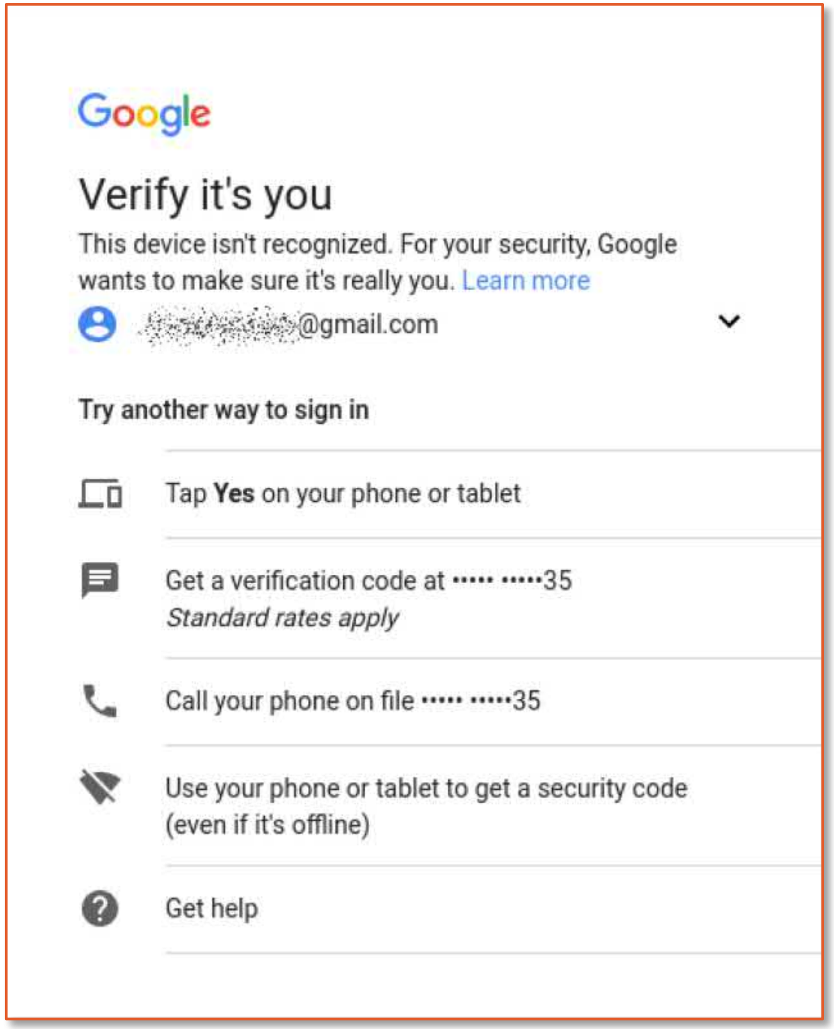
Approve your login on another computer ○



Enter your security code

This appears to be a new device, browser, or location. A security code has been sent to: [redacted]@gmail.com

Enter the security code to continue.



Google

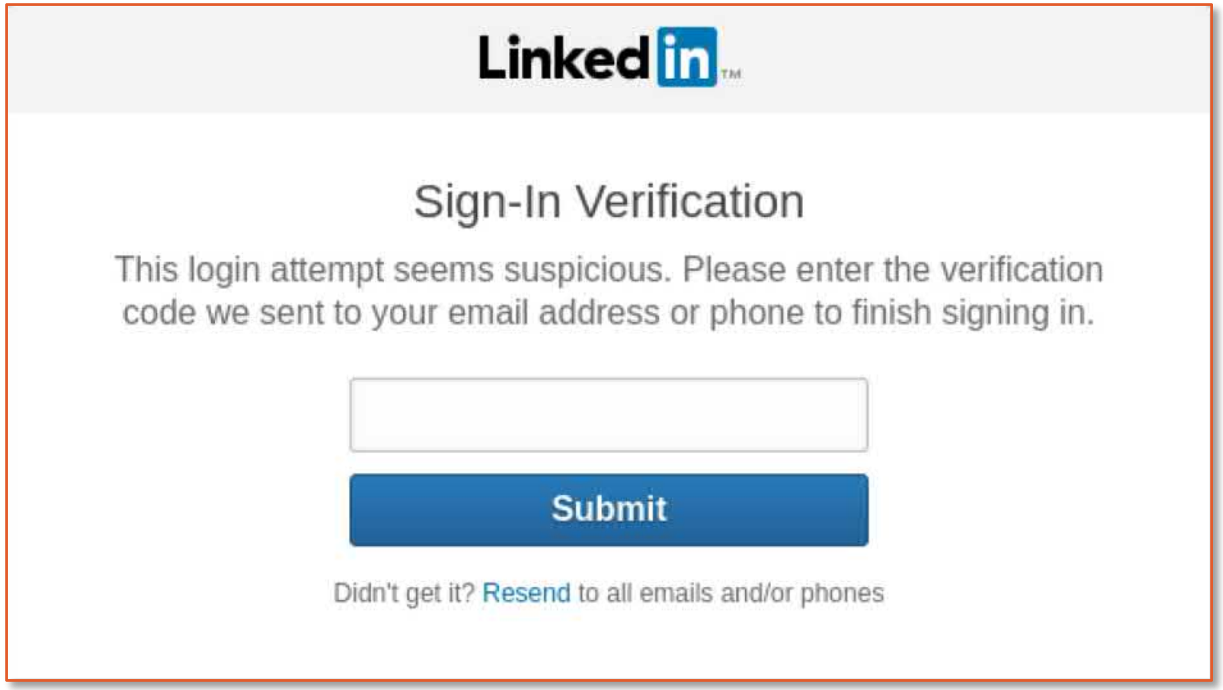
Verify it's you

This device isn't recognized. For your security, Google wants to make sure it's really you. Learn more

[redacted]@gmail.com

Try another way to sign in

- Tap **Yes** on your phone or tablet
- Get a verification code at ••••• •••••35 *Standard rates apply*
- Call your phone on file ••••• •••••35
- Use your phone or tablet to get a security code (even if it's offline)
- Get help



LinkedIn

Sign-In Verification

This login attempt seems suspicious. Please enter the verification code we sent to your email address or phone to finish signing in.

Didn't get it? Resend to all emails and/or phones

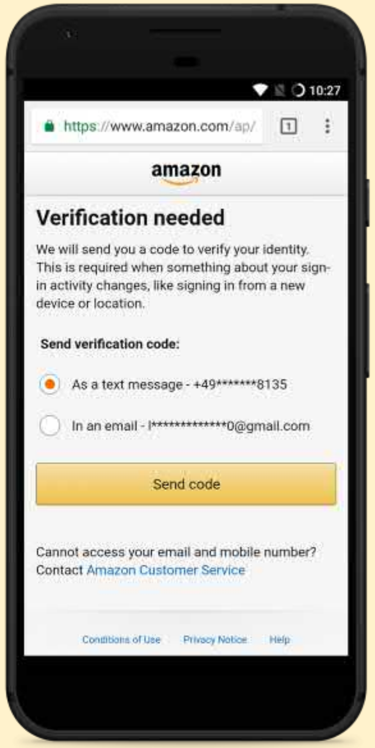
Results

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)*

*: Authentication factor was offered in all tested parameter variations

Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences

/DAS>
Data and Application Security Group



Verification needed

We will send you a code to verify your identity. This is required when something about your sign-in activity changes, like signing in from a new device or location.

Send verification code:

● As a text message - +49*******8135

○ In an email - l*************0@gmail.com

Cannot access your email and mobile number? Contact Amazon Customer Service

More Than Just Good Passwords?

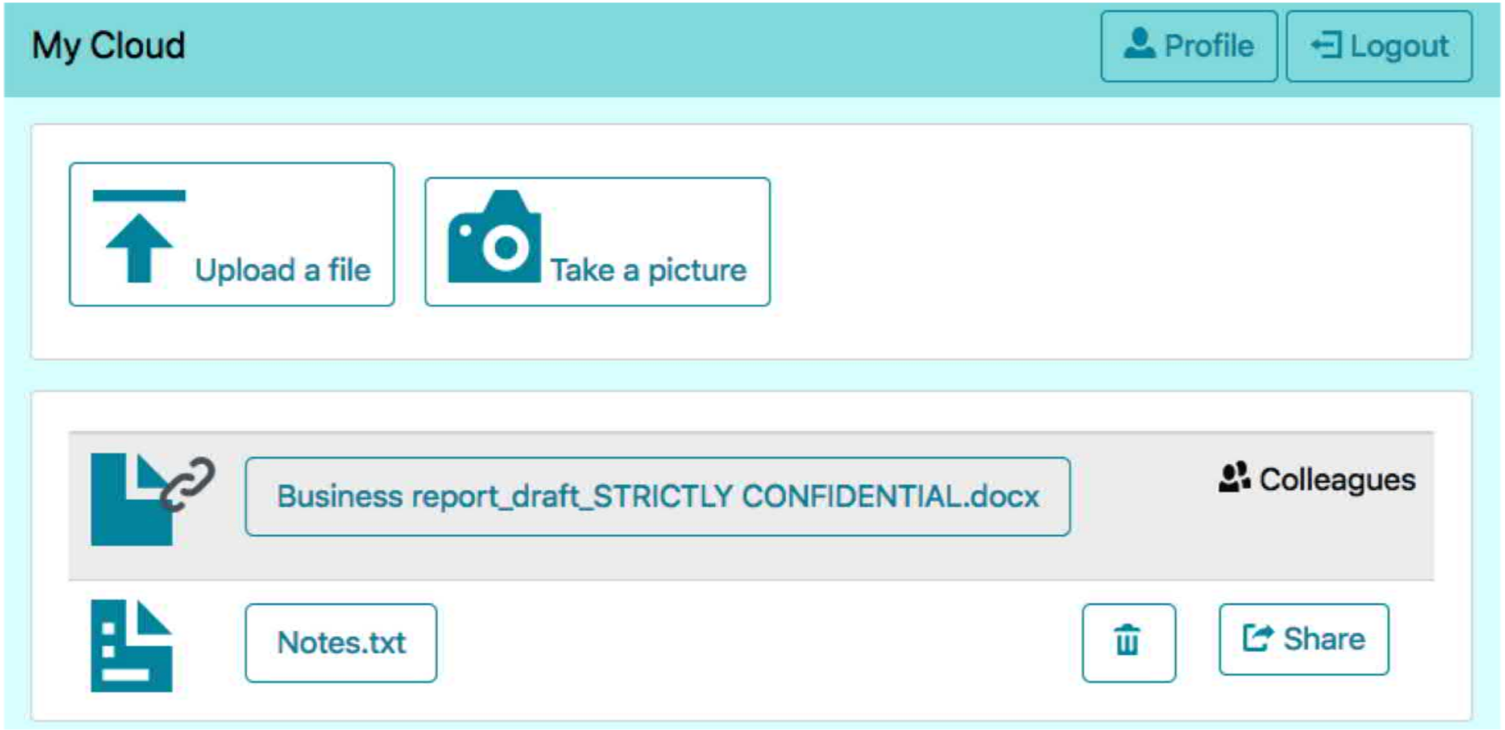
A Study on Usability and Security Perceptions of Risk-based Authentication

Stephan Wiefling*#, Markus Dürmuth#, Luigi Lo Iacono*

H-BRS University of Applied Sciences (*)

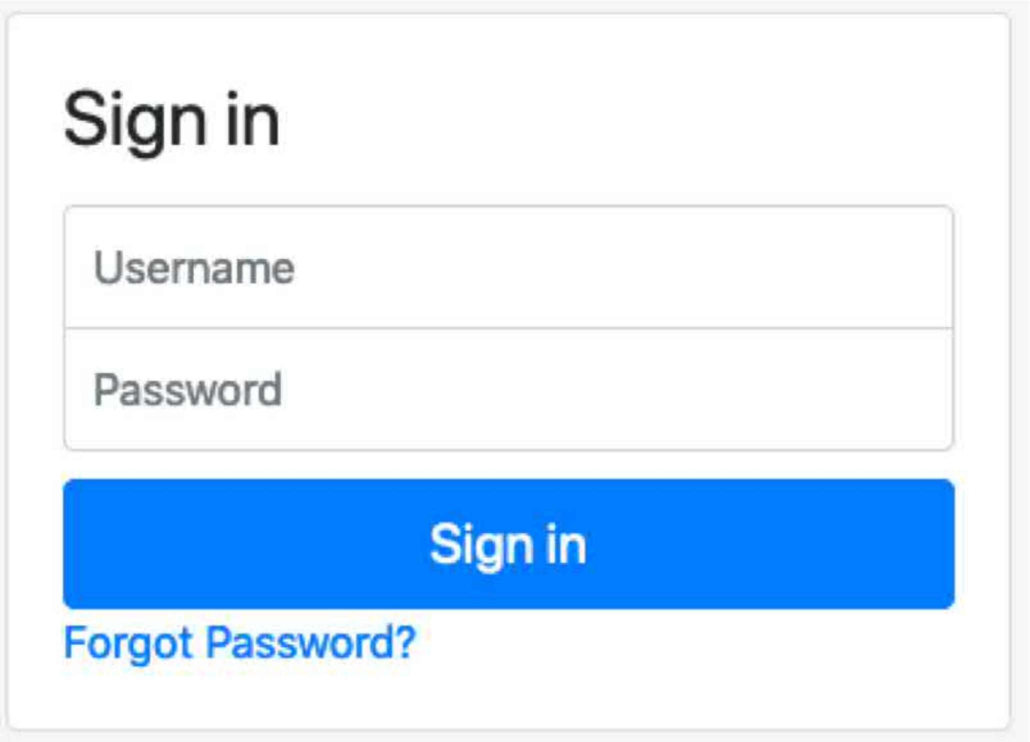
Ruhr University Bochum (#)

Study Website



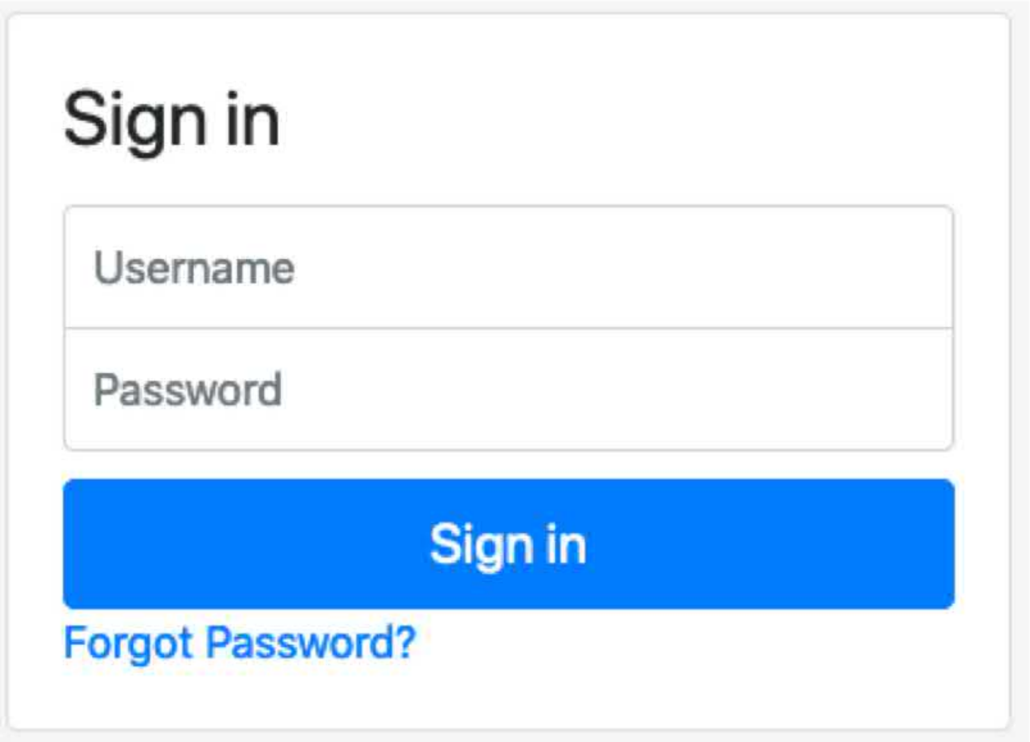
- Introduced as external website to distract from study purpose
- Asked to test website to avoid bias

Study Procedure



Sign in

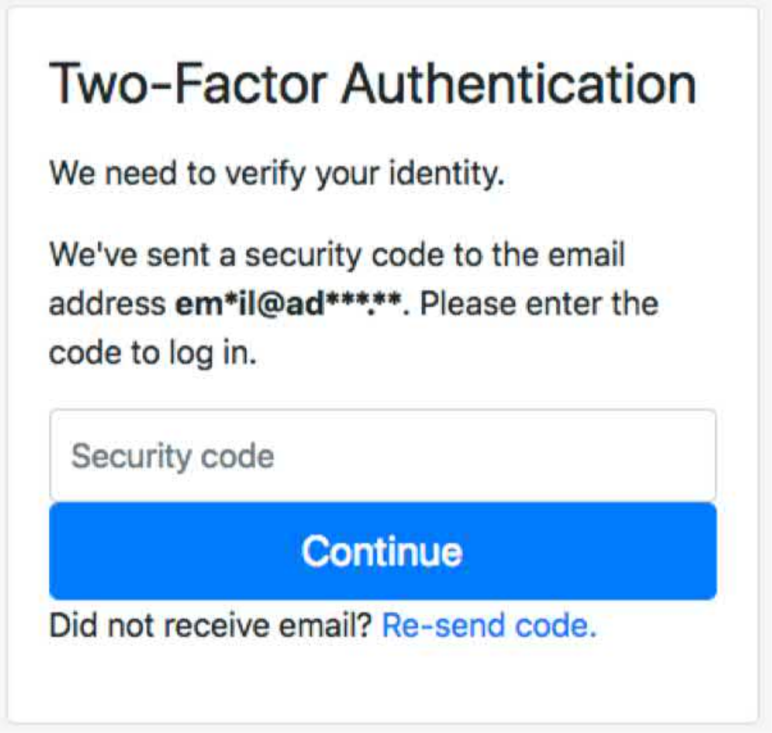
Study Procedure



- 2FA
- RBA-DEVICE
- RBA-LOCATION
- PASSWORD-ONLY

Study Procedure

- 2FA
- RBA-DEVICE
- RBA-LOCATION
- PASSWORD-ONLY



Two-Factor Authentication

We need to verify your identity.

We've sent a security code to the email address **em*il@ad*******. Please enter the code to log in.

Did not receive email? Re-send code.

Always prompted

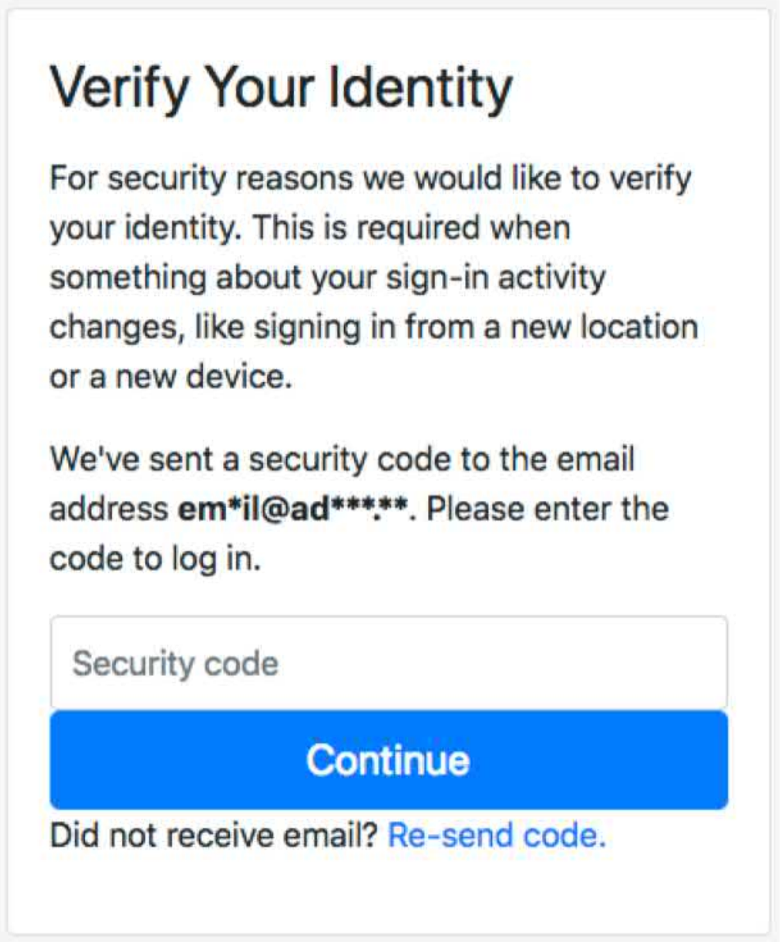
Study Procedure

2FA

RBA-DEVICE

RBA-LOCATION

PASSWORD-ONLY



Verify Your Identity

For security reasons we would like to verify your identity. This is required when something about your sign-in activity changes, like signing in from a new location or a new device.

We've sent a security code to the email address **em*il@ad*****.**. Please enter the code to log in.

Did not receive email? Re-send code.

Prompted on unknown device

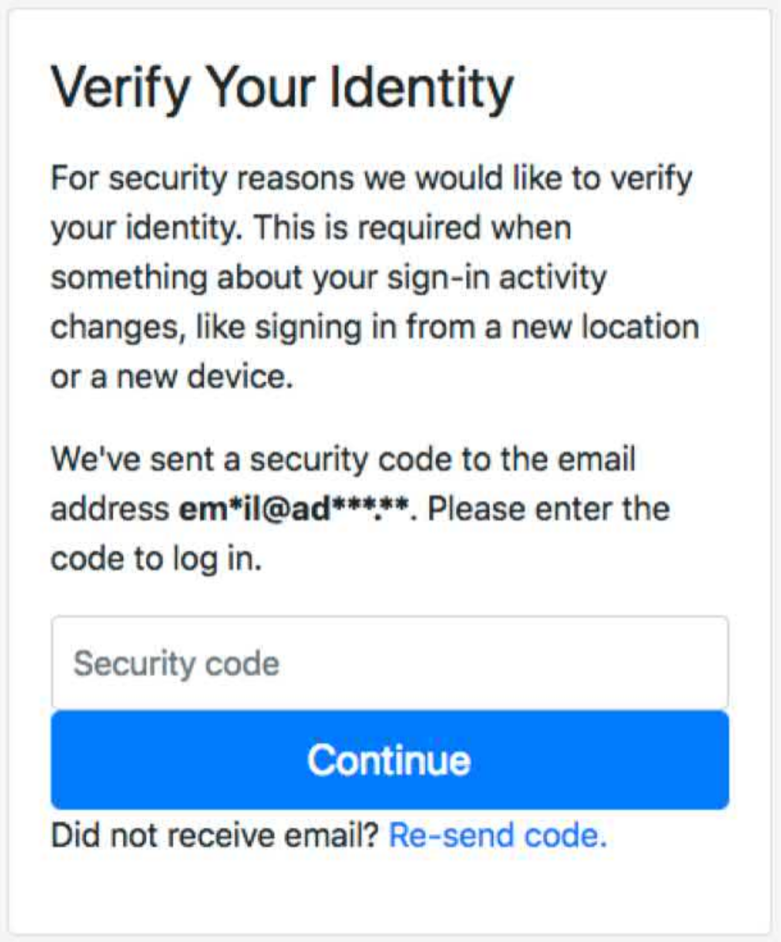
Study Procedure

2FA

RBA-DEVICE

RBA-LOCATION

PASSWORD-ONLY



Verify Your Identity

For security reasons we would like to verify your identity. This is required when something about your sign-in activity changes, like signing in from a new location or a new device.

We've sent a security code to the email address **em*il@ad***.****. Please enter the code to log in.

Did not receive email? Re-send code.

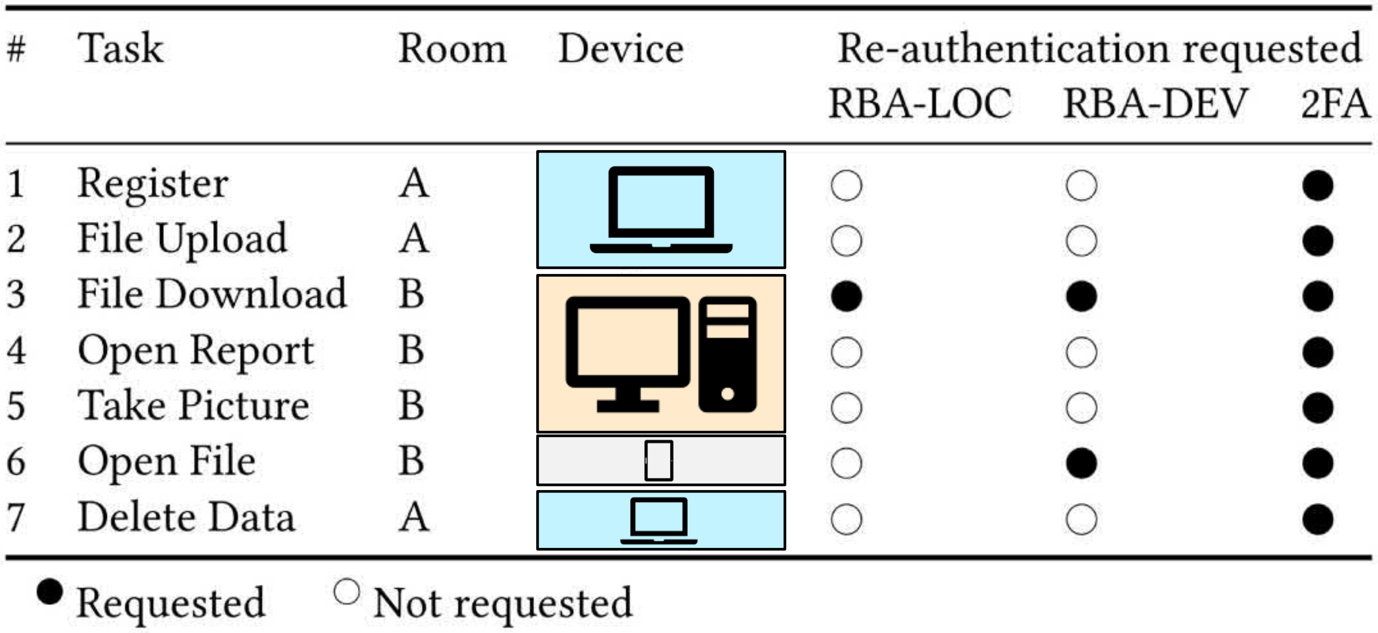
Prompted on unknown location

Study Procedure

- 2FA
- RBA-DEVICE
- RBA-LOCATION
- **PASSWORD-ONLY**

Never prompted

Study Tasks

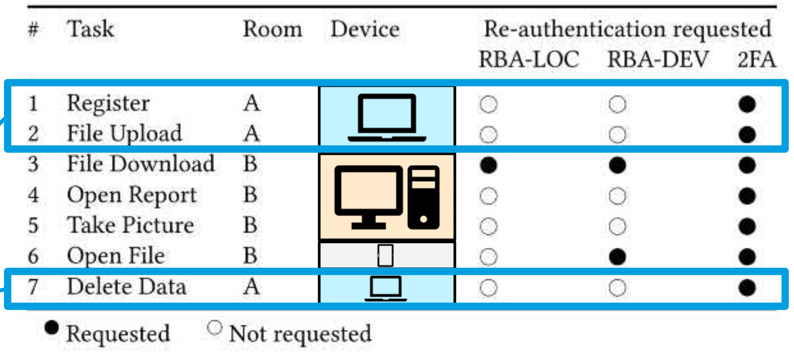


#	Task	Room	Device	Re-authentication requested		
				RBA-LOC	RBA-DEV	2FA
1	Register	A	💻	○	○	●
2	File Upload	A		○	○	●
3	File Download	B	🖥️	●	●	●
4	Open Report	B		○	○	●
5	Take Picture	B		○	○	●
6	Open File	B	📱	○	●	●
7	Delete Data	A	💻	○	○	●

● Requested ○ Not requested

- Create realistic study scenario
- Involve sensitive data and personal devices to increase immersion

Study Tasks

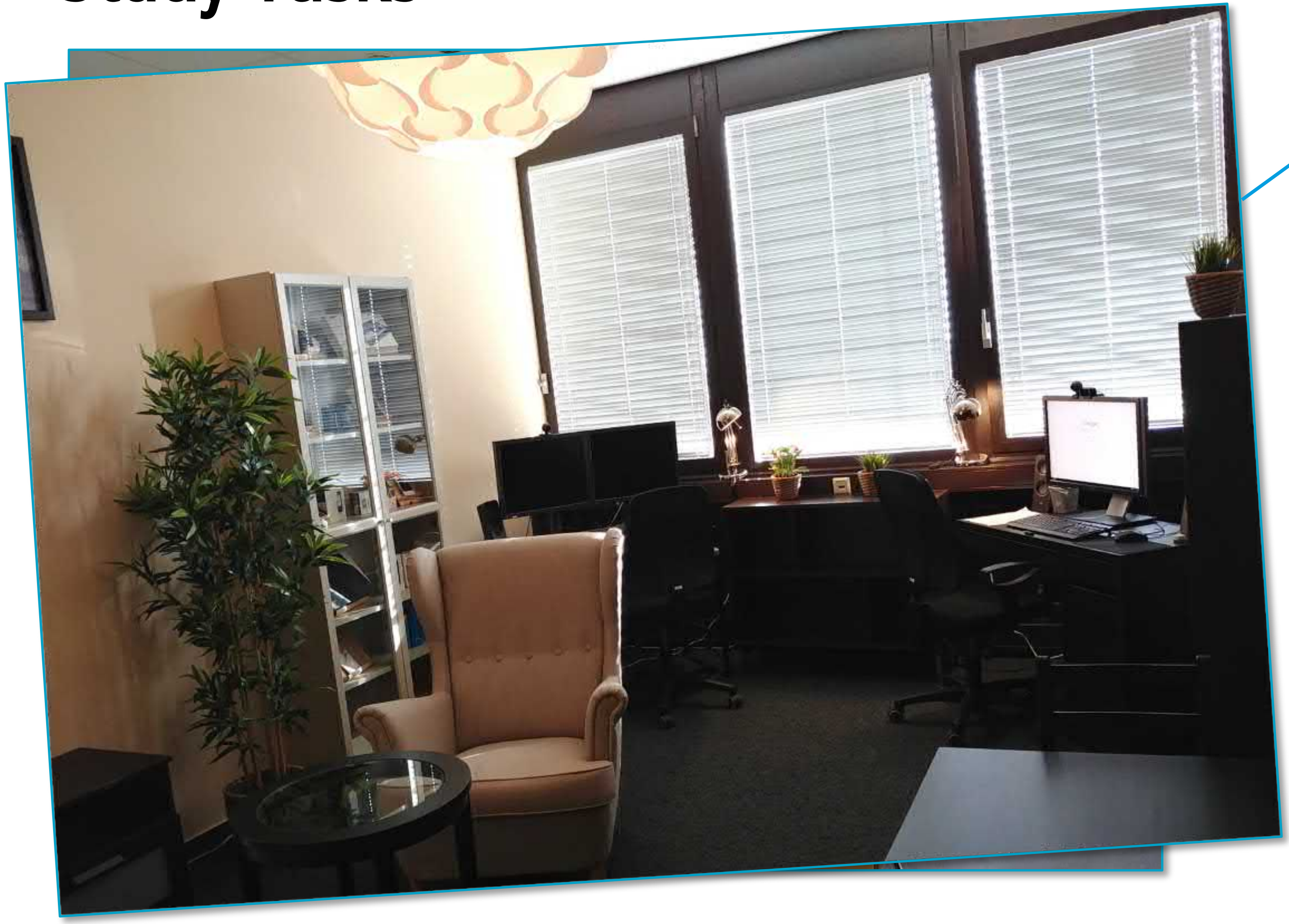


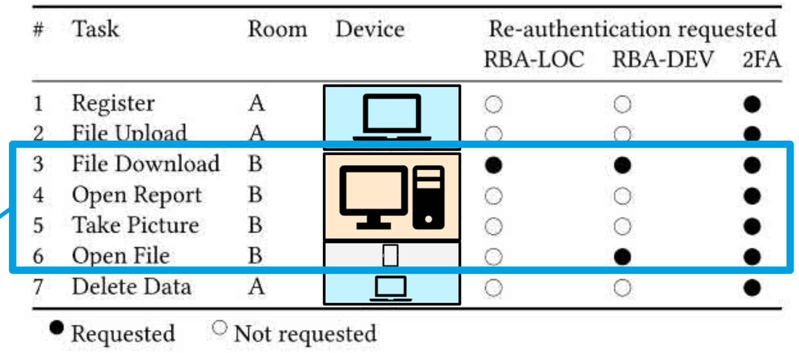
#	Task	Room	Device	Re-authentication requested		
				RBA-LOC	RBA-DEV	2FA
1	Register	A	💻	○	○	●
2	File Upload	A		○	○	●
3	File Download	B	🖥	●	●	●
4	Open Report	B		○	○	●
5	Take Picture	B		○	○	●
6	Open File	B	📱	○	●	●
7	Delete Data	A	💻	○	○	●

● Requested ○ Not requested

- Authentication as secondary task
- Room changes to support understanding

Study Tasks





#	Task	Room	Device	Re-authentication requested		
				RBA-LOC	RBA-DEV	2FA
1	Register	A	💻	○	○	●
2	File Upload	A		○	○	●
3	File Download	B	🖥	●	●	●
4	Open Report	B		○	○	●
5	Take Picture	B		○	○	●
6	Open File	B	📱	○	●	●
7	Delete Data	A	💻	○	○	●

● Requested ○ Not requested

- Authentication as secondary task
- Room changes to support understanding

Study Procedure

Exit survey*

Semi-structured interview

* Questions partially based on
Brooke, J.: SUS: A quick and dirty usability scale. (1996)
H. Khan et al.: Usability and Security Perceptions of Implicit Authentication: Convenient, Secure, Sometimes Annoying. In: SOUPS '15. USENIX (2015)
L. Agarwal et al.: Ask Me Again But Don't Annoy Me: Evaluating Re-authentication Strategies for Smartphones. In: SOUPS '16. USENIX (2016)

Study Procedure

Exit survey*

Measure usability and security perceptions

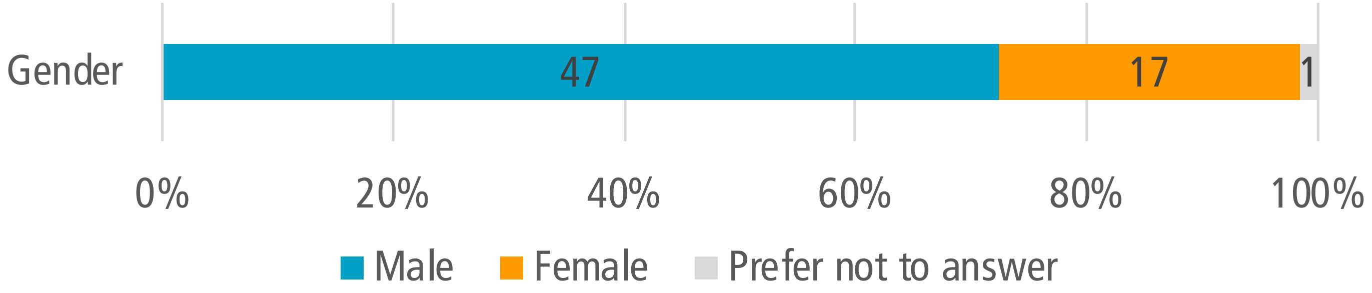
Semi-structured interview

Understand survey responses

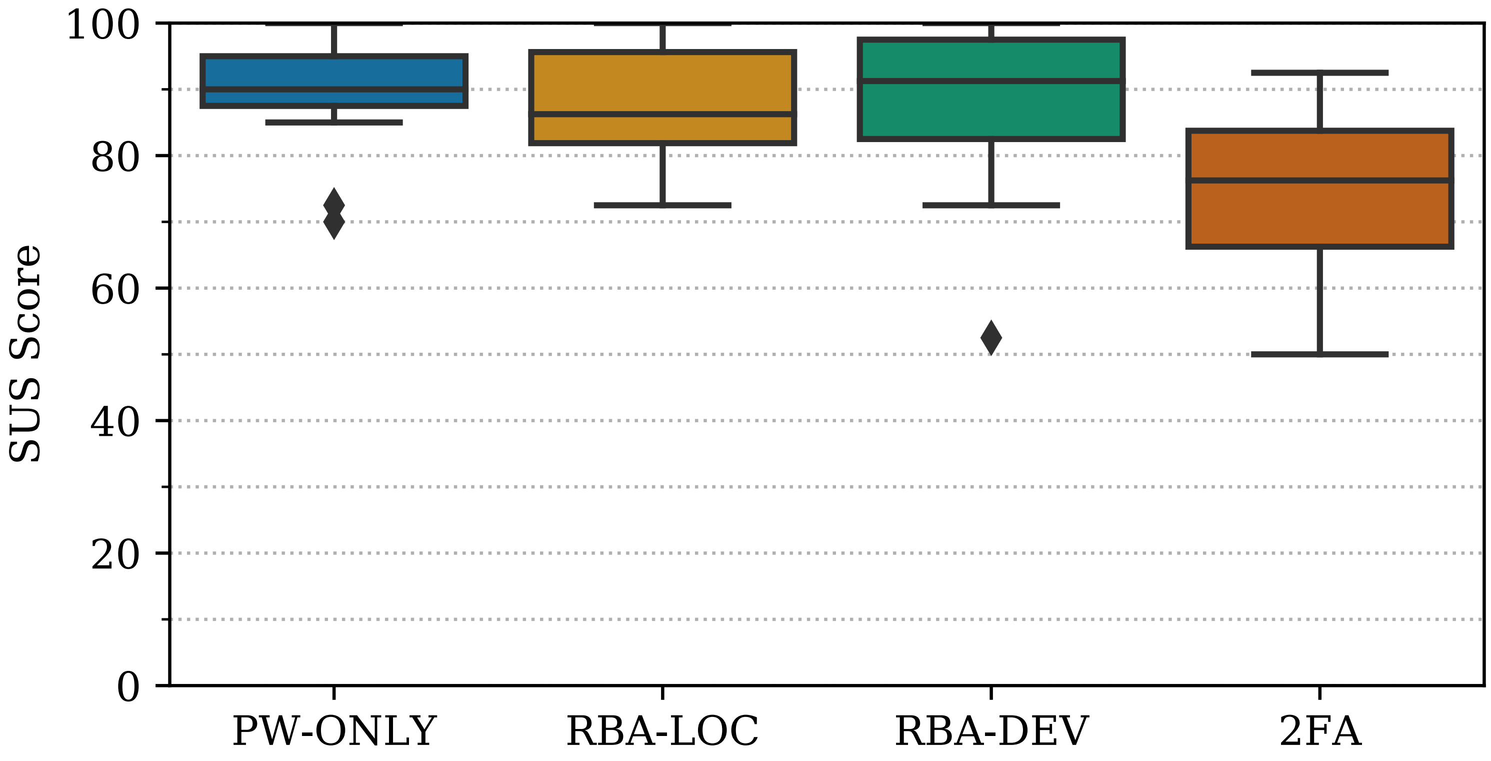
* Questions partially based on
Brooke, J.: SUS: A quick and dirty usability scale. (1996)
H. Khan et al.: Usability and Security Perceptions of Implicit Authentication: Convenient, Secure, Sometimes Annoying. In: SOUPS ‘15. USENIX (2015)
L. Agarwal et al.: Ask Me Again But Don’t Annoy Me: Evaluating Re-authentication Strategies for Smartphones. In: SOUPS ‘16. USENIX (2016)

Demographics

- N=65
  - 17 in PW-ONLY
  - 16 all other conditions
- Age: 19-33 years
  (mean: 24.57, SD: 3.22)



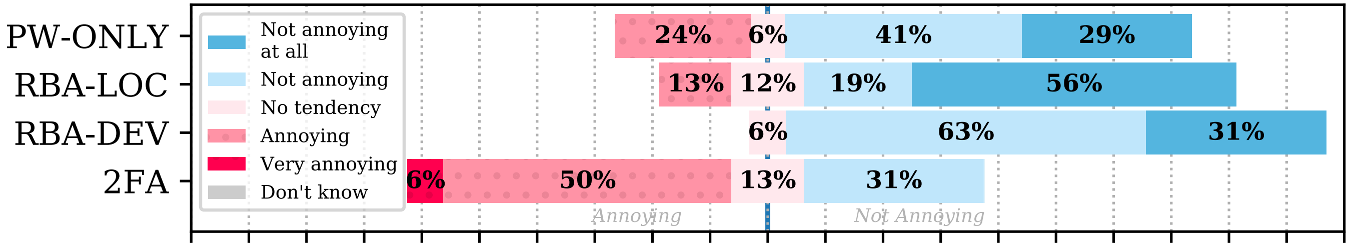
RBA and PW-ONLY Usability higher than 2FA



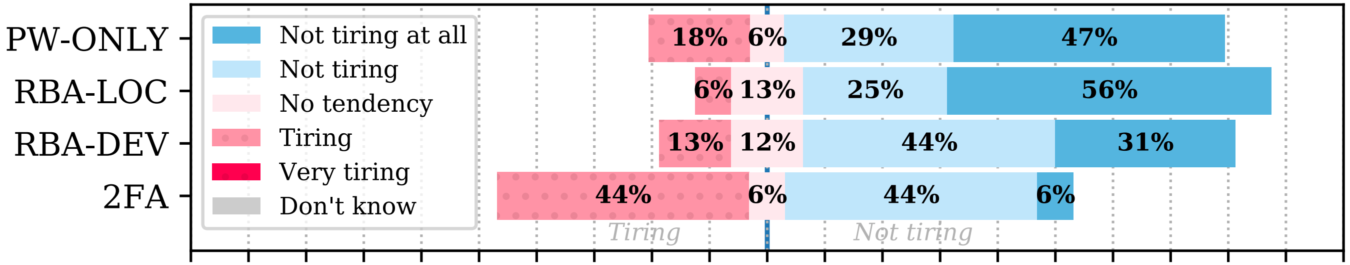
- System Usability Scale (SUS) scores or subquestion answers significantly lower for 2FA ($p<0.05$)

RBA more accepted than 2FA

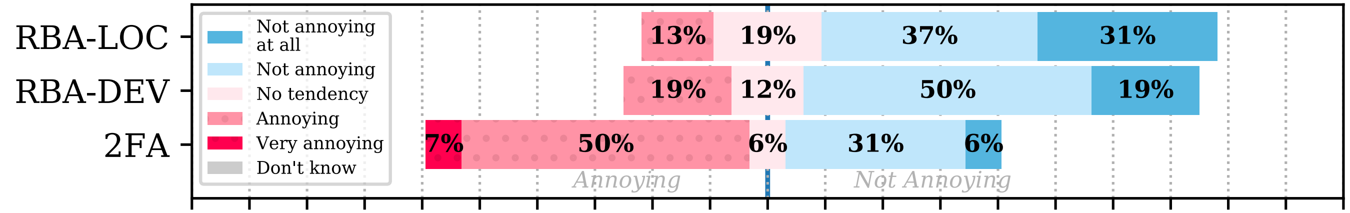
(U1a) How annoying or not annoying did you perceive this login procedure?



(U1b) How tiring or not-tiring did you find this login procedure?

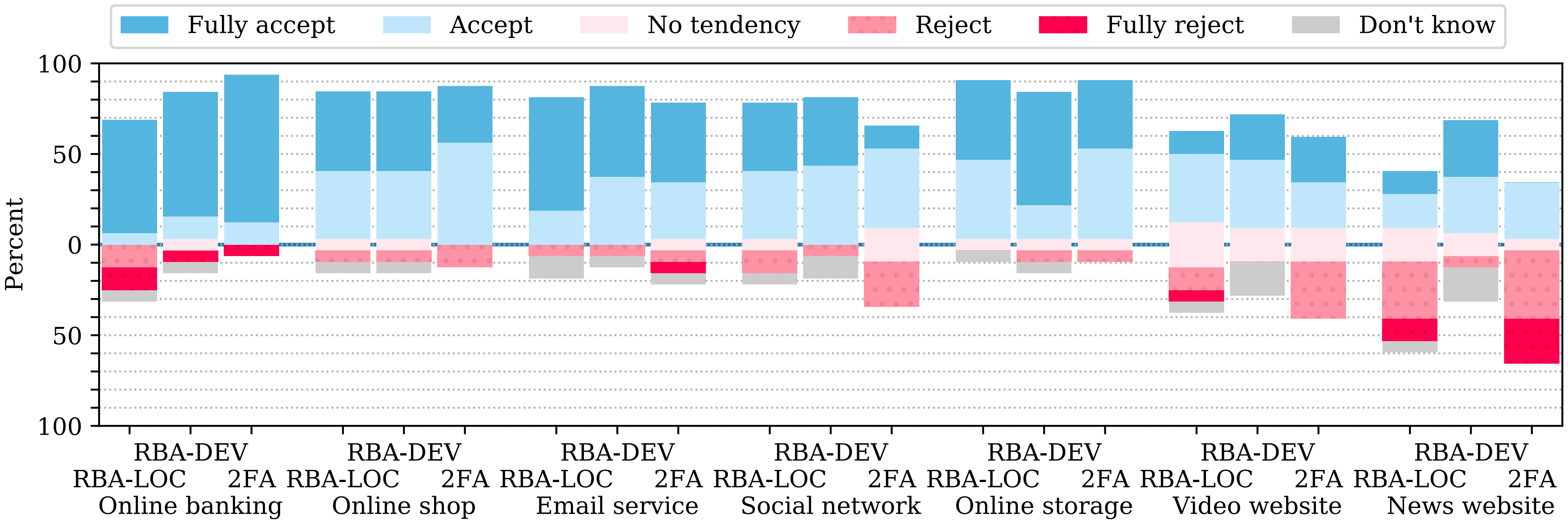


(U1c) How did you perceive the interruptions for confirming the identity?



- RBA in many cases significantly higher than 2FA

But: Acceptance differs



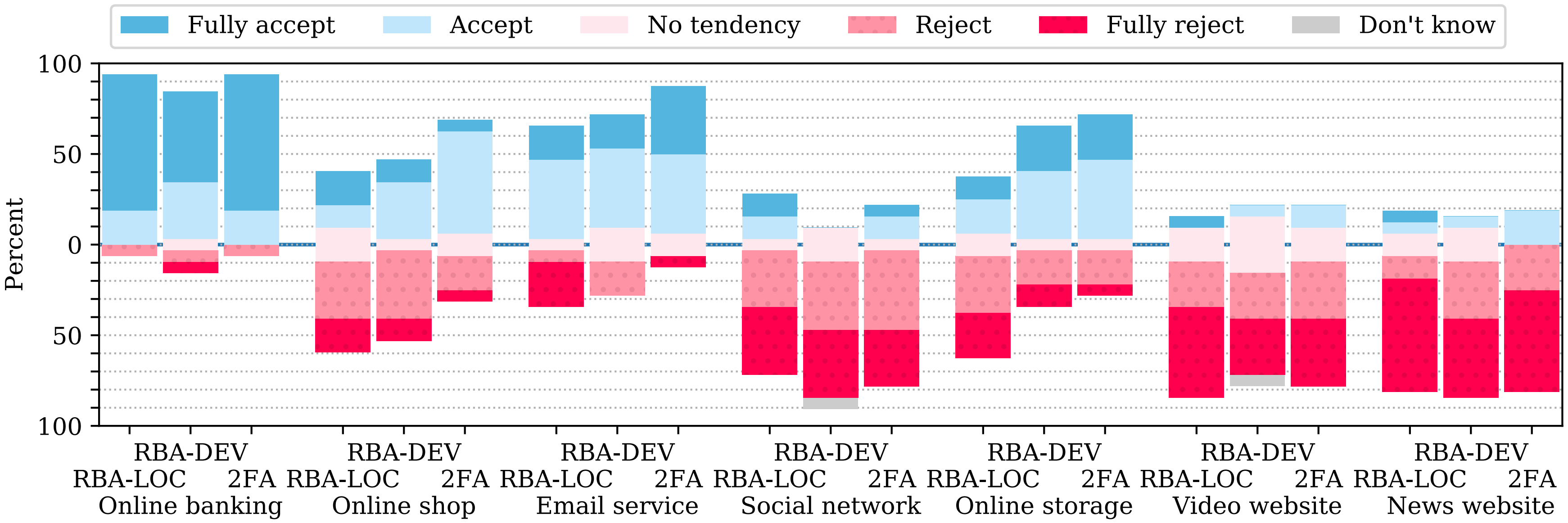
E-Mail

Phone number

App

- Re-authentication factor
- Data sensitivity in use case scenario

But: Acceptance differs



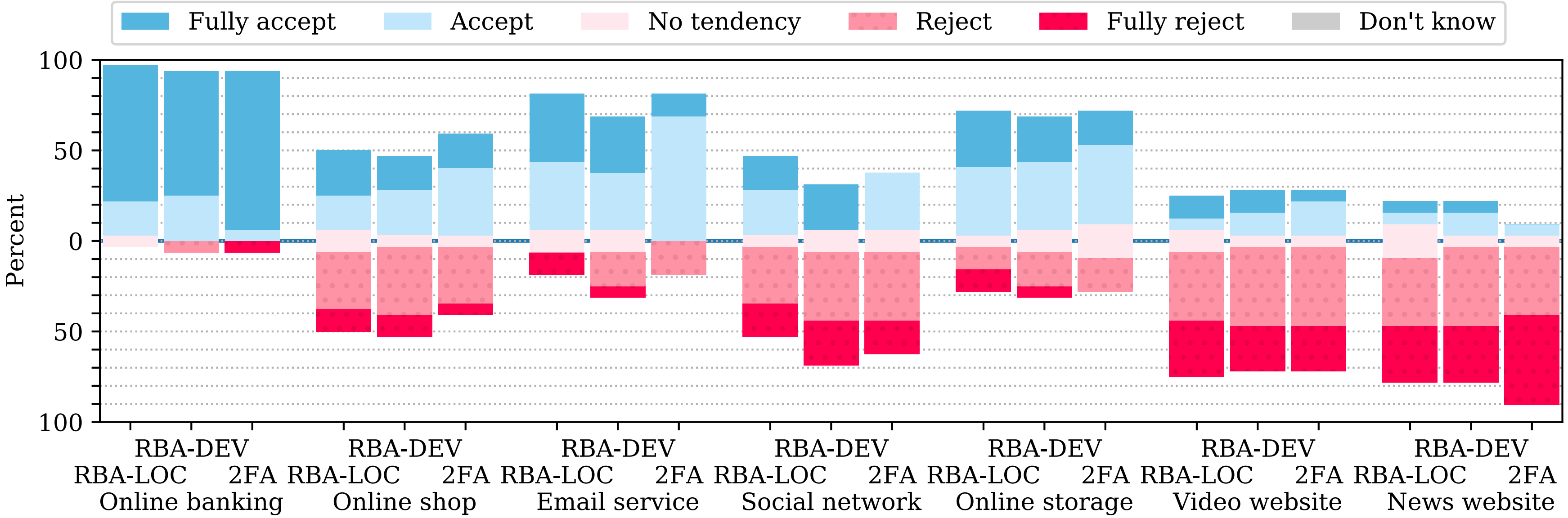
E-Mail

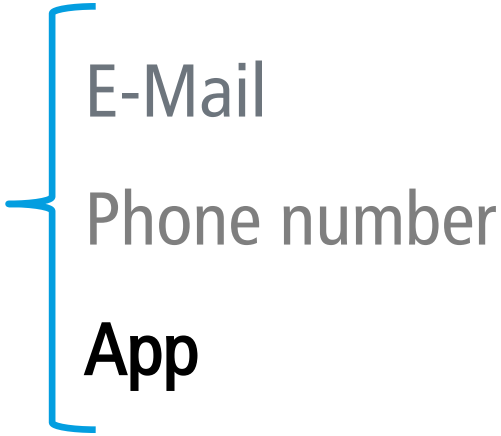
Phone number

App

- Re-authentication factor
- Data sensitivity in use case scenario

But: Acceptance differs





- Re-authentication factor
- Data sensitivity in use case scenario

Factors influencing acceptance

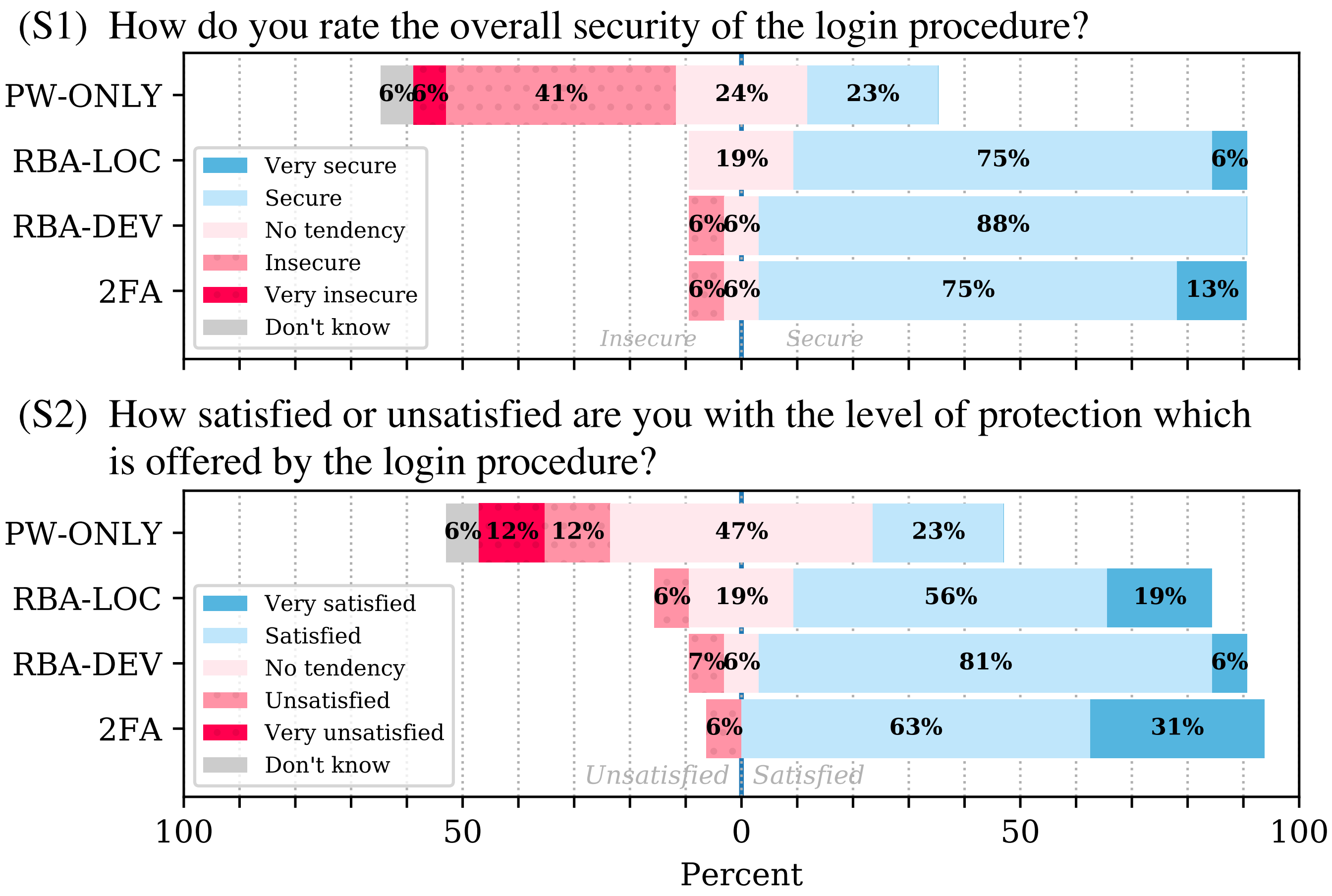
Trust in online service

“[I’m not providing my phone number] because […] I made experiences in the past where I was partly spammed. I received some curious messages, although I only wanted to log in in a secure way.” (P17)

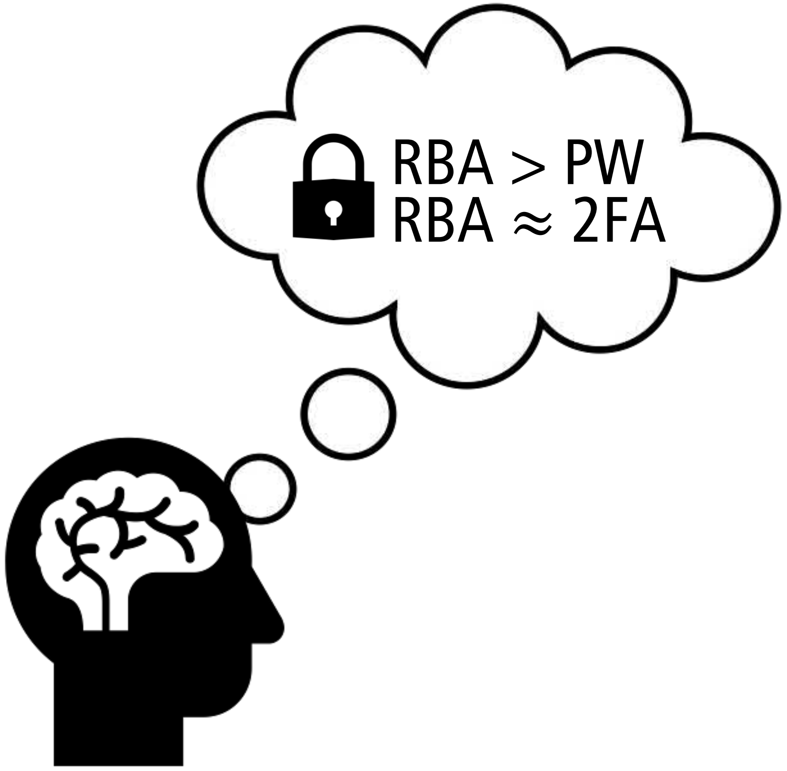
Device involved

“because […] I want to log in quickly and watch something now. [. . .] on Netflix […] you do more on the TV […] and then it's just critical.” (P31)

RBA and 2FA perceived more secure (p<0.05)

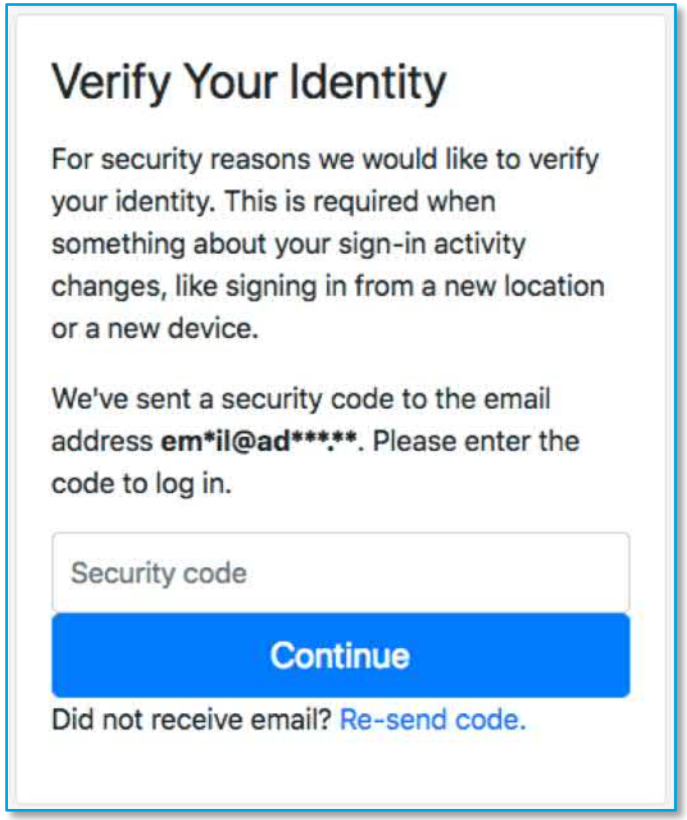

(S1) How do you rate the overall security of the login procedure?

(S2) How satisfied or unsatisfied are you with the level of protection which is offered by the login procedure?


RBA > PW
RBA ≈ 2FA

Additional Findings

Deadlock Problem



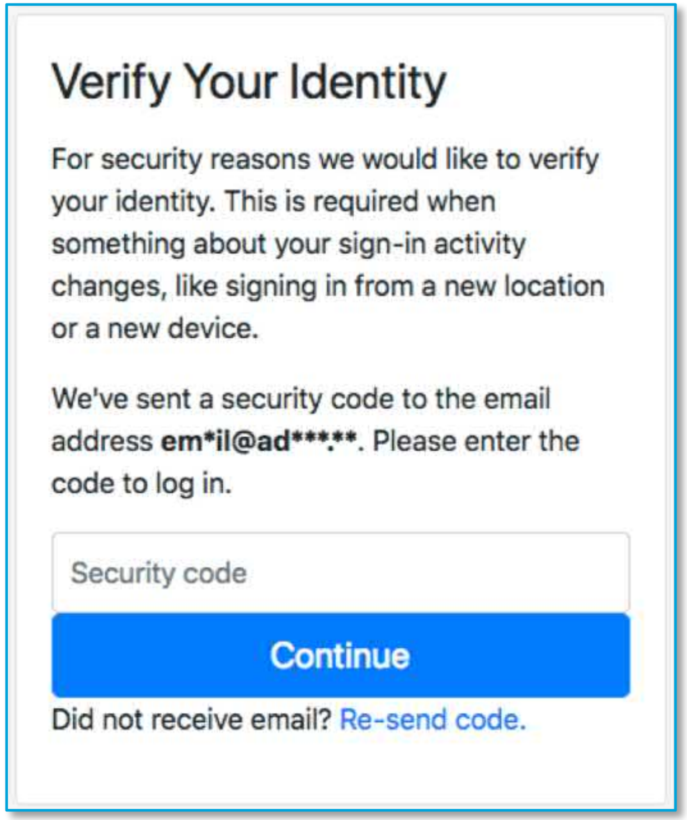
Verify Your Identity

For security reasons we would like to verify your identity. This is required when something about your sign-in activity changes, like signing in from a new location or a new device.

We've sent a security code to the email address **em*il@ad*****.**. Please enter the code to log in.

Did not receive email? Re-send code.

Deadlock Problem



Verify Your Identity

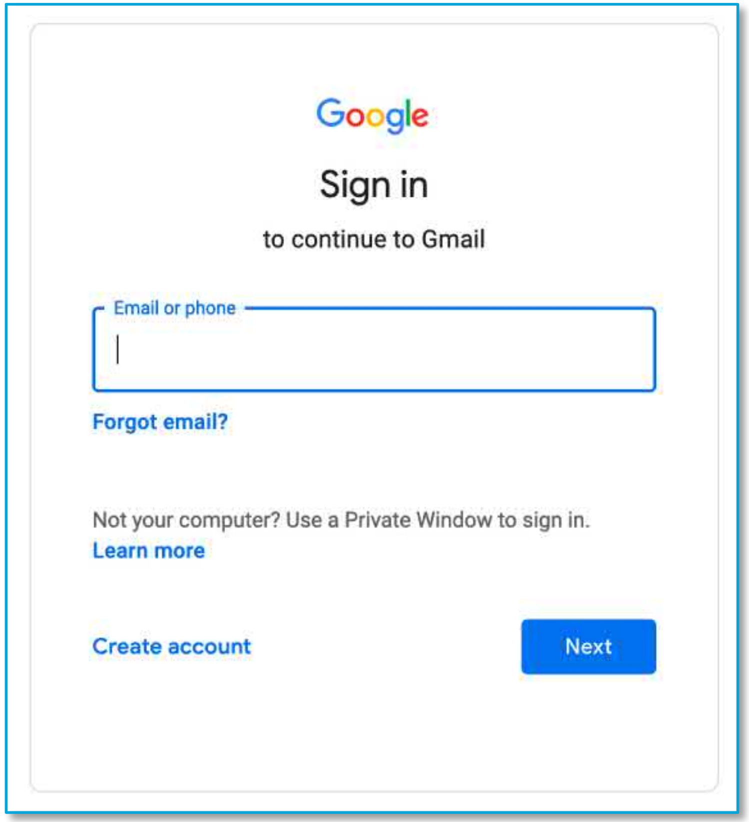
For security reasons we would like to verify your identity. This is required when something about your sign-in activity changes, like signing in from a new location or a new device.

We've sent a security code to the email address **em*il@ad***.****. Please enter the code to log in.

Security code

Did not receive email? Re-send code.

→



Google

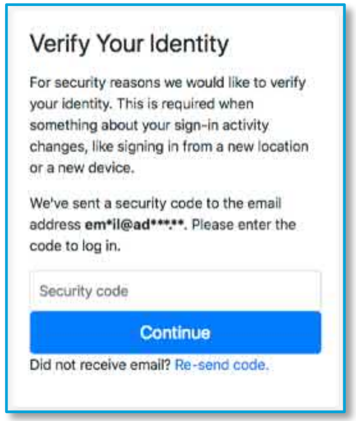
Sign in

to continue to Gmail

Email or phone

Not your computer? Use a Private Window to sign in.
Learn more

Deadlock Problem



Verify Your Identity

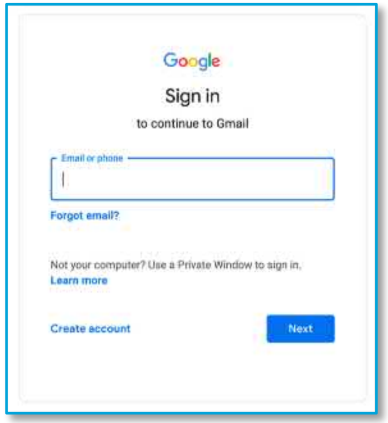
For security reasons we would like to verify your identity. This is required when something about your sign-in activity changes, like signing in from a new location or a new device.

We've sent a security code to the email address **em*il@ad***.****. Please enter the code to log in.

Security code

Continue

Did not receive email? Re-send code.



Google

Sign in

to continue to Gmail

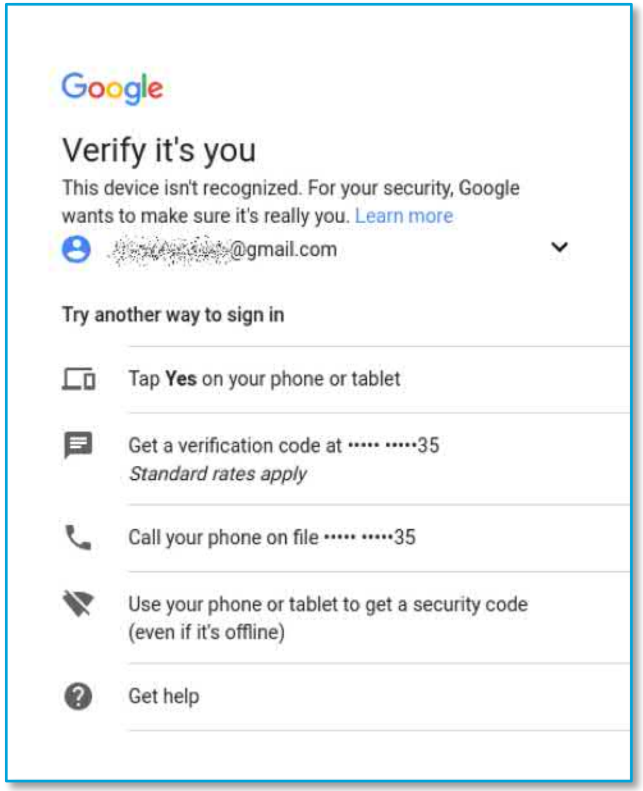
Email or phone

Forgot email?

Not your computer? Use a Private Window to sign in. Learn more

Create account

Next



Google

Verify it's you

This device isn't recognized. For your security, Google wants to make sure it's really you. Learn more

[redacted]@gmail.com

Try another way to sign in

Tap **Yes** on your phone or tablet

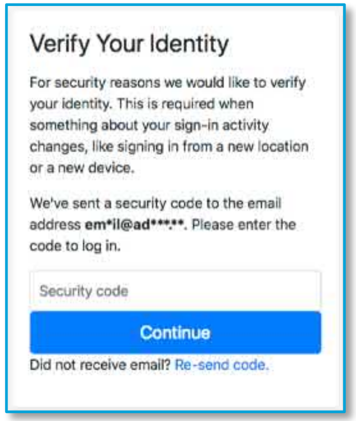
Get a verification code at ••••• •••••35
Standard rates apply

Call your phone on file ••••• •••••35

Use your phone or tablet to get a security code (even if it's offline)

Get help

Deadlock Problem

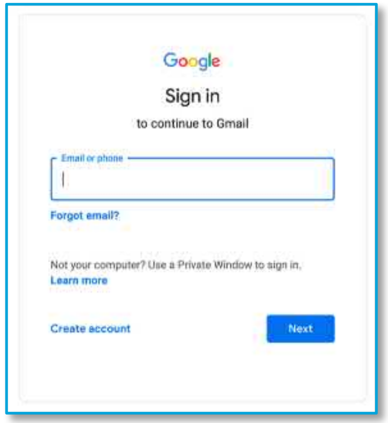


Verify Your Identity

For security reasons we would like to verify your identity. This is required when something about your sign-in activity changes, like signing in from a new location or a new device.

We've sent a security code to the email address **em*il@ad***.****. Please enter the code to log in.

Did not receive email? Re-send code.

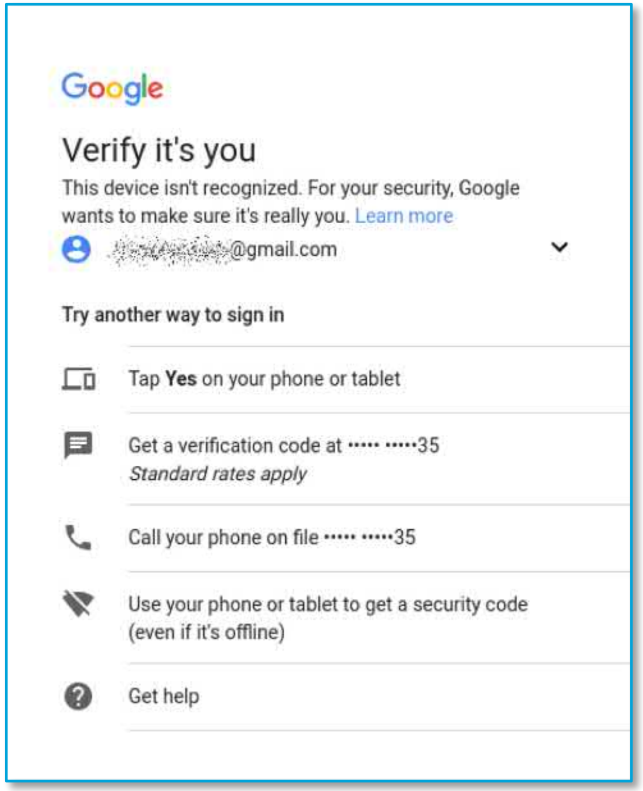


Google

Sign in

to continue to Gmail

Not your computer? Use a Private Window to sign in. Learn more



Google

Verify it's you

This device isn't recognized. For your security, Google wants to make sure it's really you. Learn more

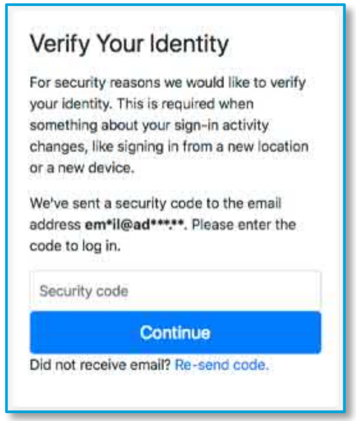
[redacted]@gmail.com

Try another way to sign in

- Tap **Yes** on your phone or tablet
- Get a verification code at ••••• •••••35
  Standard rates apply
- Call your phone on file ••••• •••••35
- Use your phone or tablet to get a security code (even if it's offline)
- Get help

Don't have phone with me?!!

Deadlock Problem



Verify Your Identity

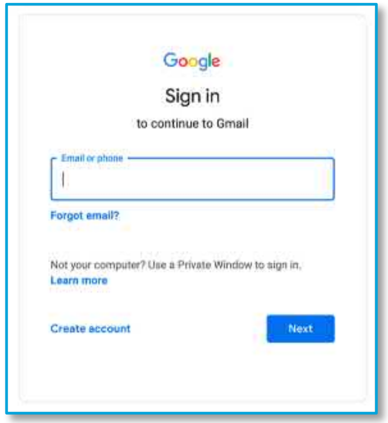
For security reasons we would like to verify your identity. This is required when something about your sign-in activity changes, like signing in from a new location or a new device.

We've sent a security code to the email address **em*il@ad***.**. Please enter the code to log in.

Security code

Continue

Did not receive email? Re-send code.



Google

Sign in

to continue to Gmail

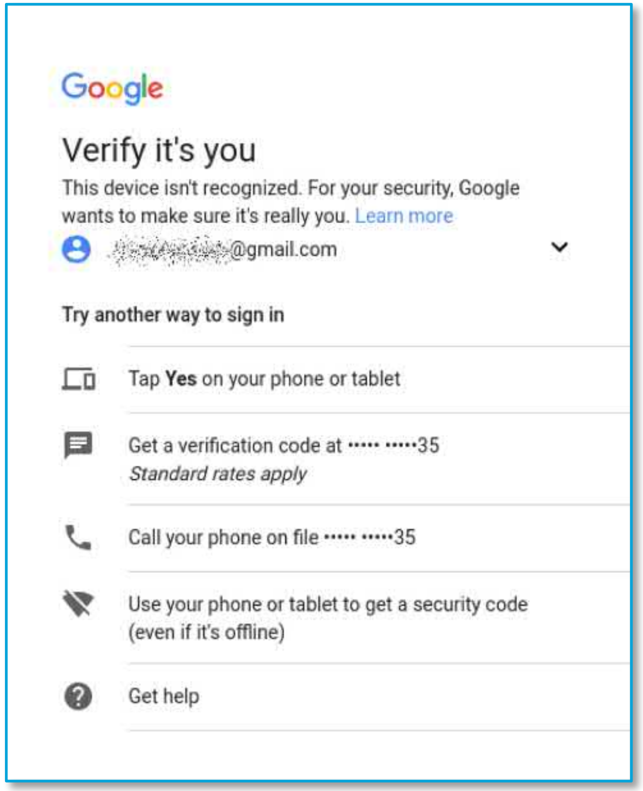
Email or phone

Forgot email?

Not your computer? Use a Private Window to sign in. Learn more

Create account

Next



Google

Verify it's you

This device isn't recognized. For your security, Google wants to make sure it's really you. Learn more

[redacted]@gmail.com

Try another way to sign in

Tap **Yes** on your phone or tablet

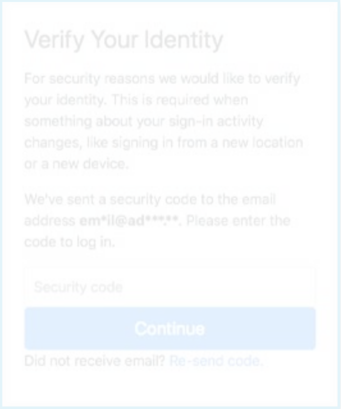
Get a verification code at ••••• •••••35
Standard rates apply

Call your phone on file ••••• •••••35

Use your phone or tablet to get a security code (even if it's offline)

Get help

Deadlock Problem

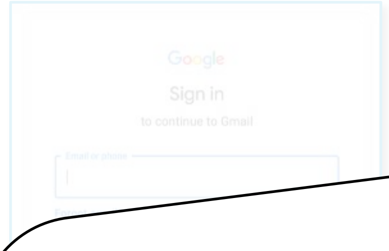


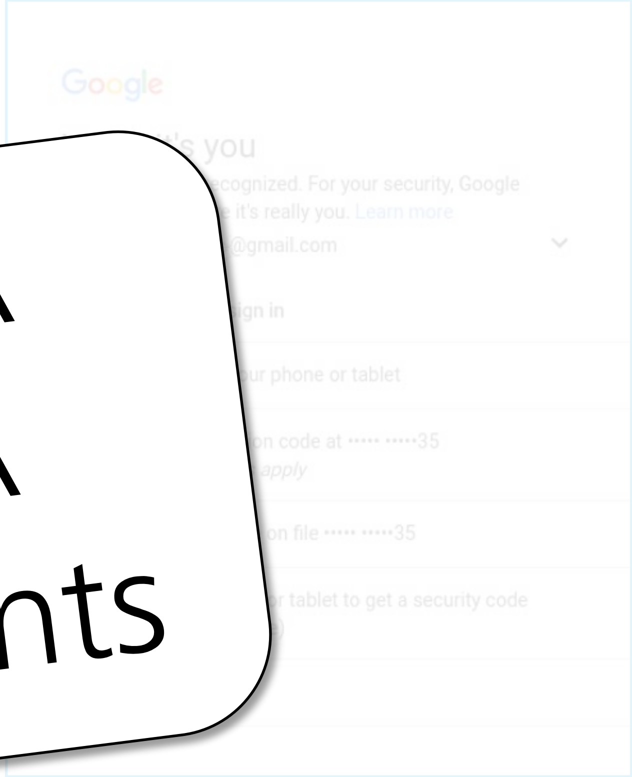
Verify Your Identity

For security reasons we would like to verify your identity. This is required when something about your sign-in activity changes, like signing in from a new location or a new device.

We've sent a security code to the email address **em*il@ad***.****. Please enter the code to log in.

Did not receive email? Re-send code.





's you

ecognized. For your security, Google
e it's really you. Learn more

@gmail.com

ign in

ur phone or tablet

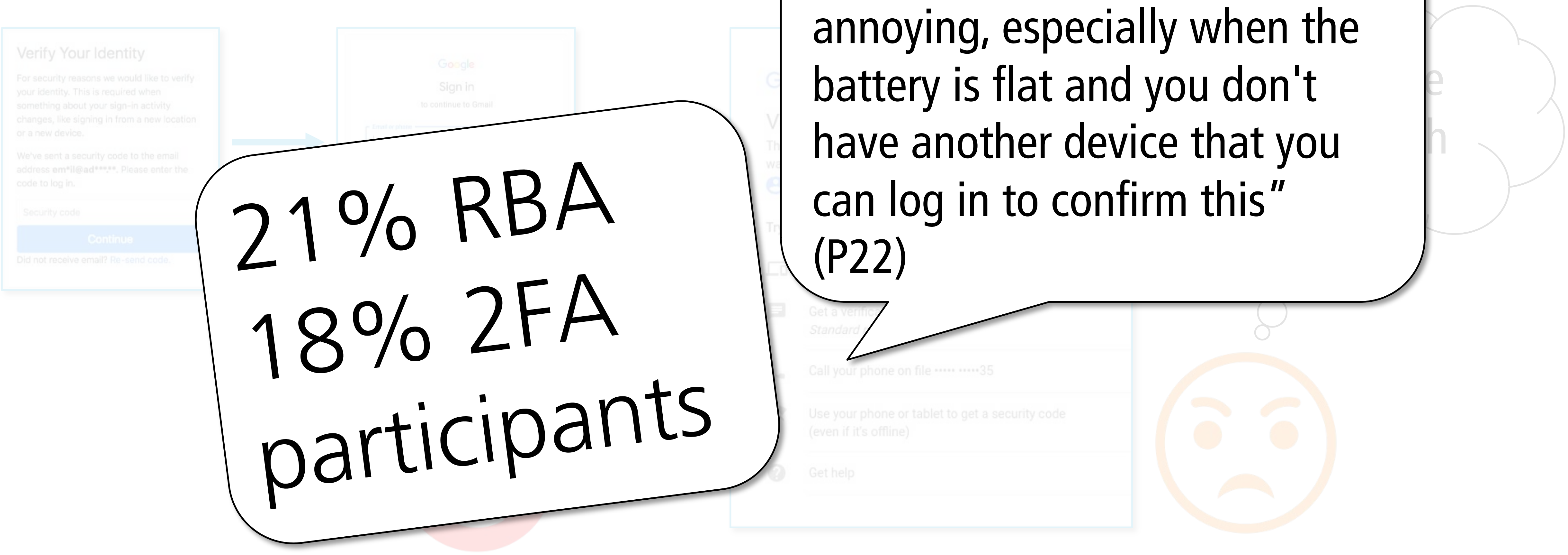
on code at ••••• •••••35
apply

on file ••••• •••••35

r tablet to get a security code

21% RBA
18% 2FA
participants

Deadlock Problem



Verify Your Identity

For security reasons we would like to verify your identity. This is required when something about your sign-in activity changes, like signing in from a new location or a new device.

We've sent a security code to the email address em*il@ad***.**. Please enter the code to log in.

Security code

Continue

Did not receive email? Re-send code.

Google

Sign in

to continue to Gmail

Get a verific...

Standard...

Call your phone on file ••••• •••••35

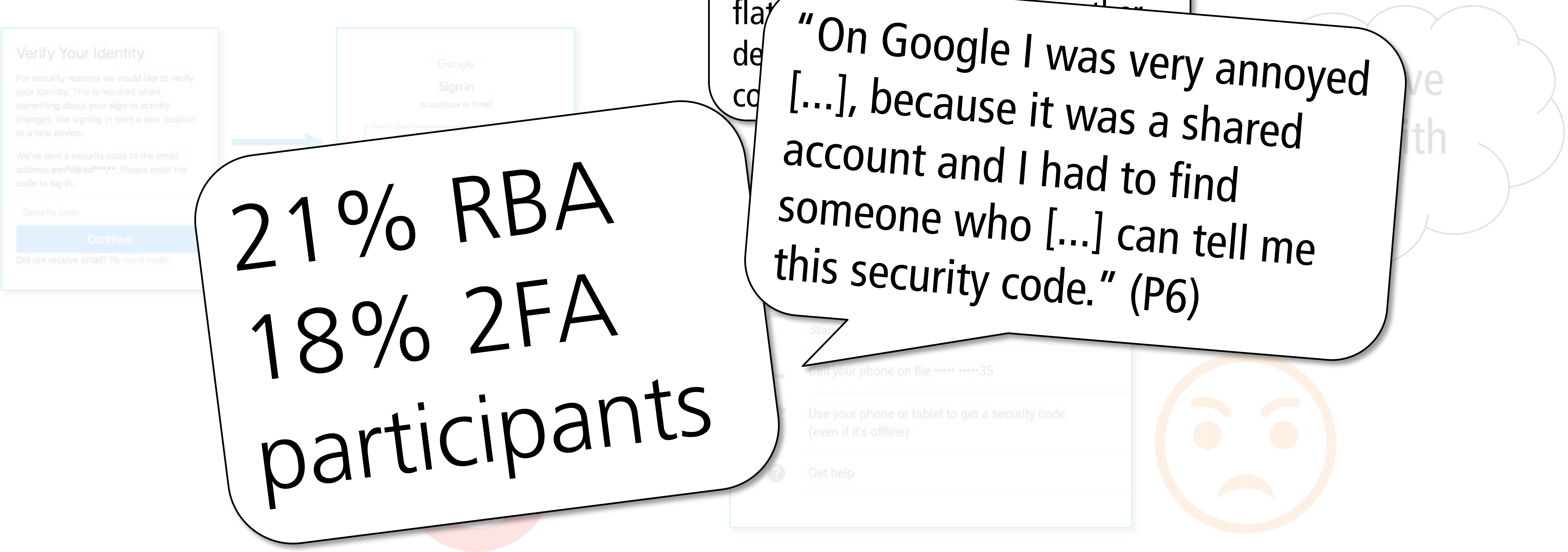
Use your phone or tablet to get a security code (even if it's offline)

Get help

21% RBA
18% 2FA
participants

“Sometimes [it's] very annoying, especially when the battery is flat and you don't have another device that you can log in to confirm this” (P22)

Deadlock Problem



Verify Your Identity

For security reasons we would like to verify your identity. This is required when something about your sign-in activity changes, like signing in from a new location or a new device.

We've sent a security code to the email address **em*il@ad***.****. Please enter the code to log in.

Security code

Continue

Did not receive email? Re-send code.

Call your phone on file ••••• •••••35

Use your phone or tablet to get a security code (even if it's offline)

Get help

“Sometimes [it's] very annoying, especially when the battery is fla
de
co

“On Google I was very annoyed […], because it was a shared account and I had to find someone who […] can tell me this security code.” (P6)

21% RBA
18% 2FA
participants