

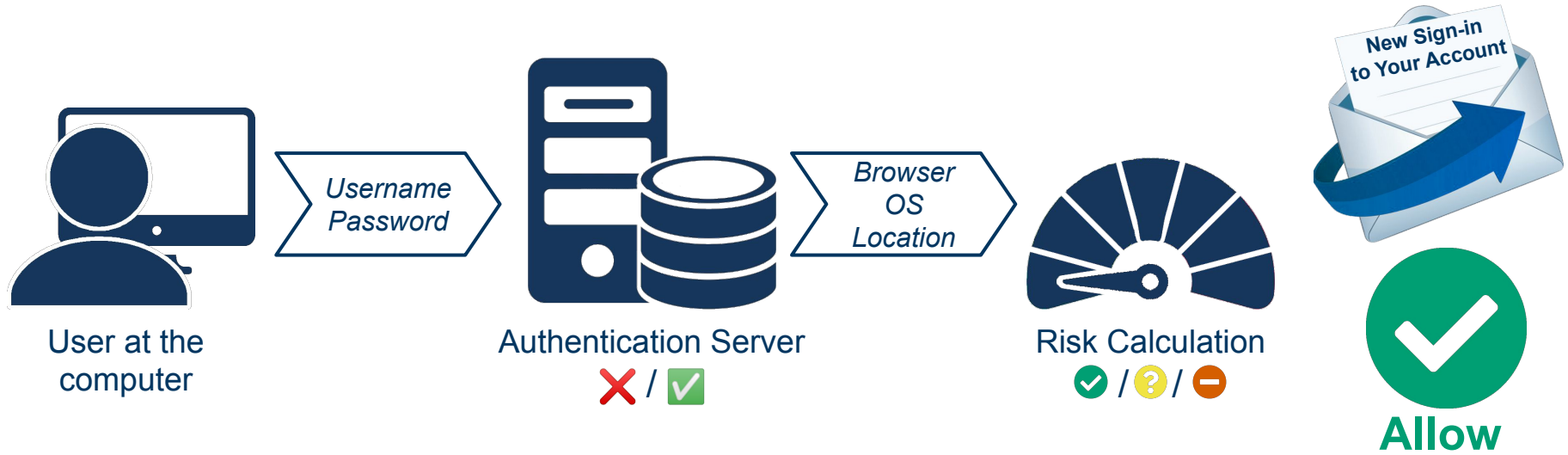
Usability and Security of Risk-based Authentication

Philipp Markert

Thesis Defense • July 28, 2023 • Bochum

Risk-based Authentication (RBA) As a Way to Add Security

During the login of a user, **calculate a risk based on contextual factors**.



Risk-based Authentication (RBA) As a Way to Add Security

During the login of a user, calculate a risk based on contextual factors.

Increases security while limiting unnecessary security prompts to a minimum.



Please provide the following code to complete your login: 123456

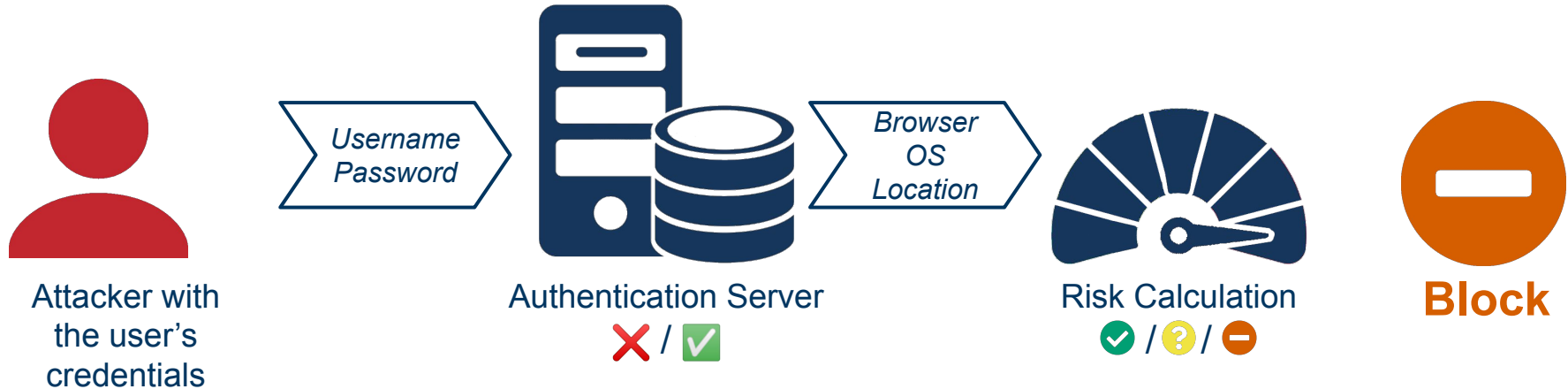


Challenge

Risk-based Authentication (RBA) As a Way to Add Security

During the login of a user, calculate a risk based on contextual factors.

Increases security while limiting unnecessary security prompts to a minimum.



17 Publications since 2019

Thesis

**Security of
Knowledge-based
Authentication**
IEEE SP 20

**Two-Factor
Authentication
With the German ID**
*EuroUSEC 22**

**Configuration of
Risk-based
Authentication**
SOUPS 22

**Users' Interaction
With Login
Notifications**
*USENIX Sec. 24***

Publications Extending the Thesis Scope



Mobile Authentication

*ACM TOPS 21, SOUPS 20 & 21,
USENIX Sec. 22, EuroUSEC 23*



(Fallback) Authentication

USEC 19, WAY 19, CANS 21



Account Remediation

WIPS 21, ACSAC 22, USEC 23

Today: Practitioners' and End-Users' Perspective on RBA

Configuration of
Risk-based
Authentication
SOUPS 22



Luis Alvarez | Getty Images

Users' Interaction
With Login
Notifications
*USENIX Sec. 24**



monkeybusinessimages | Getty Images

How do administrators configure RBA?

How do users interact with login notifications?

Understanding How Administrators Configure RBA Is Crucial

Appropriately configured, RBA increases security while limiting unnecessary security prompts to a minimum.



	Allow	Optional MFA	Require MFA	Block
Low risk	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Medium risk	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
High risk	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Admins Don't Rely on the Default Risk Behavior



Behavior:  Allow  Optional MFA  Required MFA  Block

“As soon as it’s a risk, I want to require MFA.” (P7)

Low Risk



Required MFA

Medium Risk



Required MFA

High Risk



Required MFA

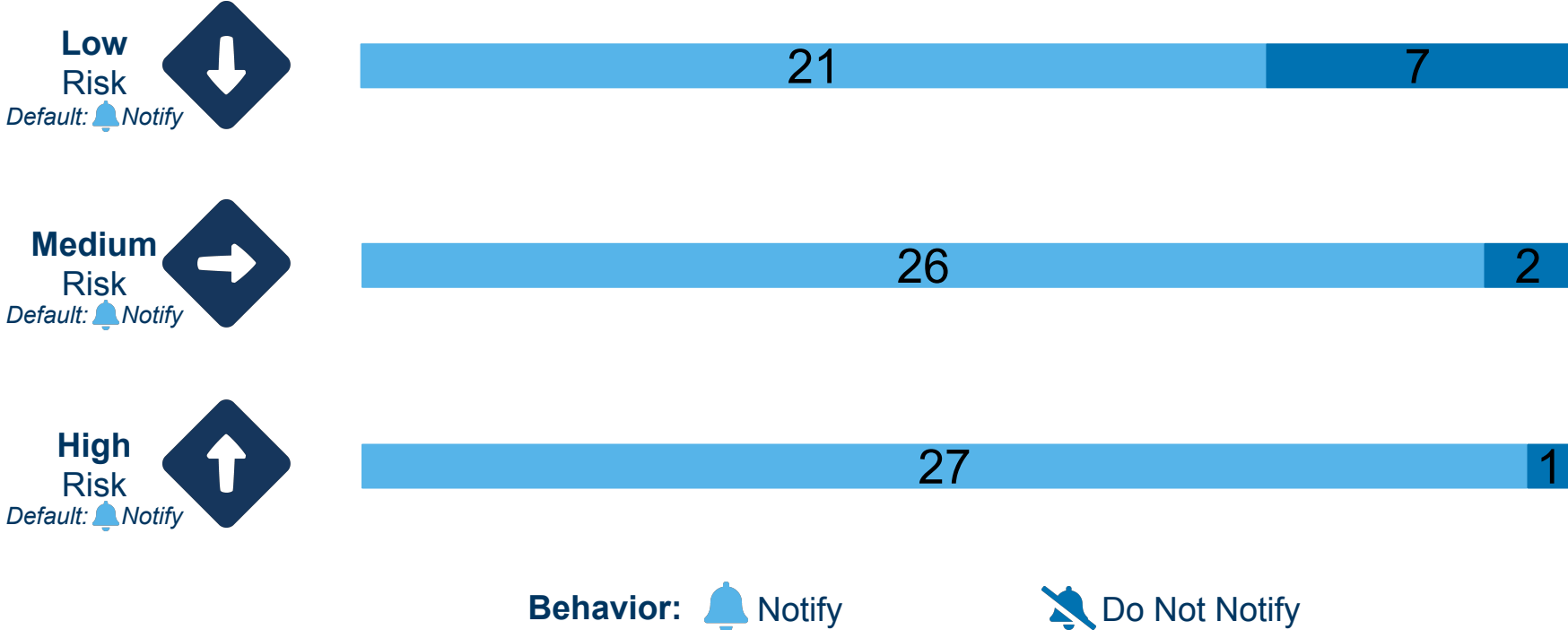
Understanding How Administrators Configure RBA Is Crucial

Appropriately configured, RBA increases security while limiting unnecessary security prompts to a minimum.



	Allow	Optional MFA	Require MFA	Block	Notify Users
Low risk	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Medium risk	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
High risk	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>

Admins Stick With the Notification Defaults



“If you get bombarded with login notifications, you get annoyed. [...] So I chose to only notify when there’s a reason.” (P1)



Today: Practitioners' and End-Users' Perspective on RBA

Configuration of
Risk-based
Authentication
SOUPS 22



Users' Interaction
With Login
Notifications
*USENIX Sec. 24**



How do administrators configure RBA? ✓

How do users interact with login notifications?



Hi Philipp,

We noticed you recently tried to sign in to your LinkedIn account from a new device.

If you're having trouble signing in, please visit the [LinkedIn Help Center](#).

Thanks for using LinkedIn!
The LinkedIn Team

When and where this happened:

Date: July 28, 2023, 2:09 PM (GMT)

Browser: Firefox

Operating System: Linux

Approximate Location: Essen, Nordrhein-westfalen, Deutschland

Didn't do this? Be sure to [change your password](#) right away.

Two Possible Cases With Four Outcomes



Case 1: User signs in



Case 2: Attacker signs in



1



Lipton | Be More Tea | 2014

User does nothing

2



Wise | 10 Things That Are Green | 2023

User starts inspecting

3



Lipton | Be More Tea | 2014

User does nothing

4



Wise | 10 Things That Are Green | 2023

User starts inspecting

Representative Notification Based on 60+ Real-World Notifications



Hi Philipp,

We noticed you recently tried to sign in to a new device.

If you're having trouble signing in, please visit the [Help Center](#).

Thanks for using LinkedIn!
The LinkedIn Team

When and where this happened:

Date: July 28, 2023

Browser: Firefox


Operating System: Linux

Approximate Location: Essen, North Rhine-Westphalia

Didn't do this? Be sure to [change your password](#).

TABLE 3. INFORMATION CONTAINED IN NOTIFICATIONS SENT BY REAL-WORLD SERVICES.

Rank	Domain	Account Name	Browser	Country	State	City	IP	OS	Time	Time Zone	Instructions Legit	Instructions Malicious
1	google.com											
2	workspace.google.com											
3	facebook.com											
4	microsoft.com											
5	nethx.com											
6	twitter.com											
7	instagram.com											
8	apple.com											
9	linkedin.com											
10	cloudflare.com											
11	wikipedia.org											
12	yahoo.com											
13	amazon.com											
14	pinterest.com											
15	github.com											
16	vk.com											
17	mozilla.org											
18	csdn.net											
19	tumblr.com											
20	spotify.com											
21	paypal.com											
22	dropbox.com											
23	ebay.com											
24	imdb.com											
25	soundcloud.com											
26	twitthiv											
27	sourceforge.net											
28	etsy.com											
29	researchgate.net											
30	weebly.com											
31	oracle.com											
32	booking.com											
33	samsung.com											
34	slack.com											
35	snapchat.com											
36	grammarly.com											
37	ycp.com											
38	fyvcr.com											
39	netase.com											
40	binance.com											
41	atlassian.com											
42	gifsak.com											
43	battle.net											
44	airbnb.com											
45	uber.com											
46	xing.com											
47	nintendo.com											
48	wayfair.com											
49	plex.tv											
50	1password.com											
51	lyft.com											
52	dhl.de											
53	dashlane.com											
54	porkbun.com											
55	logmein.com											
56	check24.com											
57	maxmind.com											
58	fastr.com											
59	myumidays.com											
60	n26.com											
61	neteller.com											
62	traderpublic.com											
63	stacksocial.com											
64	netatmo.com											
65	splitwise.com											
66	decathlon.com											

 New device logged in

...ice or location and want to make sure it's you.

...do anything.

...nd used it to access your account. To protect your **turn on two-factor authentication**. Also check for social media accounts (like Facebook, or Twitter).

...ize the location of the sign in. You can review [authentications/463411833](#).

...further action.

...d. Visit <https://github.com/settings/admin> to [protect your account and data secure/](#) in the GitHub Help.

...[github.com/settings/security](#)

...[github.com/contact](#)

Representative Notification Based on 60+ Real-World Notifications

New sign-in to your Spatial Reasoning Study account

From: SRS Team <spatial-reasoning@rub.de>



New sign-in to the Spatial Reasoning Study

Hi,

We noticed a new sign-in to your SRS account (jo.doe@gmail.com).

Location: North Rhine-Westphalia, Germany

Date: July 28, 2023 at 02:09 PM CET

Device: Firefox on Linux

If it was you, you can safely ignore this email.

If it wasn't you, please [change your password](#) immediately to secure your account.

Thanks,

The SRS Team

[Privacy Policy](#) | [Support Center](#)

Universitaetsstrasse 150, 44780 Bochum, Germany.

© 2022 SRS. SRS is an abbreviation for Spatial Reasoning Study.

Deception Study To Get Authentic Reactions to Notifications



Legitimate

Malicious

New sign-in to the Spatial Reasoning Study

Hi,

We noticed a new sign-in to your SRS account (jo.doe@gmail.com).

Location: North Rhine-Westphalia, Germany
Date: July 28, 2023 at 02:09 PM CET
Device: Firefox on Linux

If it was you, you can safely ignore this email.
If it wasn't you, please [change your password](#) immediately to secure your account.

Thanks,
The SRS Team

New sign-in to the Spatial Reasoning Study

Hi,

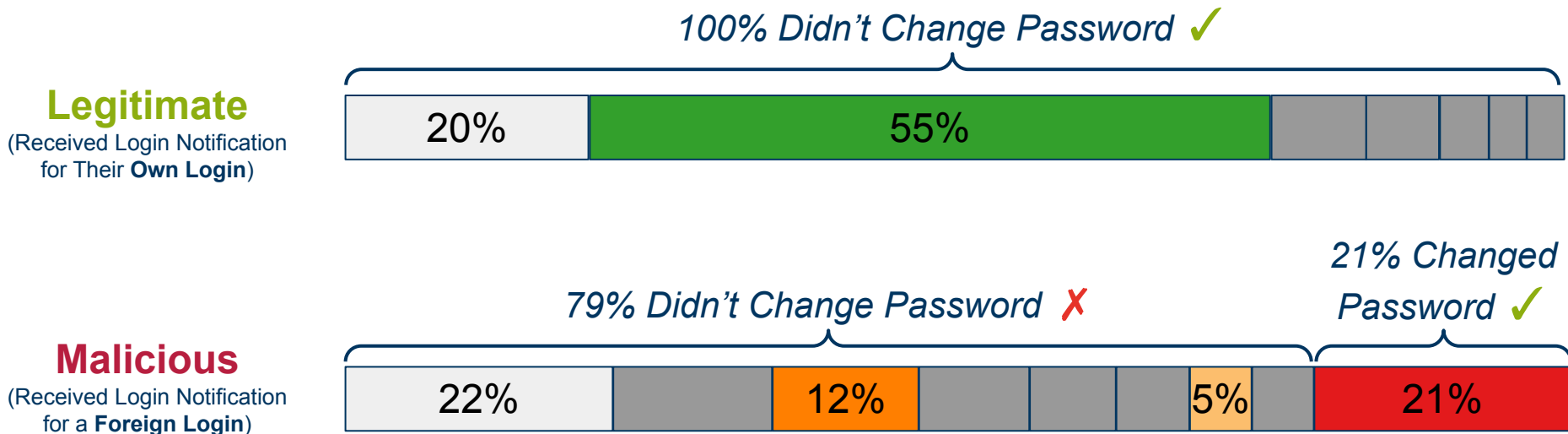
We noticed a new sign-in to your SRS account (jo.doe@gmail.com).

Location: California, USA
Date: July 28, 2023 at 05:09 AM PDT
Device: Chrome on Windows

If it was you, you can safely ignore this email.
If it wasn't you, please [change your password](#) immediately to secure your account.

Thanks,
The SRS Team

Legitimate Case Is Fine – Malicious Notifications Cause Issues

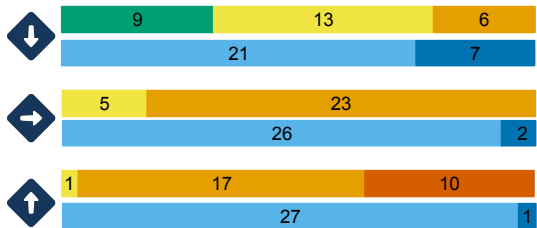


Explanation: Don't Remember Was Me Not Me Suspicious Fatigue

Admins Tend To Increase Security & Malicious Case Causes Issues

Configuration of Risk-based Authentication SOUPS 22

	Allow	Optional MFA	Require MFA	Block	Notify Users
Low risk	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Medium risk	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
High risk	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>



- Allow (Low)
- Optional MFA (Medium & High)
- Required MFA
- Block
- Notify (Low, Medium, High)
- Do Not Notify

Users' Interaction With Login Notifications USENIX Sec. 24*

New sign-in to the Spatial Reasoning Study

Hi,

We noticed a new sign-in to your SRS account (jo.doe@gmail.com).

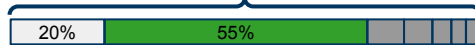
Location: California, USA
Date: July 28, 2023 at 05:09 AM PDT
Device: Chrome on Windows

If it was you, you can safely ignore this email.
 If it wasn't you, please [change your password](#) immediately to secure your account.

Thanks,
 The SRS Team

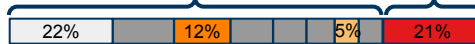
Legitimate

100% Didn't Change ✓



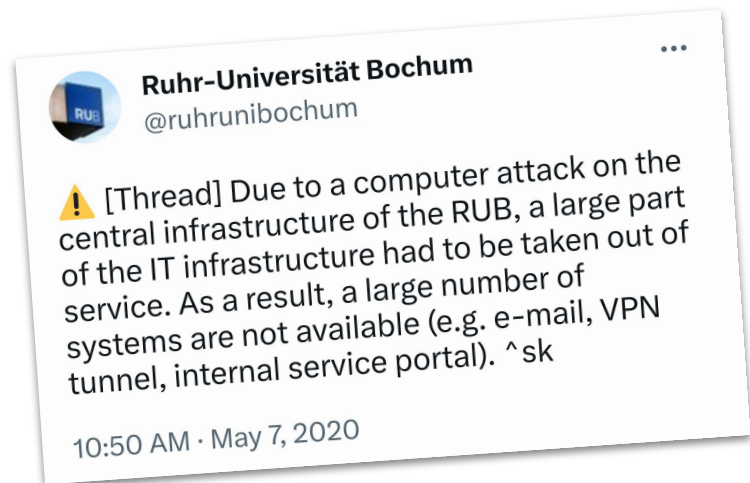
Malicious

79% Didn't Change ✗ 21% Changed ✓



- Don't Remember
- Was Me
- Not Me
- Suspicious
- Fatigue

RBA Could Have Changed the Outcome of the Attack in 2020



admin:123456 ❌
admin:password ❌
admin:12345678 ❌
...
admin:ruhruniversity ✅

Login could have been complicated or blocked



Login could have been detected



Various Directions for Future Work on Both Sides



Testing Different RBA Configuration Interfaces



Influence of Account/Device Sharing

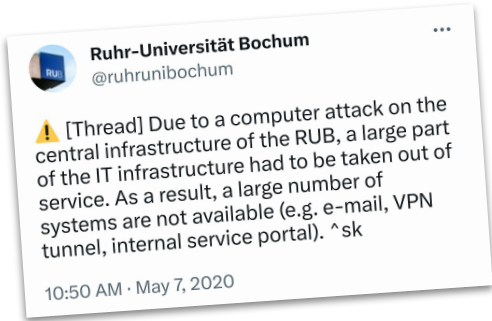


Improving Applicability with
Sample Configurations and Notifications



Weighting Positive and Negative Effects
of Login Notifications

Password Insecurity



2018: Google user-base < 10% have MFA enabled [1]

2022: "Turn on 2SV (or we will!)" [2]

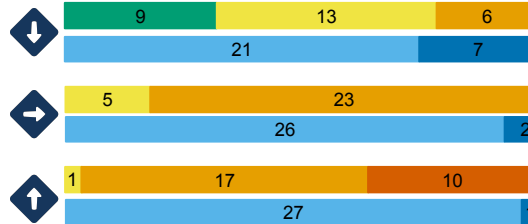


"Will We Get Rid of Passwords? In short, according to our findings, not in the near future." [3]



Admin Perspective

	Allow	Optional MFA	Require MFA	Block	Notify Users
Low risk	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Medium risk	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
High risk	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>



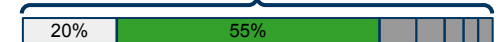
- Allow (Low)
- Optional MFA (Medium & High)
- Required MFA
- Block
- Notify (Low, Medium, High)
- Do Not Notify

End-User Perspective



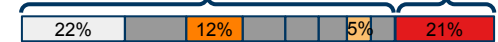
Legitimate

100% Didn't Change ✓



Malicious

79% Didn't Change ✗ 21% Changed ✓



Don't Remember Was Me Not Me

Suspicious Fatigue