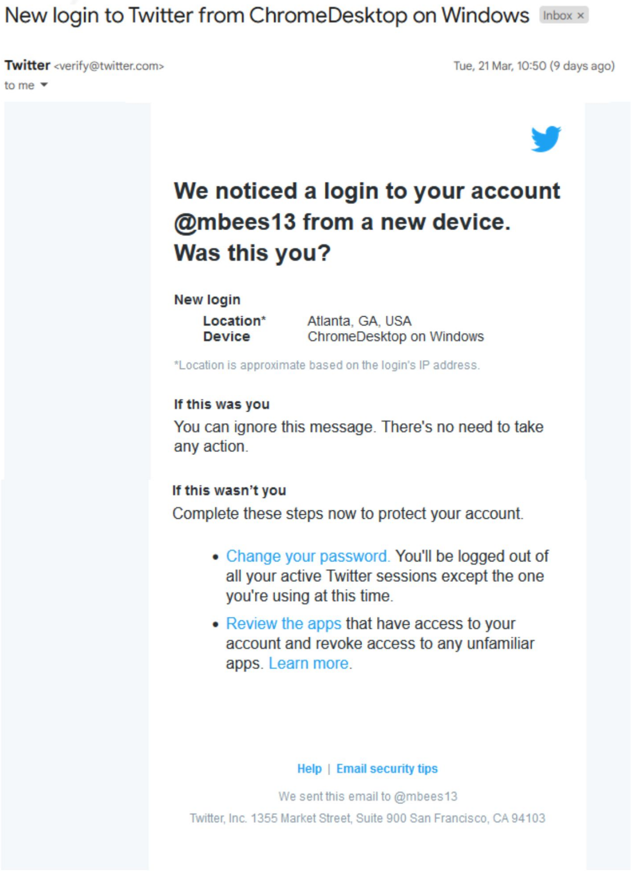
Was This You? Investigating the Design Considerations for Suspicious Login Notifications

Sena Sahin, Burak Sahin, Frank Li

Georgia Tech

Diverse Suspicious Login Notifications



New login to Twitter from ChromeDesktop on Windows

Twitter <verify@twitter.com>
to me

Tue, 21 Mar, 10:50 (9 days ago)

We noticed a login to your account @mbees13 from a new device. Was this you?

New login

Location*	Atlanta, GA, USA
Device	ChromeDesktop on Windows

*Location is approximate based on the login's IP address.

If this was you

You can ignore this message. There's no need to take any action.

If this wasn't you

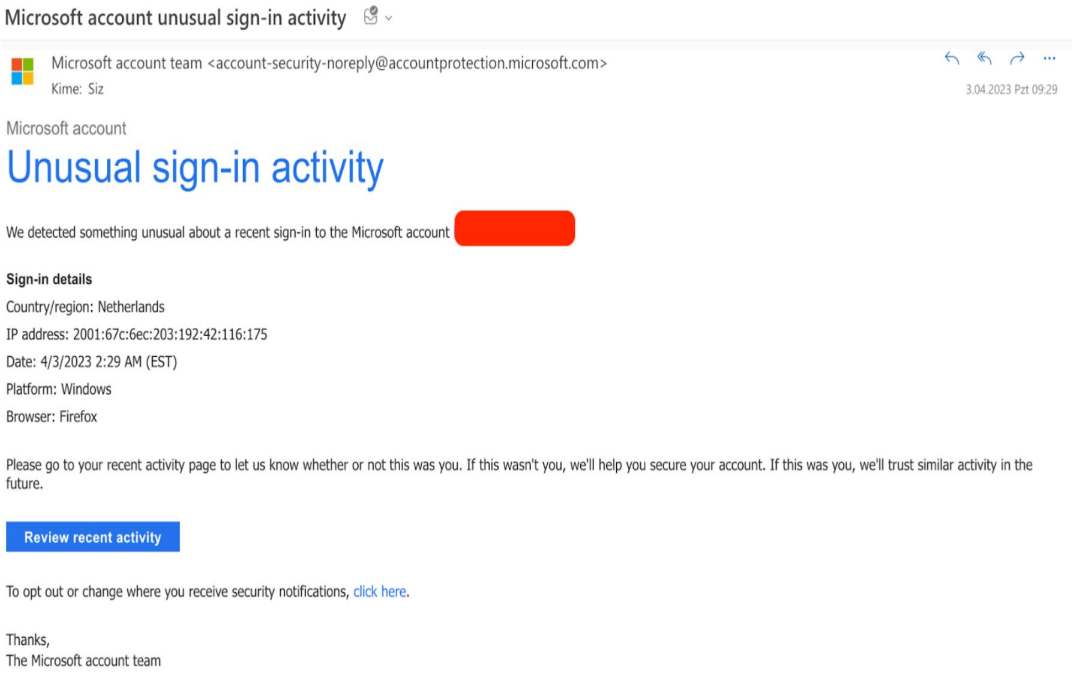
Complete these steps now to protect your account.

- Change your password. You'll be logged out of all your active Twitter sessions except the one you're using at this time.
- Review the apps that have access to your account and revoke access to any unfamiliar apps. Learn more.

Help | **Email security tips**

We sent this email to @mbees13

Twitter, Inc. 1355 Market Street, Suite 900 San Francisco, CA 94103



Microsoft account unusual sign-in activity

Microsoft account team <account-security-noreply@accountprotection.microsoft.com>
Kime: Siz

3.04.2023 Pzt 09:29

Microsoft account

Unusual sign-in activity

We detected something unusual about a recent sign-in to the Microsoft account [redacted]

Sign-in details

Country/region: Netherlands

IP address: 2001:67c:6ec:203:192:42:116:175

Date: 4/3/2023 2:29 AM (EST)

Platform: Windows

Browser: Firefox

Please go to your recent activity page to let us know whether or not this was you. If this wasn't you, we'll help you secure your account. If this was you, we'll trust similar activity in the future.

To opt out or change where you receive security notifications, click here.

Thanks,
The Microsoft account team

Research Questions

RQ1: How do components capture user attention?

RQ2: How do components help users verify authenticity?

RQ3: How do components assist in assessing legitimacy of the login?

RQ4: How do components guide users in taking remedial actions?

Research Questions

RQ1: How do components capture user attention?

RQ2: How do components help users verify authenticity?

RQ3: How do components assist in assessing legitimacy of the login?

RQ4: How do components guide users in taking remedial actions?

Method

Data Collection

Target top 100 websites

Collected 21 distinct email notifications

Lack of standardization

Sender details

Username
Domain

Subject lines

Tone
Personalization

Login details

Device brand, type, and version.
Location (text-based or map)
Ti

Action prompts

Current account security
Future suggestions
Vi

Legitimacy Signals

Logo
Greeting/closing
Legitimacy warning
Legal disclaimer

Method

Data Collection

Recruitment

Interview

Target top 100 websites

Collected 21 distinct email notifications

Lack of standardization

Prolific

U.S. based

18 and above

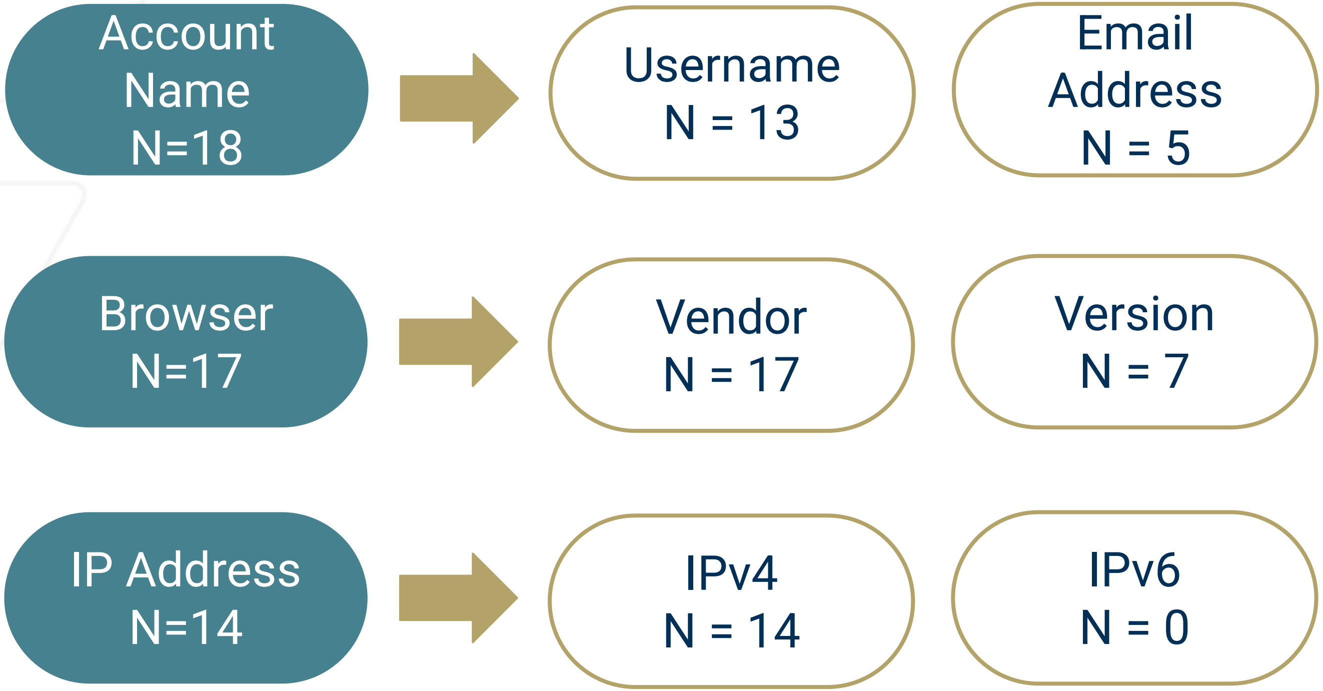
Prior experiences

Participants’ workflows

Designing notification

N = 20

RQ3: Assessing the legitimacy of the login

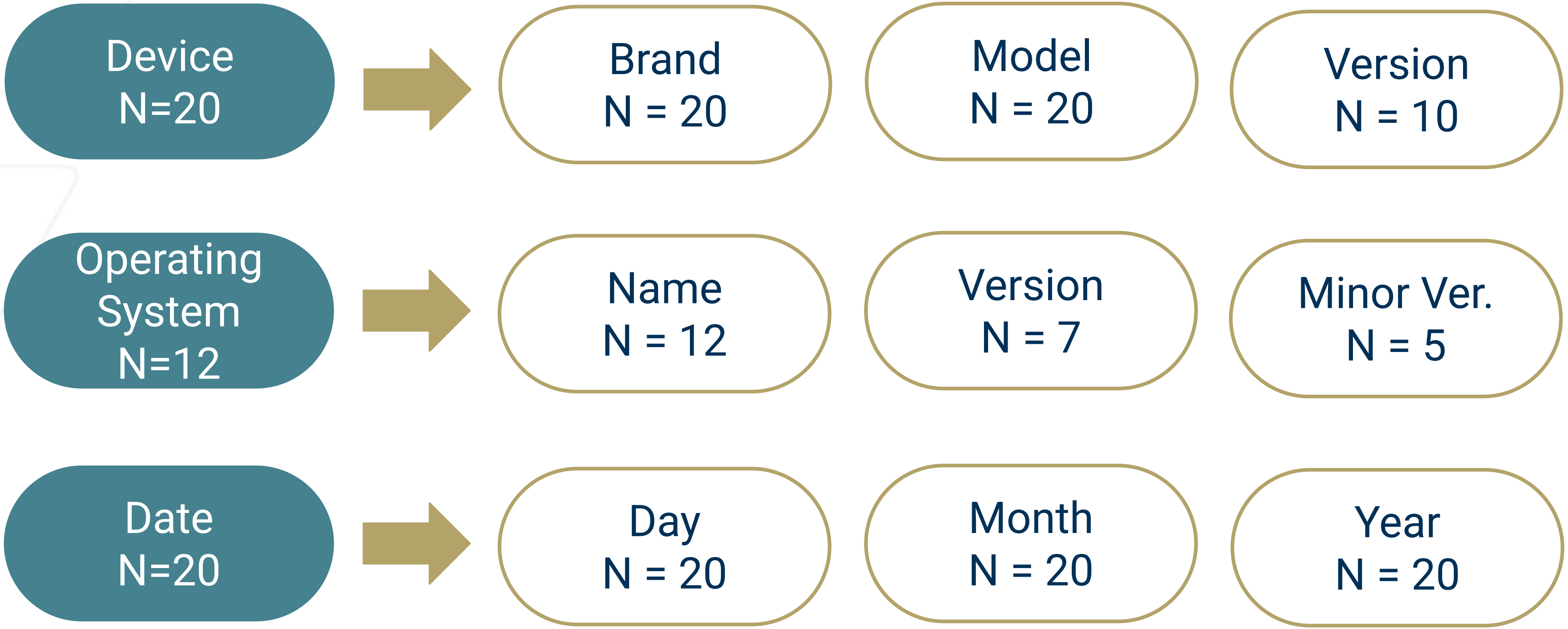


Account Name N=18 → Username N = 13; Email Address N = 5

Browser N=17 → Vendor N = 17; Version N = 7

IP Address N=14 → IPv4 N = 14; IPv6 N = 0

RQ3: Assessing the legitimacy of the login

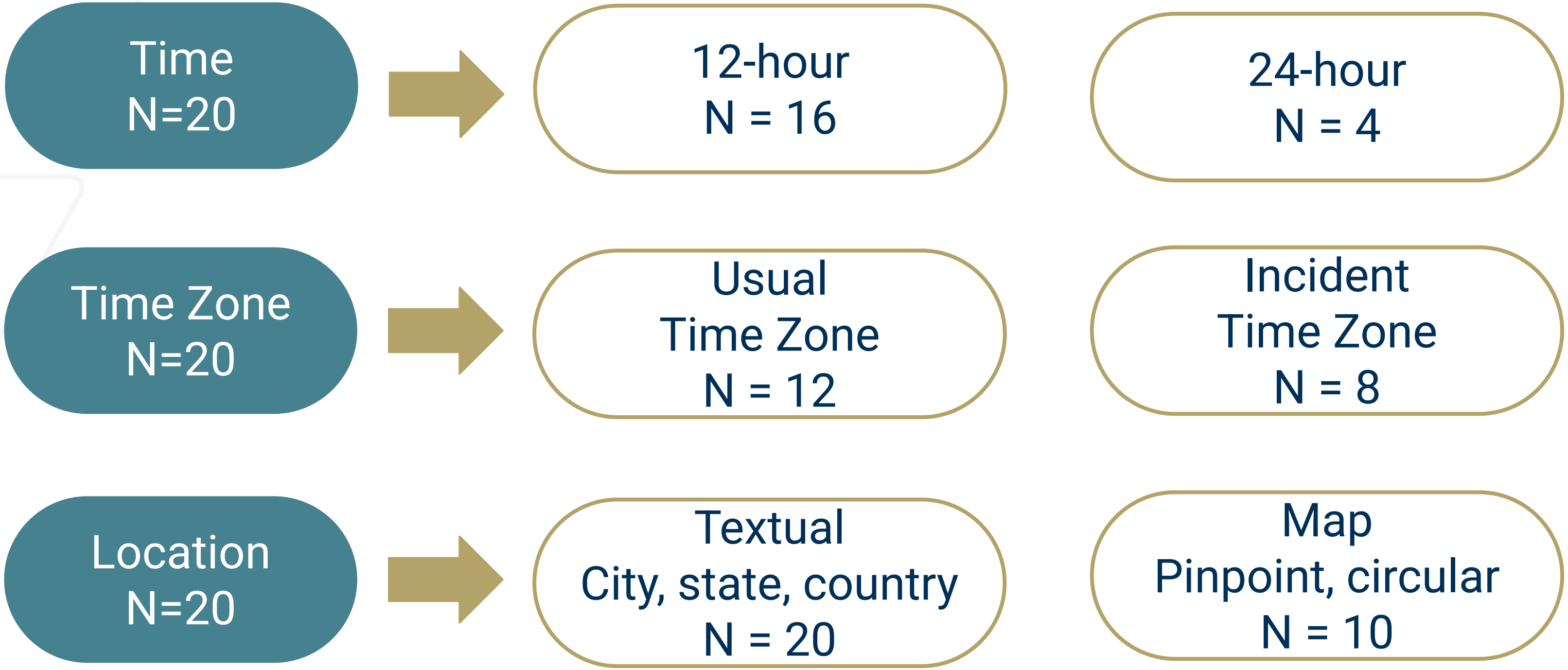


Device N=20 → Brand N = 20, Model N = 20, Version N = 10

Operating System N=12 → Name N = 12, Version N = 7, Minor Ver. N = 5

Date N=20 → Day N = 20, Month N = 20, Year N = 20

RQ3: Assessing the legitimacy of the login



Time
N=20

12-hour
N = 16

24-hour
N = 4

Time Zone
N=20

Usual
Time Zone
N = 12

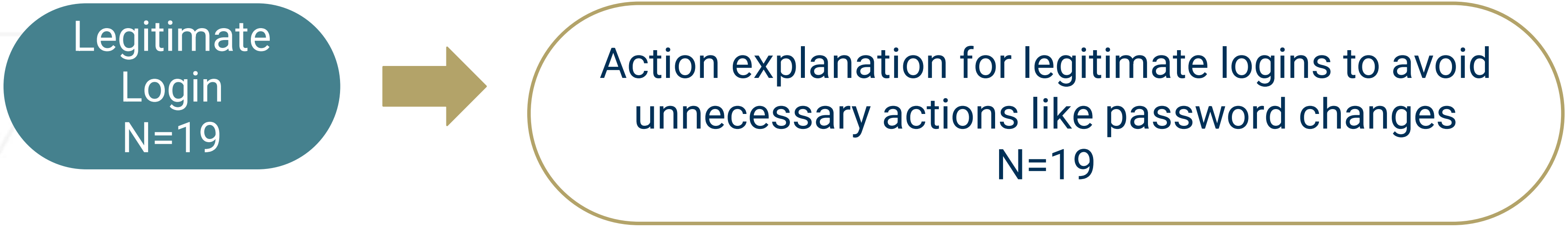
Incident
Time Zone
N = 8

Location
N=20

Textual
City, state, country
N = 20

Map
Pinpoint, circular
N = 10

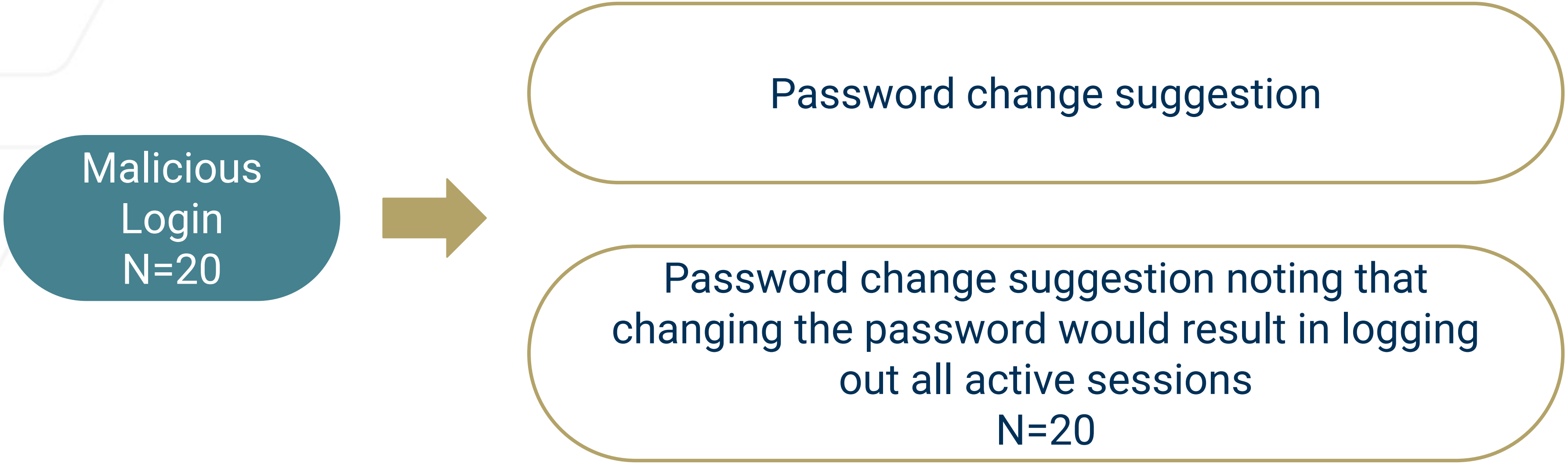
RQ4: Deciding to take an action



Legitimate Login
N=19

Action explanation for legitimate logins to avoid unnecessary actions like password changes
N=19

RQ4: Deciding to take an action

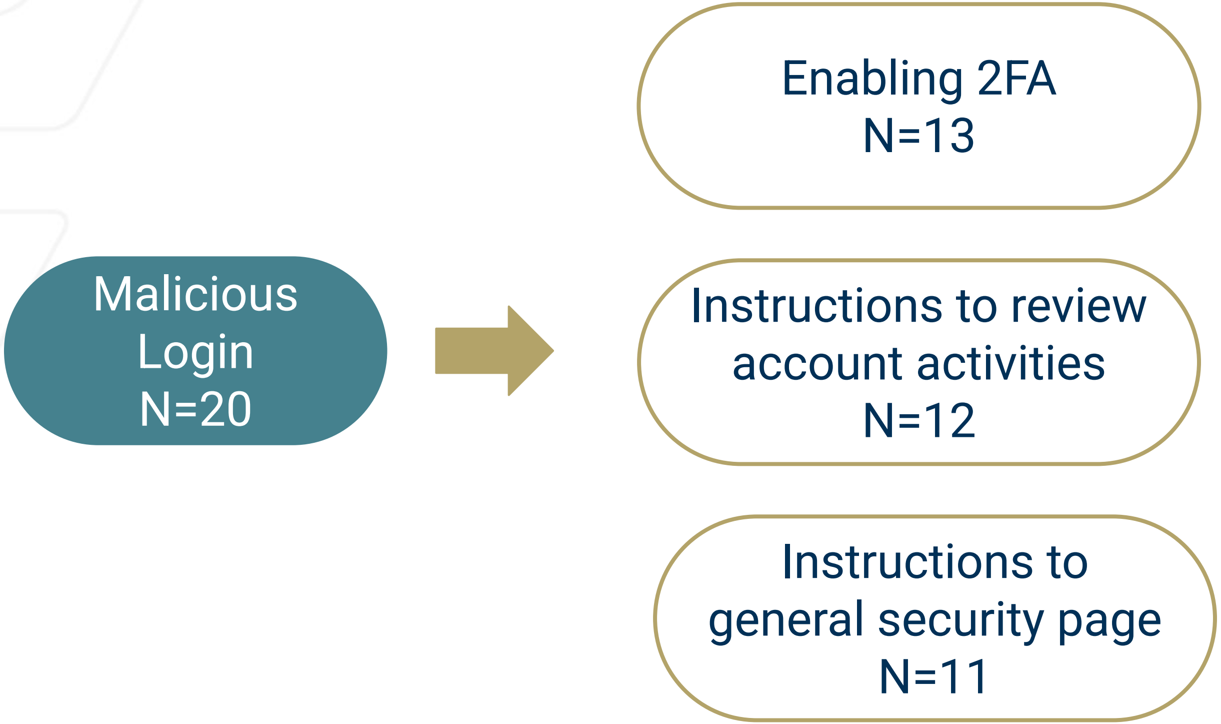


Malicious Login
N=20

Password change suggestion

Password change suggestion noting that changing the password would result in logging out all active sessions
N=20

RQ4: Deciding to take an action



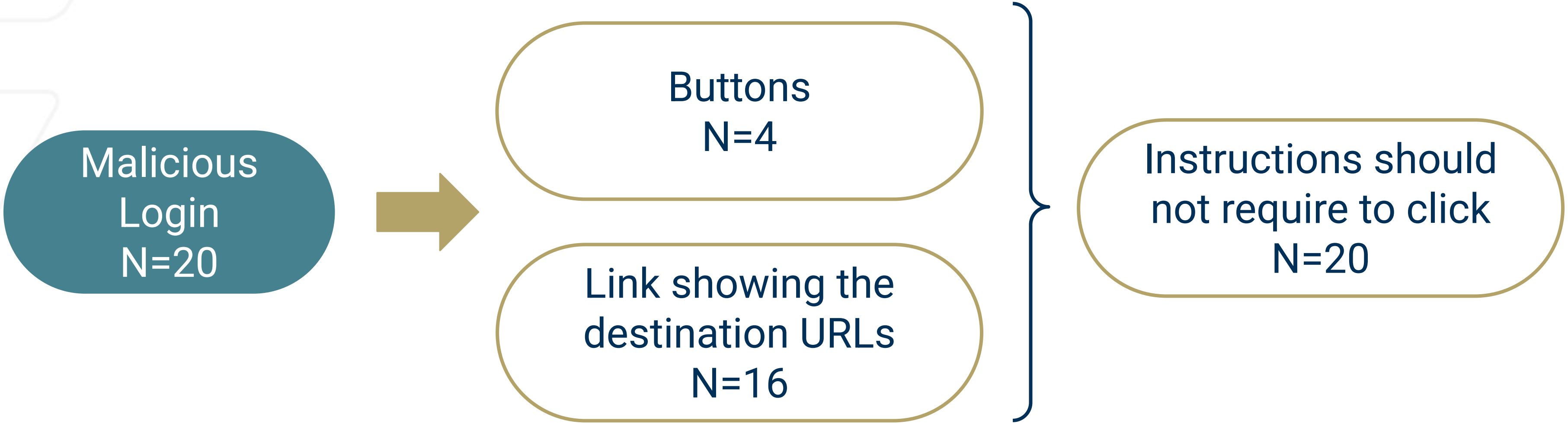
Malicious Login N=20

Enabling 2FA N=13

Instructions to review account activities N=12

Instructions to general security page N=11

RQ4: Deciding to take an action


Malicious Login N=20
Buttons N=4
Link showing the destination URLs N=16
Instructions should not require to click N=20

Suggested Design

Subject. Suspicious login to your account from AcmeCo using Chrome on Mac
Sender. noreply@acmeco.com

Explanation. Jo, We detected a suspicious login to your AcmeCo account from a new device.
Sign-in Account name: jo123 , When: May, 05 2023 3pm EST Where: Atlanta, GA, USA
Details. Device: Iphone 12, IPv4: 192.168. 1.1

Actions. If this was you, there's no need to take any action right now. If this was not you, visit your account's security settings to change your password (also available at https://acmeco.com/settings/security). You'll be logged out of all your active AcmeCo sessions except the one you're using at this time. We recommend that you enable two-factor authentication to secure your account.
Closing. Thanks, AcmeCo Security Team

Legitimacy Check before you click! AcmeCo will never ask you for personal information in an email.
Warning. When you click on a link the address should always contain "acmeco.com/". Visit the security.acmeco.com/phishing FAQ site to learn more.

Legal info. AcmeCo, Inc. 1453 Legend Street, Suite 610 San Francisco, CA 90101

Takeaways

➢ User preferences align with familiar prior experiences.

➢ Cross-reference data to handle inaccuracies and shared accounts.

➢ Clear, context-aware language tailored to diverse user needs and understanding

Call to Action

1. Standardized notification design.

2. Thoughtful design with holistic components.

3. Language, tone and framing considering all user groups.

Thank you!

✉ ssahin8@gatech.edu