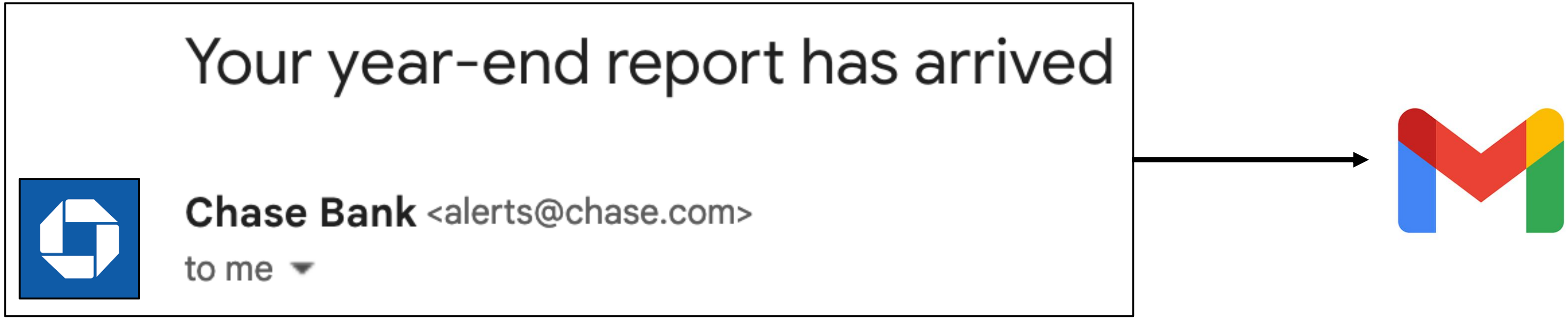
Understanding the Viability of Gmail’s Origin Indicator for Identifying the Sender

Enze “Alex” Liu, Lu Sun, Alex Bellon, Grant Ho*,
Geoffrey M. Voelker, Stefan Savage, Imani N. S. Munyaka

*UC San Diego, *University of Chicago*

Authenticating an Email from chase.com



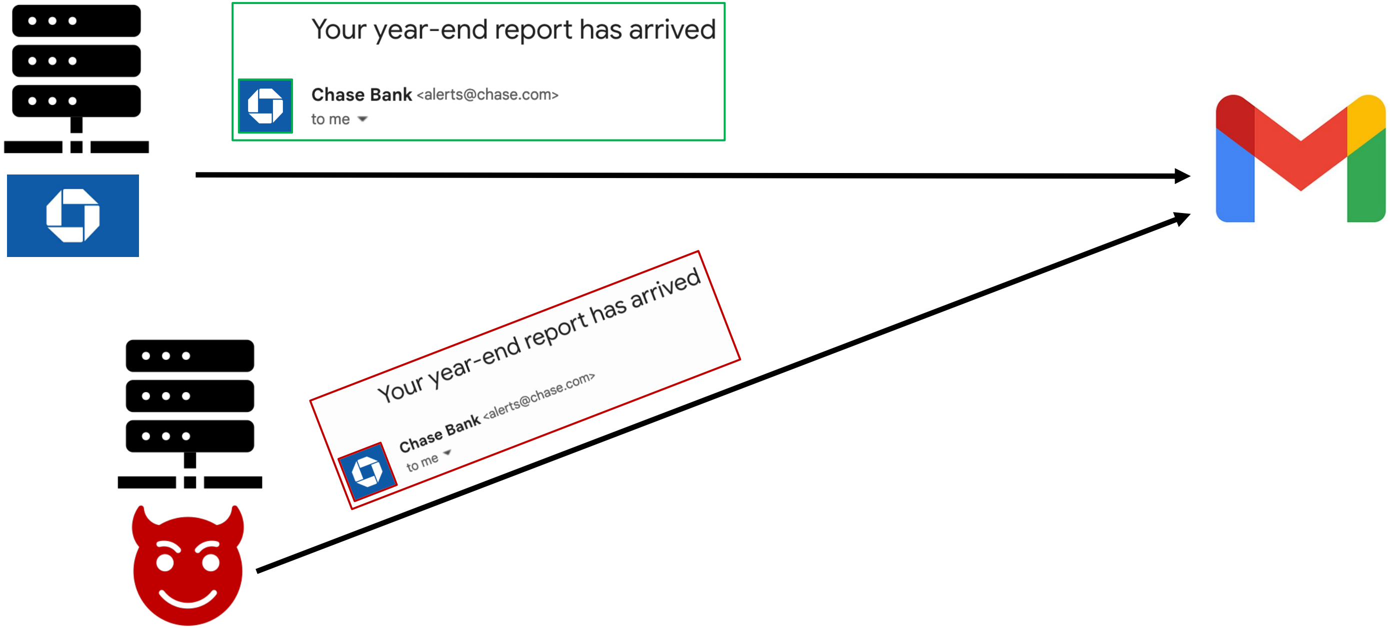
Your year-end report has arrived

Chase Bank <alerts@chase.com>

to me

Authenticating an Email from chase.com

Authenticating the server that sends the email



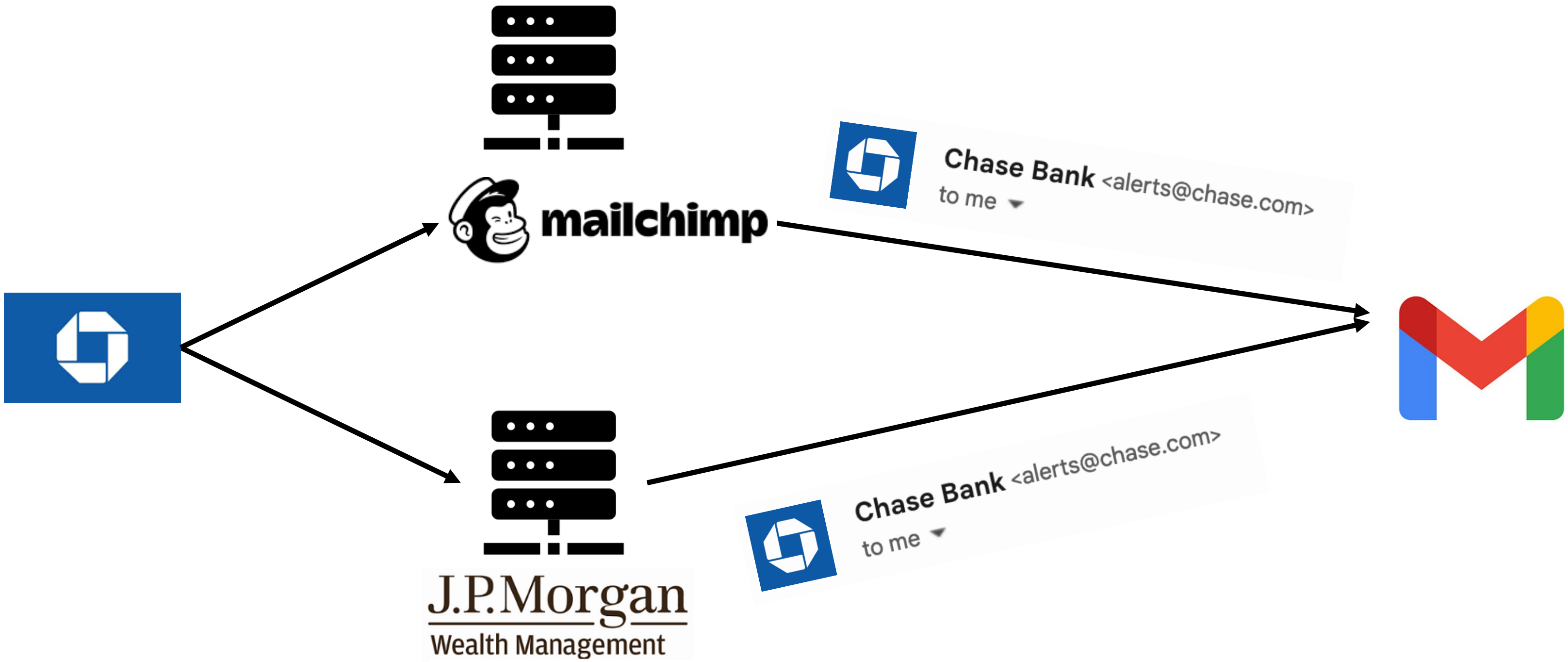
Your year-end report has arrived

Chase Bank <alerts@chase.com>
to me

Your year-end report has arrived

Chase Bank <alerts@chase.com>
to me

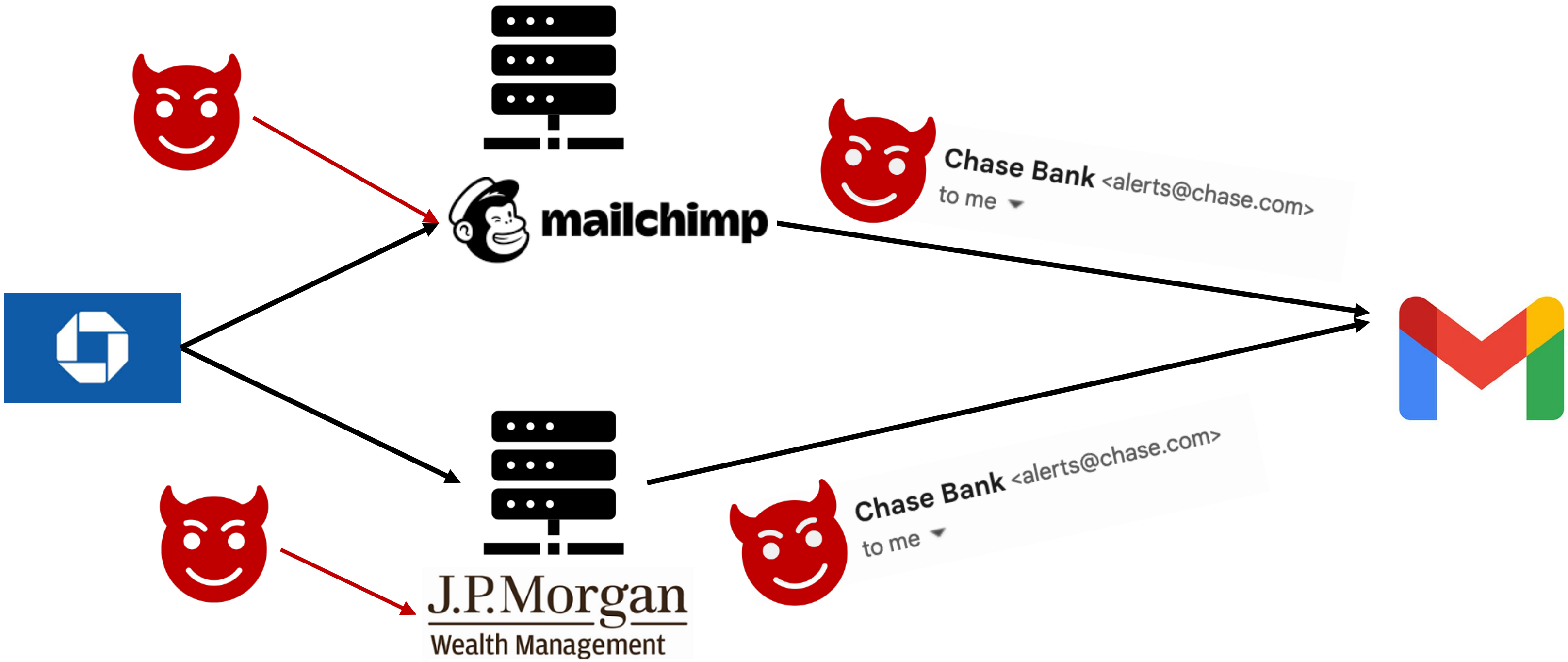
Everything Works Great Until



Chase Bank <alerts@chase.com>
to me

Chase Bank <alerts@chase.com>
to me

Everything Works Great Until

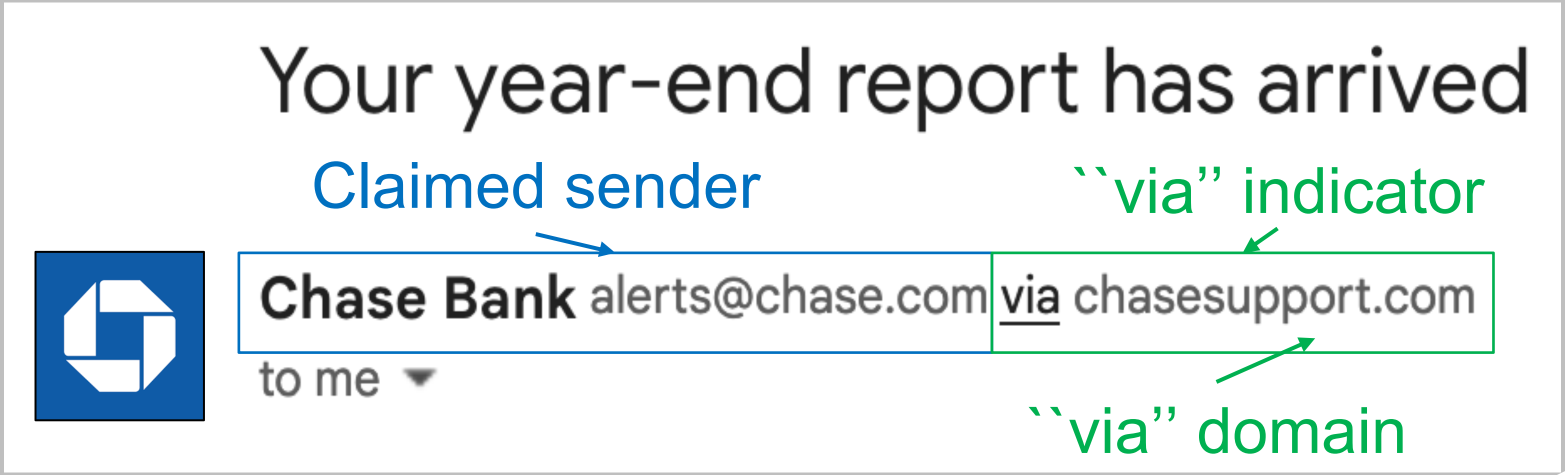


Chase Bank <alerts@chase.com>
to me

Chase Bank <alerts@chase.com>
to me

[1] Chen et al., A Case Study of Email Sender Authentication (Usenix Security ‘20)
[2] Liu et al., On the Security Implications of Email Forwarding Mechanism and Policy (EuroS&P ‘23)

Everything Wo



Your year-end report has arrived

Chase Bank alerts@chase.com via chasesupport.com

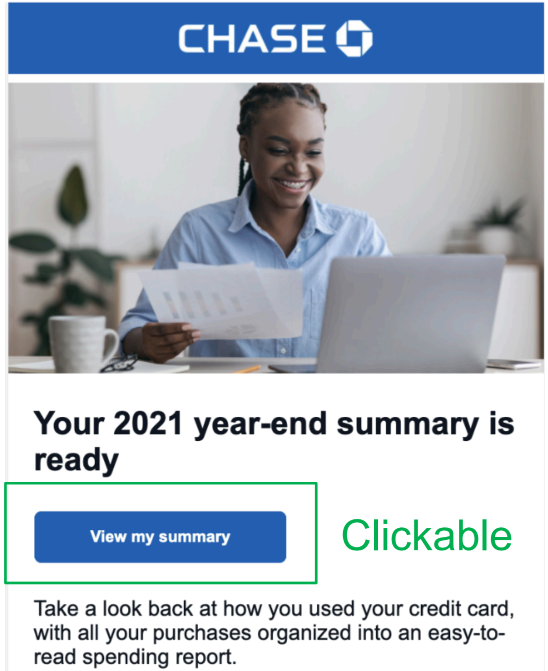
to me

[1] Chen et al., A Case Study of Ema ix Security ‘20)
[2] Liu et al., On the Security Implications Mechanism and Policy (EuroS&P ‘23)

Participants

- Prolific
- 180 Gmail users
  - 82% with 4+ YOE
- 53% male
- 59% college educated

Experimental Setup



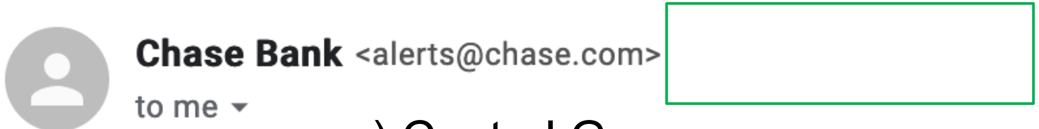
CHASE

Your 2021 year-end summary is ready

View my summary

Clickable

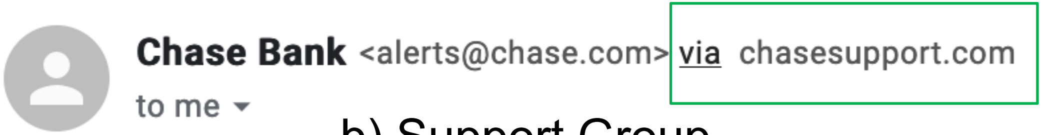
Take a look back at how you used your credit card, with all your purchases organized into an easy-to-read spending report.



Chase Bank <alerts@chase.com>

to me

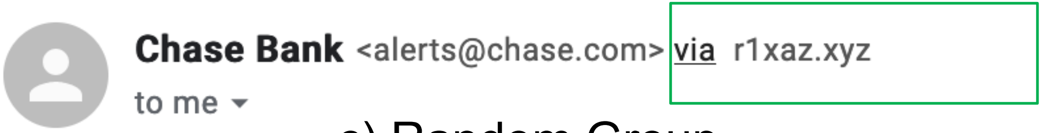
a) Control Group



Chase Bank <alerts@chase.com> via chasesupport.com

to me

b) Support Group



Chase Bank <alerts@chase.com> via r1xaz.xyz

to me

c) Random Group

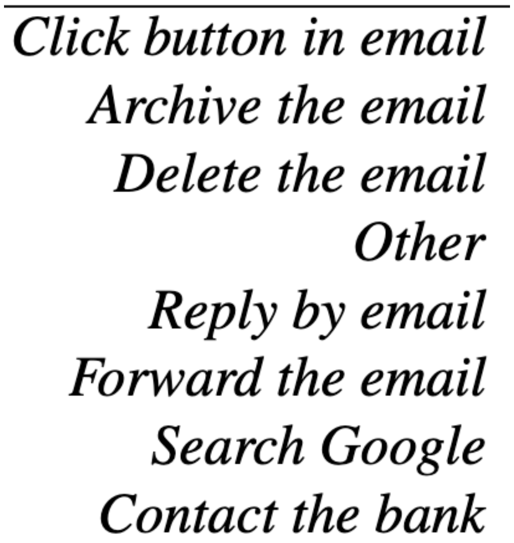
RQ1: Do users notice the “via” indicator?

107 (89%, n=120) participants noticed “via”

RQ1: Do users notice the “via” indicator? ✓

RQ2: Does the “via” indicator nudge users to make safer actions?

Actions



Click button in email

Archive the email

Delete the email

Other

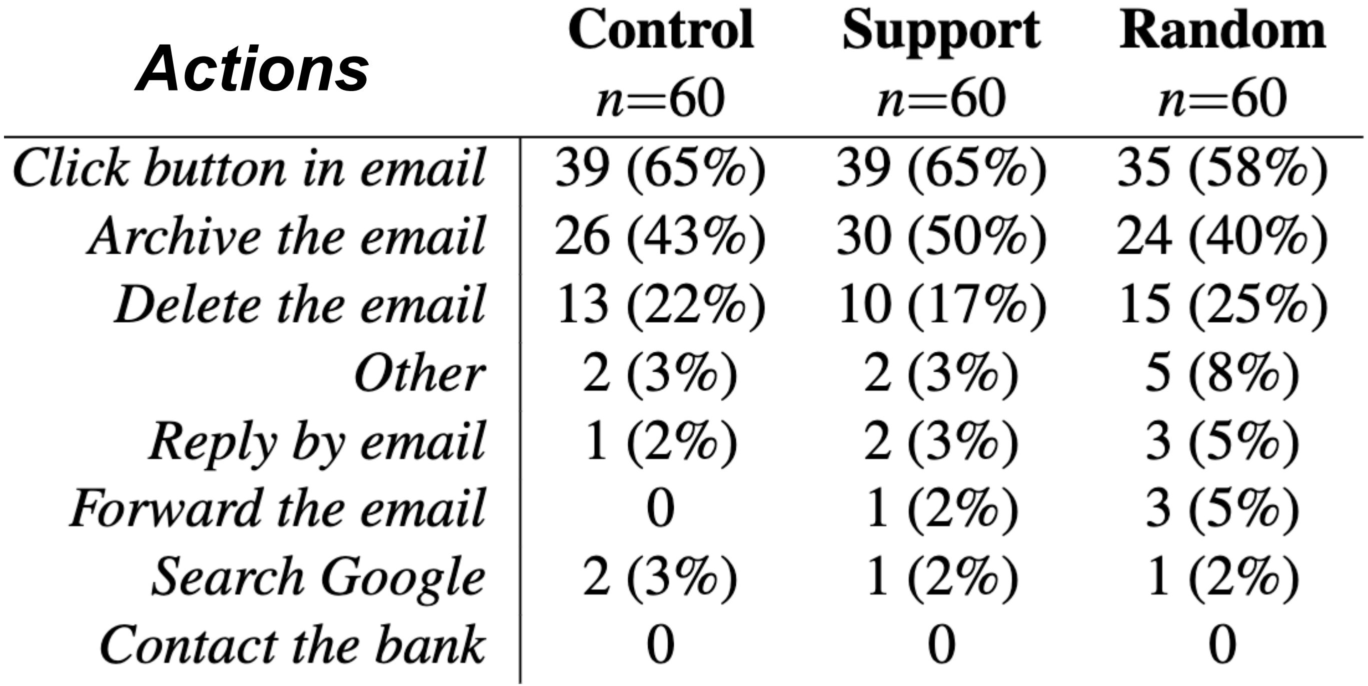
Reply by email

Forward the email

Search Google

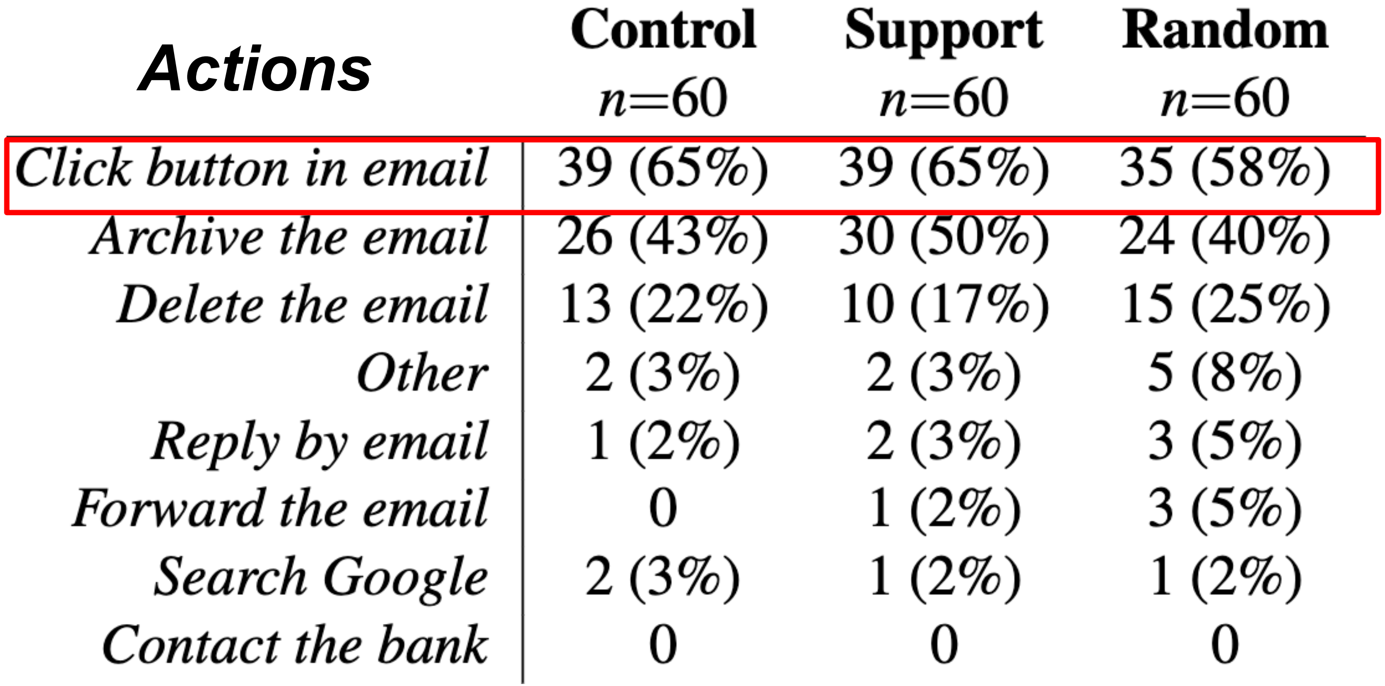
Contact the bank

[1] Downs et al., Decision Strategies and Susceptibility to Phishing (SOUPS ‘06)



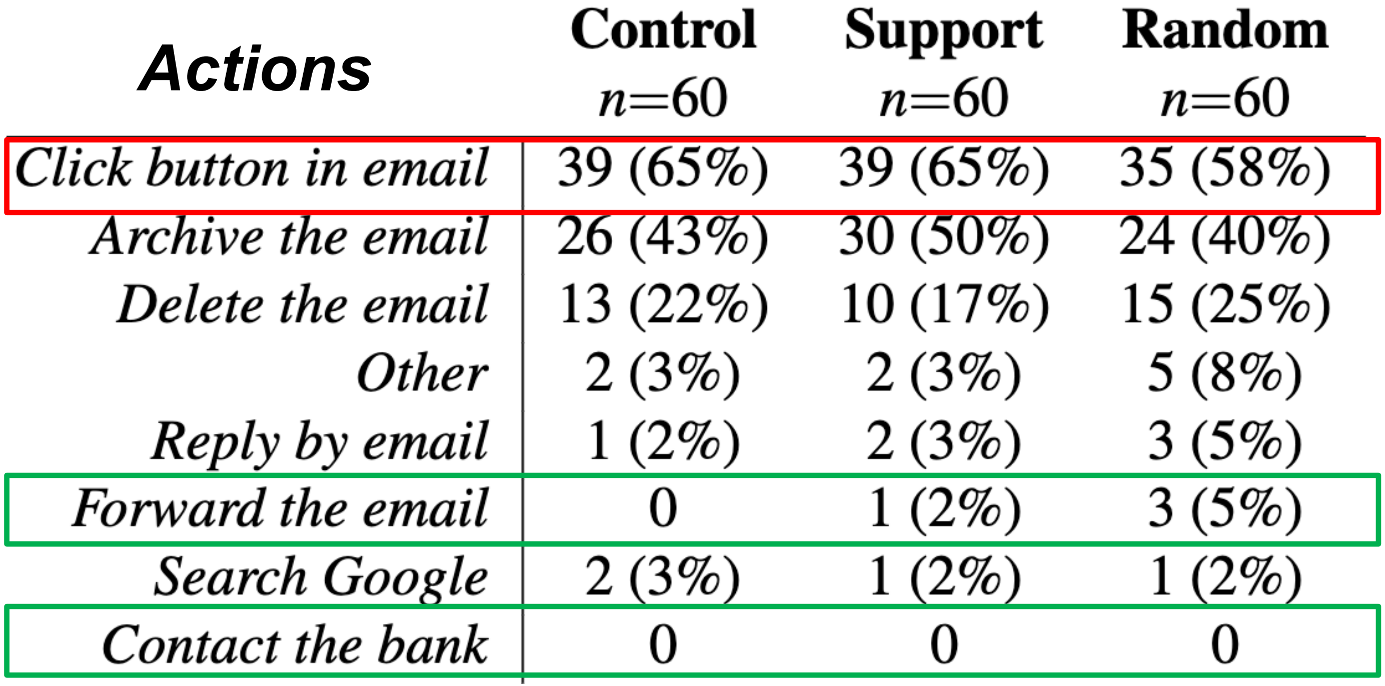
Actions	Control *n*=60	Support *n*=60	Random *n*=60
Click button in email	39 (65%)	39 (65%)	35 (58%)
Archive the email	26 (43%)	30 (50%)	24 (40%)
Delete the email	13 (22%)	10 (17%)	15 (25%)
Other	2 (3%)	2 (3%)	5 (8%)
Reply by email	1 (2%)	2 (3%)	3 (5%)
Forward the email	0	1 (2%)	3 (5%)
Search Google	2 (3%)	1 (2%)	1 (2%)
Contact the bank	0	0	0

[1] Downs et al., Decision Strategies and Susceptibility to Phishing (SOUPS ‘06)



Actions	Control n=60	Support n=60	Random n=60
Click button in email	39 (65%)	39 (65%)	35 (58%)
Archive the email	26 (43%)	30 (50%)	24 (40%)
Delete the email	13 (22%)	10 (17%)	15 (25%)
Other	2 (3%)	2 (3%)	5 (8%)
Reply by email	1 (2%)	2 (3%)	3 (5%)
Forward the email	0	1 (2%)	3 (5%)
Search Google	2 (3%)	1 (2%)	1 (2%)
Contact the bank	0	0	0

[1] Downs et al., Decision Strategies and Susceptibility to Phishing (SOUPS ‘06)



Actions	**Control** n=60	**Support** n=60	**Random** n=60
Click button in email	39 (65%)	39 (65%)	35 (58%)
Archive the email	26 (43%)	30 (50%)	24 (40%)
Delete the email	13 (22%)	10 (17%)	15 (25%)
Other	2 (3%)	2 (3%)	5 (8%)
Reply by email	1 (2%)	2 (3%)	3 (5%)
Forward the email	0	1 (2%)	3 (5%)
Search Google	2 (3%)	1 (2%)	1 (2%)
Contact the bank	0	0	0

[1] Downs et al., Decision Strategies and Susceptibility to Phishing (SOUPS ‘06)

RQ2: Does the "via" indicator nudge users to make safer actions? ✗

[1] Downs et al., Decision Strategies and Susceptibility to Phishing (SOUPS '06)

RQ3: Do users know what the “via” indicator means?

“via” means through (38, 32%, n=120)

“…came via an intermediary…”

“via” indicates the sender (37, 31%, n=120)

“…the true origin of the email…”

“via” indicates group association (16, 27%, n=60)

“…comes from a different department [chasesupport]…”

“via” encourages caution (13, 22%, n=60)

“another website has been used…[suspect] a phishing attempt”

RQ3: Do users know what the “via” indicator means? ✓

However, the “via” domain affects the information conveyed

RQ4: Do users understand that “via” does not signal the relationship between Chase and the “via” domain?

Chase used or instructed the “via” domain to send the email

Support Group: 44, 73%, n=60   Random Group: 31, 52%, n=60

chasesupport.com is part of Chase (12, 20%, n=60)

“…both emails are from the same company…”

RQ4: Do users understand that “via” does not signal the relationship between Chase and the “via” domain? ✗

The “via” domain affects users’ perceptions of the relationship

Moving Forward

- Improving “via”
  - Augment w/ domain info *(Althobaiti et al., CHI, 2021)*
  - Be more explicit
  - Better design *(Bauer et al., CMU-CyLab-13-002, 2013)*
  - Forcing user attention *(Volkamer et al., Information & Comp. Sec., 2016)*
- Throwing away “via”
  - Domain to organization is hard *(Althobaiti et al., CHI, 2021)*
  - Headers not very useful *(Zheng et al., SOUPS, 2022)*
  - Users overloaded with clues

The “viability” of Gmail’s “via” indicator

Most users did notice the indicator

Didn’t effectively nudge users to take safer actions

Most users did understand that a third-party was involved

Most users didn’t understand the risk and relationship between Chase and the third-party

Information conveyed is domain-sensitive

✉ e7liu@ucsd.edu

e7liu.github.io