Assessing Suspicious Emails with Banner Warnings Among Blind and Low-Vision Users in Realistic Settings

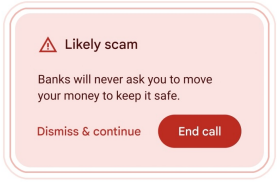
Filipo Sharevski[1], Aziz Zeidieh[2]

[1]DePaul University, Chicago; [2]University of Illinois at Urbana-Champaign

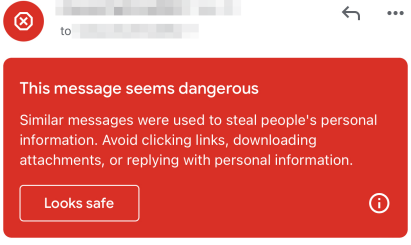
33rd USENIX Security Symposium

Centering Security to Users...

Nudges → Password meters



Warnings → Phone Scams



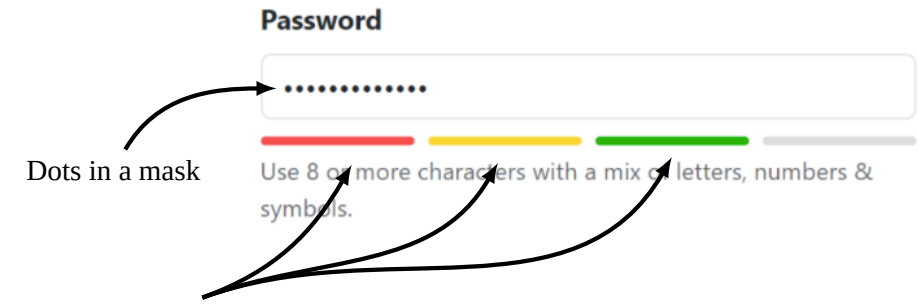
Banners → Email

Centering Security to Users...

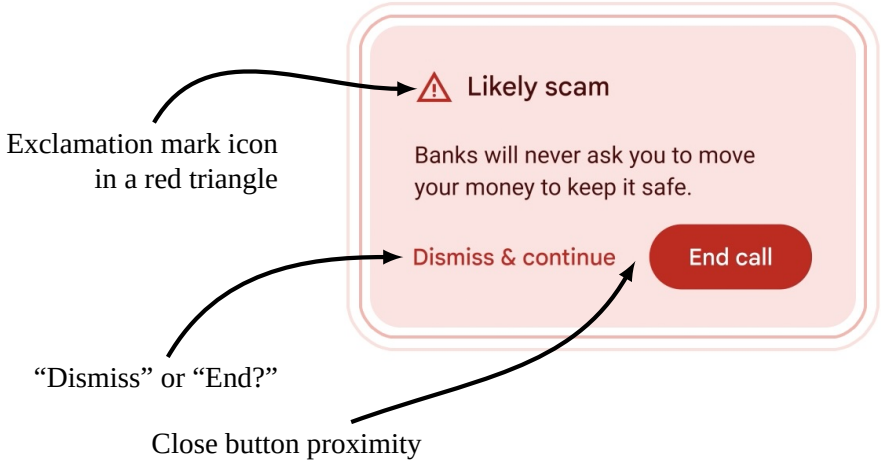
..some of which, are blind or low vision [1]

[1] Legally blind with acuity of 20/200 or field-of-view of 20 degrees or less in the better eye with correction; low vision with acuity up to 20/70 and field-of-view larger than 20 degrees in the better eye with correction

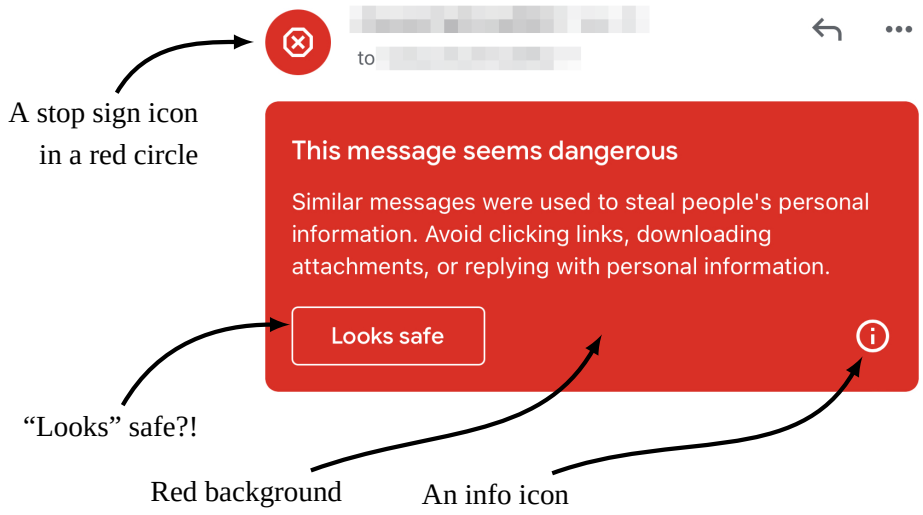
Blind and Low Vision Users (Password Meters)



Blind or Low Vision Users (Phone Scam Warnings)



Blind or Low Vision Users (Email Banners)



Experiments with User-Centered Security...

Laboratory or Realistic Settings

All but capturing actual passwords, revealing personal information or installing malware on a personal device)

Experiments with User-Centered Security...

Laboratory Settings

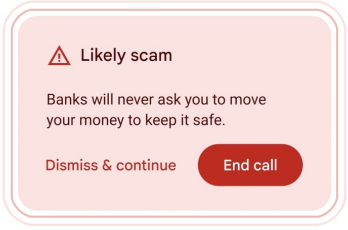
Password Meters → **Dummy** passwords

Scam Calls → **Researcher-controlled** calling numbers (called numbers, devices) and **dummy** personal information

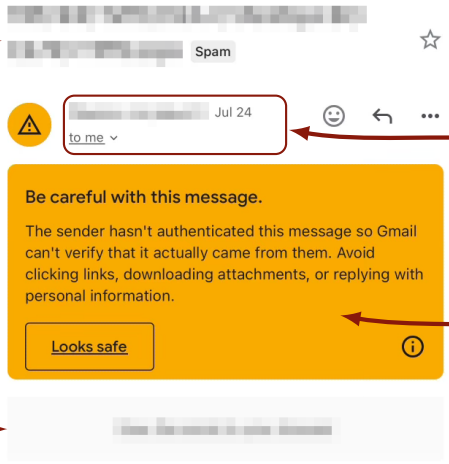
Realistic Settings

Password Meters → **Real** passwords

Scam Calls → **Own** called numbers, **own** devices, **own** personal information



Laboratory Settings

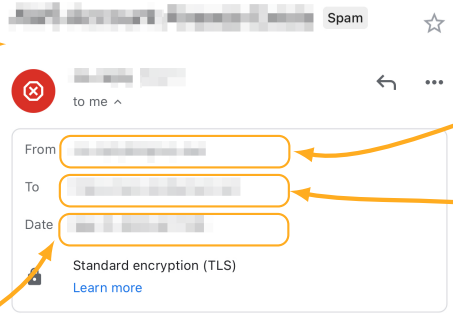


Subject & Body
researcher-selected
usually *phishing*

Unrelated
email address(es)

Non-personal
assistive technology

Realistic Settings



Subject & Body
participant-selected
phishing and *spam*

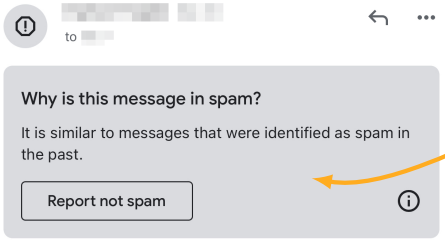
Present time

Related
sender address

Own
receiver address

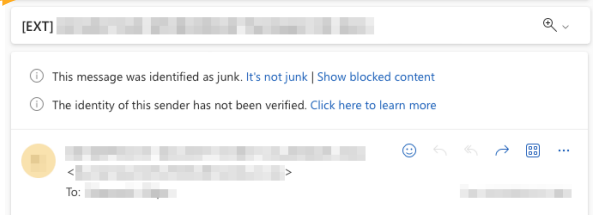
Personal
assistive technology

Realistic Settings... (cont'd)



Spam banners too...

Personal email client



Our study, then...

Assessing Suspicious Emails with Banner Warnings Among Blind and Low-Vision Users in Realistic Settings

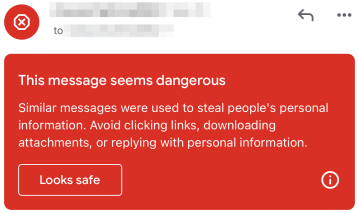
Research Questions

RQ1 → How a) **accessible** and b) **usable** are the *phishing* or *spam* banner warnings sent to their ***own*** email addresses?

RQ2 → Do blind and low vision individuals a) **adhere** and b) **continue to pay attention** to banner warnings?

RQ3 → What **email assessment cues** do blind and low vision individuals employ and what actions they perform)?

RQ4 → What **improvements** do blind and low recommend re: a) **accessibility** and b) **usability** of banner warnings?



Study Sample

Demographic Distribution

Gender		
Female 11	Male 9	**Non-Binary** 1
Racial/Ethnic Self Identification		
White 14	Latinx 3	Asian 1
Black 1	Other 2	
Age		
[18-29] 2	[30-39] 7	[40-49] 7
[50-59] 5		
Education		
High-school 1	College 18	Post-Graduate 2
Visual Self Identification		
Totally Blind 4	Blind, Perception of Light 10	Low Vision 7

Technology Distribution

Device	
iPhone 12	Laptop/Windows PC 9
Provider	
Gmail 19	Outlook 2
Client	
App 16	Web 5
Assistive Technology	
Screen Reader 18	Magnifier 3

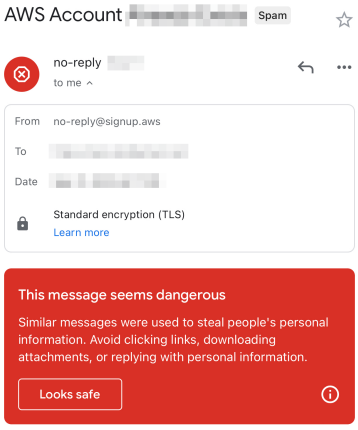
Methodology

Setting → 45-minute, audio-only, Zoom interview: ***own*** device, ***own*** email client, ***own*** assistive technology, everyday sorting of ***own*** emails in spam/junk folder

Non-disclosure / mild deception → Select any emails a participant wants → we had to ensure a higher probability that they would encounter *phishing*, *spam*, or *both*

False Positive Email → Sent to their email, knowing that Gmail or Oultook will assign a banner warning

Initiation → Instantiated on the day of participation



Personal Emails Used in the Study per Participant

P#	Gmail Spam	Gmail Phishing	Outlook Junk
P1	1	1	n/a
P2	1	1	n/a
P3	1	1	n/a
P4	2	1	n/a
P5	2	0	n/a
P6	1	1	n/a
P7	2	1	n/a
P8	2	1	n/a
P9	2	1	n/a
P10	n/a	n/a	2

P#	Gmail Spam	Gmail Phishing	Outlook Junk
P11	2	1	n/a
P12	2	1	n/a
P13	n/a	n/a	2
P14	2	1	n/a
P15	2	1	n/a
P16	2	0	n/a
P17	1	2	n/a
P18	3	0	n/a
P19	3	0	n/a
P20	2	1	n/a
P21	3	0	n/a

Our study, then...

Results

(at last!)

Study Framing

The usual stuff → The most suspicious ones? emails around "***car insurance***"

The Persuasion → *Scarcity* and *reciprocity* pretexts, reinforced with *authority* (sender)

Email Sorting → "***Screen reader was reading neither the sender nor the attachment content***" → a cue that the overall email was "***super phishy***"

Important emails → Found following an email reminder to "***check your spam folder***"

2FA Delays → An exacerbated problem for blind and low vision individuals

RQ1: Accessibility and Usability – Gmail *Phishing*

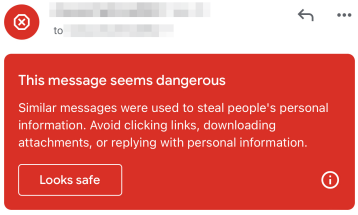
14 out 19 → Screen reader uttered the word "***phishing***" before it read the sender and the subject

Narrow Accessibility → "***It's not obvious [the banner] is a separate interactive element***"

Misaligned Ergonomics → Typically screen readers are "***set on a much faster rate than a generally spoken text***"

Confusing Apprehension → Wondering "***who's stealing the account or trying to steal personal information?***"

Danger → "***Elicit Emotional Response***" without "***really communicating the severity of how harmful an email is***"

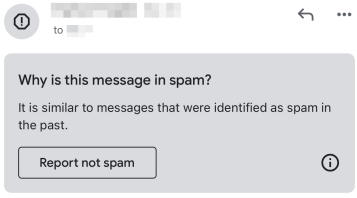


RQ1: Accessibility and Usability – Gmail *Spam*

Narrow Accessibility → ***"The button 'report not spam' is confusing as it doesn't say to whom this report goes and whether the reporting will automatically unblock all future emails from this sender to never go to spam"***

Confusing Apprehension → Inconsistency with phishing: ***"previously [it] was saying to be careful with an email and now [it] just says why the email is in the spam"***

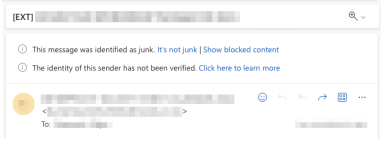
Proceed anyhow → ***"I get [what it supposed to tell me], but it didn't make sense – it's not something I've experienced before with my 'own' similar messages"***



RQ1: Accessibility and Usability – Outlook *Junk*

Narrow Accessibility → “***have easily missed it or went pass through it because it appears before header details***” (unlike the Gmail’s banners)

Confusing Apprehension → Double layered warnings “***too cumbersome and confusing in the first sentence and the follow-up link***”



Proceed anyhow → *Who* is the one that “***identified [an email they received] as junk – the provider, the email owner, or someone else***”

RQ2: Adherence and Attention

Adherence → “***Trust Gmail/Outlook to filter the spam and phishing out for them***”

Accessibility Context → “***Mentioning a ‘danger’ without clear danger ahead is confusing***”

Usability Context → “***‘Report not spam’ feature doesn’t solve the problem with one click***”

Adherence Exceptions → Tedious “***getting legit emails from spam back to inbox***”

Attention → Attenuation → avoid “***paying much attention after the first one***”

Repetition → “***Keywords like ‘spam’ or ‘phishing’ are eclipsed by the convoluted text of the warning itself***”

RQ3: Suspicious Email Assessment Strategies

Cues → "***Random letters and numbers and 'weird' addresses***," "***grammatical errors***," "***spelling errors, omitted letters, or extra letters***"

Accessibility Context → Screen readers to the rescue: "***spam seems to have a lot more punctuation or symbols instead of letters***"

Email Narrative → Warnings might not help → "***too general and doesn't mention examples such as passwords when speaking of 'personal' information***"

Lack of Training → Only **30% of the participants** got a formal phishing training

Phishing Victims → **Six out of 21 participants** fell for a phish → "***email requesting a change of the expiration date of a payment method***"

RQ4: Design Input and Recommendations

Utterance → "***Gmail marked this email as a phishing/spam; tab to see why***" → on the tab action, a full warning "***explaining the features and the decision making of the particular email message that got it marked***"

Risk Level → "***Numeric or categorization system***" would help "***quickly assess***" the email without the need to tab to the main warning

Aural Warning → Bookend the warning text with "***a very short and somewhat unobtrusive sound***" → "***immediate aural connection***"

Interactive Elements → "***Block this sender/subject***," "***delete email***," or "***move email to inbox***"

Low Vision → Use a "***pallet for colorblind users***," "***experimenting with a different shape than the rectangle***," or "*smart glance*"

Thank you!

Questions, Comments, Concerns