RBA notifications

Motivation

- RBA notifications: important, unintuitive, untrustworthy
  - Users and security teams feel RBA emails are important tools
  - A lot of inconsistency in RBA email design
  - Phishing attacks often exploit RBA notifications

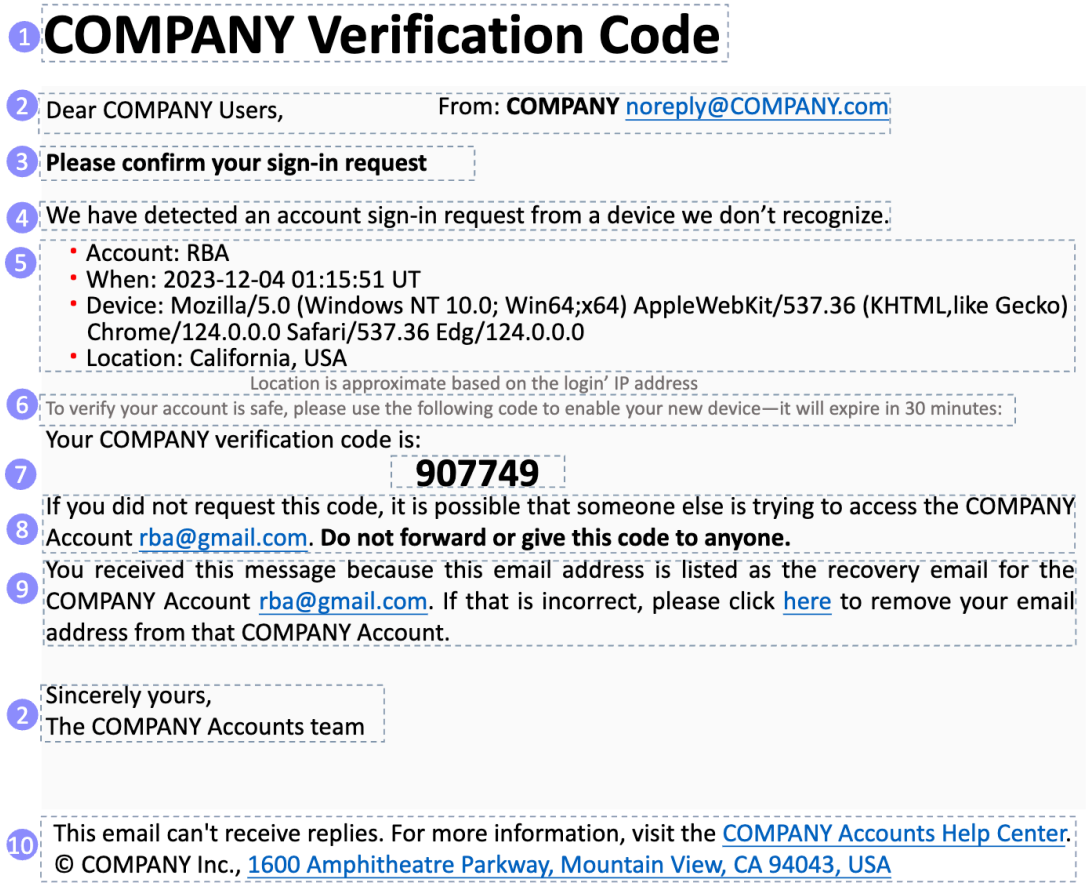
Goals

- How do users *feel* about the notifications?
  - Nervous/anxious/suspicious
- What do users *do* about the notifications?
  - Investigate, change passwords, enable MFA, report as phishing
  - Immediacy of response
- What factors influence people's reactions and actions?
  - Notification features, account importance, etc.

Study Approach

- Collect RBA notifications from 251 real websites
  - Identify common elements of notifications
- Online survey of 258 respondents
  - 25 questions, 20 minutes to answer
- Offline interview of 15 people
  - Send fake RBA emails
  - Structured interview

Email Components



Demographics

TABLE II. DEMOGRAPHICS OF ONLINE PARTICIPANTS (N = 258).

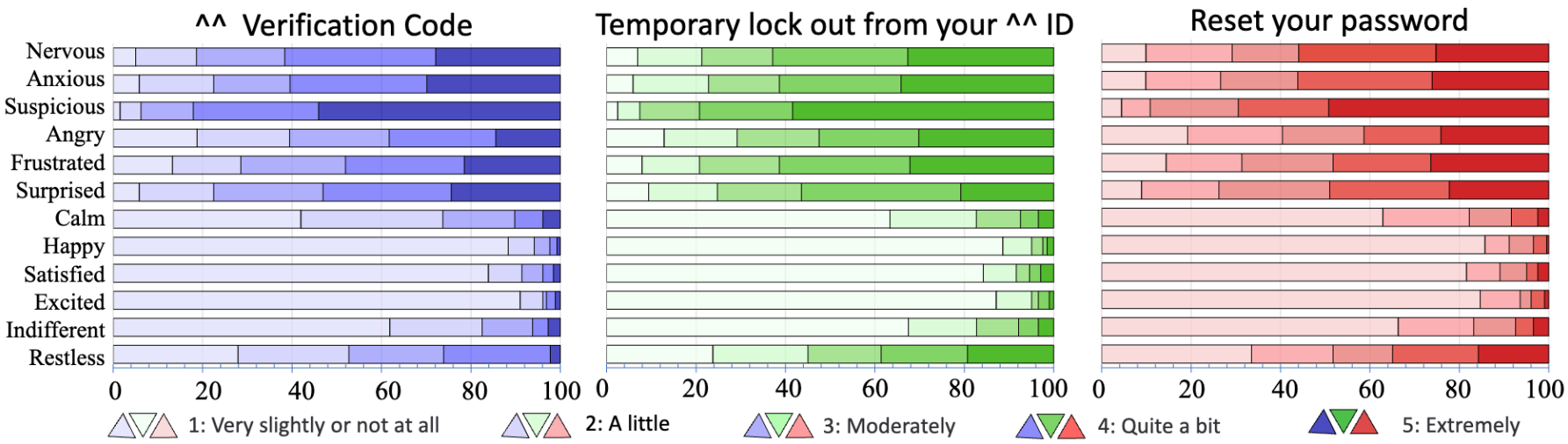
Gender	n	%	**Age**	n	%	**Education**	n	%	**Major**	n	%	**Background**	n	%
Male	103	40	18-25	71	28	High school	87	34	Natural Sciences	16	6	Basic	19	7
Female	146	57	26-35	63	24	Bachelor's	103	40	Humanities	23	9	Familiar	200	78
Non-binary	5	2	36-45	70	27	Master's	47	18	Social Science	33	13	Developer/Professional	37	14
Prefer not to say	4	2	46-55	31	12	Doctorate	5	2	Engineering and Technology	33	13	Not familiar	0	0
			56-65	13	5	Others	12	5	Business and Management	24	9	Prefer not to say	2	1
			66 or older	8	3	Prefer not to say	4	2	Health Sciences and Education	25	10			
			Prefer not to say	2	1				Others	38	15			
									Prefer not to say	66	26			

*We round to the nearest whole number when dealing with percentages, which may lead to the sum of percentages not equaling 100%.

TABLE III. OFFLINE INTERVIEWEE'S PERSONAL INFORMATION.

No.	**Gender**	**Age**	**Education**	**Proficiency**
010	Female	19	Bachelor	Basic
012	Female	23	Master	Basic
020	Male	25	Master	Developer
021	Female	20	Bachelor	Familiar
022	Female	25	Bachelor	Familiar
023	Female	24	Bachelor	Basic
024	Female	22	Bachelor	Basic
025	Female	19	Bachelor	Familiar
026	Female	20	Bachelor	Familiar
027	Male	24	Master	Basic
028	Female	21	Bachelor	Familiar
029	Female	21	Bachelor	Familiar
030	Male	23	Master	Developer
031	Male	24	Master	Developer
032	Male	25	Doctor	Familiar

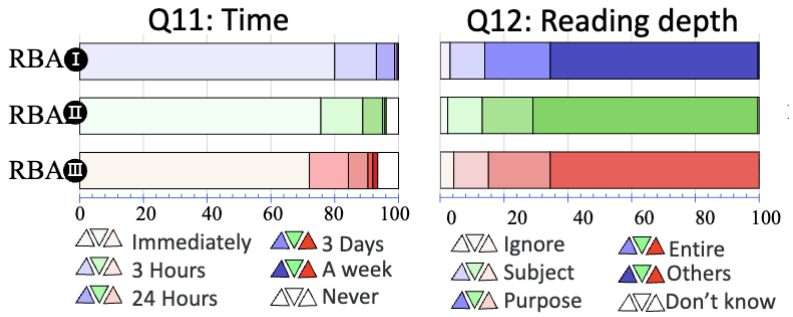
RBA notifications and the 7 dwarfs



- 46% people felt this might be phishing!

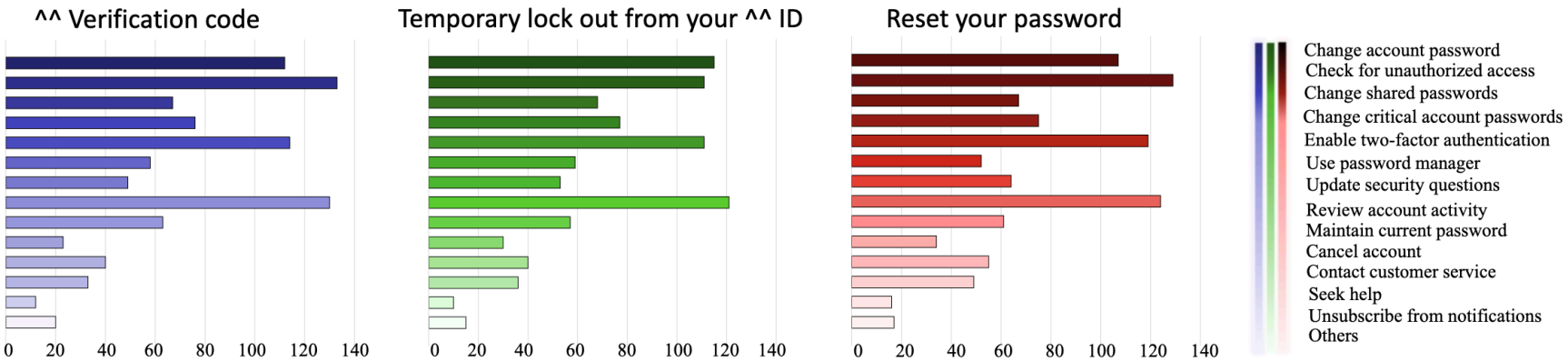
Notification Importance

- Users overwhelmingly feel notifications are important and useful (90%)
- Users largely read entirety of notification and respond immediately
- Some notification fatigue seen by some users



Reaction

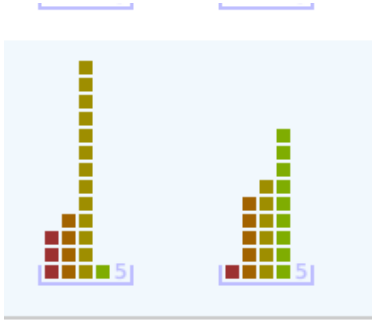
- What's the right response?



Reactions

- Muti-method study
- Real-world RBA notifications
- Recommendations
- Clear figures

- Sampling / generalizability
- Simulated emails / self-reporting
- Too many percentages



Useful Tool? Or burden shifting?

- Do the notifications help users?
- Do the users know what to do?
- How do we split RBA between system actions (lockout, rate limits, extra auth, investigation) and user actions?

Phishing

- RBA emails look like phishing email!
  - Cause a stress reaction
  - Encourage you to log in to account / change password
- How do we make this less likely?

The authority of the sender and the integrity of RBA notification metadata are key factors in establishing user trust. In our interviews, participant P022 states, *"I do not respond to any unfamiliar emails unless I know they are sent by an authoritative institution."* When asked what makes her believe an email is from an authoritative source, she mentions, *"Initially, it is the design of the email that must look formal and professional."* Based on this insight, we deconstruct the RBA notifications and invite participants to assess the necessity of

Habituation

- Do these notifications *need*
  - Deep reading
  - Action
- Can we reduce number of alerts?

Design of RBAs

- What components are most useful?
- How to balance the amount of detail to make them useful but readable / not scary?