

DEPARTMENT OF SECURITY AND CRIME SCIENCE

DAWES CENTRE FOR FUTURE CRIME



**UCL**

# Checking, nudging or scoring? Evaluating e-mail user security tools

*7 August 2023 – SOUPS*

Sarah Zheng, Ingolf Becker  
sarah.zheng.16@ucl.ac.uk



## Scope for usable e-mail security tools

- Even automated detection tools with high accuracies will still let some phishing e-mails through to users, e.g. Oest et al. (2020)
- **Most** methods to help users detect phishing e-mails rely on **training** (Franz et al., 2021)
- Phishing awareness training may not be effective enough (Hillman et al., 2023; Lain et al., 2022; Zheng & Becker, 2022; Reinheimer et al., 2020), because they do not provide guidance **during** critical decision-making moments
- **Underexplored** use of **nudges** (Franz et al., 2022); URL **checking tools** embedded in inboxes showed promising results (Petelka et al., 2019; Volkamer et al., 2017)

# How usable are nudging and checking tools for e-mail security?

## 1. “Check” button

- Objective: assist user when in doubt
- Shows parsed sender details, links and past correspondence – applies to legitimate e-mails, too
- Advice in case of mismatching details

## 2. Nudge 1: Collegiate phishing report

- Objective: raise phishing awareness
- *“This e-mail was reported as suspicious today by one of our colleagues”*
- Shows phishing e-mail example with suspicious signals annotated

## 3. Nudge 2: Suspicion score

- Objective: raise phishing awareness
- *“Are you sure you can trust this e-mail?”*
- Shows e-mail suspicion score + recommends user actions

# Study design

## Qualitative think-aloud task

- Reflective thematic analysis on users' reasoning about e-mails in simulated Outlook web inbox without and then with each tool
- Questions before & after main task; rated which design they found most useful
- Open-sourced Outlook inbox simulation [https://github.com/ucbtszh/mock\\_inbox](https://github.com/ucbtszh/mock_inbox) and study protocol <https://osf.io/xp9ys/>

## Implementation-focused formative evaluation

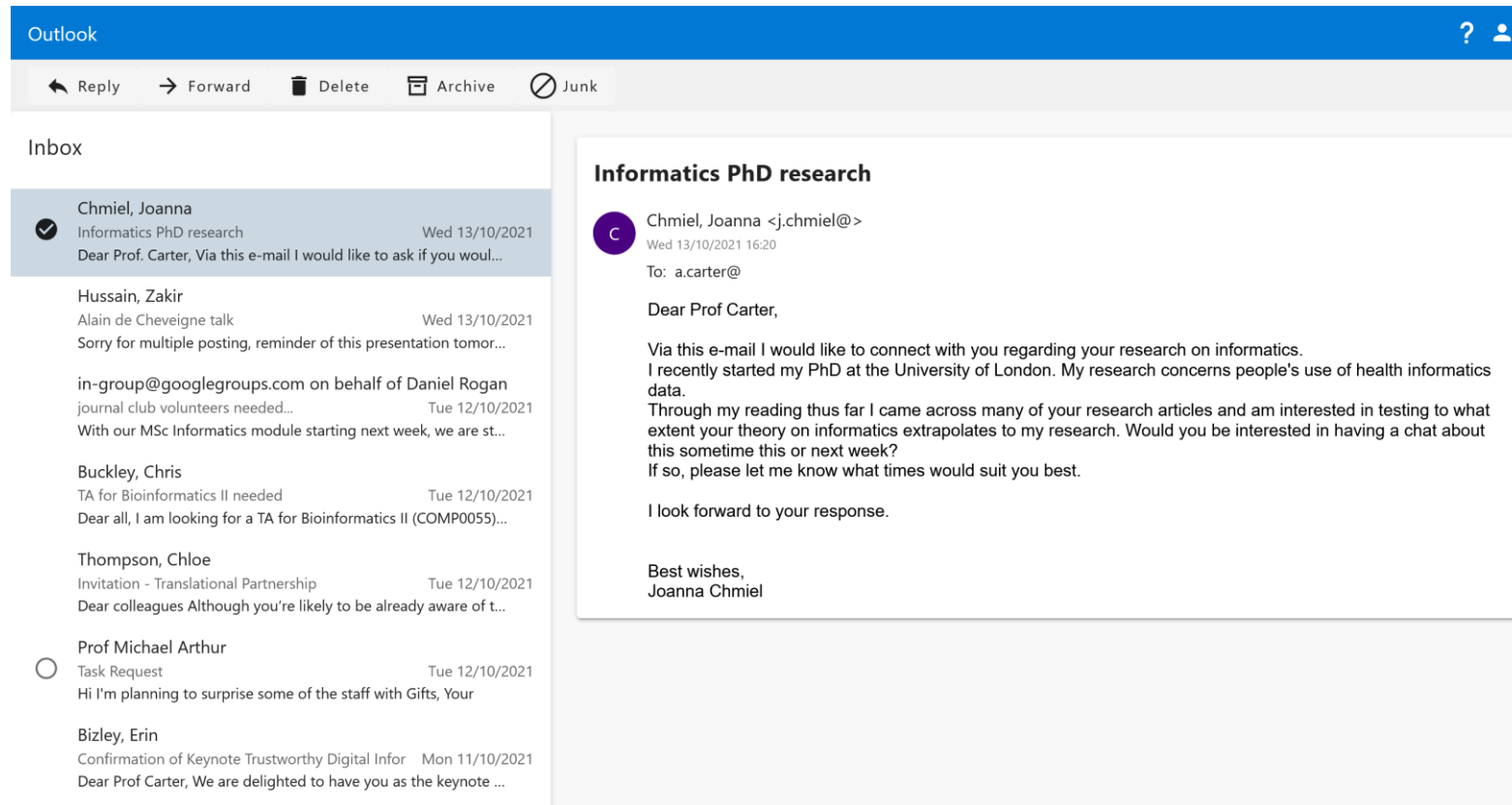
- *How do the tools affect users' e-mail processing behaviour?*
- **Iterative design:** tools were updated after 5 users gave same feedback

## Professional e-mail users (N=27)

- UCL staff; mean age: 33.3, 48% male, 18 recalled cybersecurity training; 19 studied technical subject
- Sessions ran consecutively
- Ethics approval from UCL department

# Simulated Outlook web inbox

Try it yourself: <https://mock-inbox.web.app/> - 33 legitimate & 6 phishing e-mails, academic context



The screenshot shows a simulated Outlook web inbox. The interface includes a blue header bar with the word "Outlook" and a user profile icon. Below the header is a toolbar with icons for Reply, Forward, Delete, Archive, and Junk. The main area is divided into two panes: an "Inbox" list on the left and a detailed email view on the right.

**Inbox List:**

- Chmiel, Joanna** (checked) - Informatics PhD research - Wed 13/10/2021 - Dear Prof. Carter, Via this e-mail I would like to ask if you woul...
- Hussain, Zakir** - Alain de Cheveigne talk - Wed 13/10/2021 - Sorry for multiple posting, reminder of this presentation tomor...
- in-group@googlegroups.com** on behalf of Daniel Rogan - journal club volunteers needed... - Tue 12/10/2021 - With our MSc Informatics module starting next week, we are st...
- Buckley, Chris** - TA for Bioinformatics II needed - Tue 12/10/2021 - Dear all, I am looking for a TA for Bioinformatics II (COMP0055)...
- Thompson, Chloe** - Invitation - Translational Partnership - Tue 12/10/2021 - Dear colleagues Although you're likely to be already aware of t...
- Prof Michael Arthur** (unread) - Task Request - Tue 12/10/2021 - Hi I'm planning to surprise some of the staff with Gifts, Your
- Bizley, Erin** - Confirmation of Keynote Trustworthy Digital Infor - Mon 11/10/2021 - Dear Prof Carter, We are delighted to have you as the keynote ...

**Selected Email: Informatics PhD research**

**From:** Chmiel, Joanna <j.chmiel@>  
**Date:** Wed 13/10/2021 16:20  
**To:** a.carter@

Dear Prof Carter,

Via this e-mail I would like to connect with you regarding your research on informatics. I recently started my PhD at the University of London. My research concerns people's use of health informatics data. Through my reading thus far I came across many of your research articles and am interested in testing to what extent your theory on informatics extrapolates to my research. Would you be interested in having a chat about this sometime this or next week? If so, please let me know what times would suit you best.

I look forward to your response.

Best wishes,  
 Joanna Chmiel

# Evaluation of check button

**A**

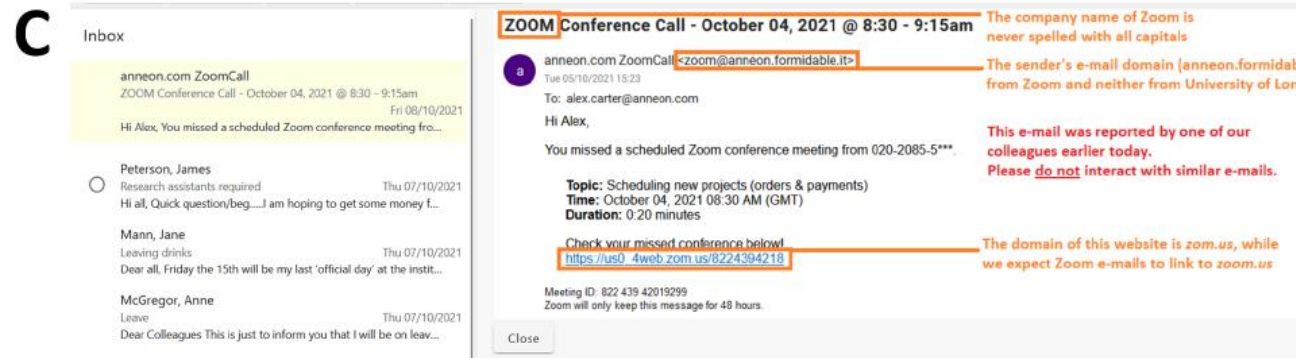
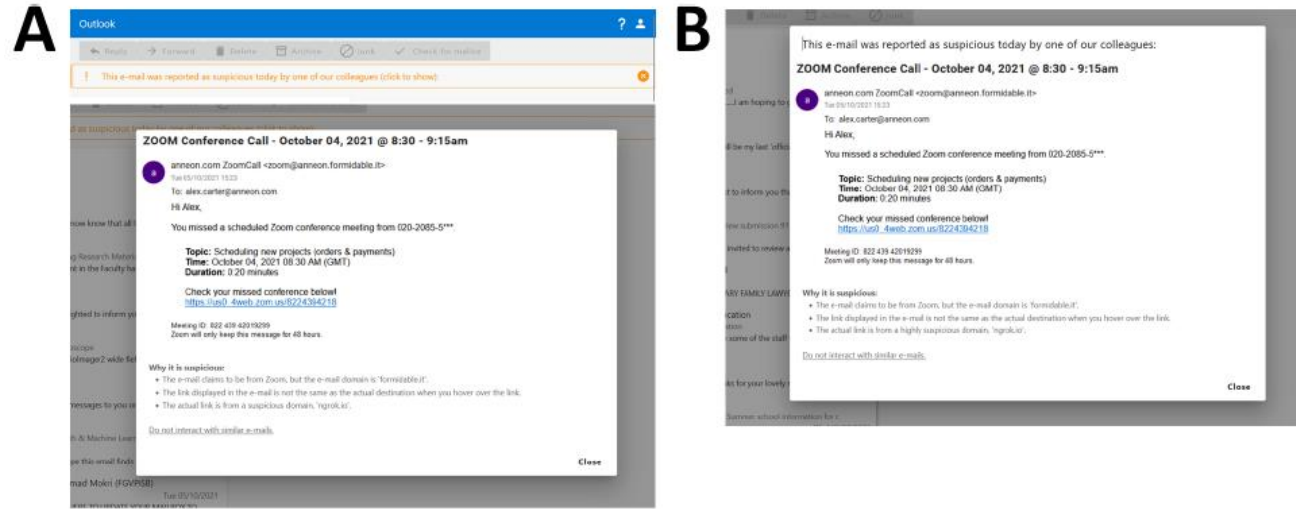
**B**

**C**

**D**

Iteration	Check button
1 ( $N = 8$ )	The majority of users were unaware of the button until nudged towards it (after 2–3 minutes); users did not explore all sub menu items
2 ( $N = 7$ )	Users remained unaware of the button until the researcher pointed it out, but also often did not see the benefit of the provided information.
3 ( $N = 5$ )	Users remained unaware of the button until the researcher pointed it out; the ‘past correspondence’ element was deemed useful
4 ( $N = 7$ )	Most users who noticed and started using the button found it very useful

# Evaluation of collegiate phishing report nudge



## Iteration Nudge 1: Collegiate phishing report

- ( $N = 8$ ) Users tended not to click on the warning banner or got confused about which e-mail the warning is referring to
- ( $N = 7$ ) Users did not like pop-up windows and often felt urged to close it right away
- ( $N = 5$ ) (design did not change)
- ( $N = 7$ ) More users skimmed over the warning content, some users found this and the suspicion score generally useful as they alerted them of suspicious e-mails



# Evaluation of suspicion score nudge

**A** IT

**!** Are you sure you can trust this e-mail?  
 Junk filters rate this e-mail as 0.71 on a scale of 0 (trustworthy) to 1 (highly suspicious).  
 Please double check the sender's e-mail address and any URLs in the e-mail before communicating further with them.

M Muhammad Asheq Ahmad Mokri (FGVPISB) <asheq.am@fgvholdings.com>  
 Tue 05/10/2021 10:04  
 To: a.carter@uol.ac.uk

Dear Users,  
 Please [CLICK HERE](#) TO UPDATE YOUR MAILBOX TO AVOID DEACTIVATION.

Microsoft Admin Help Desk  
 Copyright © 2022 Information Center.

**B** IT

**!** Are you sure you can trust this e-mail?  
 Junk filters rate this e-mail as 0.71 on a scale of 0 (trustworthy) to 1 (highly suspicious).

Double check the sender's e-mail address and any URLs in the e-mail before communicating further with them.

M Muhammad Asheq Ahmad Mokri (FGVPISB) <asheq.am@fgvholdings.com>  
 Tue 05/10/2021 10:04  
 To: a.carter@uol.ac.uk

Dear Users,  
 Please [CLICK HERE](#) TO UPDATE YOUR MAILBOX TO AVOID DEACTIVATION.

Microsoft Admin Help Desk  
 Copyright © 2022 Information Center.

---

## Iteration Nudge 2: Suspicion score

---

1 ( $N = 8$ ) Users did not read all provided information, but found the orange colour positively alerting and useful

2 ( $N = 7$ ) (design did not change)

3 ( $N = 5$ ) (design did not change)

4 ( $N = 7$ ) Users did not read all provided information, but found the orange colour positively alerting and useful; subtle text formatting edits did not lead to significantly more users applying the recommended actions

---



## Overall usability drivers

“**Most useful**”: suspicion score nudge (N=9), past correspondence check (N=7), both (N=4)

1. **Usability of security information:** technical security-related information was perceived as too much, difficult to understand and/or often ignored; users did adopt intuitive cues of legitimacy, e.g. past correspondence check
2. **Productivity vs. security:** users did not engage with tools that seem irrelevant to get the primary task done
3. **Concerns on false positives:** suspicion score nudge let users actively think about e-mail legitimacy; may not fully prevent wrong conclusions
4. **Ignorance toward security features:** when users find the tool’s functionality unclear or unnecessary, they did not explore it

# Conclusion

Guidelines for future usable e-mail security tool development

Embedded e-mail user security tools can be effective *if* they:

1. **Highlight cues of desired (i.e. legitimate) communication** instead of what is undesired (e.g. phishing)
2. **Enhance users' existing behaviour** instead of technical knowledge
  - To avoid warning fatigue, provide contextually relevant information only when helpful
3. **Do not** interfere with users' productivity (i.e., primary task)

DEPARTMENT OF SECURITY AND CRIME SCIENCE

DAWES CENTRE FOR FUTURE CRIME



**UCL**

# Checking, nudging or scoring? Evaluating e-mail user security tools

*7 August 2023 – SOUPS*

Sarah Zheng, Ingolf Becker  
sarah.zheng.16@ucl.ac.uk

