Falling for Phishing: An Empirical Investigation into People's Email Response Behaviors

Dr Asangi Jayatilaka (Presenter)

Dr Nalin Asanka Gamagedara Arachchilage and

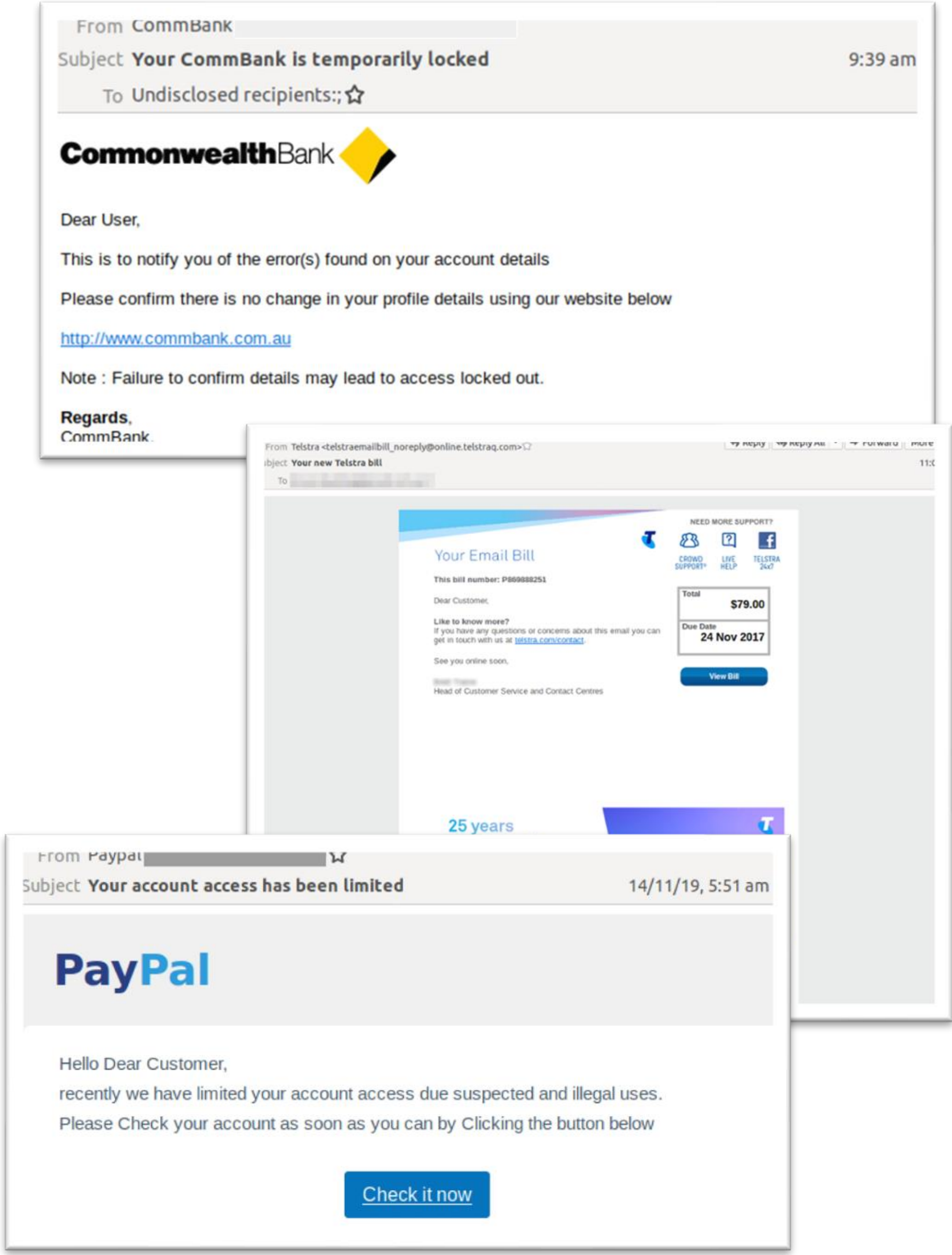
Professor Ali Babar

Introduction — Email and Phishing

- In today's world, email is a vital tool for communication

- As result of the ease of communication and widespread usage, emails have attracted many exploitations in the form of phishing attacks

- The FBI’s Internet Crime Report shows that in 2020, over $1.8 billion cost incurred only due to business email compromise attacks



From CommBank

Subject Your CommBank is temporarily locked 9:39 am

To Undisclosed recipients:;

CommonwealthBank

Dear User,

This is to notify you of the error(s) found on your account details

Please confirm there is no change in your profile details using our website below

http://www.commbank.com.au

Note : Failure to confirm details may lead to access locked out.

Regards,
CommBank

From Telstra <telstraemailbill_noreply@online.telstraq.com>

bject Your new Telstra bill 11:

To [redacted]

Your Email Bill

This bill number: P869888251

Dear Customer,

Like to know more?
If you have any questions or concerns about this email you can get in touch with us at telstra.com/contact.

See you online soon,

[redacted]
Head of Customer Service and Contact Centres

Total $79.00

Due Date 24 Nov 2017

25 years

From Paypal [redacted]

Subject Your account access has been limited 14/11/19, 5:51 am

PayPal

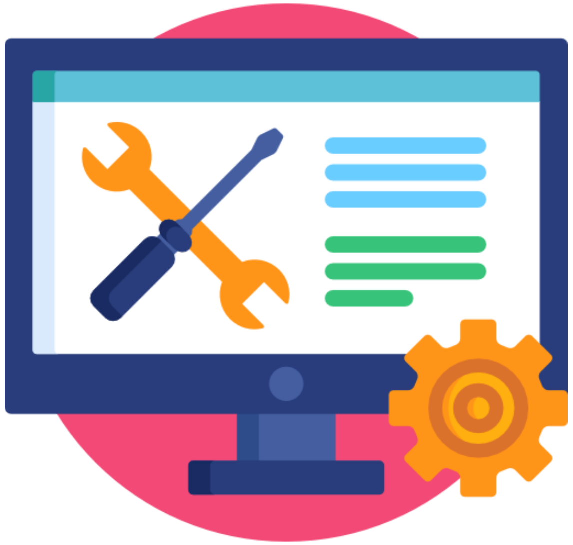
Hello Dear Customer,

recently we have limited your account access due suspected and illegal uses.

Please Check your account as soon as you can by Clicking the button below

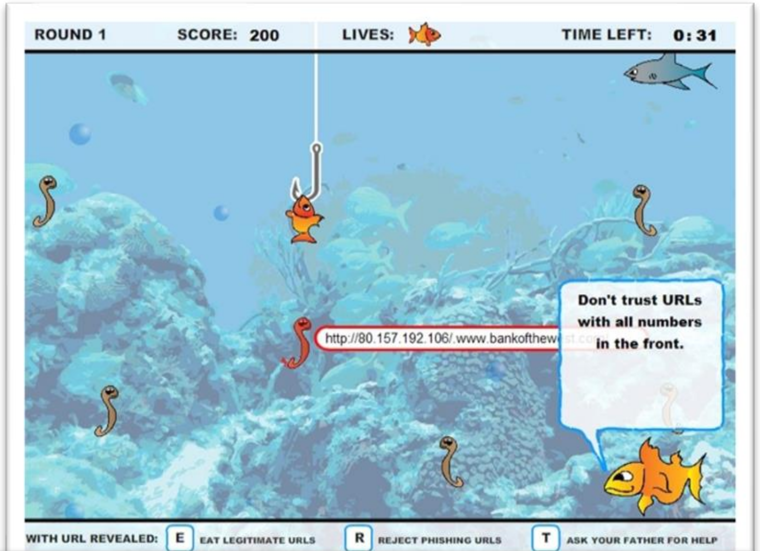
Phishing email detection

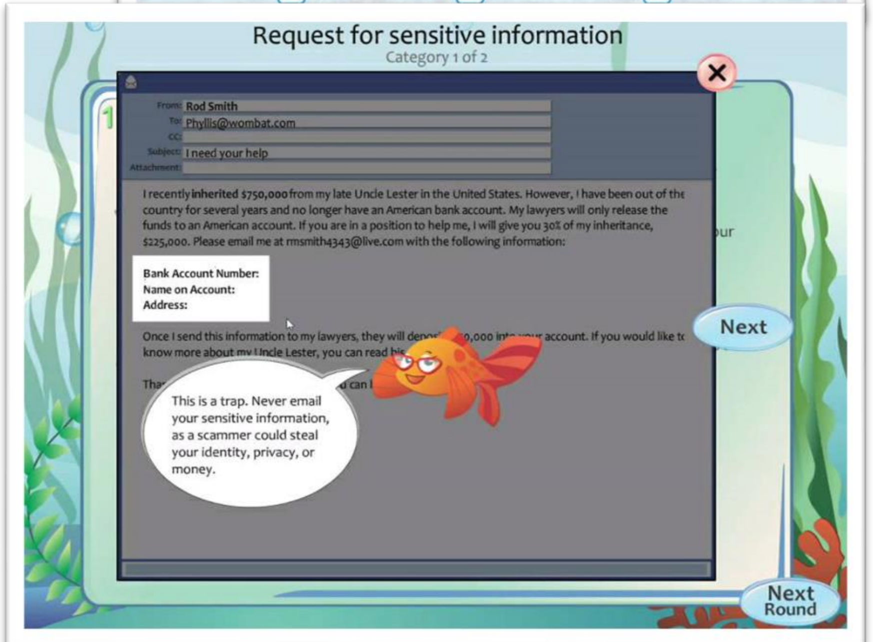
- Various phishing email detection tools and techniques are built
- Even the most sophisticated anti-phishing tools and techniques are not always accurate
    - ✓ Some phish are missed and some genuine items are flagged as phish
    - ✓ Therefore, they cannot be considered a comprehensive solution to protect users from sophisticated phishing attacks



- Human are considered the weakest link in phishing email attacks

- An increased attention to phishing awareness mechanisms, including gamified approaches to educate users and enhance their capability to thwart phishing attacks
  - ✓ The teaching content could easily get outdated
  - ✓ Sometimes the teaching is done outside the email context
  - ✓ Education and training may not be reflected through people’s behaviors


ROUND 1
SCORE: 200
LIVES:
TIME LEFT: 0:31
http://80.157.192.106/.www.bankofthewest.com
Don't trust URLs with all numbers in the front.
WITH URL REVEALED:
E EAT LEGITIMATE URLS
R REJECT PHISHING URLS
T ASK YOUR FATHER FOR HELP


Request for sensitive information
Category 1 of 2
Next
This is a trap. Never email your sensitive information, as a scammer could steal your identity, privacy, or money.
Next Round

From: Rod Smith
To: Phyllis@wombat.com
CC:
Subject: I need your help
Attachment:

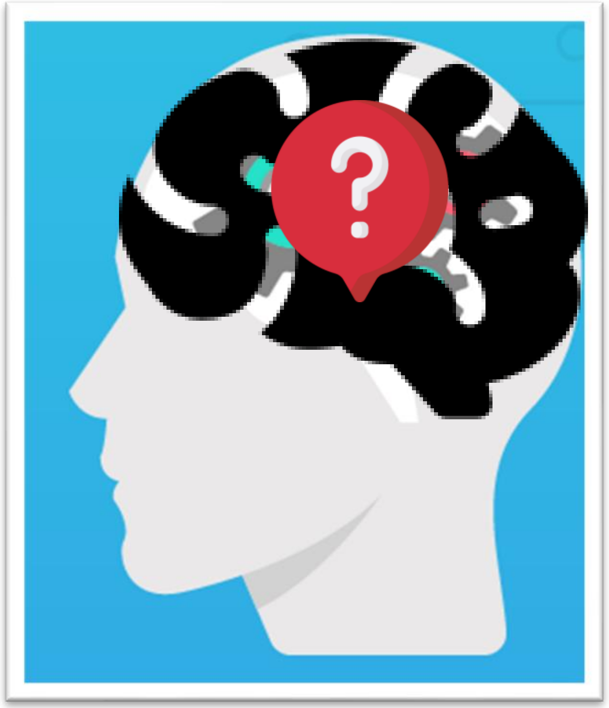
I recently **inherited $750,000** from my late Uncle Lester in the United States. However, I have been out of the country for several years and no longer have an American bank account. My lawyers will only release the funds to an American account. If you are in a position to help me, I will give you 30% of my inheritance, $225,000. Please email me at rmsmith4343@live.com with the following information:

Bank Account Number:
Name on Account:
Address:

Once I send this information to my lawyers, they will depo 0,000 in account. If you would like t know more about my Uncle Lester, you can read his

Tha u can l

In-depth insights into how people interact with emails are vital to better design any anti-phishing intervention, strategy and system



Users' thought process when deciding how to respond to their emails is mostly a black box

What factors influence people's response decisions when reading their emails?

Related work

Understanding user behaviour

- Most of the studies in this space focus on phishing websites or phishing URLs[1]

- Only a limited number of studies have been conducted in the phishing email context, where researchers have looked into the demographic or personality characteristics of people who fall for phishing attack[2]

- Several studies have investigated behavioral responses to phishing emails in order to further explain why people fall into phishing emails[3]
  - ✓ Use images of the emails in the experiment
  - ✓ Use of follow-up surveys for data collection
  - ✓ Limits the users’ decisions while reading the emails

[1] Albakry, Sara, Kami Vaniea, and Maria K Wolters. 2020. "What is this URL's Destination? Empirical Evaluation of Users' URL Reading." In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1-12.

[2] Lawson, Patrick, Carl J Pearson, Aaron Crowson, and Christopher B Mayhorn. 2020. 'Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy', Applied ergonomics, 86: 103084.

[3] Williams, Emma J., and Danielle Polage. 2019. 'How persuasive is phishing email? The role of authentic design, influence and current events in email judgements', Behaviour & Information Technology, 38: 184-97

Methodology

Overview

1 Study protocol

- Define the methodology
  - Decide the participants and method of data collection (Think-aloud role-play experiment and follow-up interview)
  - Select of the emails and URLs
  - Adapt the emails to the scenario
- Develop the email client

2 Pilot study

- Two pilot interviews
- Two researchers
- Changes identified for the study protocol
  - A sample email for participants to get familiarized with the email client
  - The wording of the first question
  - When the follow up questions are asked

3 Data collection

- One researcher conducted data collection via Zoom with screen sharing
- Researcher taking down notes about observed participant behaviors
- 19 participants
- Approximately 90 min session with each participant
- Zoom session recorded with participant consent

4 Data analysis

- Transcription of qualitative data
- Open coding followed up by thematic analysis
- All researchers reviewed and agreed on codes and themes for subset of data before proceeding with the analysis of all the data
- Descriptive statistics to analyze observational data and participant demographics

Methodology

Study protocol

1 Study protocol

- Define the methodology
  - Decide the participants and method of data collection (Think-aloud role-play experiment and follow-up interview)
  - Select of the emails and URLs
  - Adapt the emails to the scenario
- Develop the email client

Email Selection

12 phishing and 12 corresponding legitimate emails for this study by adapting real emails to a given scenario

- ✓ Different life domains
- ✓ Phishing emails were sourced from various venues including UC Berkeley phishing archive and Sensors tech forum etc.
- ✓ Clicking on links, replying to emails and downloading attachments
- ✓ Variety of attacker strategies
- ✓ Legitimate emails were sourced from researchers' personal email correspondences

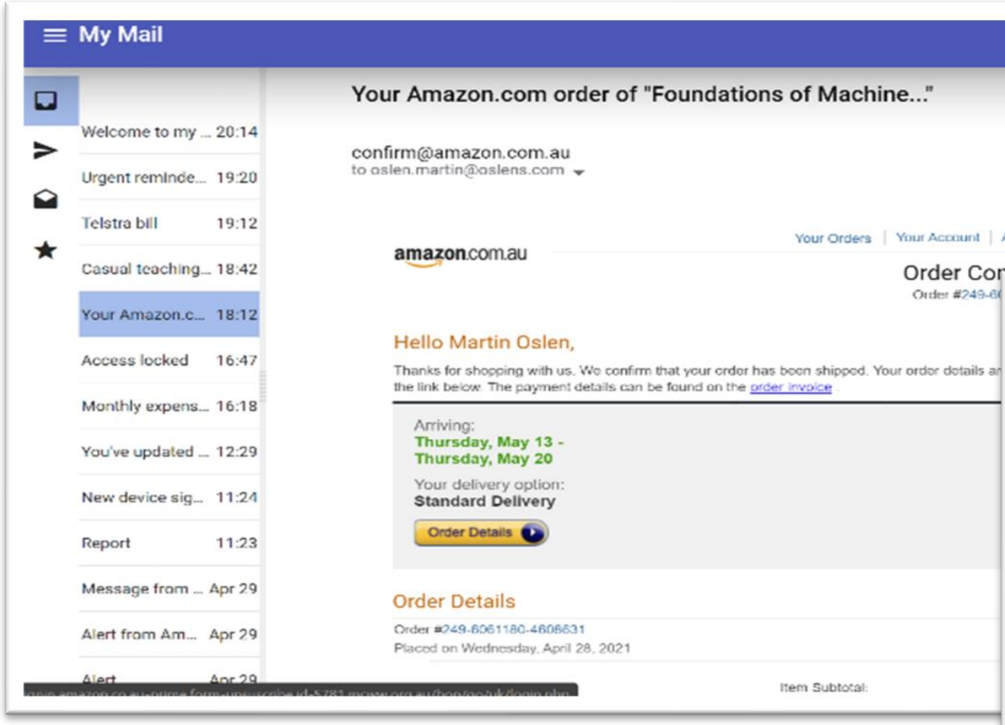
Phishing URL selection

- ✓ Phishing URLs were adopted from real phishing links from PhishTank
- ✓ 5 URL obfuscation techniques

[1] https://security.berkeley.edu/education-awareness/phishing/phishing-examples-archive
[2] https://sensorstechforum.com/
[3] http://phishtank.org/

Methodology

Study protocol



Welcome to my ...	20:14
Urgent reminde...	19:20
Telstra bill	19:12
Casual teaching...	18:42
Your Amazon.c...	18:12
Access locked	16:47
Monthly expens...	16:18
You've updated ...	12:29
New device sig...	11:24
Report	11:23
Message from ...	Apr 29
Alert from Am...	Apr 29
Alert	Apr 29

Your Amazon.com order of "Foundations of Machine..."

confirm@amazon.com.au
to oslen.martin@oslens.com

Order Confirmation
Order #249-6

Hello Martin Oslen,

Thanks for shopping with us. We confirm that your order has been shipped. Your order details a
the link below. The payment details can be found on the order invoice .

Arriving:
**Thursday, May 13 -
Thursday, May 20**

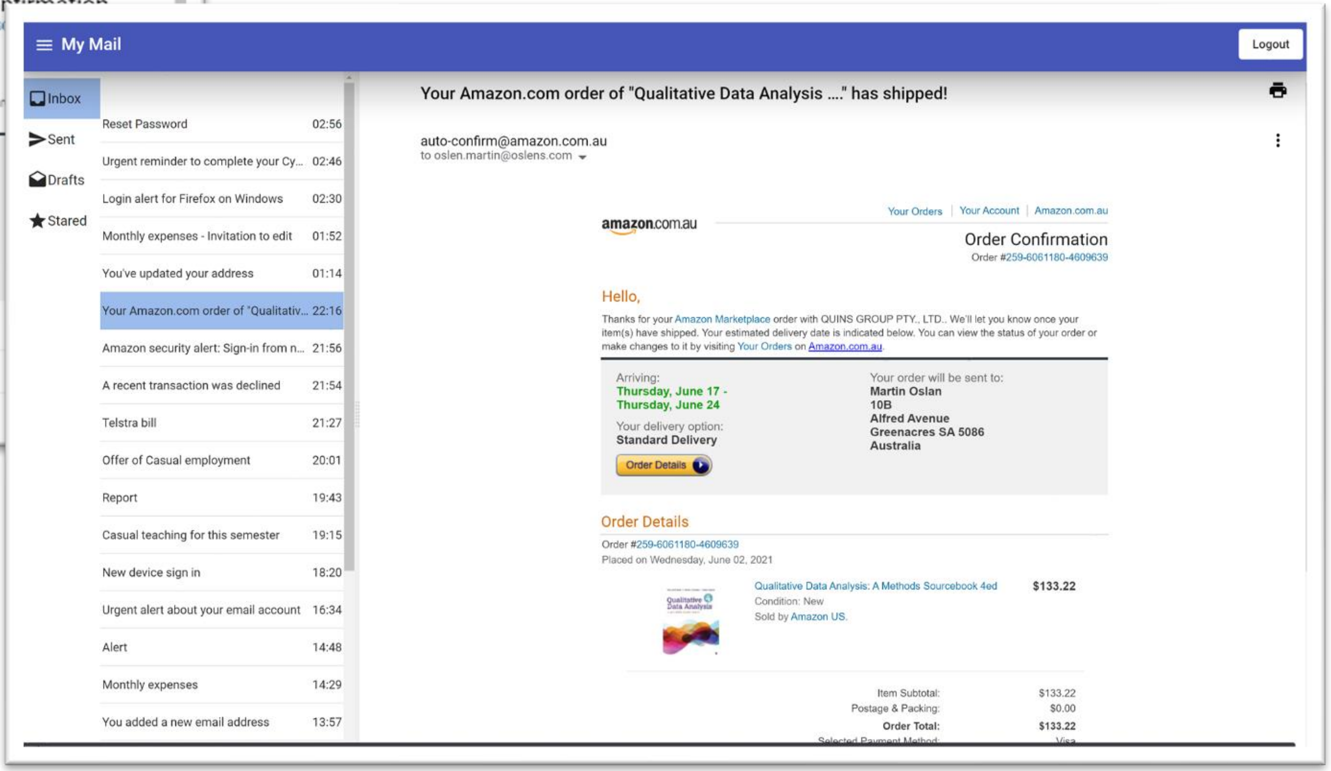
Your delivery option:
Standard Delivery

Order Details

Order #249-6061180-4608631
Placed on Wednesday, April 28, 2021

Item Subtotal:

Phishing email



Reset Password	02:56
Urgent reminder to complete your Cy...	02:46
Login alert for Firefox on Windows	02:30
Monthly expenses - Invitation to edit	01:52
You've updated your address	01:14
Your Amazon.com order of "Qualitativ...	22:16
Amazon security alert: Sign-in from n...	21:56
A recent transaction was declined	21:54
Telstra bill	21:27
Offer of Casual employment	20:01
Report	19:43
Casual teaching for this semester	19:15
New device sign in	18:20
Urgent alert about your email account	16:34
Alert	14:48
Monthly expenses	14:29
You added a new email address	13:57

Your Amazon.com order of "Qualitative Data Analysis ...." has shipped!

auto-confirm@amazon.com.au
to oslen.martin@oslens.com

Order Confirmation
Order #259-6061180-4609639

Hello,

Thanks for your Amazon Marketplace order with QUINS GROUP PTY., LTD.. We'll let you know once your item(s) have shipped. Your estimated delivery date is indicated below. You can view the status of your order or make changes to it by visiting Your Orders on Amazon.com.au.

Arriving:
**Thursday, June 17 -
Thursday, June 24**

Your delivery option:
Standard Delivery

Your order will be sent to:
**Martin Oslan
10B
Alfred Avenue
Greenacres SA 5086
Australia**

Order Details

Order #259-6061180-4609639
Placed on Wednesday, June 02, 2021

Qualitative Data Analysis: A Methods Sourcebook 4ed **$133.22**
Condition: New
Sold by Amazon US.

Item Subtotal:	$133.22
Postage & Packing:	$0.00
Order Total:	**$133.22**
Selected Payment Method:	Visa

Legitimate email

Methodology

Pilot study

1 Study protocol

- Define the methodology
  - Decide the participants and method of data collection (Think-aloud role-play experiment and follow-up interview)
  - Select of the emails and URLs
  - Adapt the emails to the scenario
- Develop the email client

2 Pilot study

- Two pilot interviews
- Two researchers
- Changes identified for the study protocol
  - A sample email for participants to get familiarized with the email client
  - The wording of the first question
  - When the follow up questions are asked

Methodology

Data collection

1 Study protocol

- Define the methodology
  - Decide the participants and method of data collection (Think-aloud role-play experiment and follow-up interview)
  - Select of the emails and URLs
  - Adapt the emails to the scenario
- Develop the email client

2 Pilot study

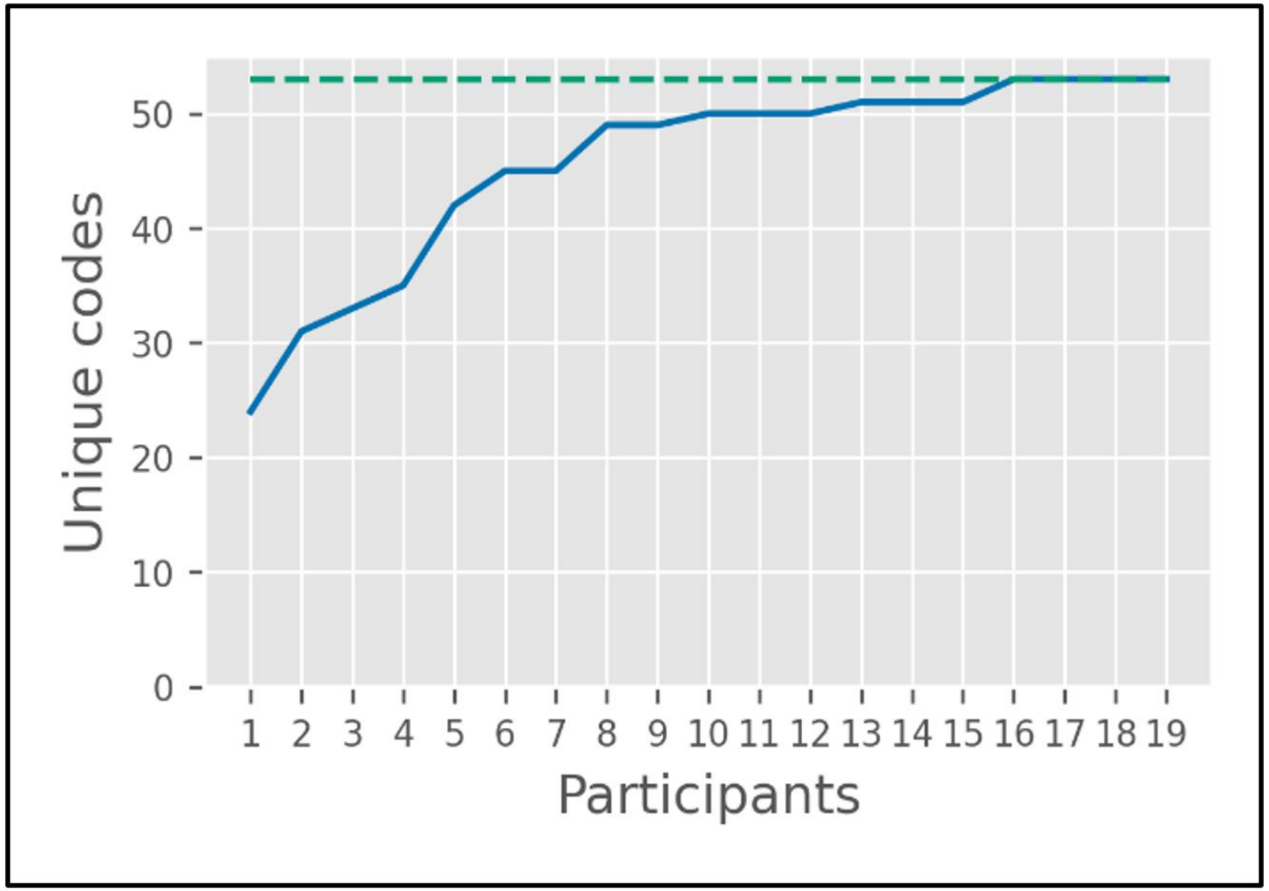
- Two pilot interviews
- Two researchers
- Changes identified for the study protocol
  - A sample email for participants to get familiarized with the email client
  - The wording of the first question
  - When the follow up questions are asked

3 Data collection

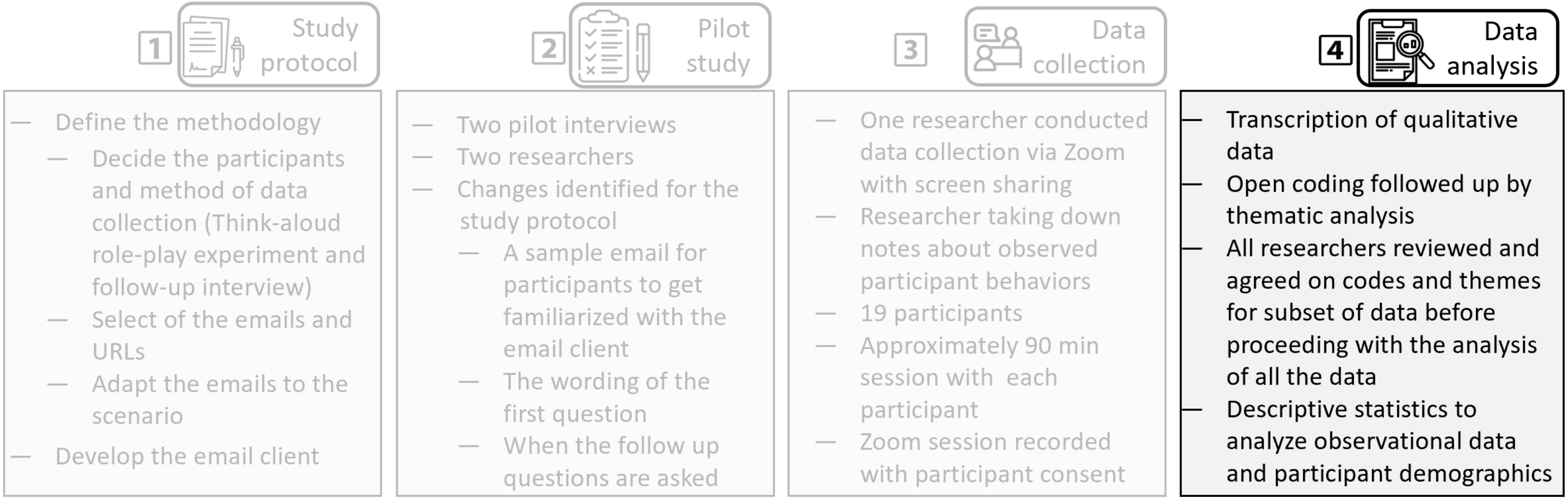
- One researcher conducted data collection via Zoom with screen sharing
- Researcher taking down notes about observed participant behaviors
- 19 participants
- Approximately 90 min session with each participant
- Zoom session recorded with participant consent

1 Stud
protoc

- Define the methodology
  - Decide the participants and method of data collection (Think-aloud role-play experiment a follow-up interview)
  - Select of the emails an URLs
  - Adapt the emails to the scenario
- Develop the email client



Methodology › Data analysis



1 Study protocol

- Define the methodology
  - Decide the participants and method of data collection (Think-aloud role-play experiment and follow-up interview)
  - Select of the emails and URLs
  - Adapt the emails to the scenario
- Develop the email client

2 Pilot study

- Two pilot interviews
- Two researchers
- Changes identified for the study protocol
  - A sample email for participants to get familiarized with the email client
  - The wording of the first question
  - When the follow up questions are asked

3 Data collection

- One researcher conducted data collection via Zoom with screen sharing
- Researcher taking down notes about observed participant behaviors
- 19 participants
- Approximately 90 min session with each participant
- Zoom session recorded with participant consent

4 Data analysis

- Transcription of qualitative data
- Open coding followed up by thematic analysis
- All researchers reviewed and agreed on codes and themes for subset of data before proceeding with the analysis of all the data
- Descriptive statistics to analyze observational data and participant demographics

User study findings — Overview

- 11 factors that explain what influences users' email response decisions when reading them.

- Perception about links in emails
- Need for validation
- Emotions
- Sender legitimacy
- Familiarity of the email title and body
- Professionalism of the email title and body
- Perceived likelihood of receiving an email
- Length and granularity of information
- Previous phishing experiences
- Sense of security from auxiliary security content
- Individual habits

- Based on each factor we explained how people can be susceptible for phishing emails.

Perception about links in emails

Participants felt less vigilant when there are no links in the email

“Without the links, then you don't have like those things that people are trying to get you to click on to, you know, download the viruses and what not” [P09—L]

Where links are available, the participants tend to decide the URL legitimacy based on the link appearance.

“This button says it will take me to the website I am able to review this unusual logging, I would believe that it would take me to a web site that I will review log in” [P04—L].

“Usually it would say that www dot uber slash something change password something. That might be a bit more convincing than just clicking on the link that says change password now [button]” ” [P10—P]

“But what gives me a bit of confidence is this HTTPS secure server. So secured servers are unlikely, to be phishing sites so that would give me strength” [P10—L]

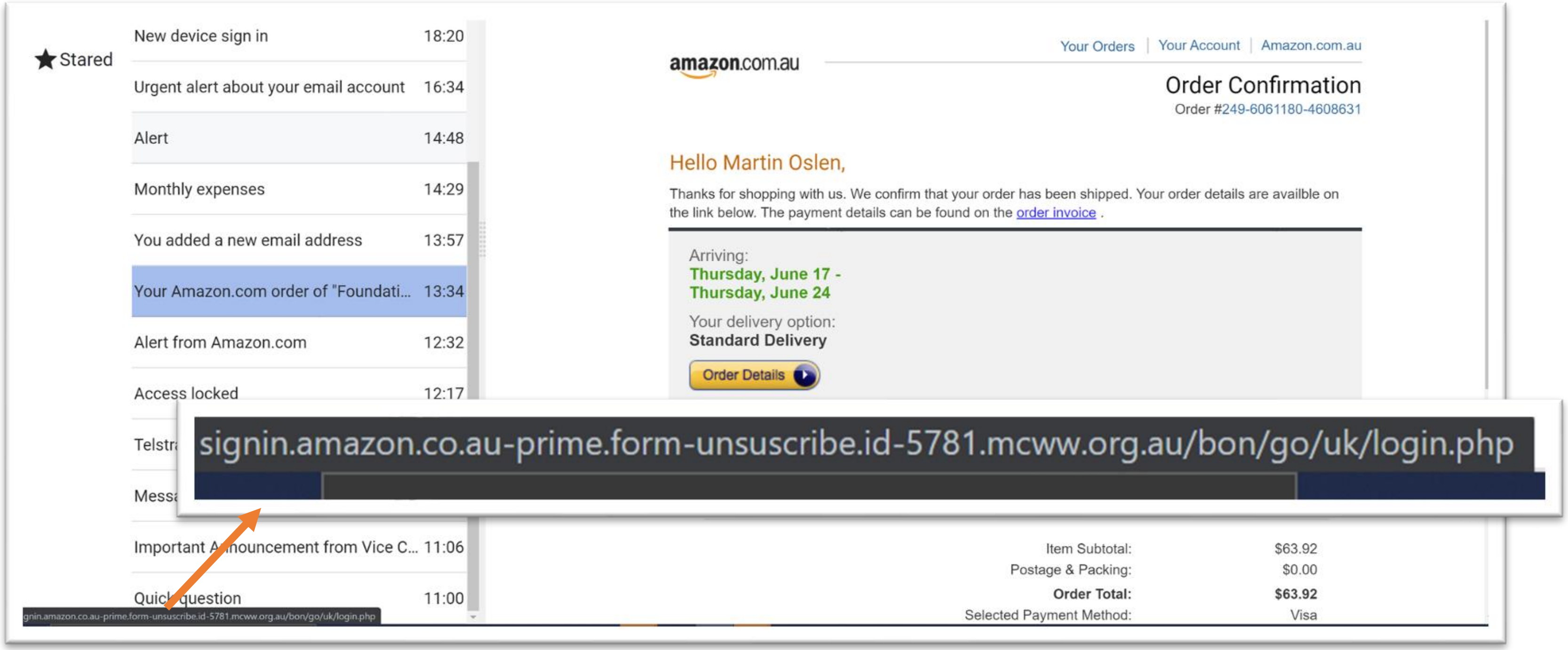
User study findings

Perception about links in emails

Only few (7) looked at the link destination at least once to decide the link reliability

- ✓ None of them consistently check the link destination for all emails
- ✓ Can make wrong decisions about the URL legitimacy even after identifying the link destination

“Yeah, it's popping up on the bottom left-hand side. It says sign in dot amazon dot com dot au slash and a few more things. But um, yeah, just that sign in dot Amazon, which I guess makes sense” [P9—P].



★Stared

New device sign in	18:20
Urgent alert about your email account	16:34
Alert	14:48
Monthly expenses	14:29
You added a new email address	13:57
Your Amazon.com order of "Foundati...	13:34
Alert from Amazon.com	12:32
Access locked	12:17
Telstr	
Mess	
Important Announcement from Vice C...	11:06
Quick question	11:00

amazon.com.au

Your Orders | Your Account | Amazon.com.au

Order Confirmation

Order #249-6061180-4608631

Hello Martin Oslen,

Thanks for shopping with us. We confirm that your order has been shipped. Your order details are availble on the link below. The payment details can be found on the order invoice .

Arriving:
Thursday, June 17 -
Thursday, June 24

Your delivery option:
Standard Delivery

Order Details

Item Subtotal:	$63.92
Postage & Packing:	$0.00
Order Total:	**$63.92**
Selected Payment Method:	Visa

gnin.amazon.co.au-prime.form-unsuscribe.id-5781.mcww.org.au/bon/go/uk/login.php

signin.amazon.co.au-prime.form-unsuscribe.id-5781.mcww.org.au/bon/go/uk/login.php

Susceptibility to phishing emails based on this factor

- ✓ People can be deceived by phishing emails composed without any links but requesting reply or download attachments
- ✓ People can be deceived by phishing emails with legitimate looking buttons or URLs
- ✓ People could make wrong judgements about URL safety by looking only at the network communication protocol mentioned in the URL
- ✓ People can be deceived by phishing links that appear as non-mandatory
- ✓ People can be deceived by phishing emails having a destination URL that is different to the URL text
- ✓ Even people who understand techniques to identify the URL destination can be still susceptible to manipulation as they fail to consistently apply those techniques into practice
- ✓ Even after looking into the destination URL, people can be susceptible to phishing due to the lack of awareness about URL obfuscation and URL structures

User study findings

Need for validation

Need for validating an email when they were suspicious about the email or when they were extra vigilant even when they thought the email looks legitimate

Participants validate emails using information gathered externally to the email

Using mobile app/web site separately

Searching for information mentioned in the email on the internet e.g. logo, company information

Participants validate emails using information gathered from the email it-self

Assume that it is safe to click on links if they are not providing information on the landing page

Not clicking on the main link but would click the other links to make a decision legitimacy of the main link

Clicking on the links on the email to get help and more information about the email

User study findings

Need for validation

Susceptibility to phishing emails based on this factor

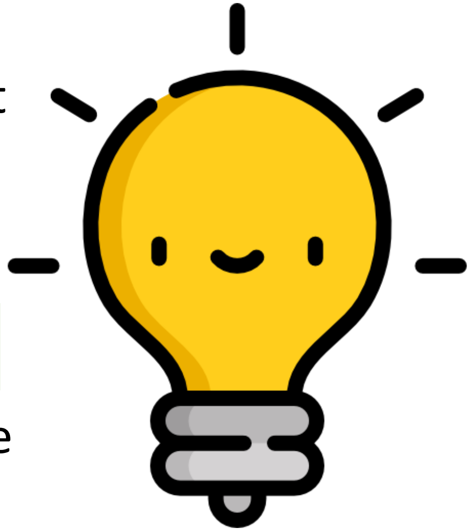
- ✓ People can be deceived through publicly available information that is mentioned in emails
- ✓ People can be deceived by legitimate-looking landing pages for phishing links. Although people may not provide their details on these landing pages, it could still download malware (i.e., malicious IT application) to the victim’s computer system.
- ✓ People can feel safe to click on secondary links available in the phishing emails to validate the main link without understanding that the secondary links could be phishing links as well
- ✓ People can be deceived by seeing various ways (e.g. contact us links) to get help about the email in the email itself.

User study findings | Summary

In-depth insights into how people make email response decisions and how they are susceptible to manipulation due to the flaws in decision making.

Similarities of the findings when compared with previous literature

- People tend to trust emails targeted at them with detailed information and/or look professional
- Alignment of the phishing email to user context makes people have more trust in those emails
- The role of personal characteristics and habits in email decision making



Novel findings

- The possibility for a disconnection between email legitimacy judgment and the email response
- Insights into how perception about email links affects email decision making
- Insights into difficulties in deciding sender legitimacy
- Unsafe ways of validating email content
- Issues in applying knowledge gained from formal education and lessons learnt from exposure to phishing emails
- Insights into how pre-conceived judgements affect people’s response decisions.

The possibility for a disconnection between email legitimacy judgment and the email response

- Simply understanding how people judge email legitimacy is not adequate to obtain a holistic picture of why people fall for phishing emails

- There could be situations where there is a disconnection between the email response and the judgement on email legitimacy.

- People could click on links, reply, and download attachments without even thinking about the email's legitimacy due to emotions and individual habits.

- People could click on email links or reply to emails even after identifying phishing emails or when they are unsure of the email legitimacy

User study findings | Novel findings

Insights into how perception about email links affects email decision making

- People tend to have more trust in emails without links.

- For emails with links, participants could use unsafe techniques
  - ✓ Clicking on links that appear to be non-mandatory
  - ✓ Consider button or URL appearance to assess the link legitimacy.

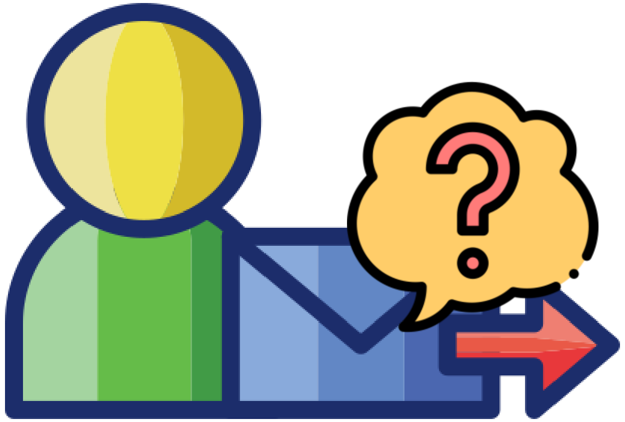
- Often participants do not know to identify the URL destination and those who know do not consistently apply their knowledge.

- Even after identifying the destination link, people may struggle to identify its legitimacy due to a lack of knowledge of URL obfuscation.

Insights into difficulties in deciding sender legitimacy

- People often look at the header information to make email decisions

- Additional insights into misconceptions people have when making judgments about the sender's reliability.
  - ✓ People lack knowledge about sender spoofing.
  - ✓ Get confused with the structure of the sender’s email address (i.e. domain, sub-domain, username),
  - ✓ Get confused with email display name
  - ✓ Get confused with reply-to address
  - ✓ Get confused with email addresses specified in the email body



Unsafe ways of validating email content

- People may not be willing to make a final decision on the email legitimacy while going through an email and may intend to validate the email before making the final decision.

- Although validating an email can be considered a precautionary measure, our findings reveal that some techniques used to validate the email could be unsafe and result in people being victims of phishing attacks.

- This has consequences to how we train users in organizational settings and also what tool we provide them so that they can check the validity of an email.

User study findings → Novel findings

Issues in applying knowledge gained from formal education and lessons learnt from exposure to phishing emails

- Our study findings confirmed that formal education and previous phishing related experiences could provide necessary skills in identifying phishing attacks.

- Additional insights
  - ✓ People learn inaccurate strategies for identifying phishing emails from past experiences
  - ✓ Could make people scared to respond to emails in any way, even when they feel those are legitimate.
  - ✓ People can be still susceptible to manipulation because of the inconsistencies in applying the knowledge to practice.

Insights into how pre-conceived judgements affect people’s response decisions.

- Previous research suggests that urgency arousing cues embedded in a phishing email are positively related to phishing susceptibility.
- Our findings point out that this may be not always true. People can be extra vigilant in some of these situations due to pre-conceived judgements about specific types of emails.

Conclusion

- We identify eleven factors that influence people’s email response decisions while reading their emails.
- Our findings provide novel insights into flaws in the general email decision-making behaviors that could make people more susceptible to phishing attacks
- The findings of the user study can be used to design effective anti-phishing tools and techniques.

On-going and future work

- Designing and developing an email plugin, which can nudge people's email response behaviors by making the potential phishing features of a given email context easily comprehensible
  - ✓ When and how to nudge based on the findings of the user study

- Evaluating the performance of the such behavioural interventions considering usability and privacy

- Validate the findings with diverse populations possibly through surveys

THE UNIVERSITY of ADELAIDE

CREST

asangi.jayatilaka@adelaide.edu.au