Phishing

INFR11158/11230 Usable Security and Privacy

Dr. Jingjie Li

16/02/2024

THE UNIVERSITY *of* EDINBURGH

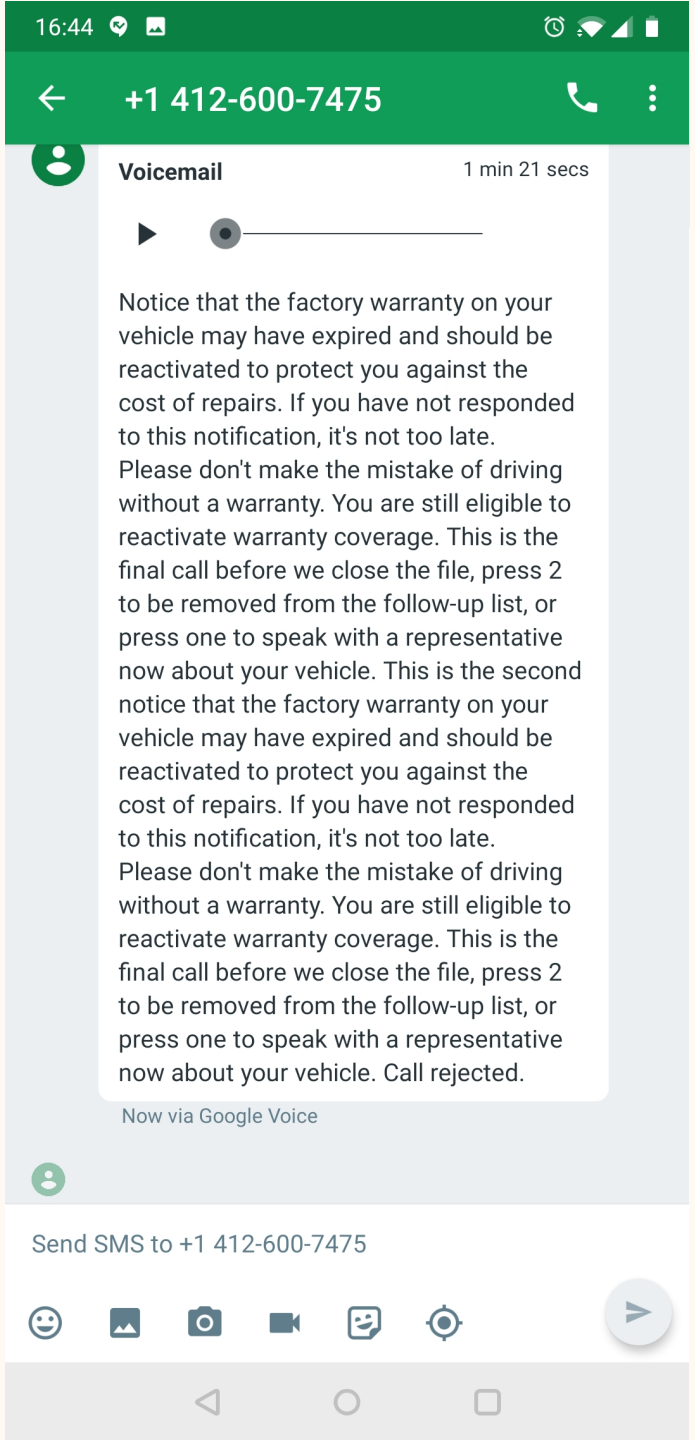
Overview

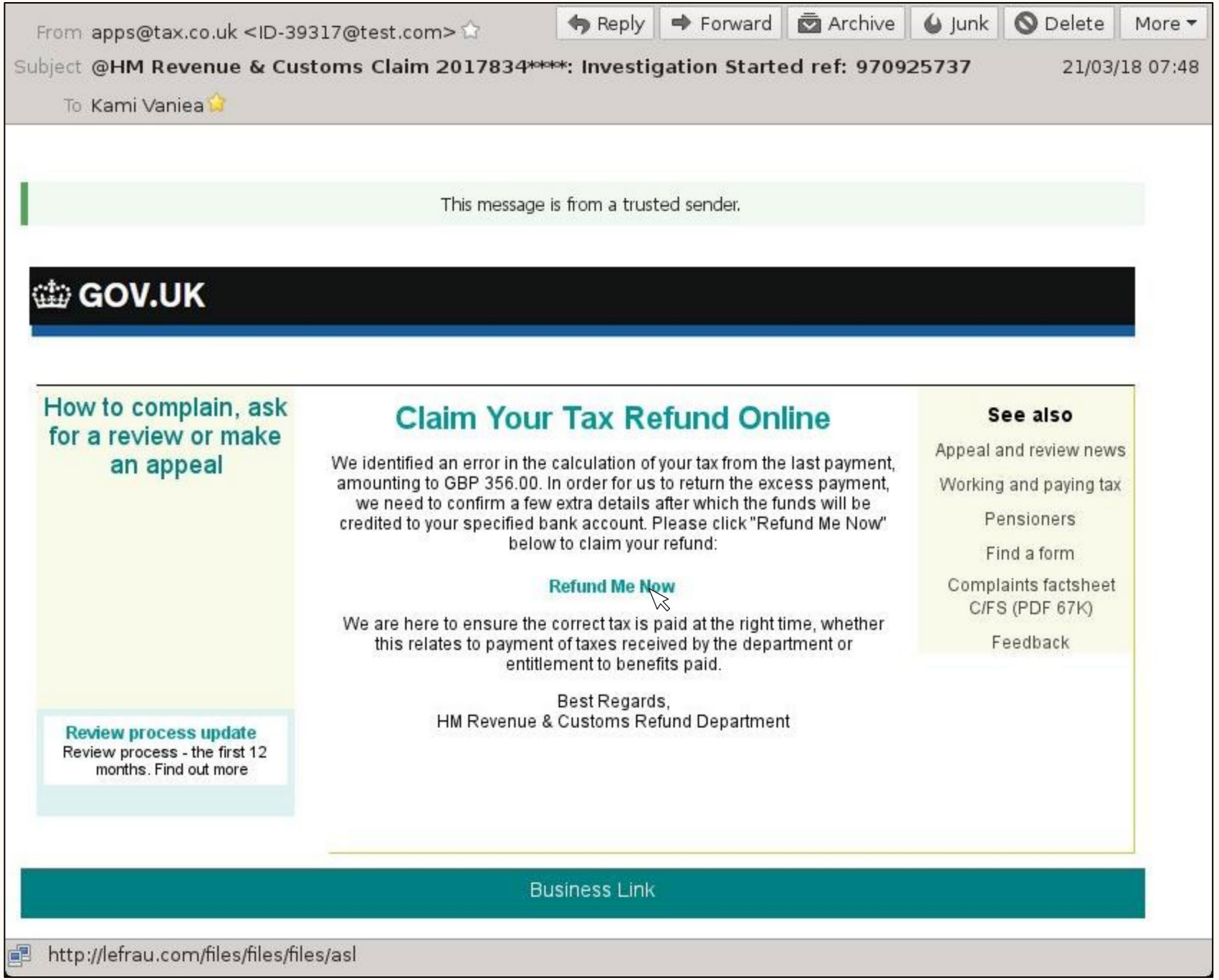
- Warm up and reminder
- Phishing: overview, elements, and countermeasures
- Take-home

Overview

https://www.youtube.com/watch?v=3tI_4QzyhE8

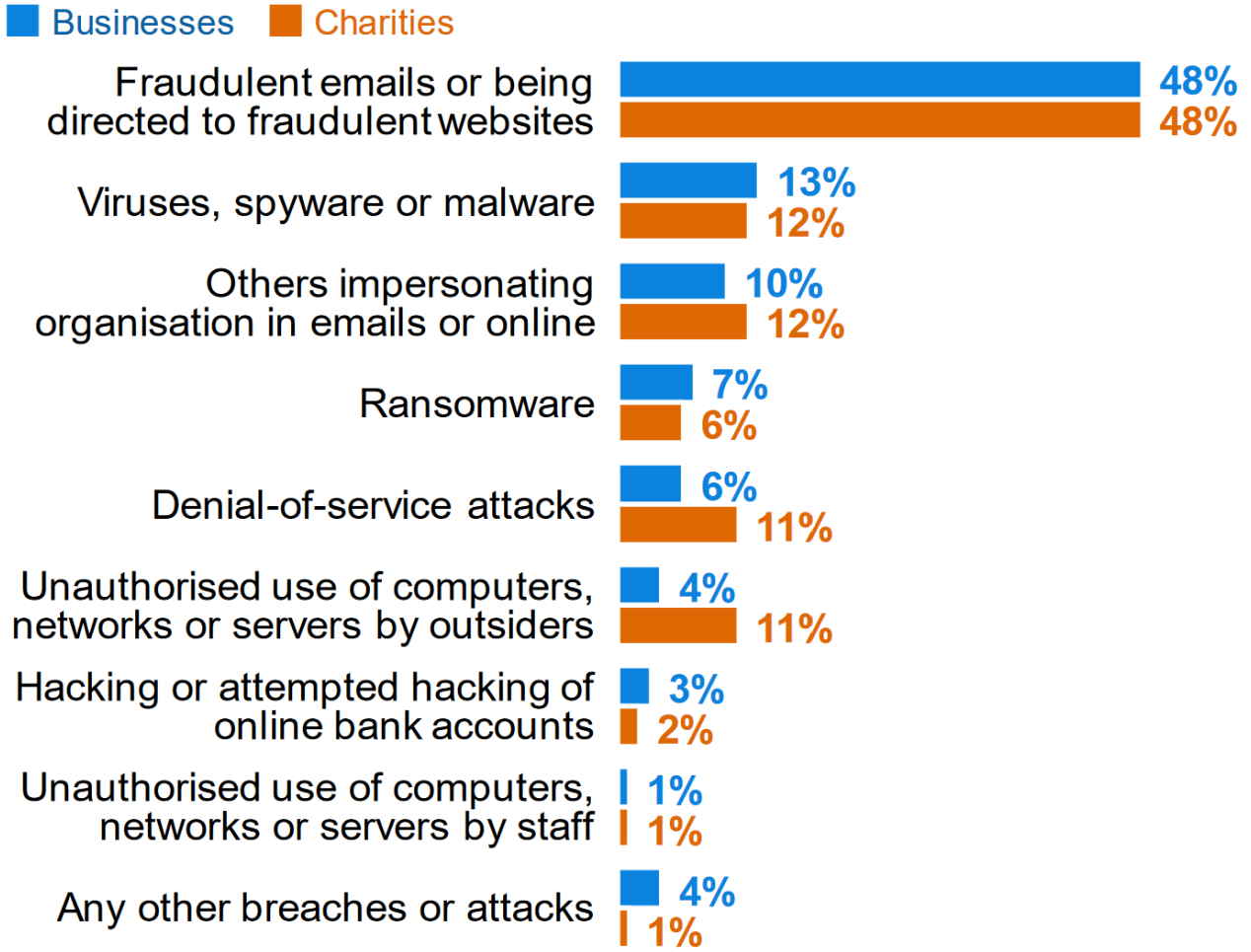
Phishing: when criminals attempt to trick people in doing “the wrong thing”
(https://www.ncsc.gov.uk/files/Phishing-attacks-dealing-suspicious-emails-infographic.pdf)


16:44
+1 412-600-7475
Voicemail
1 min 21 secs
Notice that the factory warranty on your vehicle may have expired and should be reactivated to protect you against the cost of repairs. If you have not responded to this notification, it's not too late. Please don't make the mistake of driving without a warranty. You are still eligible to reactivate warranty coverage. This is the final call before we close the file, press 2 to be removed from the follow-up list, or press one to speak with a representative now about your vehicle. This is the second notice that the factory warranty on your vehicle may have expired and should be reactivated to protect you against the cost of repairs. If you have not responded to this notification, it's not too late. Please don't make the mistake of driving without a warranty. You are still eligible to reactivate warranty coverage. This is the final call before we close the file, press 2 to be removed from the follow-up list, or press one to speak with a representative now about your vehicle. Call rejected.
Now via Google Voice
Send SMS to +1 412-600-7475


From apps@tax.co.uk <ID-39317@test.com>
Reply
Forward
Archive
Junk
Delete
More
Subject @HM Revenue & Customs Claim 2017834****: Investigation Started ref: 970925737
21/03/18 07:48
To Kami Vaniea
This message is from a trusted sender.
GOV.UK
How to complain, ask for a review or make an appeal
Review process update
Review process - the first 12 months. Find out more
Claim Your Tax Refund Online
We identified an error in the calculation of your tax from the last payment, amounting to GBP 356.00. In order for us to return the excess payment, we need to confirm a few extra details after which the funds will be credited to your specified bank account. Please click "Refund Me Now" below to claim your refund:
Refund Me Now
We are here to ensure the correct tax is paid at the right time, whether this relates to payment of taxes received by the department or entitlement to benefits paid.
Best Regards,
HM Revenue & Customs Refund Department
See also
Appeal and review news
Working and paying tax
Pensioners
Find a form
Complaints factsheet C/FS (PDF 67K)
Feedback
Business Link
http://lefrau.com/files/files/files/asl

Phishing is very common and very disruptive to UK businesses

Q. What was the one cyber security breach, or related series of breaches or attacks, that caused the most disruption to your organisation in the last 12 months?



Bases: 778 businesses that identified a breach or attack in the last 12 months; 218 charities

HMG Department for Digital, Culture, Media & Sport. Cyber Security Breaches Survey 2019. July 2019.

Commonalities among breaches in 2018.

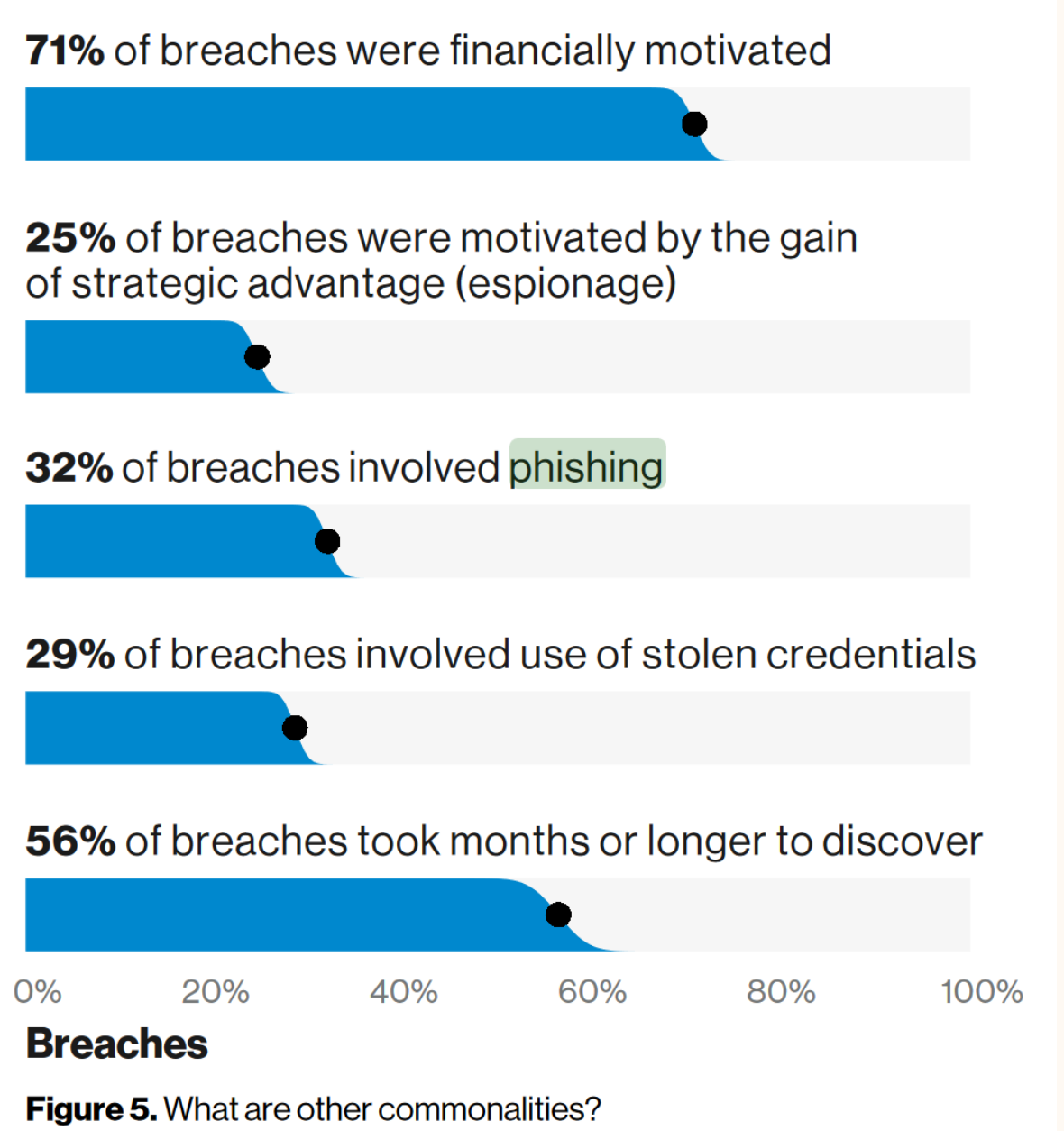
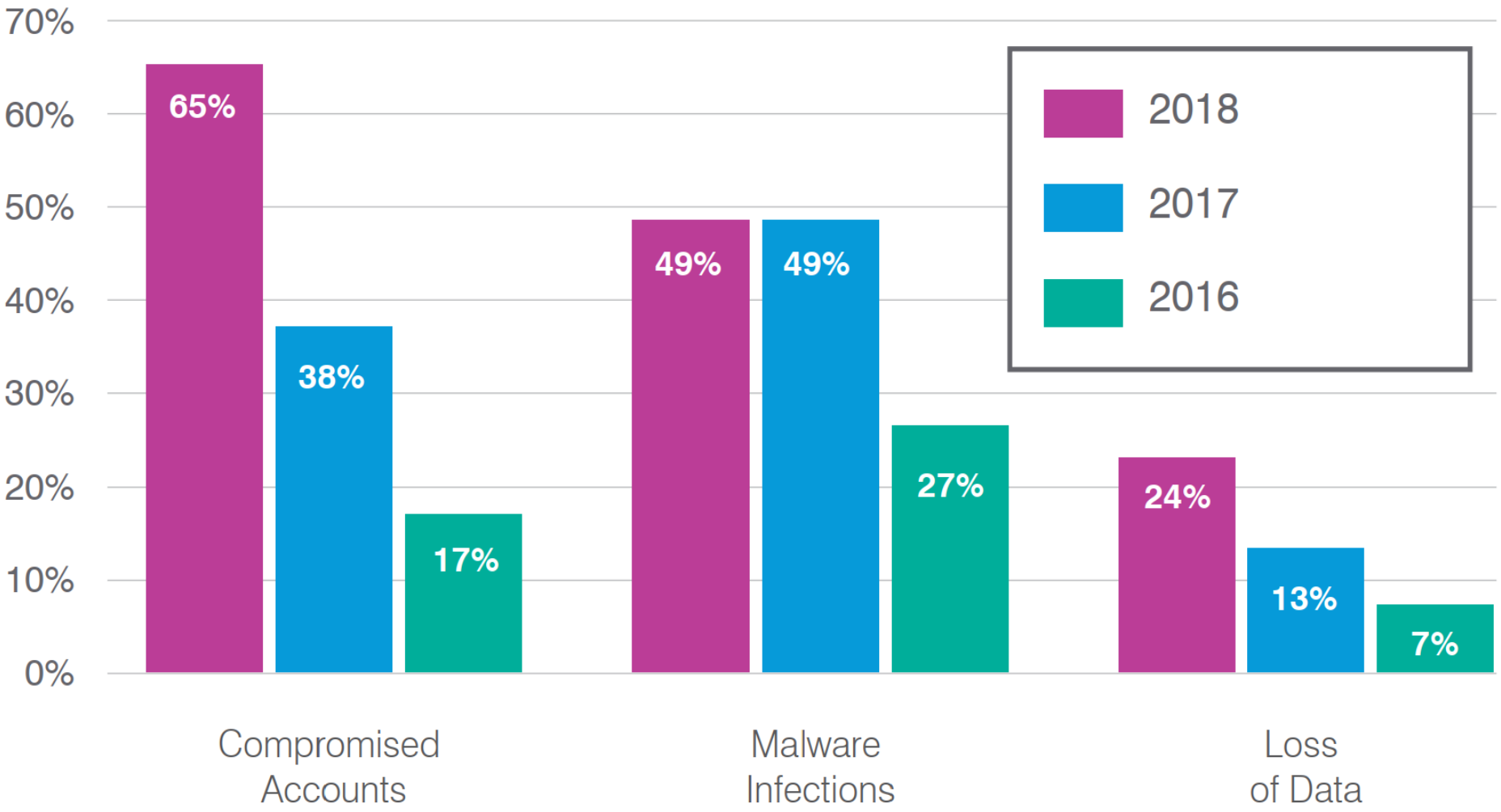


Figure 5. What are other commonalities?

Verizon. 2019 Data Breach Investigation Report. p5

Phishing Impacts Experienced*

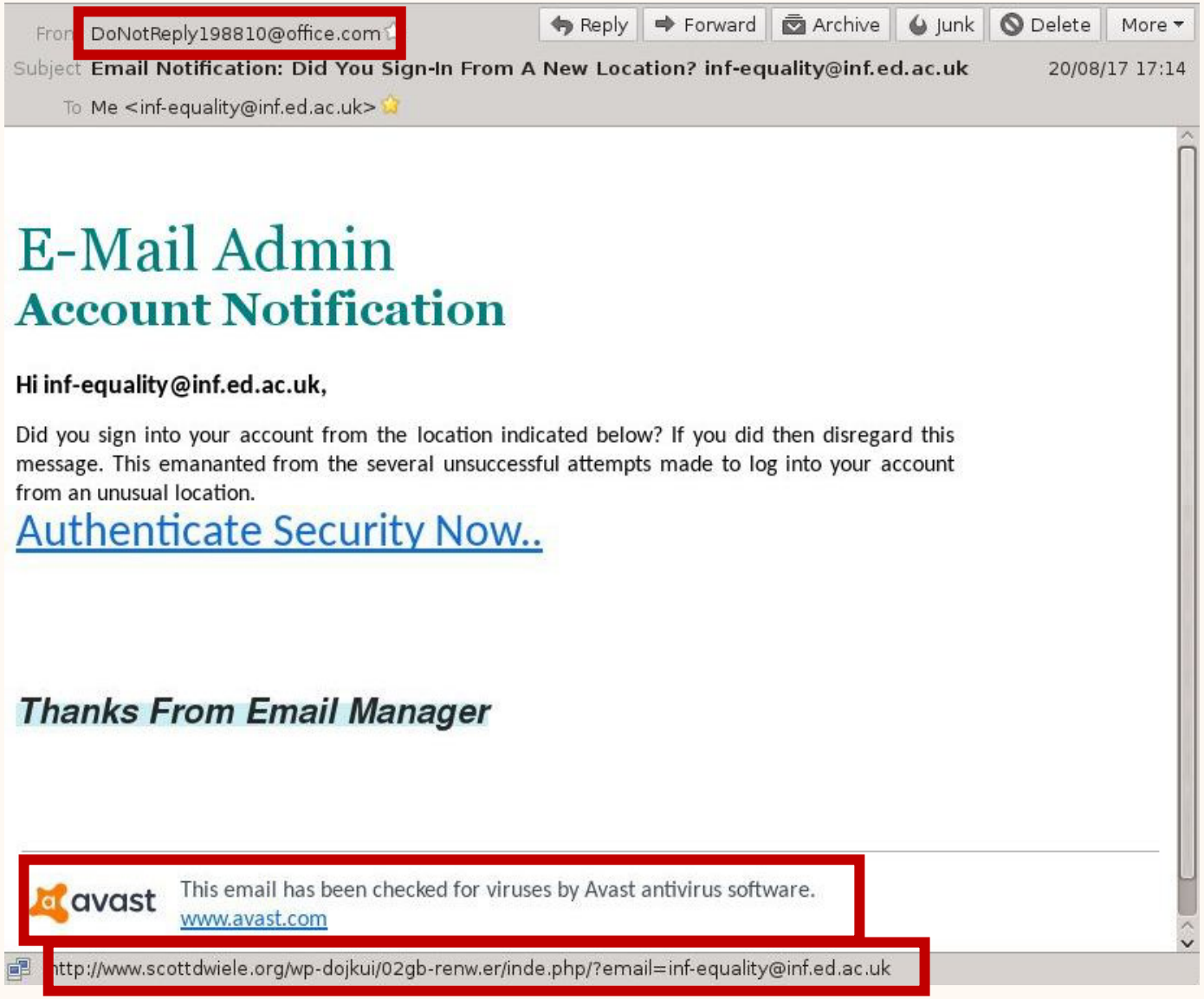


Multiple responses permitted

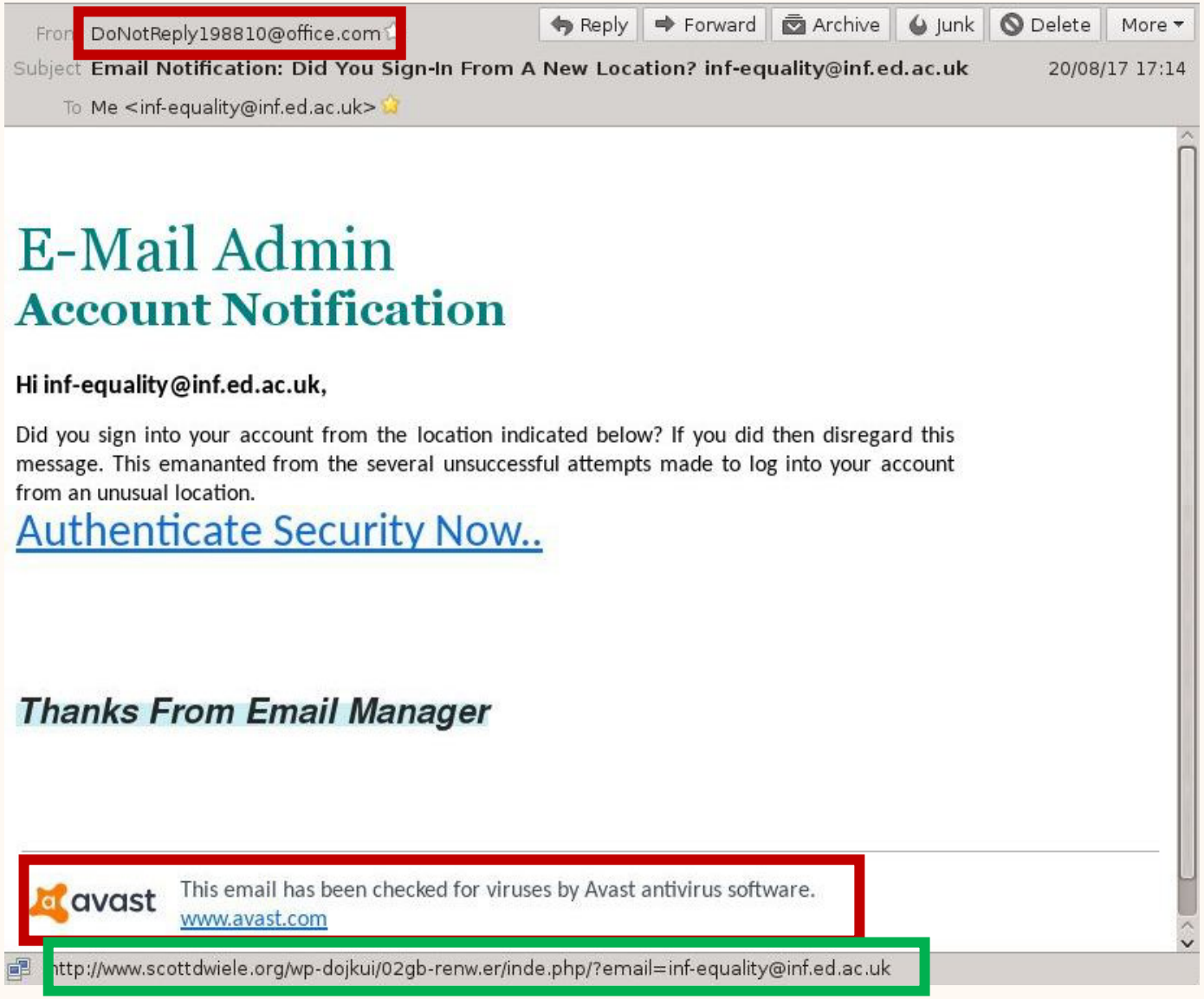
Proofpoint. State of the Phish 2019 Report. http://proofpoint.com/security-awareness

Email phishing

What on this email can be trusted when judging if it is legitimate or not?



What on this email can be trusted when judging if it is legitimate or not?



I asked my Computer Security class what info they were using to decide phishing or not phishing

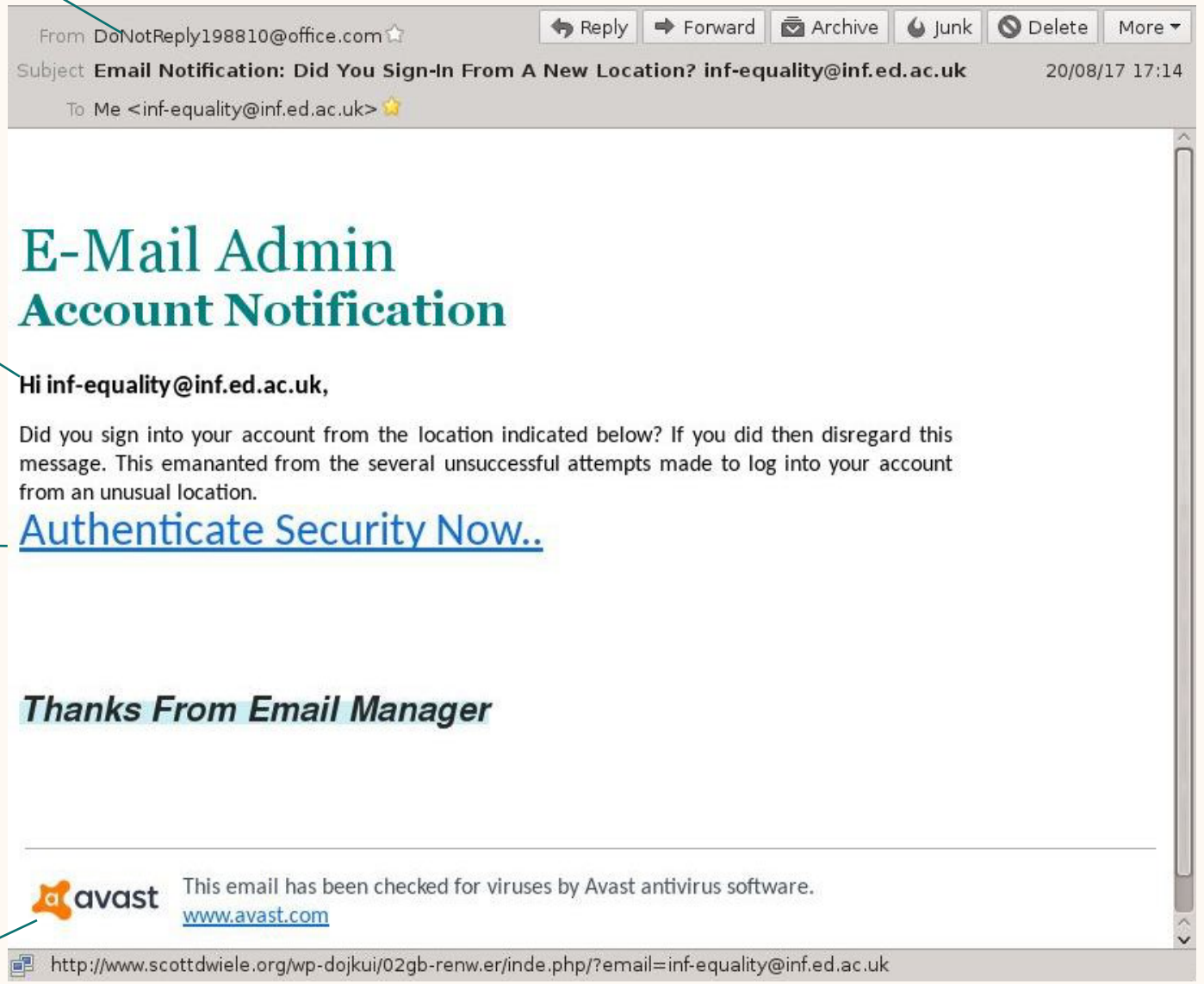
Lots of interesting I in this email

Email from “office.com” my email is through Office365

Uses my email address as a way of saying that it knows who I am and therefore can be trusted

Clearly explains what it wants the user to do. “Explained” and “Actionable” from SPRUCE

Appeal to authority by using a well known anti-virus name and claiming it has already been checked for viruses

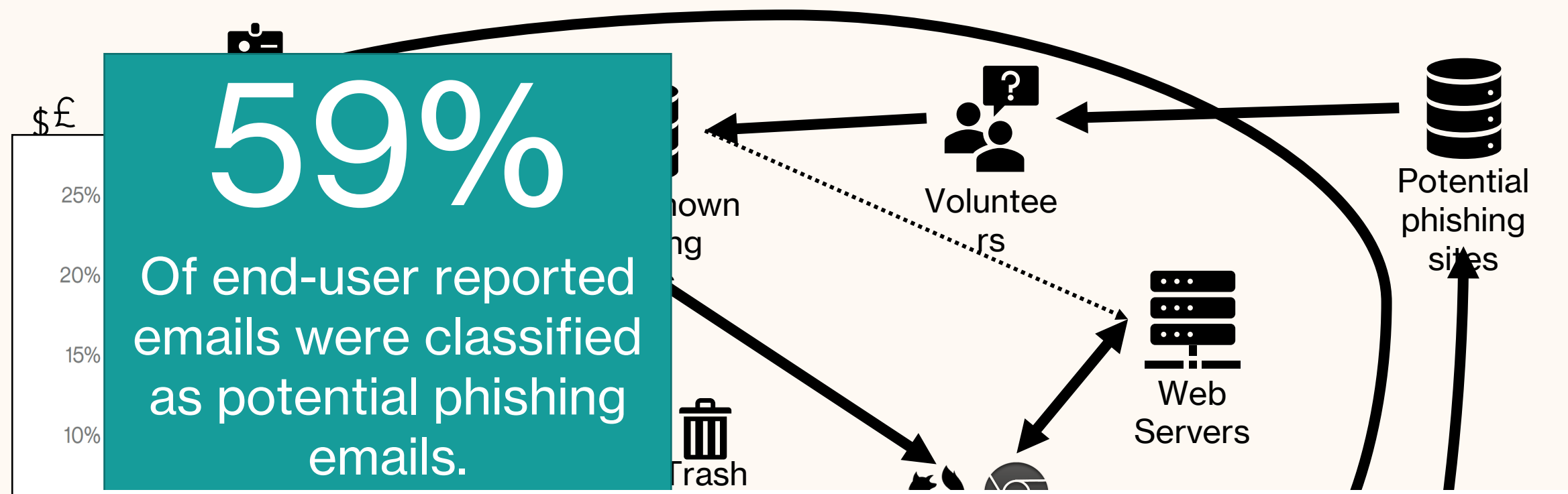


Common phishing elements

- **Automated** – Typically directed against many people.
- **Impersonation** – Communication claims to be from someone trusted or that they are not. For example, from a bank.
- **Direction to a website** – Links that look like they go somewhere legitimate but in fact go somewhere controlled by the attacker.
- **Contain an attachment** – Attachment asks for information to be sent back or contains malicious code.
- **Authentication info requested** – The communication aims to get authentication information.

59%

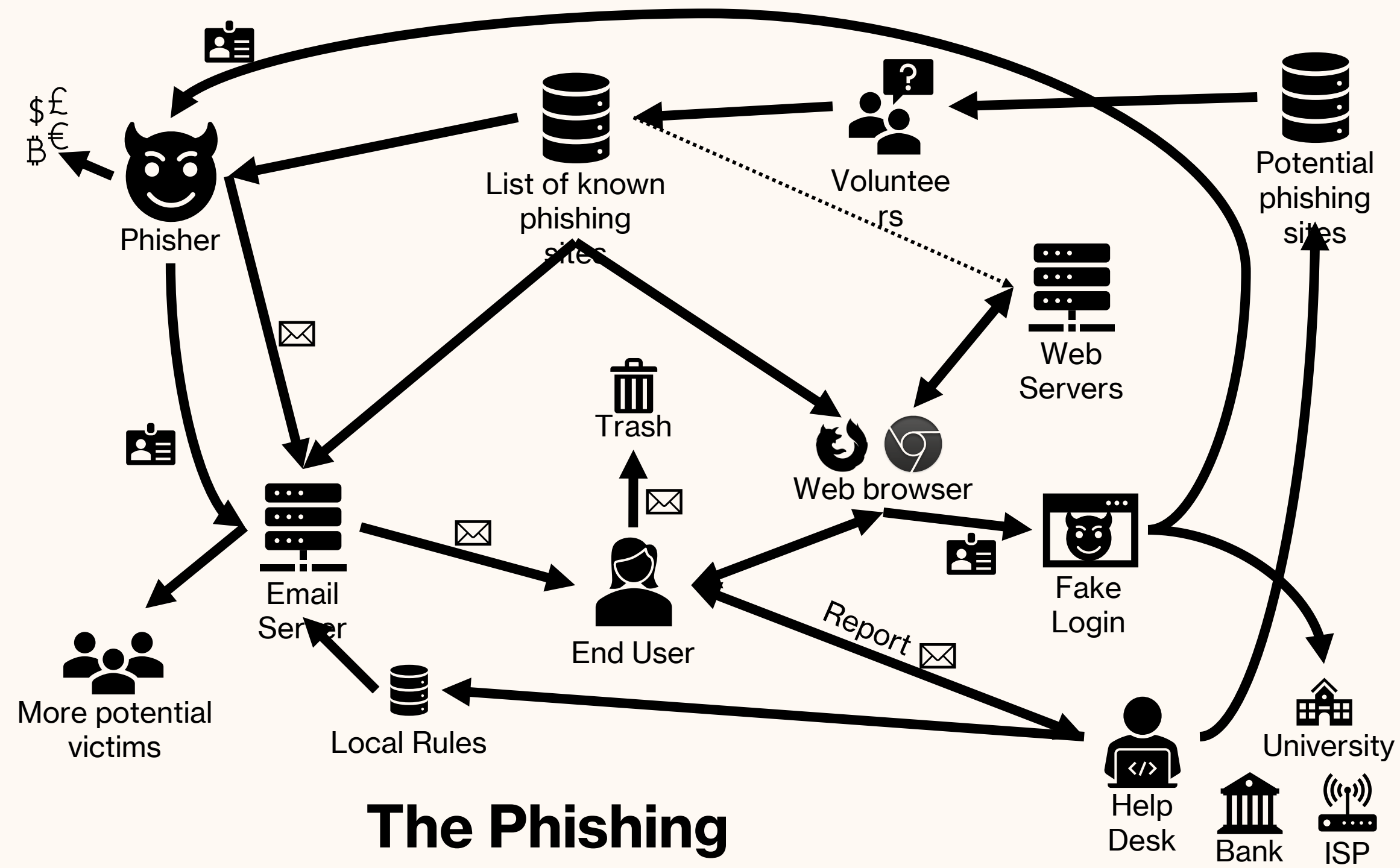
Of end-user reported emails were classified as potential phishing emails.



	April	May	June
Number of unique phishing Web sites detected	59,756	61,820	60,889
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	37,054	40,177	34,932
Number of brands targeted by phishing campaigns	341	308	289

APWG. Phishing Activity Trends Report, 2nd Quarter 2019.

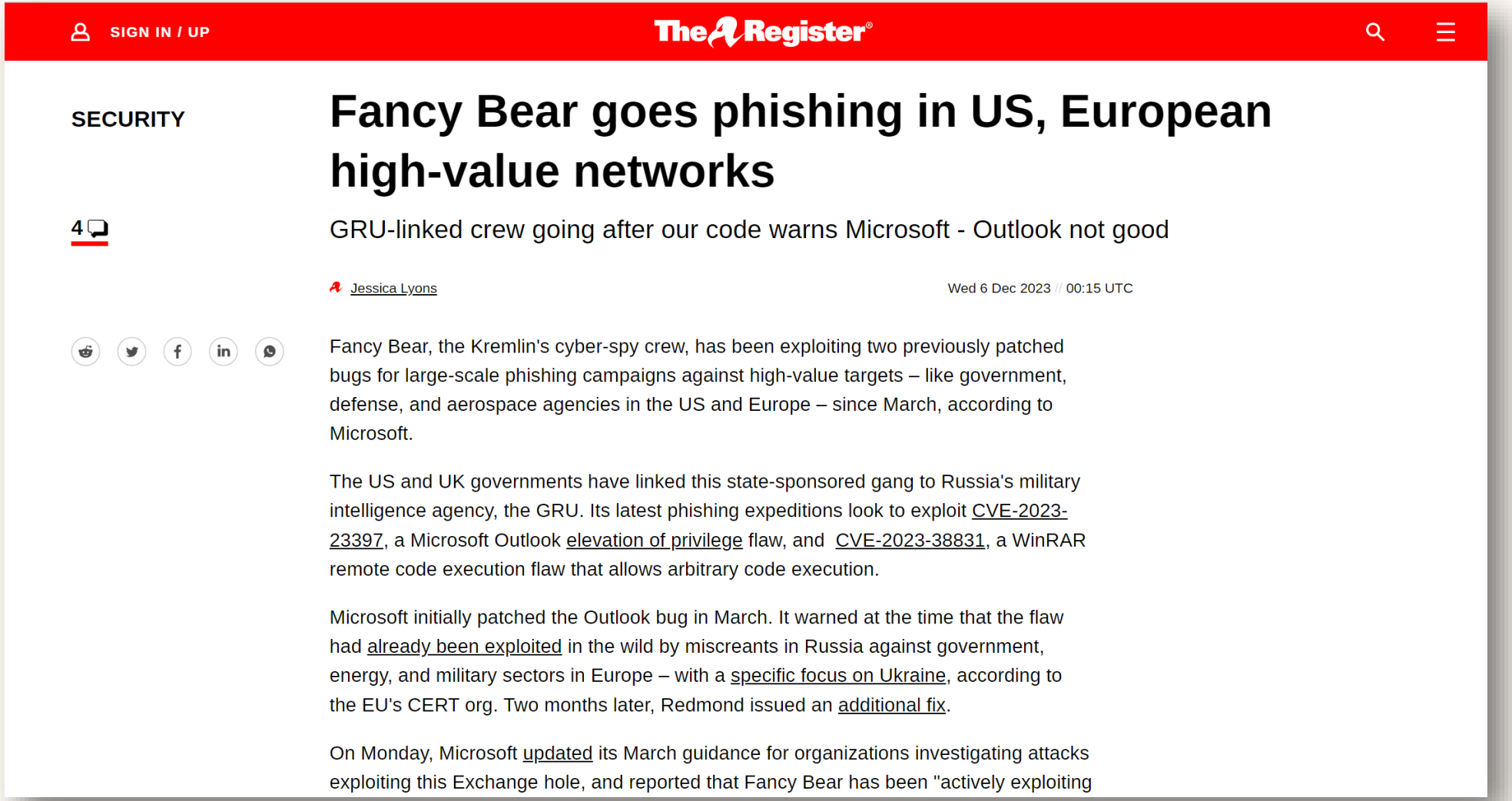
Desk Bank ISP



The Phishing

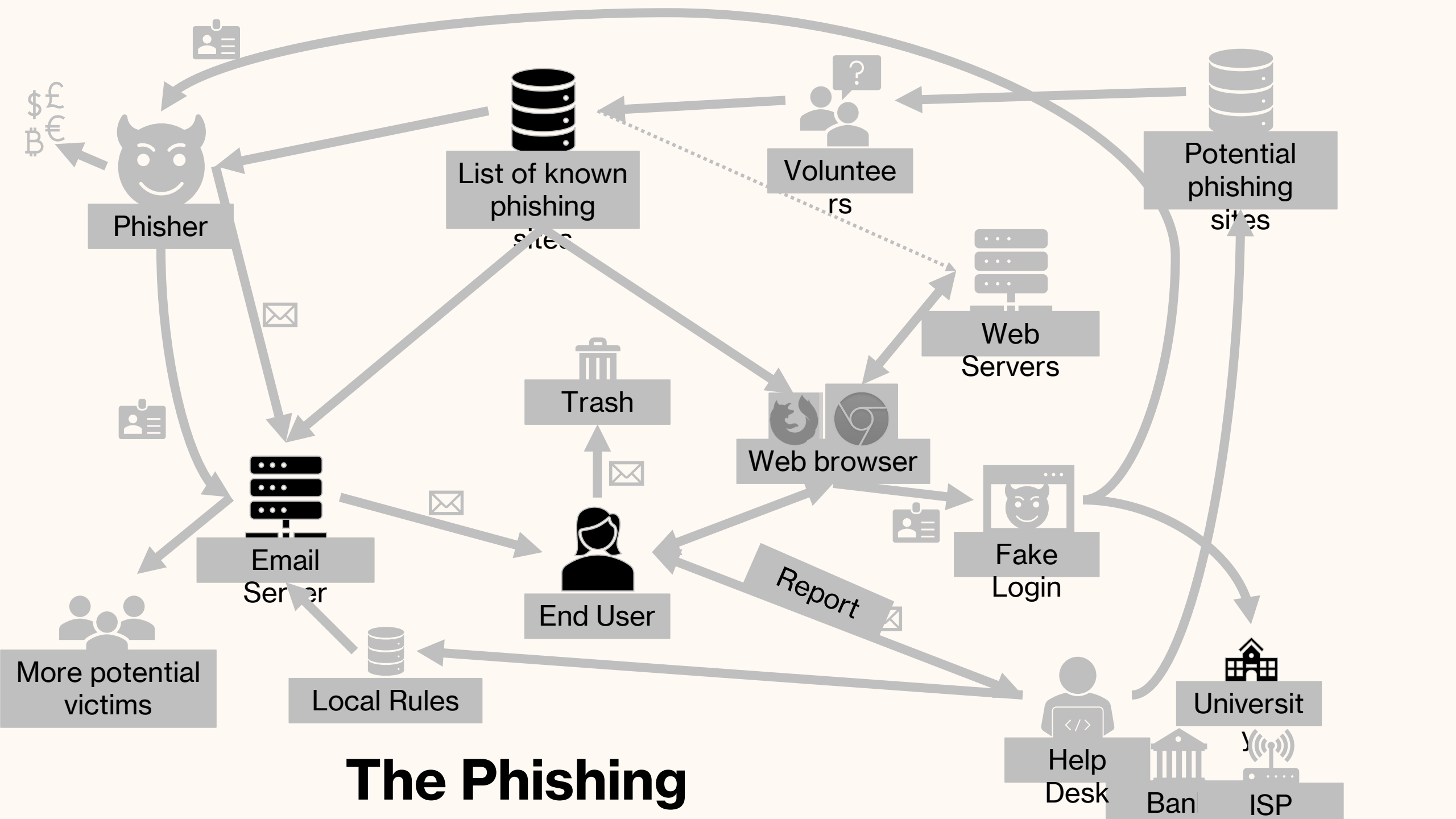
Who are the adversaries?

https://edition.cnn.com/2023/12/19/china/myanmar-conflict-china-scam-centers-analysis-intl-hnk/index.html



https://www.theregister.com/2023/12/06/fancy_bear_phishing_microsoft/

Solving phishing



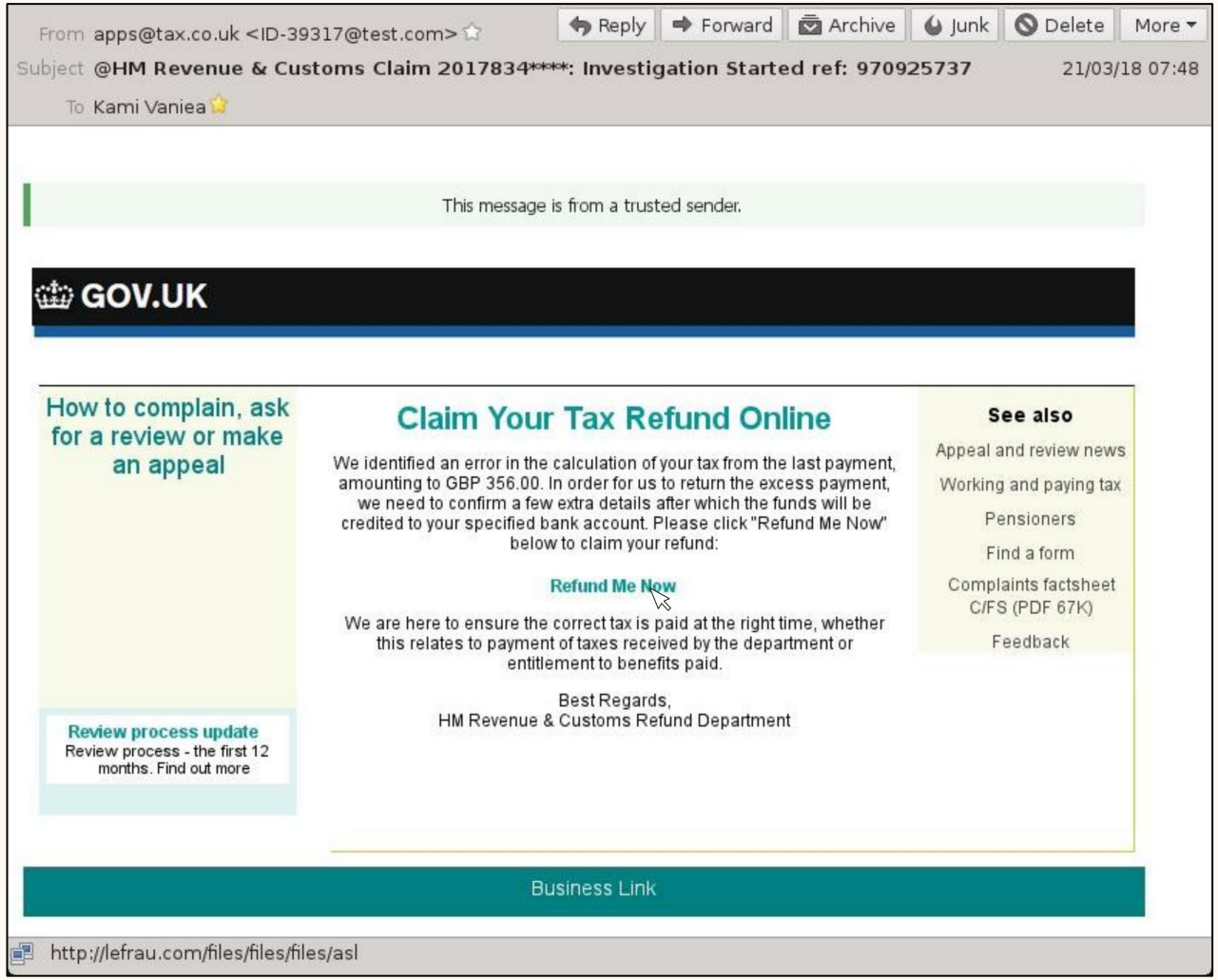
The Phishing

Main “solutions”

- **Automatically block attacks using filters**
  - Stop email from even arriving in inboxes
  - Block people from visiting known bad websites
- **Train users**
  - Provide users with training on how to identify phishing attacks
- **Support users**
  - Show UI indicators to help users tell the difference between real and fake sites
    - Also known as “passive indicators”, like the lock icon
  - Provide feedback when phishing is reported or blocked
- **Improve protection of authentication credentials**
  - Make it harder to impossible for a user to give away credentials
  - Limit the damage of credential sharing to one transaction

Automation

- Automatically scan all incoming emails for features
  - Attachments for malware
  - URLs for links to phishing pages
  - Spoofed from addresses from highly targeted companies (Paypal)
- Low tolerance for errors
- Low delay also important



Features for phishing URL detection

Feature Category	Feature Subcategory	Most popular feature	Use of the features			Criteria		
			Automated	*Human education*	*Human support*	*Time*	*Storage*	*Dependency*
Lexical	Domain	Domain	Low	High	High	Low	Low	No
	Other URL components	Authentication	High	Mid	Low	Low	Low	No
	Special Characters	Number of dots	High	Low	Low	Low	Low	No
	Length	Length of URL	High	NA	NA	Low	Low	No
	Numeric Representation	Raw IP address	High	High	Mid	Low	Low	No
	Tokens & Keywords	Phishing keywords	High	Low	NA	Mid	Mid	No
	Deviated domains	Similarity with PhishTank	High	High	High	Mid	Mid	No
	Embedded URL		Low	NA	Low	Low	Low	Maybe
Host	Whois	Domain age	Mid	NA	Low	Mid	Low	Yes
	DNS	No records	Mid	NA	NA	Mid	Low	Yes
	Connection	Connection speed	Mid	NA	NA	Mid	Low	Yes
Rank	Domain Popularity	Alexa Rank	High	NA	Low	Mid	Low	Yes
	PageRank	Google PageRank	High	NA	NA	Mid	Low	Yes
Redirection		No. of Redirections	Mid	NA	Low	Mid	Mid	No
Certificate	Encryption	Is it HTTPS?	High	Mid	Low	Low	Low	No
	Certificate values	Is EV?	Low	NA	Low	Low	Low	Maybe
Search Engines		Query the Full URL	Mid	High	Low	Mid	Low	Yes
Black/White lists	Simple List	PhishTank	High	NA	Mid	Low	Low	Yes
	Proactive List	Blacklisting the IP	Mid	NA	Low	Mid	High	Yes

Kholoud Althobaiti, Ghaidaa Rummani, and Kami Vaniea. A Review of Human- and Computer-Facing URL Phishing Features. In the European Workshop on Usable Security (EuroUSEC), June 2019.

Automation + Encryption

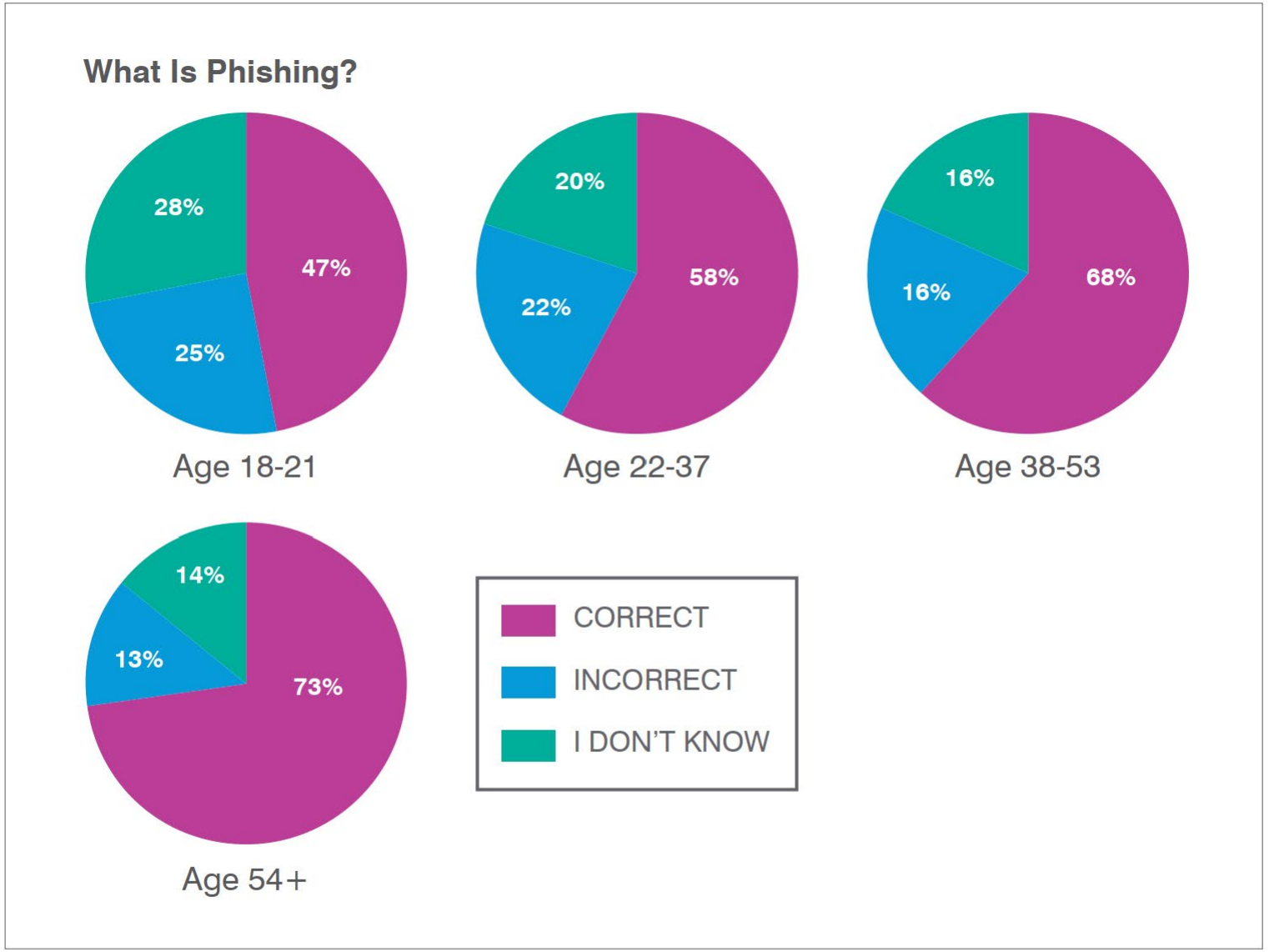
- “Going dark” due to encryption isn’t just a problem for law enforcement.
- Encryption also makes scanning for phishing more challenging.
- Do users know that their more private WhatsApp chats may have more dangerous content than in web browsers or emails?

Main “solutions”

- **Automatically block attacks using filters**
  - Stop email from even arriving in inboxes
  - Block people from visiting known bad websites
- **Train users**
  - Provide users with training on how to identify phishing attacks
- **Support users**
  - Show UI indicators to help users tell the difference between real and fake sites
    - Also known as “passive indicators”, like the lock icon
  - Provide feedback when phishing is reported or blocked
- **Improve protection of authentication credentials**
  - Make it harder to impossible for a user to give away credentials
  - Limit the damage of credential sharing to one transaction

The older generation is surprisingly aware of phishing as compared to younger people.

The difference is likely due to life experience with fraud.



Note: According to Pew Research, millennials fell into the 22-37 age bracket and baby boomers were 54 and older in 2018.

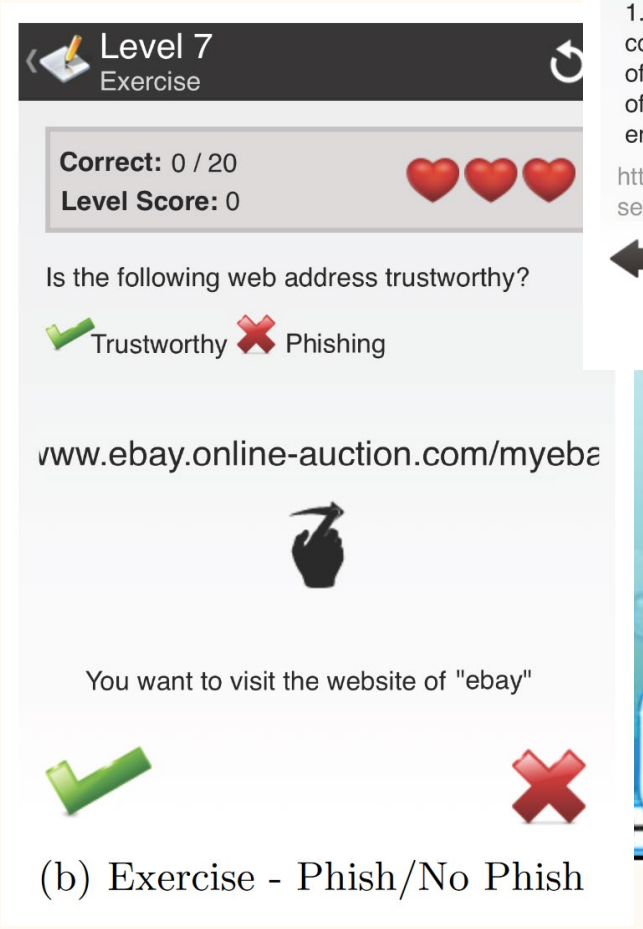
Proofpoint. State of the Phish 2019 Report. http://proofpoint.com/security-awareness

Training users

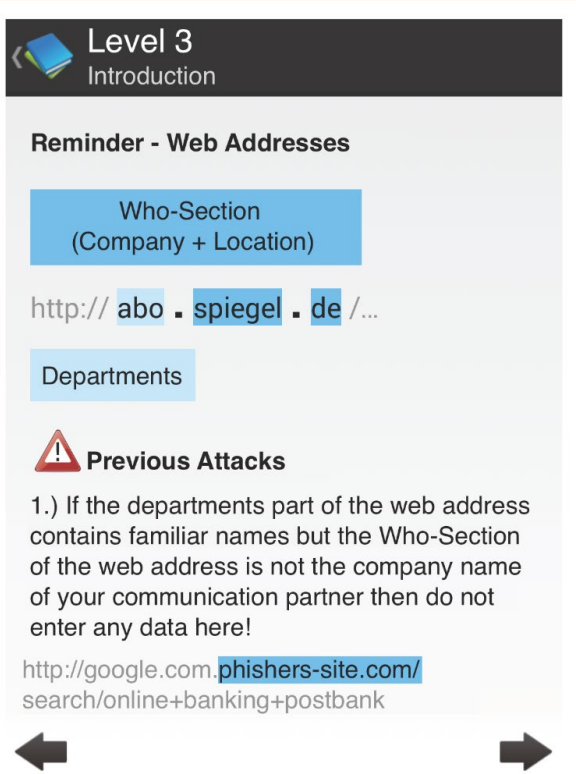
- Up-front training
  - Games
  - Advice web pages
  - Training videos
- Embedded training
  - Information provided in websites
  - Feedback given by help desk to phishing reports
- Evaluate impact of training
  - Send out fake phishing emails to test staff
  - Measure reporting behaviors

NoPhish anti-phishing training app

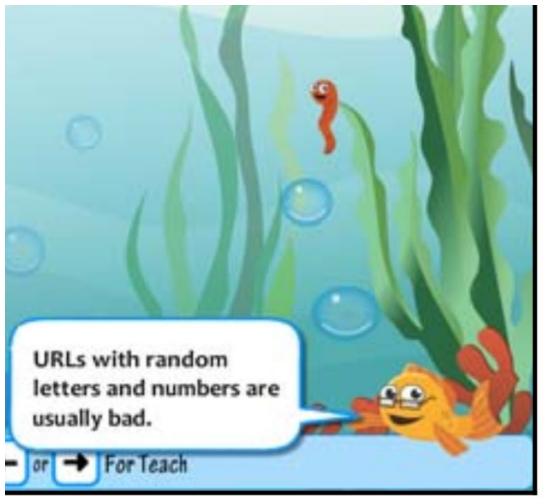
Anti-Phishing



(b) Exercise - Phish/No Phish



(a) Reminder



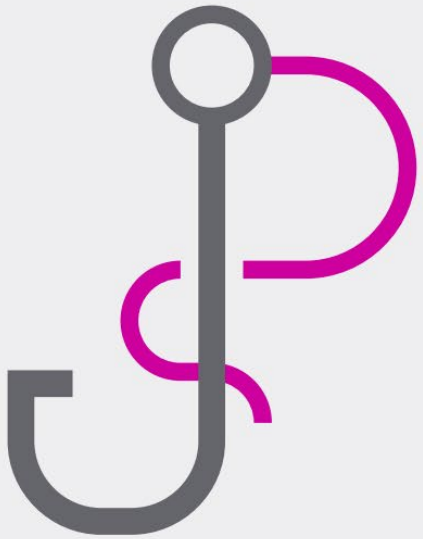
Who want to/is responsible to train users?

Local Government Association

What is phishing?

WHAT ARE THE MOST 'SUCCESSFUL' PHISHING CAMPAIGNS?

As we all know, some phishing tests are trickier than others. Here are some of the subject lines that **garnered the highest failure rates** among end users for campaigns that were sent to a minimum of 1,500 recipients:



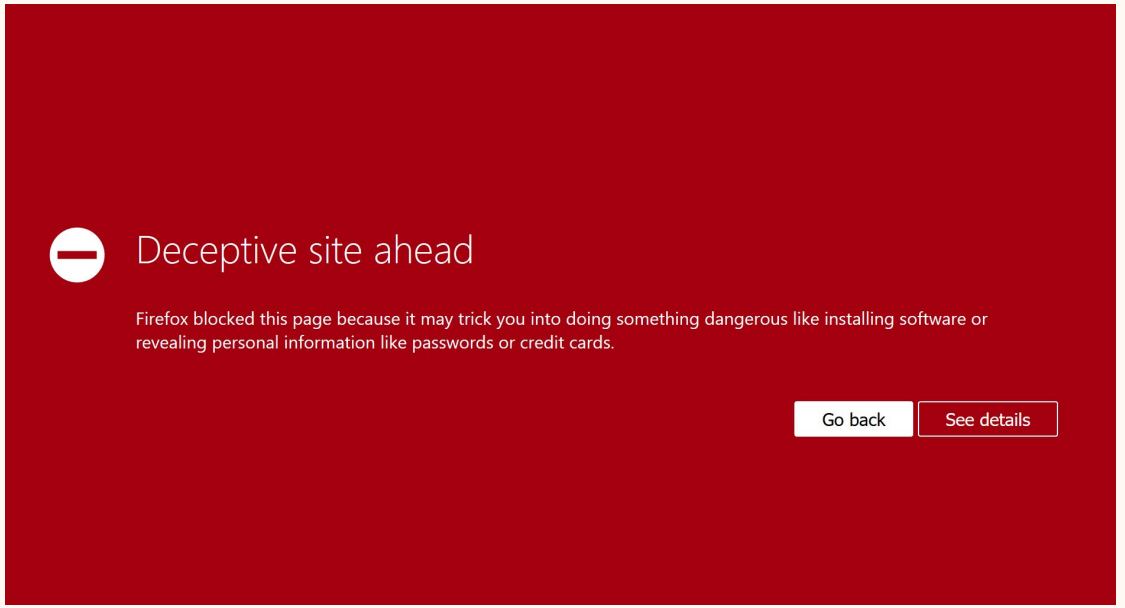
- Toll Violation Notification
- [EXTERNAL]: Your Unclaimed Property
- Updated Building Evacuation Plan (also among the highest failure rates in 2017)
- Invoice Payment Required
- February 2018 – Updated Org Chart
- Urgent Attention (a notification requesting an email password change)

Proofpoint. State of the Phish 2019 Report. http://proofpoint.com/security-awareness

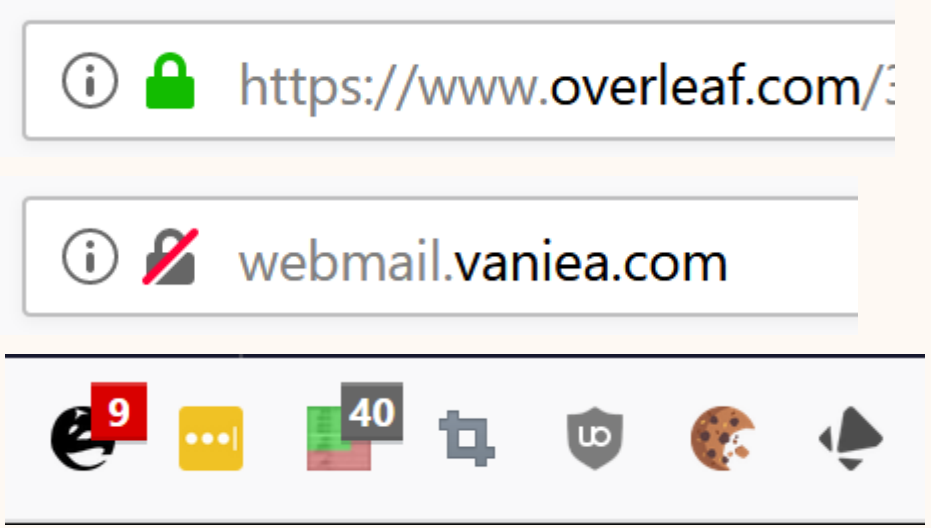
Managing phishing

- Block people from visiting sites
  - Browser blocks sites automatically
  - ISPs take down sites
- Provide indicators to help people differentiate between intended and malicious websites
  - Lock icon
  - Plugins with feedback
  - Show only the URL domain to reduce confusion
  - Stating what email server sent an email

Active Warning



Passive Warnings



A well designed phishing site fools 90% of people. Security cues in the browser are not seen, ignored, or not understood.

Why Phishing Works

Rachna Dhamija
rachna@deas.harvard.edu
Harvard University

J. D. Tygar
tygar@berkeley.edu
UC Berkeley

Marti Hearst
hearst@sims.berkeley.edu
UC Berkeley

ABSTRACT

To build systems shielding users from fraudulent (or *phishing*) websites, designers need to know which attack strategies work and why. This paper provides the first empirical evidence about which malicious strategies are successful at deceiving general users. We first analyzed a large set of captured phishing attacks and developed a set of hypotheses about why these strategies might work. We then assessed these hypotheses with a usability study in which 22 participants were shown 20 web sites and asked to determine which ones were fraudulent. We found that 23% of the participants did not look at browser-based cues such as the address bar, status bar and the security indicators, leading to incorrect choices 40% of the time. We also found that some visual deception attacks can fool even the most sophisticated users. These results illustrate that standard security indicators are not effective for a substantial fraction of users, and suggest that alternative approaches are needed.

Author Keywords

Security Usability, Phishing.

ACM Classification Keywords

H.1.2 [User/Machine Systems]: Software psychology; K.4.4 [Electronic Commerce]: Security.

INTRODUCTION

What makes a web site credible? This question has been addressed extensively by researchers in computer-human interaction. This paper examines a twist on this question: what makes a *bogus* website credible? In the last two years, Internet users have seen the rapid expansion of a scourge on the Internet: *phishing*, the practice of directing users to fraudulent web sites. This question raises fascinating questions for user interface designers, because both phishers and anti-phishers do battle in user interface space. Successful phishers must not only present a high-credibility web presence to their victims; they must create a presence that is so impressive that it causes the victim to fail to recognize security measures installed in web browsers.

Data suggest that some phishing attacks have convinced up to 5% of their recipients to provide sensitive information to spoofed websites [21]. About two million users gave information to spoofed websites resulting in direct losses of $1.2 billion for U.S. banks and card issuers in 2003 [20].[1]

If we hope to design web browsers, websites, and other tools to shield users from such attacks, we need to understand which attack strategies are successful, and what proportion of users they fool. However, the literature is sparse on this topic.

This paper addresses the question of why phishing works. We analyzed a set of phishing attacks and developed a set

Why Phishing Works

Rachna Dhamija
rachna@deas.harvard.edu
Harvard University

J. D. Tygar
tygar@berkeley.edu
UC Berkeley

Marti Hearst
hearst@sims.berkeley.edu
UC Berkeley

to determine which ones were fraudulent. We found that 23% of the participants did not look at browser-based cues such as the address bar, status bar and the security indicators, leading to incorrect choices 40% of the time. We also found that some visual deception attacks can fool even the most sophisticated users. These results illustrate that standard security indicators are not effective for a substantial fraction of users, and suggest that alternative approaches are needed.

Acknowledgements: Dr. Dhamija is currently at the Center for

This paper addresses the question of why phishing works. We analyzed a set of phishing attacks and developed a set

Developers and admins are users too.

Provide help for those who are trying to counter phishing at their organizations.

A Joint Program of the APWG and Carnegie Mellon CUPS

How to Redirect a Phishing Site Web Page to the APWG.ORG Phishing Education Page

Important note to program participants: To verify any communication about the APWG/CMU Phishing Education Landing Page Program, please open a new browser &ndash do not click on any links in email or instant message - to go to the homepage of the APWG and click on the link for the redirect education initiative. This way you can be sure that the redirect you are creating is going to a legitimate APWG web page.

The APWG and Carnegie Mellon Cylab Usable Privacy and Security Laboratory (CUPS) are working to educate consumers on the perils of phishing and how to avoid them. As part of this initiative, we are requesting that instead of disabling phish sites, ISP, registrars, and other infrastructure entities put an HTTP redirect in place of the phishing page at the phishing URL. The redirect would send a user who has been tricked into visiting a phish site to go to the **Phishing Education Landing Page** at the "most teachable moment".

In addition, by including a parameter that is the URL of the website that was taken down, you will also help the APWG and CMU's Cylab Usable Privacy and Security Laboratory to track the success rates of the various phishing education campaigns. This is invaluable information and we appreciate your cooperation in including this parameter in the redirect URL. Your efforts can help educate consumers and enterprise computing users so that they can better protect themselves from electronic crime.

This page has information on how to implement a redirect to the education page.

Implementing a redirect in Apache

There are several ways to implement a redirect in Apache, but the following method is one of the simplest.

http://phish-education.apwg.org/r/how_to.h

Common phishing elements

- **Automated** – Typically directed against many people.
- **Impersonation** – Communication claims to be from someone trusted or that they are not. For example, from a bank.
- **Direction to a website** – Links that look like they go somewhere legitimate but in fact go somewhere controlled by the attacker.
- **Contain an attachment** – Attachment asks for information to be sent back or contains malicious code.
- **Authentication info requested** – The communication aims to get authentication information.

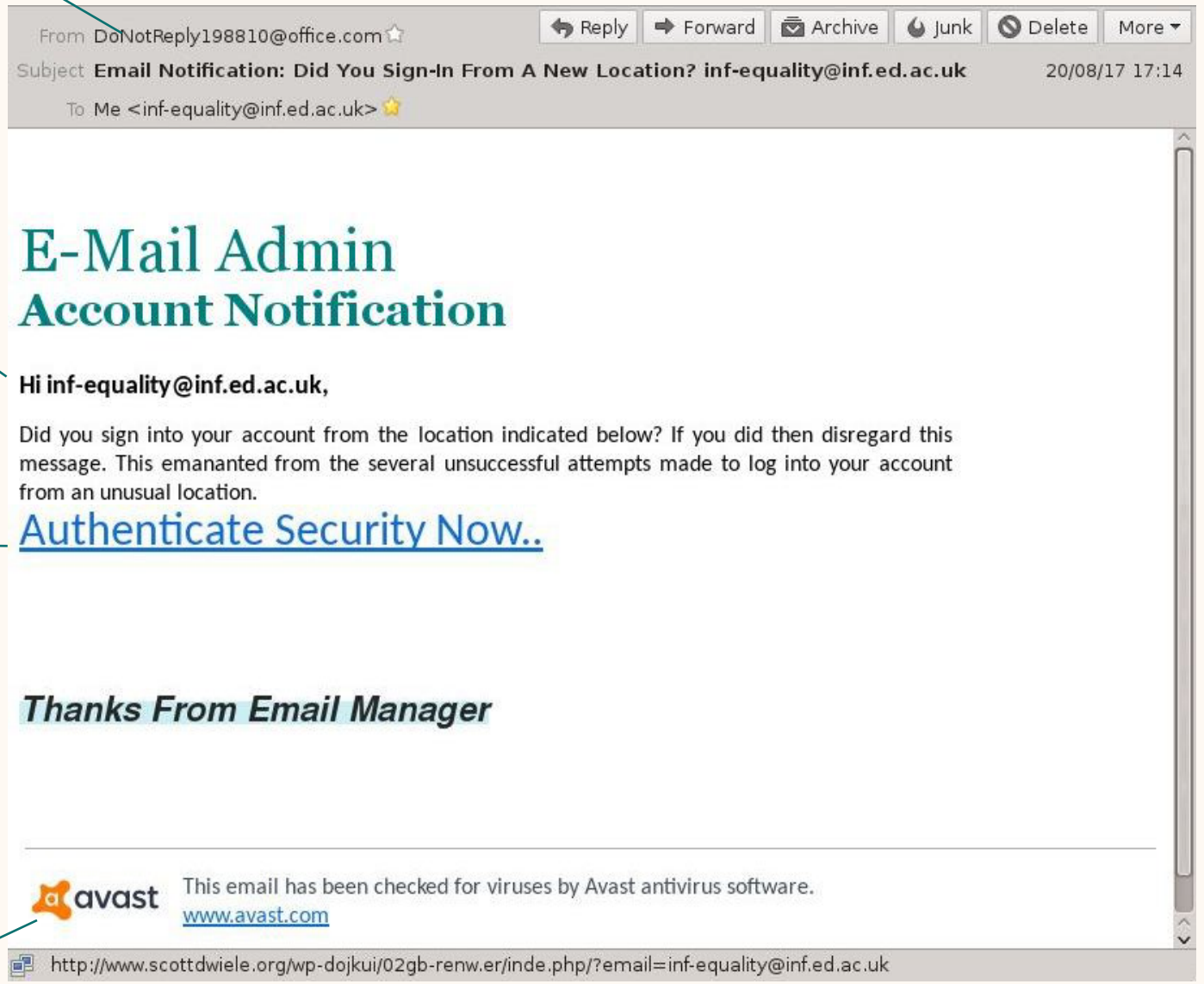
Lots of interesting I in this emai

Email from “office.com” my email is through Office365

Uses my email address as a way of saying that it knows who I am and therefore can be trusted

Clearly explains what it wants the user to do. “Explained” and “Actionable” from SPRUCE

Appeal to authority by using a well known anti-virus name and claiming it has already been checked for viruses



Questions

Take-home

- **(Blog)** Althobaiti, K., Meng, N. and Vaniea, K., 2021, May. I don't need an expert! Making URL phishing features human comprehensible. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-17).
- **(Blog)** CNBC - Generative AI financial scammers are getting very good at duping work email