Phishing and Fraud

INFR11158/11230 Usable Security and Privacy

Dr. Jingjie Li

04/03/2024

THE UNIVERSITY of EDINBURGH

Overview

- Warm up and reminder

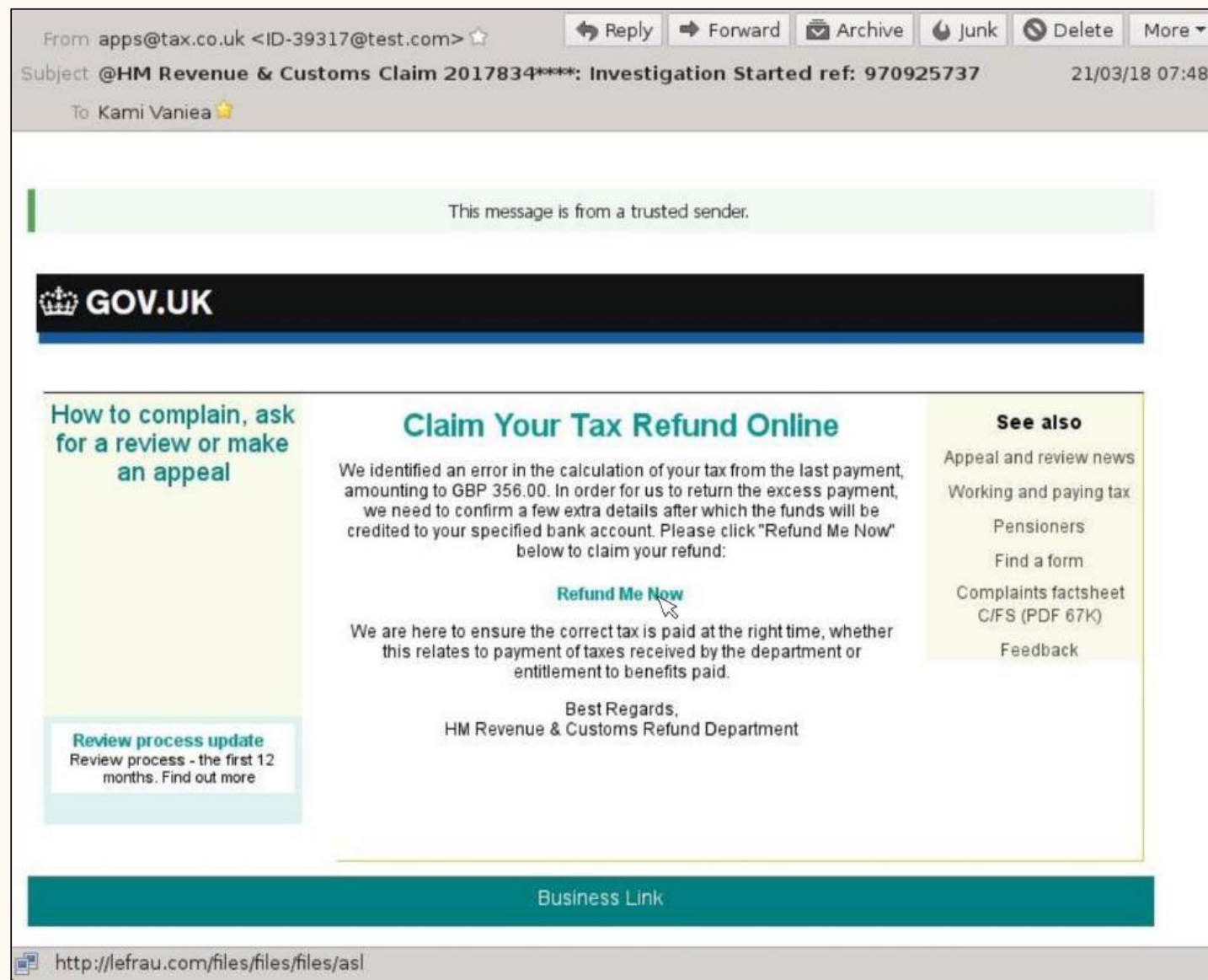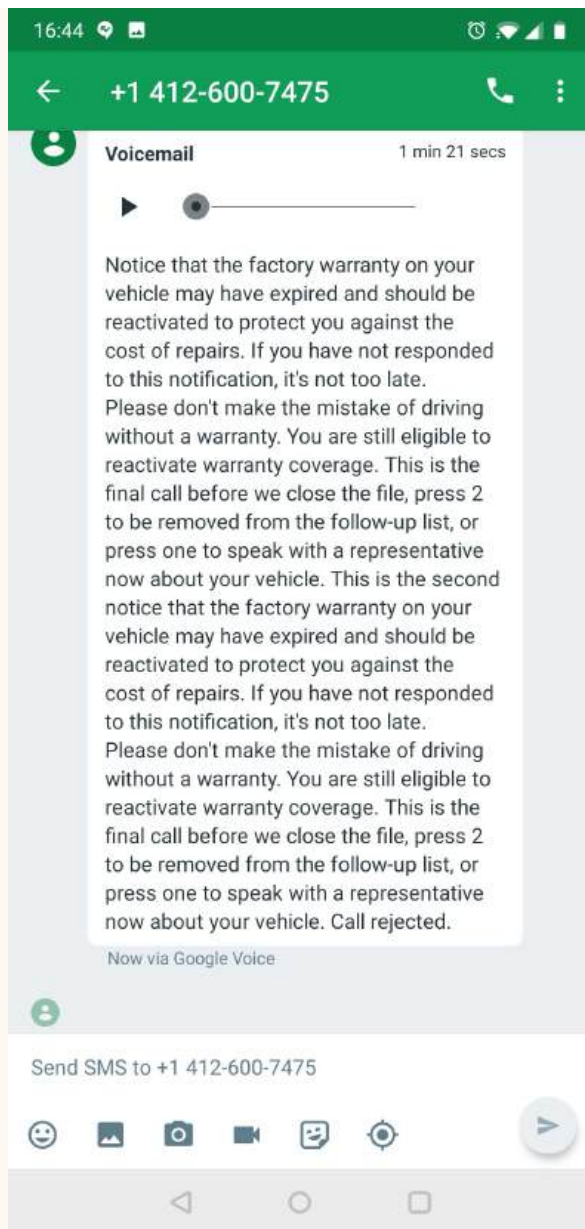- Phishing: overview, elements, and countermeasures

- Fraud overview

- Take-home
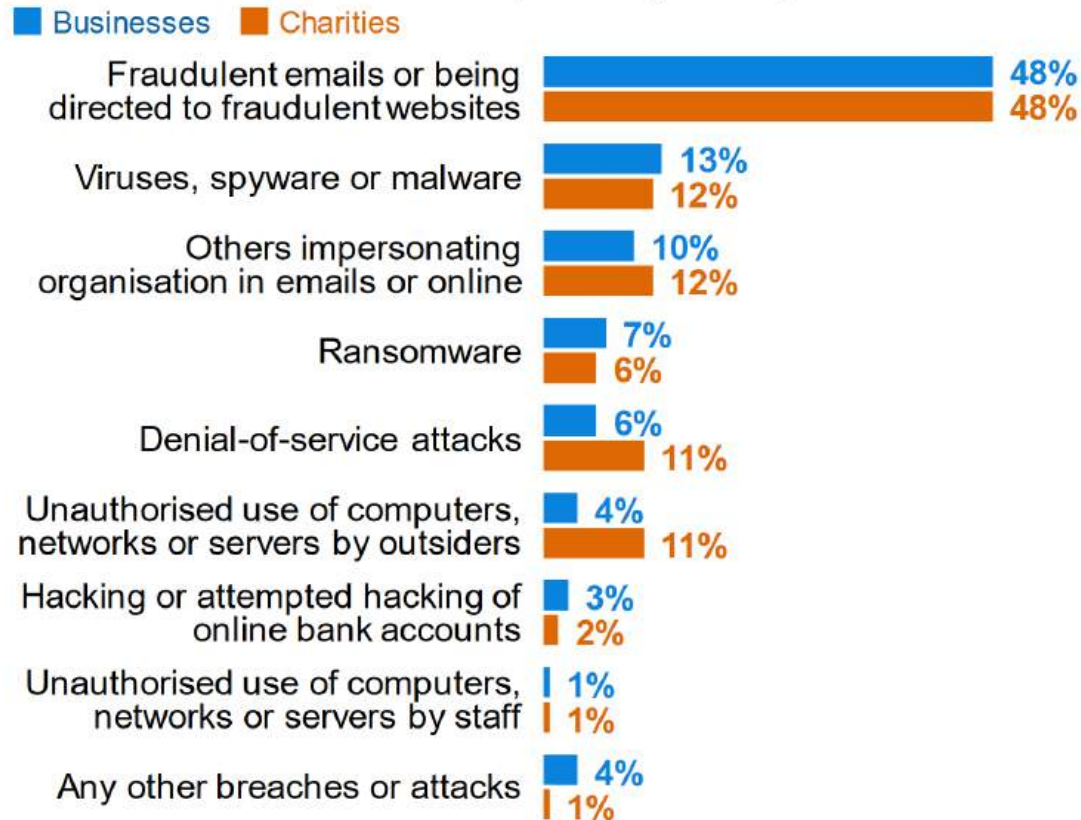
Overview

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)

Left panel (SMS/Voicemail)

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

Right panel (Email)

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

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

Review process update
Review process - the first 12 months. Find out more

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?**

■ Businesses ■ Charities

Type	Businesses	Charities
Fraudulent emails or being directed to fraudulent websites	48%	48%
Viruses, spyware or malware	13%	12%
Others impersonating organisation in emails or online	10%	12%
Ransomware	7%	6%
Denial-of-service attacks	6%	11%
Unauthorised use of computers, networks or servers by outsiders	4%	11%
Hacking or attempted hacking of online bank accounts	3%	2%
Unauthorised use of computers, networks or servers by staff	1%	1%
Any other breaches or attacks	4%	1%

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.

71% of breaches were financially motivated

25% of breaches were motivated by the gain of strategic advantage (espionage)

32% of breaches involved phishing

29% of breaches involved use of stolen credentials

56% of breaches took months or longer to discover

0% 20% 40% 60% 80% 100%

Breaches

Figure 5. What are other commonalities?

Verizon. 2019 Data Breach Investigation Report. p5

Phishing Impacts Experienced*

*Multiple responses permitted

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
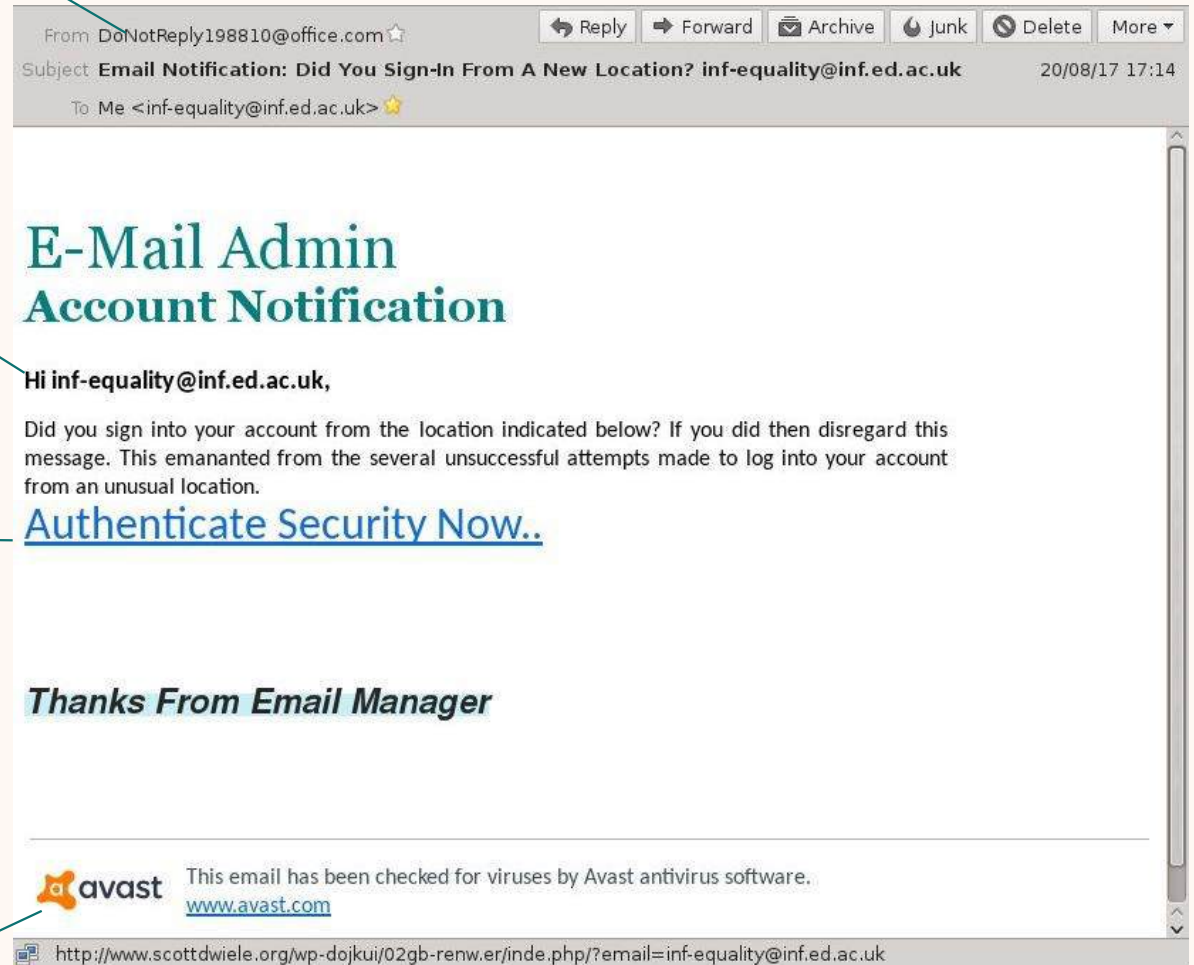
Lots of interesting [things] in this email

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

---

From DoNotReply198810@office.com ☆   ↩ Reply   ➡ Forward   🗄 Archive   🔥 Junk   🚫 Delete   More ▼

Subject **Email Notification: Did You Sign-In From A New Location? inf-equality@inf.ed.ac.uk**   20/08/17 17:14

To Me <inf-equality@inf.ed.ac.uk> ⭐

E-Mail Admin
Account Notification

Hi inf-equality@inf.ed.ac.uk,

Did you sign into your account from the location indicated below? If you did then disregard this message. This emanated from the several unsuccessful attempts made to log into your account from an unusual location.

Authenticate Security Now..

Thanks From Email Manager

🅰 **avast**   This email has been checked for viruses by Avast antivirus software.
www.avast.com

🖳 http://www.scottdwiele.org/wp-dojkui/02gb-renw.er/inde.php/?email=inf-equality@inf.ed.ac.uk

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%

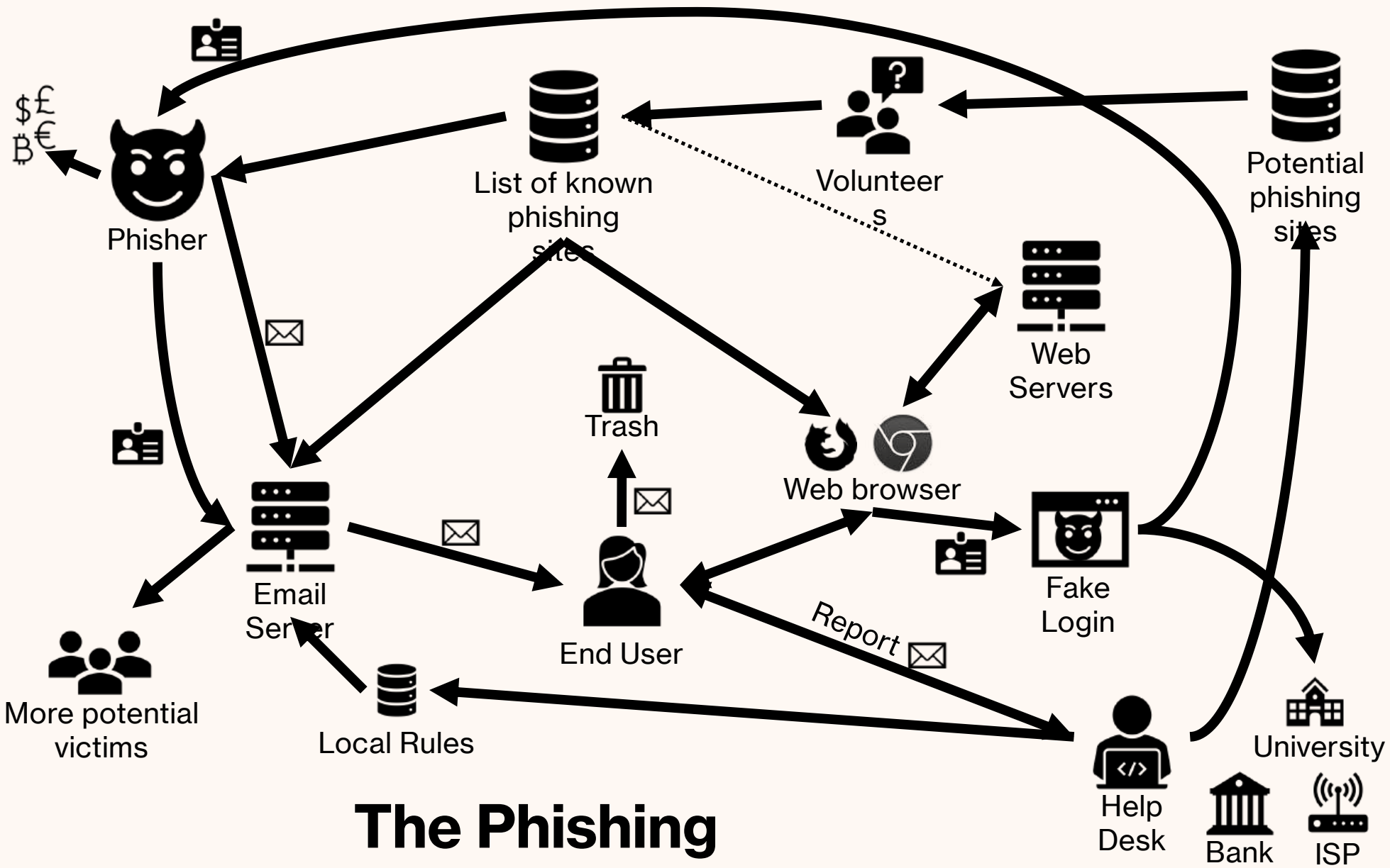Of end-user reported emails were classified as potential phishing emails.

Volunteers

Potential phishing sites

Web Servers

Trash
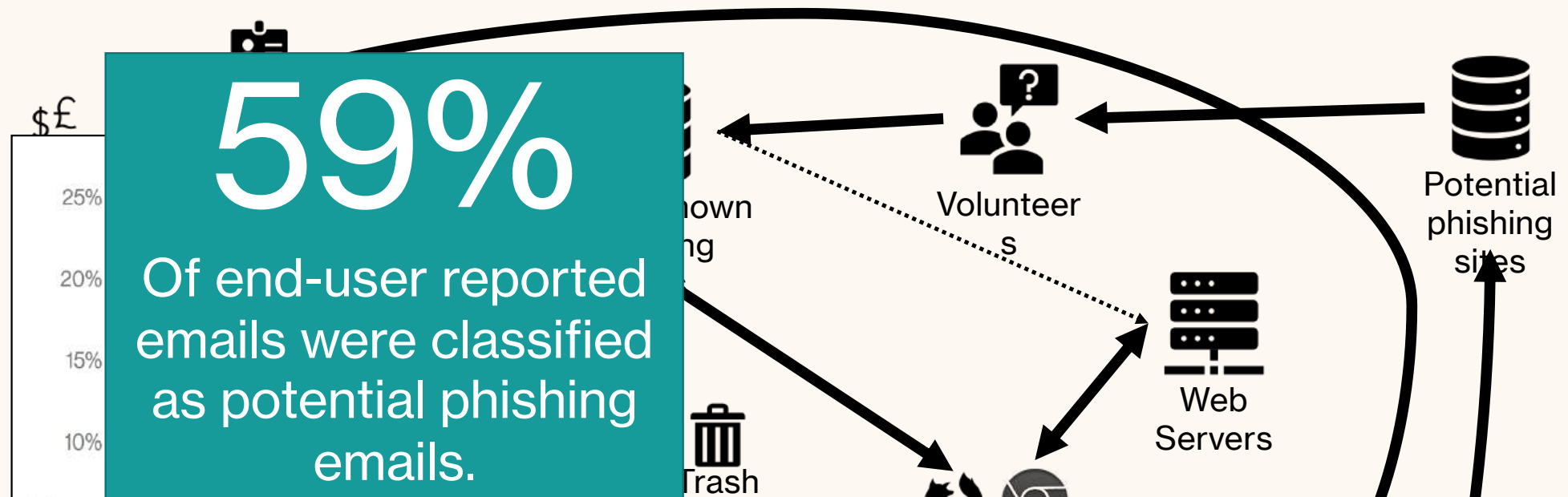
Clicked

	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

Desk   Bank   ISP

The Phishing

$ £ € ฿

Phisher

List of known phishing sites

Volunteers

Potential phishing sites

Web Servers

Trash

Web browser

Fake Login

Email Server

End User

More potential victims

Local Rules

Report

Help Desk

University

Bank

ISP

Who are the adversaries?

The Register

SECURITY

Fancy Bear goes phishing in US, European high-value networks

4 💬

GRU-linked crew going after our code warns Microsoft - Outlook not good

Jessica Lyons   Wed 6 Dec 2023 | 00:15 UTC

Fancy Bear, the Kremlin's cyber-spy crew, has been exploiting two previously patched bugs for large-scale phishing campaigns against high-value targets – like government, defense, and aerospace agencies in the US and Europe – since March, according to Microsoft.
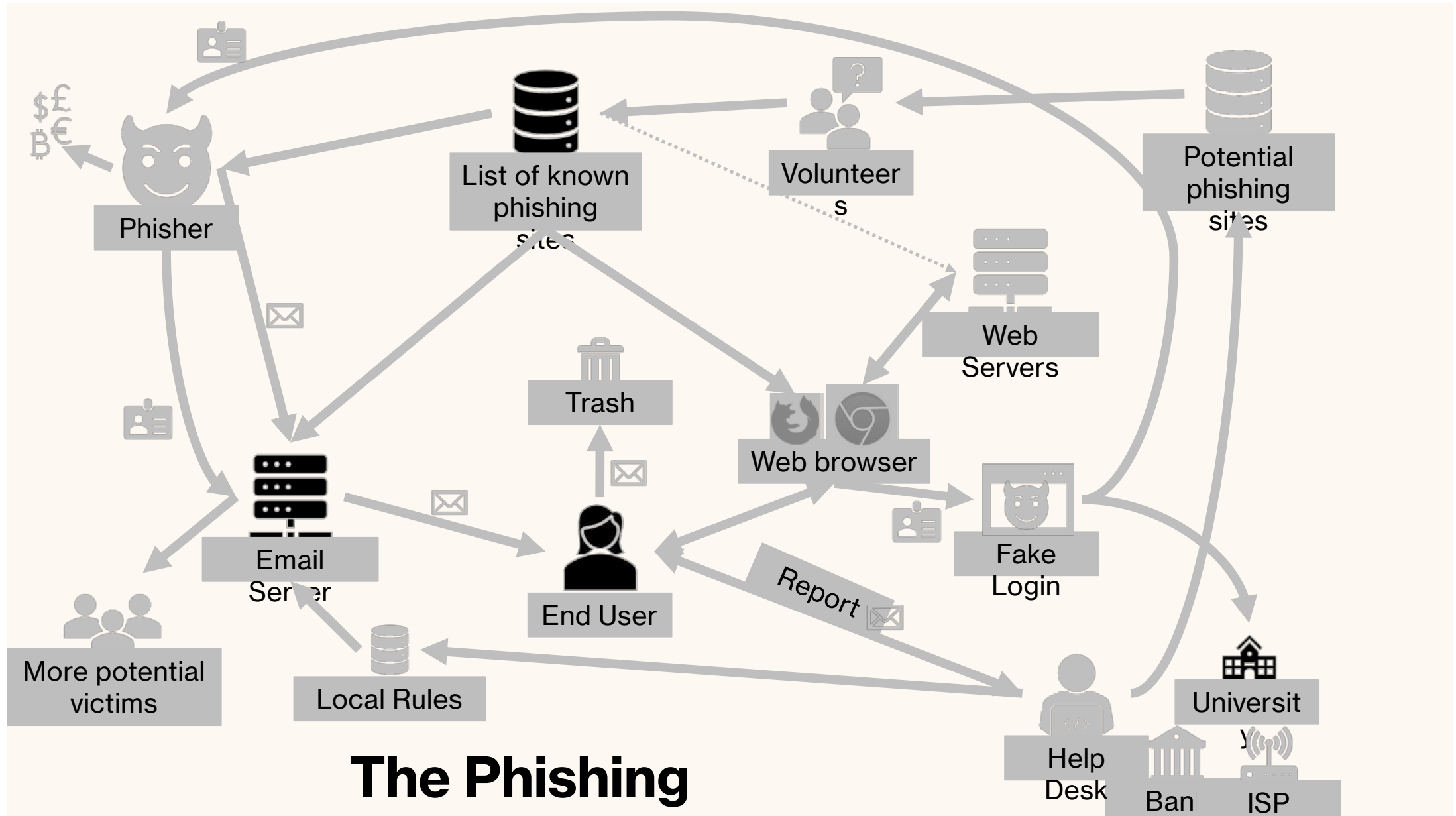
The US and UK governments have linked this state-sponsored gang to Russia's military intelligence agency, the GRU. Its latest phishing expeditions look to exploit CVE-2023-23397, a Microsoft Outlook elevation of privilege flaw, and CVE-2023-38831, a WinRAR remote code execution flaw that allows arbitrary code execution.

Microsoft initially patched the Outlook bug in March. It warned at the time that the flaw had already been exploited in the wild by miscreants in Russia against government, energy, and military sectors in Europe – with a specific focus on Ukraine, according to the EU's CERT org. Two months later, Redmond issued an additional fix.

On Monday, Microsoft updated its March guidance for organizations investigating attacks exploiting this Exchange hole, and reported that Fancy Bear has been "actively exploiting

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

19

Solving phishing

The Phishing

Phisher

List of known phishing sites

Volunteers

Potential phishing sites

Web Servers

Trash

Web browser

Email Server

End User

Report

Fake Login

More potential victims

Local Rules

Help Desk

University

Ban

ISP

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
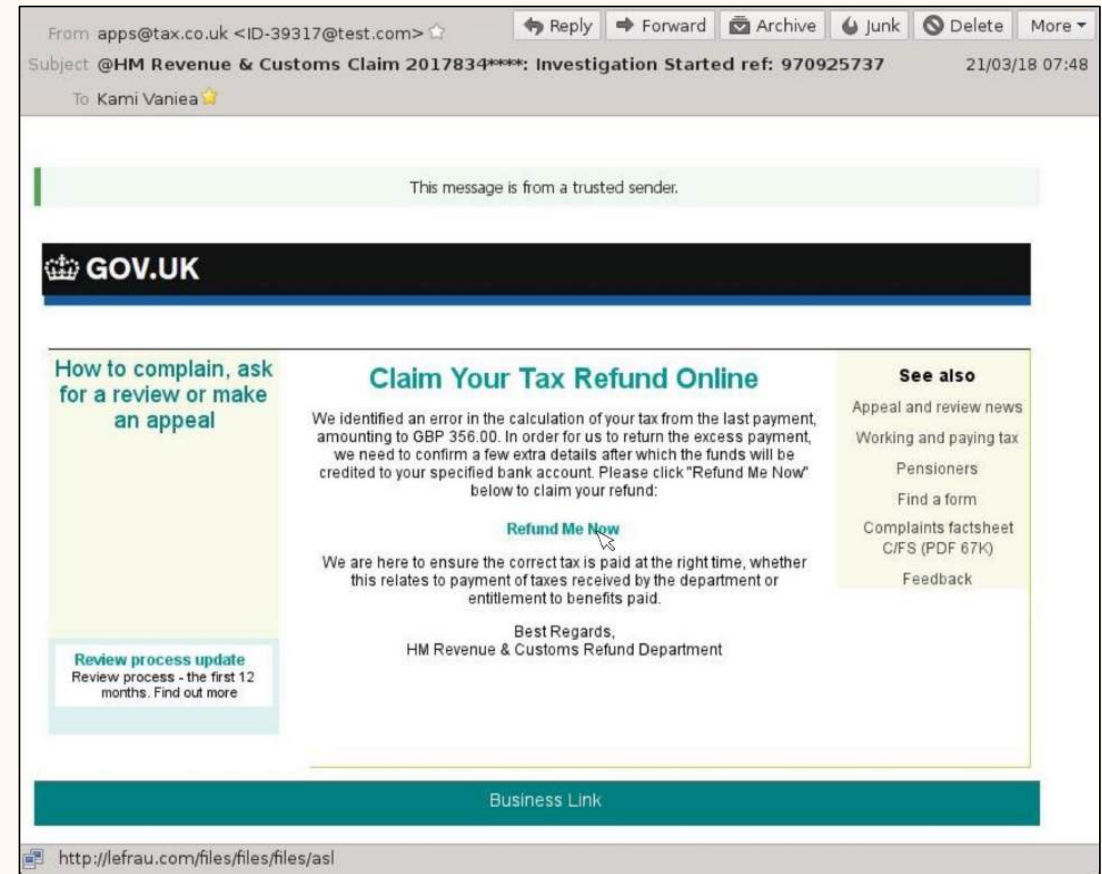
Features for phishing URL detection

Feature Category	Feature Subcategory	Most popular feature	Use of the features		Human support	Time	Storage	Dependency
			Automated	*Human education*				
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.
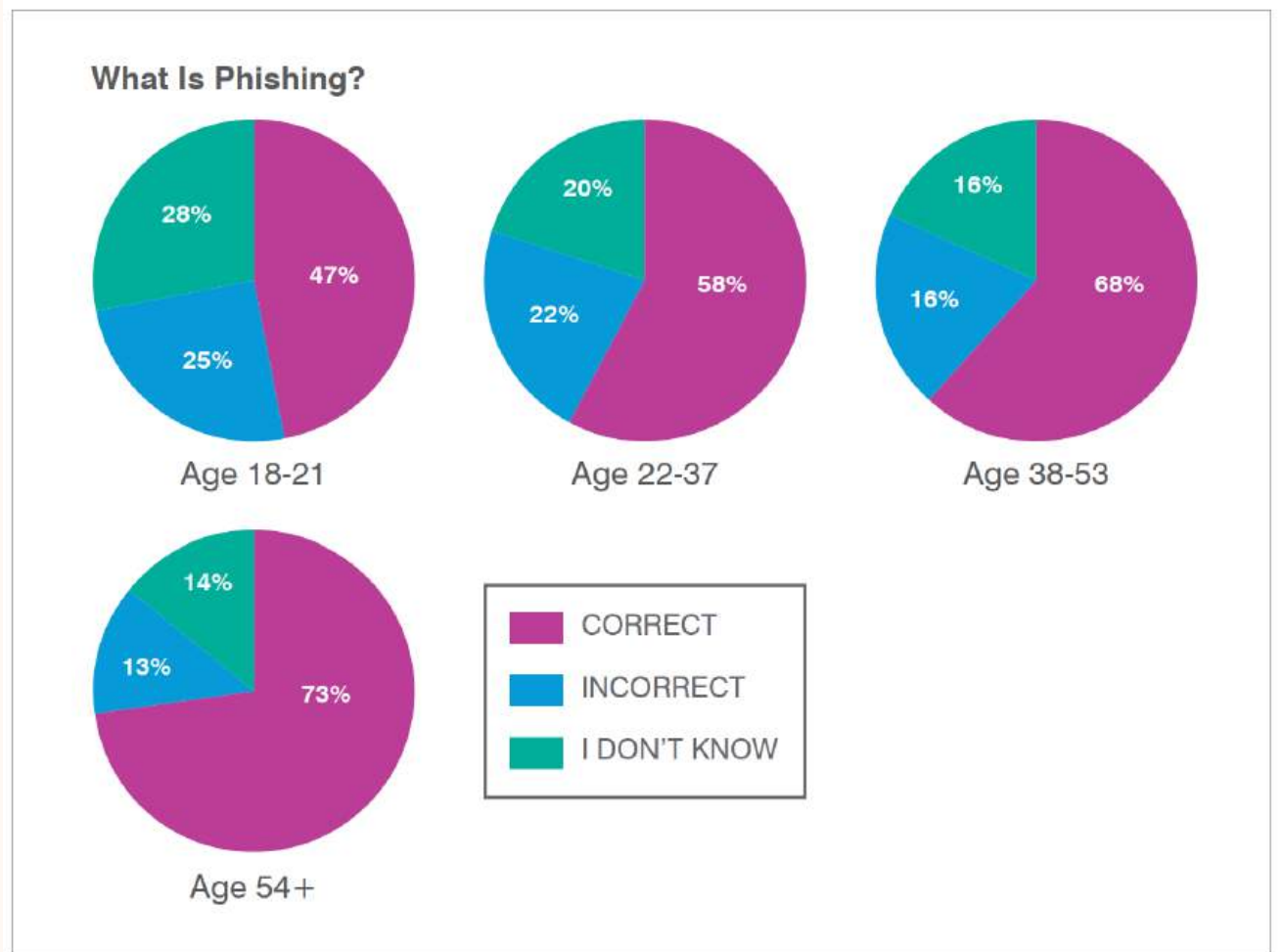
Automation + Encryption

- "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?

25

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.

What Is Phishing?

Age 18-21 — 47% / 25% / 28%

Age 22-37 — 58% / 22% / 20%

Age 38-53 — 68% / 16% / 16%

Age 54+ — 73% / 13% / 14%

CORRECT
INCORRECT
I DON'T KNOW

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

Training users

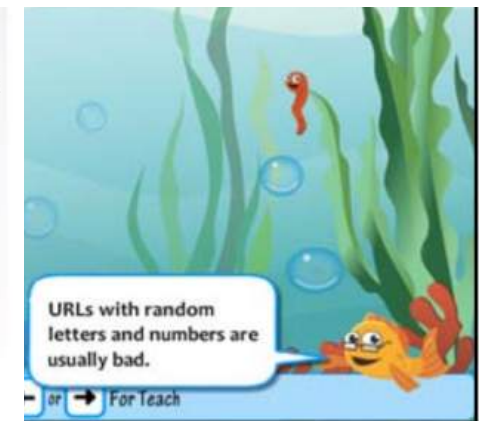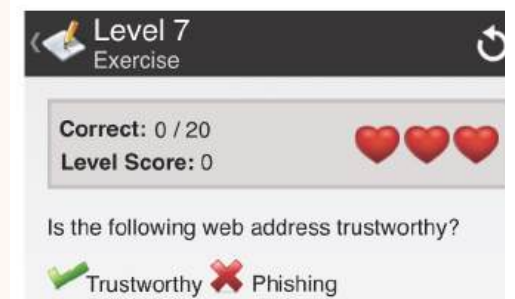- Up-front training
  - Games
  - Advice web pages
  - Training videos
- Embedded training
  - Information provided in websites
  - Feedback given by help desk to phishing reports
- Evaluate impact of training
  - Send out fake phishing emails to test staff
  - Measure reporting behaviors

NoPhish anti-phishing training app

Anti-Phishing

Level 7
Exercise

Correct: 0 / 20
Level Score: 0

Is the following web address trustworthy?

✔ Trustworthy   ✘ Phishing

vww.ebay.online-auction.com/myeba

You want to visit the website of "ebay"

(b) Exercise - Phish/No Phish

Level 3
Introduction

Reminder - Web Addresses

Who-Section
(Company + Location)

http:// abo . spiegel . de /...

Departments

⚠ Previous Attacks

1.) If the departments part of the web address contains familiar names but the Who-Section of the web address is not the company name of your communication partner then do not enter any data here!

http://google.com.phishers-site.com/search/online+banking+postbank

(a) Reminder

URLs with random letters and numbers are usually bad.

Who want to/is responsible to train users?

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)

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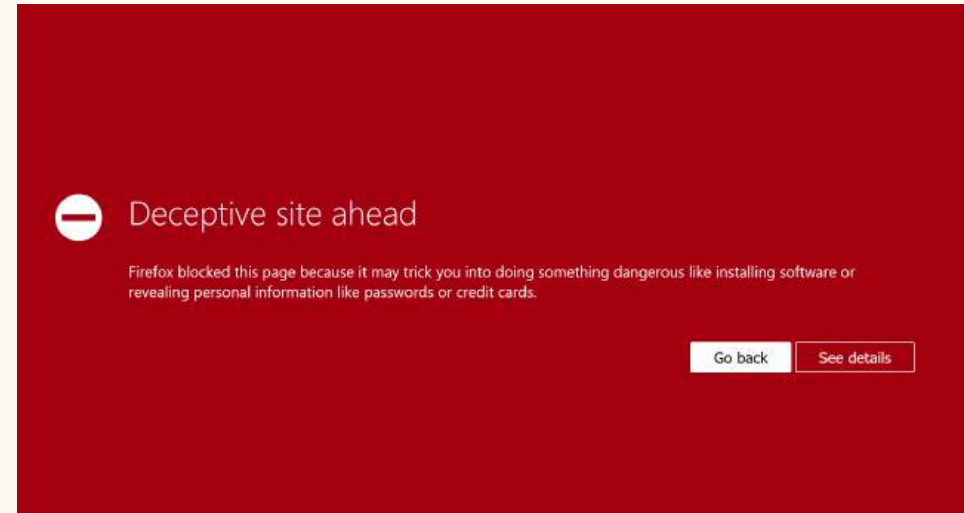
Passive Warnings
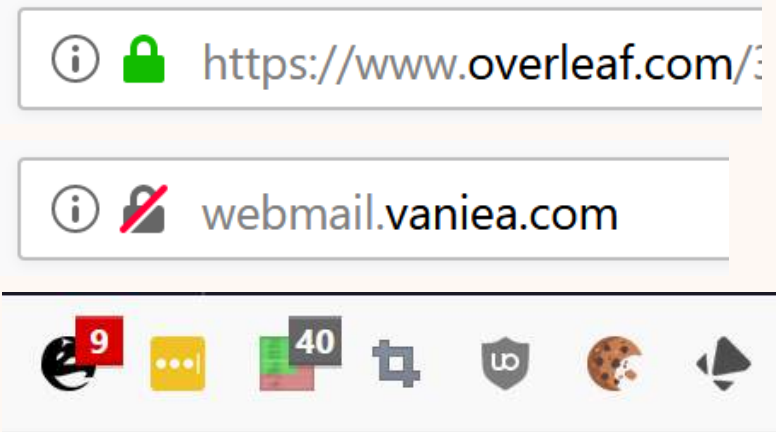
A well designed phishing site fools 90% of people. Security cues in the browser are not seen, ignored, or not understood.

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.

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.

APWG

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 – 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.

APWG
Public Education Initiative

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

35

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.
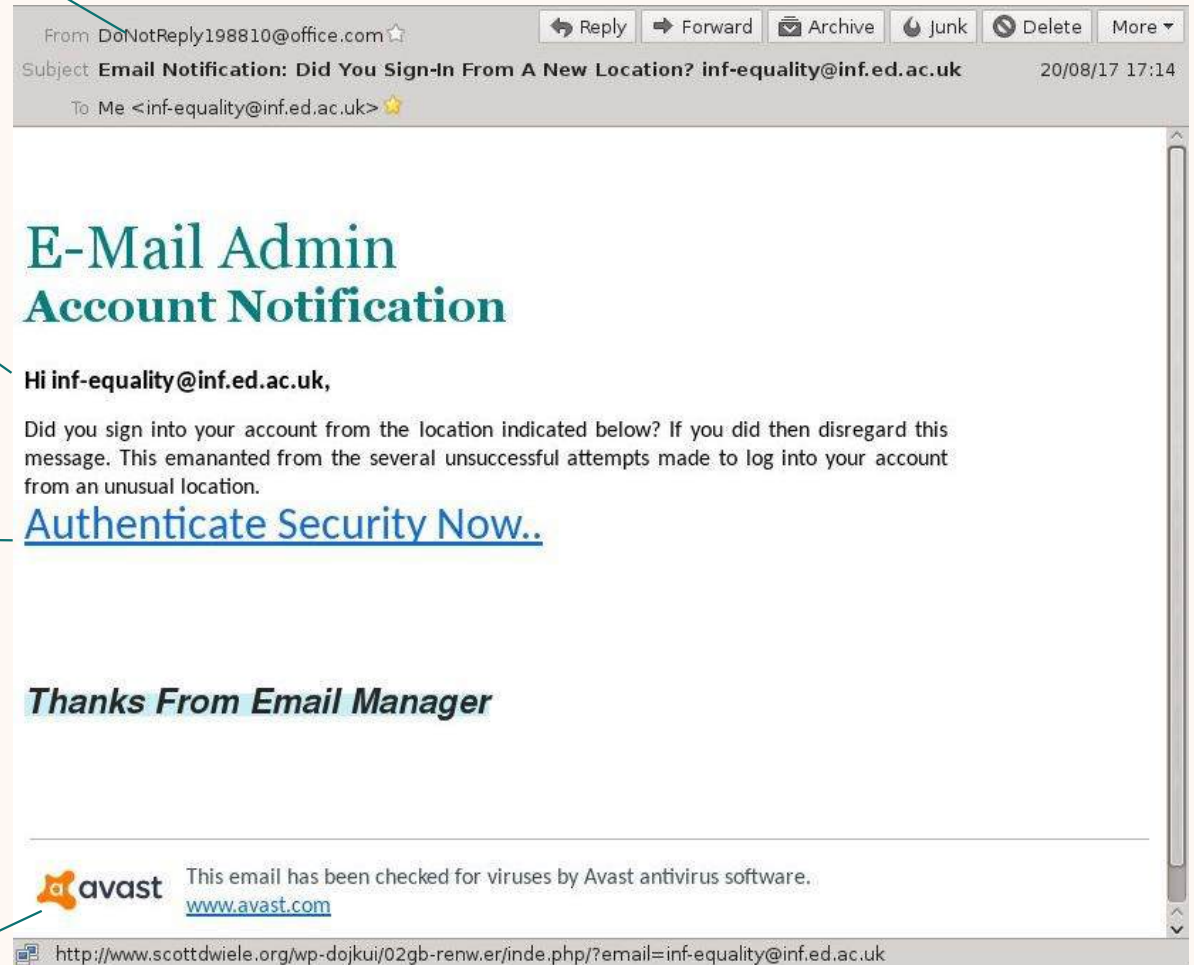
Lots of interesting [things] in this email

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

From DoNotReply198810@office.com

Subject **Email Notification: Did You Sign-In From A New Location? inf-equality@inf.ed.ac.uk**   20/08/17 17:14

To Me <inf-equality@inf.ed.ac.uk>

↩ Reply   → Forward   📥 Archive   🔥 Junk   🚫 Delete   More ▼

E-Mail Admin
Account Notification

Hi inf-equality@inf.ed.ac.uk,

Did you sign into your account from the location indicated below? If you did then disregard this message. This emanated from the several unsuccessful attempts made to log into your account from an unusual location.

Authenticate Security Now..

Thanks From Email Manager

avast   This email has been checked for viruses by Avast antivirus software.
www.avast.com

http://www.scottdwiele.org/wp-dojkui/02gb-renw.er/inde.php/?email=inf-equality@inf.ed.ac.uk
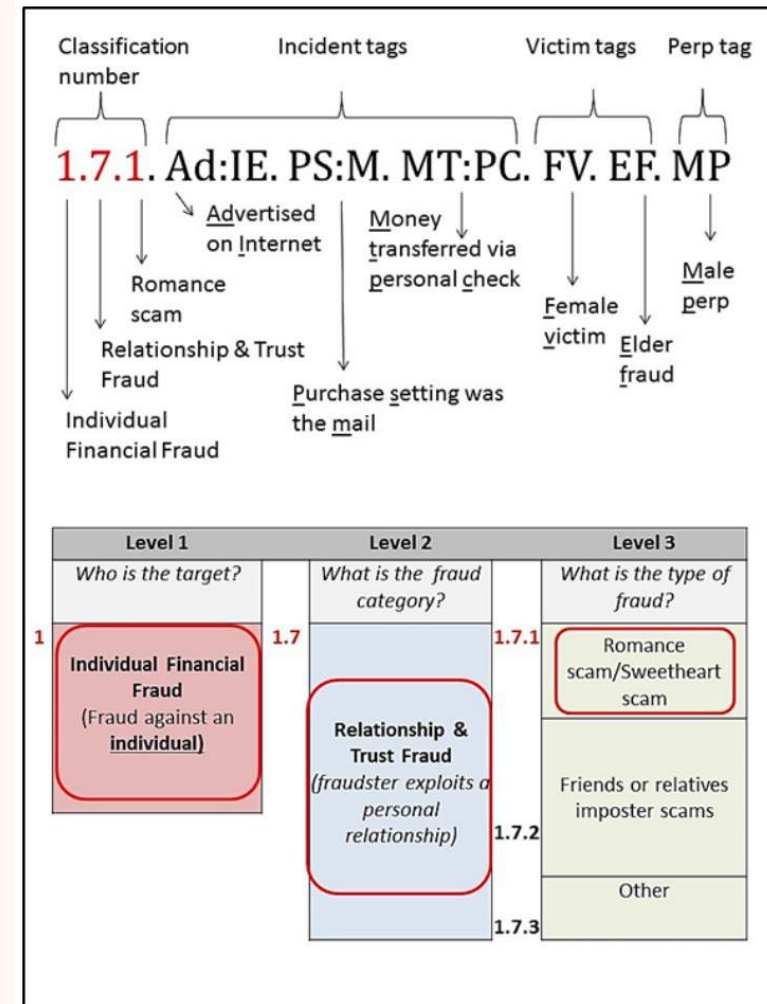
What are the other types of fraud?

Stanford Fraud Taxonomy

Mary, age 67, reports that her online relationship started out as a friendship. Mary found the man on a social networking site. The two "lovers" would tell each other about themselves and later spoke to one another over the phone. He told her he was stuck in Nigeria and needed help to fly home. Mary started mailing checks to help her lover. She blew through her own money and eventually had to start taking out loans to help him.

40

Stanford Fraud Taxonomy

Mary, age 67, reports that her online relationship started out as a friendship. Mary found the man on a social networking site. The two "lovers" would tell each other about themselves and later spoke to one another over the phone. He told her he was stuck in Nigeria and needed help to fly home. Mary started mailing checks to help her lover. She blew through her own money and eventually had to start taking out loans to help him.

https://longevity.stanford.edu/financial-fraud-research-center/wp-content/uploads/2016/03/Full-Taxonomy-report.pdf

Overview of Stanford Fraud Taxonomy

- Consumer Investment Fraud
  - Securities fraud
    - Equity investment fraud
      - Penny stock fraud
      - …
    - …
  - …
- Consumer Products and Services Fraud
  - …
    - *Phishing websites/emails/calls*
- Employment Fraud
- Prize and Grant Fraud
- Phantom Debt Collection Fraud
- Charity Fraud
- Relationship and Trust Fraud

Overview of Stanford Fraud Taxonomy

- Consumer Investment Fraud
  - Investors gain and lose money in financial markets for a variety of legitimate reasons, yet the following definitions refer to investment fraud, where someone knowingly misleads an investor on the basis of false information. While many investment vehicles listed below have legitimate versions, they can also be used in investment scams where the earnings are grossly misrepresented or the investment itself is nonexistent.
- Consumer Products and Services Fraud
  - This broad category covers all fraud related to the purchase of tangible goods and services. It also includes vacations and travel, house/apartment rentals, purchase of pets, concerts/performances, and other events or items the victim paid for but did not receive as promised.
- Employment Fraud
  - In this broad category of fraud schemes, the expected benefit is employment or training to develop a profitable business. Fraudsters advertise work opportunities that require few skills or qualifications, but claim to provide above average financial rewards
- Prize and Grant Fraud
  - The hallmark of this category of fraud is that victims are led to believe they will receive winnings in the form of a prize, lottery, grant, or windfall of money, provided that they first purchase certain products or make advance payments to cover fictitious fees and taxes.

Overview of Stanford Fraud Taxonomy

- Phantom Debt Collection Fraud
  - This category of fraud refers to fake debt collectors who deceive and possibly threaten individuals to convince them to pay debts they don't owe.
- Charity Fraud
  - This category of fraud involves scam artists collecting money by posing as a genuine charity. There is no expected benefit or product/service resulting from the transaction. Instead, the expected outcome from the perspective of the victim is organized charitable giving.
- Relationship and Trust Fraud
  - In these schemes, the fraudster exploits a personal relationship with the victim and there is no expectation of a product or service from the interaction. Instead, the expected outcome from the perspective of the victim is the fostering of a personal relationship.

What are the new frauds today? And how would you categorize frauds?

Take-home

- **(Blog)** Chen, X., Doublet, S., Sergeeva, A., Lenzini, G., Koenig, V. and Distler, V., 2024. What Motivates and Discourages Employees in Phishing Interventions: An Exploration of {Expectancy-Value} Theory. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)* (pp. 487-506).

- **(Blog)** BBC - 'Vinted scammer reeled in my 15-year-old daughter'