UNIVERSITY OF PLYMOUTH

Social Engineering & Phishing

Dr Hai-Van Dang

Centre for Security, Communications and Network Research

Learning outcome checklist

1. Recognize the use of psychological trigger(s) in a potential social engineering attack [1,2]
2. Recognize how and how easy a social engineer can collect your information (reconnaissance in Cyber Kill Chain) [3]
3. Recognize a potential social engineer attack, a phishing/ spear phishing attack
4. Map strategy/ actions of a phishing attacker onto Cyber Kill Chain
5. Defend yourself against phishing with LIST
6. Defend your organization against phishing with multi-layer defense

Further reading

1. Quiel, Susanne. *Social engineering in the context of Cialdini's psychology of persuasion and personality traits*. Diss. Technische Universität Hamburg, 2013 – section 3.1
2. The Ultimate Guide to Social Engineering – on DLE
3. https://www.sophos.com/en-us/press-office/press-releases/2007/08/facebook

Session Content

Introduction

Social Engineering concepts

Means and Methods

Phishing Threats and Studies

Conclusions

The Social Engineering threat

- Techniques that exploit human weaknesses and manipulate people into breaking security procedures
  - may involve convincing them to perform atypical actions or to divulge confidential information
- Overlaps into the worlds of psychology, confidence tricksters, and behavioural manipulation
- Often easier to exploit the users of a system rather than the technology itself
- Often overlooked by organisations:
  - lack of staff awareness / education to highlight the threats
  - lack of testing to see if the staff are susceptible

From the horse's mouth …

Kevin Mitnick

"*It's become more prevalent because you have the security technologies that make it more difficult to exploit technical vulnerabilities … plus you have attackers that are not so technically astute, who might use social engineering in any event*"

From the horse's mouth …

Kevin Mitnick

"*I think the majority of the people out there are not aware of what social engineering is because a lot of companies don't train people on this type of attack*"

Potential triggers

- Authority
  - the attacker achieves the desired response from the target by making an assertion of authority
- Commitment and consistency
  - targets are likely to act consistently with past behaviour, and in accordance with things they have committed to
- Liking and similarity
  - the attacker exploits the fact that targets are more likely to respond to someone they like, or perceive to be similar to themselves

(Cialdini, 2000)

Potential triggers

- Reciprocation
  - the target is given something, in the hope that they feel obliged to reciprocate by giving something in return
- Scarcity
  - the target is led to believe that something they desire is in short supply or only available for a limited period. They may then feel obliged to act quickly and possibly without sufficient prior thought
- Social validation
  - targets may base their decision upon the behaviour of others (increasing the chances of a request being complied with by claiming that other people have already done the same thing)

(Cialdini, 2000)

Identify the trigger

- Menti, individual

1. An attacker sends an email that includes a free coupon and then asks the user to sign up for an account.
2. They tell people that their account will deactivate in 24 hours if they don’t click on a link to get it resolved.

Identify the trigger (cont)

3. Bad actors spoof the Chief Executive Officer (CEO) to demand that the Chief Financial Officer (CFO) wire money quickly in some spear phishing campaigns. When combined with urgency, people are often afraid to say no to their boss.
4. Scammers take advantage of people's desire to be consistent by asking for something small in an initial email and then asking for more later.

Identify the trigger (cont)

5. The bad actor spoof or hack an individual's email account and then send a phishing email to that person's contacts. They are hoping that one of the hacking victim's friends won't spend much time scrutinizing the email content and will just act because the like the "sender."
6. When there is a natural disaster, there are often several illegitimate organizations posing as a charity to elicit donations.

Identify the trigger (cont)

7. The social engineer calls a help desk, and claims to be some manager who has lost his password but very desperately needs access to his e-mails.
8. The attacker impersonates someone from the IT security department, claiming that he needs ID and password of the target due to some problem with the target's computer.

Identify the trigger (cont)

9. “They’ll call you in the middle of the night: ‘Have you been calling Egypt for the last six hours?’ ‘No.’ And they’ll say, ‘well, we have a call that’s actually active right now, it’s on your calling card and it’s to Egypt and as a matter of fact, you’ve got about $2,000 worth of charges from somebody using your card. You’re responsible for the $2,000, you have to pay that...’ They’ll say, ‘I’m putting my job on the line by getting rid of this $2,000 charge for you. But you need to read off that AT&T card number and PIN and then I’ll get rid of the charge for you.’

Identify the trigger (cont)

10. You find a loose thumb drive, in your own parking lot, with your own organization's logo on it, you pick it up and insert it *because you are trying to help.* For good reason. Suppose that the CEO dropped it and it has vital business information in there?

How can we leverage Cialdini's principles to reduce social engineering?

- Menti, 3 students per group, 5 mins
- You are a security engineer team. How could you leverage Cialdini's principles to reduce social engineering attacks?

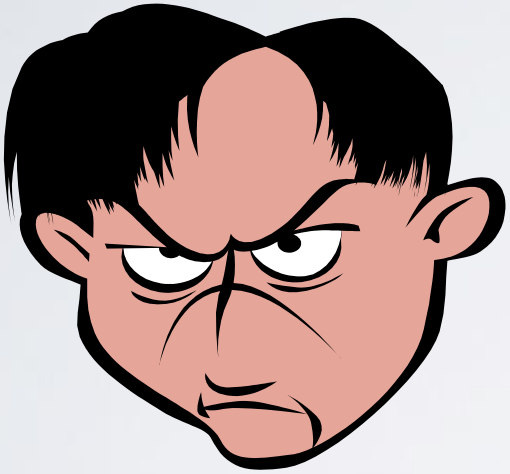
1. 1 minute for each individual to think/ search for any idea
2. Make a group
3. 3 minutes for your discussion if there is at least 1 idea. If there is no idea yet, search/ think together. Agree on the answer
4. Write it on menti

Means and Methods

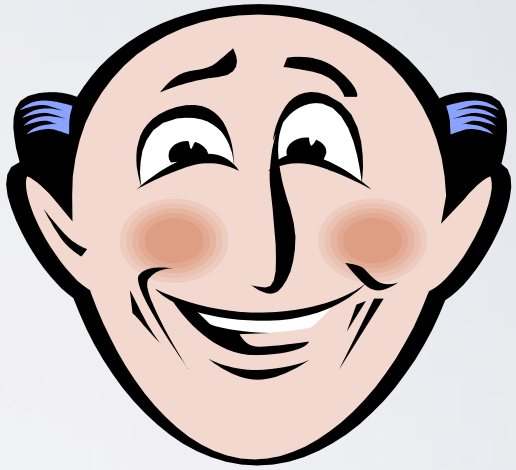
A multitude of guises

- Over the phone
  - Tech support
  - Card fraud dept.
- Physically / in person
  - The service engineer
  - The dropped drive trick
- By email
  - Malware
  - Phishing

Social Engineering



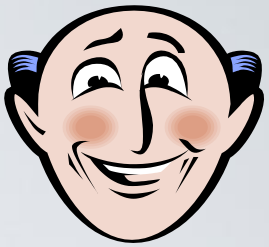
VS



- Wants information
- Able to bluff
- Convincing and persuasive

- Has useful information?
- Inclined to be helpful?
- Gullible?
- Technically naïve?

Some Simplified Social Engineering



Hacker: Good morning. I'm calling from Macrohard. We handle the IT maintenance contract for Barcminster Bank. Could you spare a few moments of your time?

User: Yes, okay.

Hacker: I need to do some remote administration on your systems, but I'm having problems with the service engineer login account. I need to login so that I can clear some jobs from your process queue.

User: What do you want me to do?

Hacker: It would probably be easiest for me to do the work, but I need to be able to login first. Could I quickly login under your account so that I can reset mine.

User: Do I need to logout first?

Hacker: No, that's okay. All I need is your username and password.

User: Okay, my username is 'jsmith' and the password is 'apples'.

Hacker: Great. I'll login now and fix the problem. Thanks a lot for your help.

An incident 3 years ago

- This man walked into a first year computing lab on the first day of teaching
- Claimed to be from IT services
- Asked students to write their usernames and passwords on Post-it notes so that he could use them to update the lab configuration
- **>80% of students admitted giving him genuine details**

Why did it work?

- Professional looking (collar and tie)
- Wearing University of Plymouth lanyard which appeared to hold an ID card (but facing the wrong way, so not showing picture)
- Appeared to know what he was talking about (informed and authoritative)
- Advised students not to let others see their post-its
  - seemed to have their security interests in mind
- ”Seemed trustworthy”

A fair test?

- Did nothing that a real attacker would not have been able to do
- Used no information that a bit of reconnaissance would not have been able to uncover
- Was it fair and appropriate to do it?
  - what are the ethics of such mock exercises?

Getting the details
Physical Sources

- Dumpster Diving (bin raiding)
  - Searching through waste bins, skips etc. outside an organisation to locate clues for accessing their systems
  - What might people throw away that could be useful?
    - Technical documentation
    - Internal telephone directories
    - Product packaging

- Talking to people
  - In person, by phone etc . . . can gradually gather a base of knowlegde

Getting the details
Online Sources

- Social networks and websites can provide information for targeted attacks
  - Information that we place in the public domain can be used by others
  - Search engines are a strong reconnaissance tool
- Spear-phishing attacks could be framed around:
  - Interests expressed on Facebook profiles
  - Themes and opinions raised in tweets
  - Workplace information gathered from company webpages
- Potential victims need to be aware of what's out there about them

Reflection

- Menti, individual
- What type of your information can be collected from your social networks (facebook, Instagram, tiktok, linkedln,…)?

Facebook Examples

- Users can share a variety of personal information:
  - birthday, contact information, photos, details of friends, wall postings
- Some of this might merit some control over who gets to see it
- Default restrictions are quite liberal for some categories of data
  - e.g. details of photos and friends are visible to the Internet
  - see mattmckeon.com/facebook-privacy/ to track the change

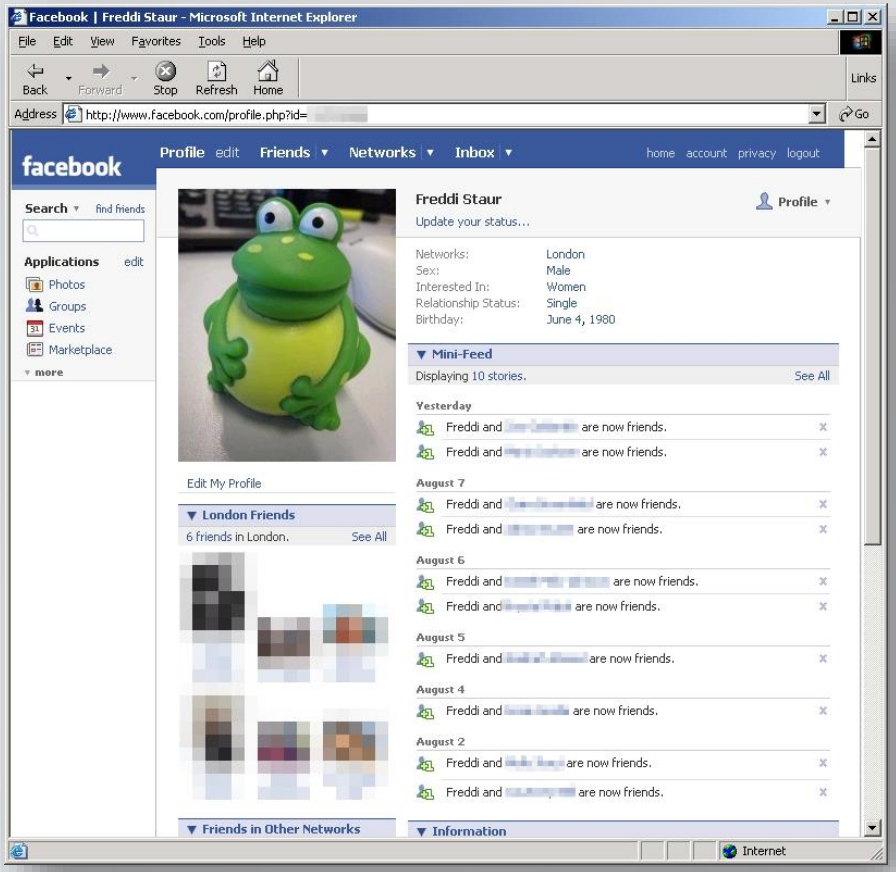
Sharing without caring?

- In some cases, restricting the accessibility won't matter … because user's will share with anyone
- Various cases illustrate users' willingness to become online 'friends' with total strangers
  - Sophos – Freddi Staur
- Results from a further experiment can illustrate the potential success here …

Who's friends with Freddi?

- In 2007, Sophos created a Facebook page for Freddi Staur
  - An anagram of 'ID Fraudster'
- 200 people were then invited being to become Freddi's friend
  - By accepting the invitation a stranger was given access to their personal data

What Freddi found out



- 87 users responded, with 82 leaking personal information
  - 72% divulged one or more email address
  - 84% listed their full date of birth
  - 87% provided details about their education or workplace
  - 78% listed their current address or location
  - 23% listed their current phone number

Sharing without thinking

- What is your pornstar name?
  - Can be introduced as a party game, social media chat etc.
  - “Take the name of your first pet and combine with your mother’s maiden name”
  - Gets you names like Fluffy McPhee, Lassie Whipson, and Bubbles Van Dyke

Have a go and share with the group

R
U
A
PORNS
TAr
?

Variations on a theme

Straight Dope Message Board > Main > Mundane Pointless Stuff I Must Share (MPSIMS) > What's your "hooker name?"

PDA

View Full Version : What's your "hooker name?"

08-12-1999, 03:24 PM

Has this been played before on the board? It's a party game of one or two year's standing. Your hooker (or drag, or porn star) name is figured out the following way:

first name: your first childhood pet

last name: the street you grew up on.

Therefore, mine would be "Tiki Greentree." I work with "Brandy Buckingham" and (the winnah!) "Midnight Cherry."

Omniscient 08-12-1999, 03:30 PM

We've all played this game before, and some variations are using your middle name/pets name/street name in a variety of orders.

Mine would be Gina George, not bad, but I'm a guy so the pets name doesn't quite fit.

Gaudere 08-12-1999, 03:32 PM

"Rusty Marion"

Pity I'm not a redhead.

"Eppur, si muove!" - Galileo Galilei

Ukulele Ike 08-12-1999, 03:33 PM

Molly Highland. Yuck. Sounds like the porn star's unattractive best friend.

'Scuse me while I put my hair in a bun and slip on the horn-rims.

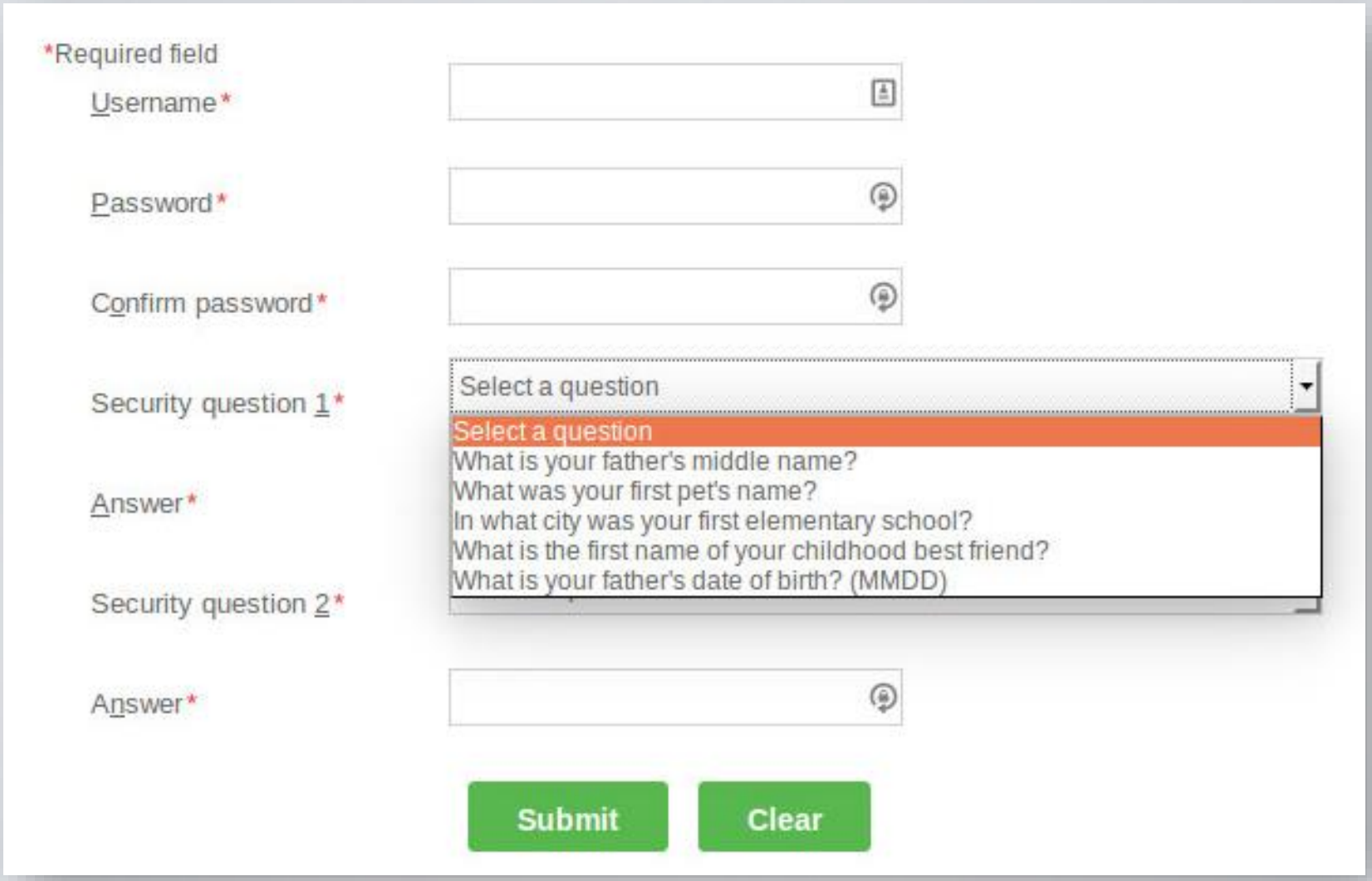
Uke

Mojo 08-12-1999, 03:36 PM

"Mommycat East Capital" doesn't quite sound right.

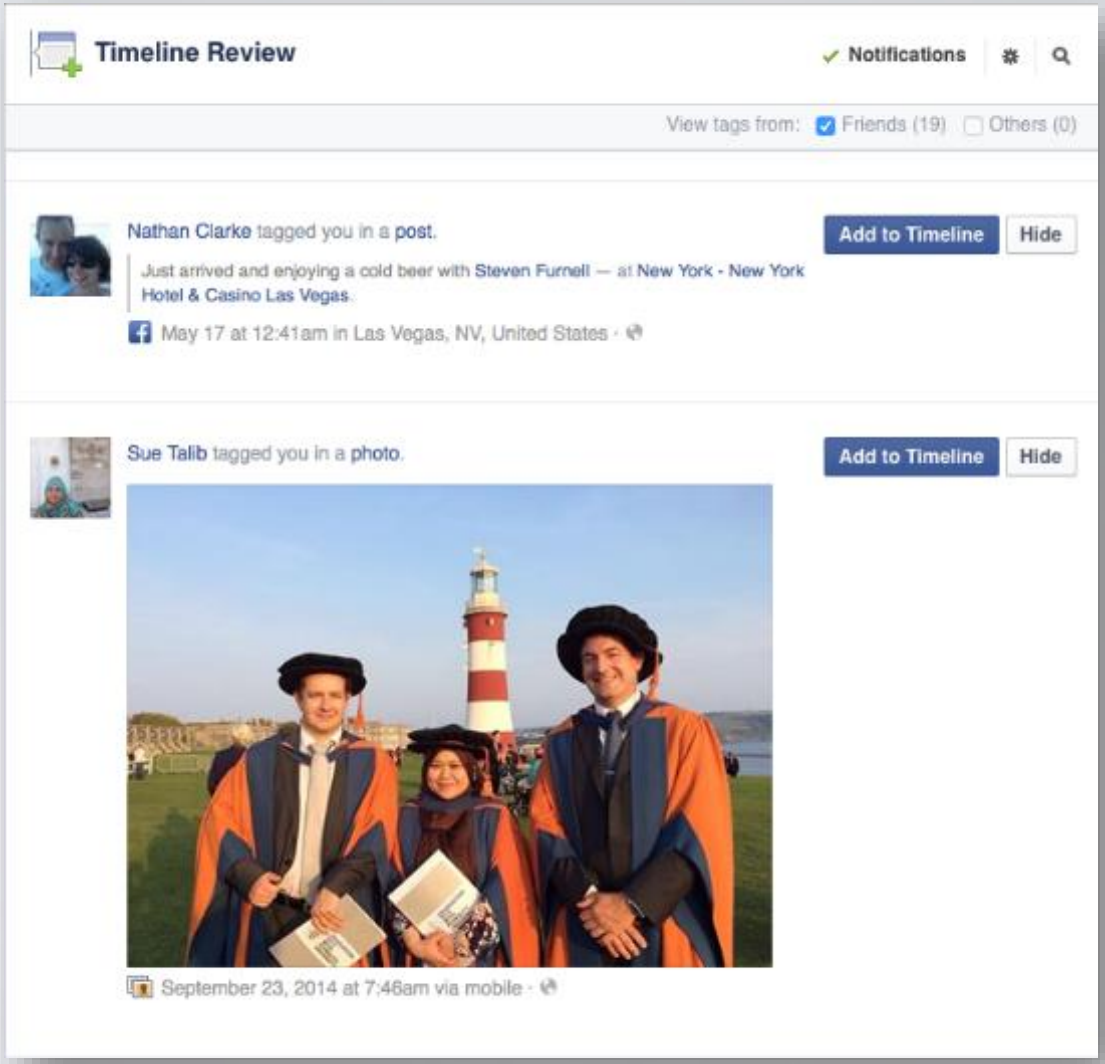
My 2nd pet/street combo, "Bob Parkwood", is better.

Where else is that info used . . . ?



Duping the dopey?

Shared on your behalf



Advance Fee Frauds

- An old problem in a new medium
  - once arrived by post or fax, now appear as spam email
  - massively increases the audience
- Basic premise involves the offer to pay a large sum of money to recipient's account
  - requires an initial fee to set transactions in motion
- Historically many originated from Nigeria
  - hence termed 419 scams, after the relevant section of the Nigerian Criminal Code

Surely an honest offer . . .

"I and my colleagues has been able to negotiate out for ourself a total sum of **twenty-four million United States Dollars, {$24,000,000}**, which we want to transfer into a reliable/save account outside Nigeria . . . But as you know the civil service rule and regulation ACT of 1999,prohibits civil servants from having foreign account, that is why I am soliciting your assistance to provide for me your account particulars, Where these money will be transferred quietly without attracting much tax and can be easily withdrawn without raising eyebrows . . . If you will play this role, of providing the receiving account, and at the same time pledge your honesty not to double cross us at the end of the transaction, **we will be willing to give you only 25% of the total sum** at the successful conclusion of the transfer."

JOB CONFIRMATION - Temporary Items

Message

Delete | Reply | Reply to All | Forward | Meeting | Attachment | Move | Junk | Rules | Read/Unread | Categorise | Follow Up

JOB CONFIRMATION

MB [redacted]

Tuesday, 4 May 2021 at 12:05

A work-from-home job with commission…?

Hello

Hi [redacted] How are you doing today. I'm glad to congratulate you as your position has been confirmed.For the next couple of weeks I'll be giving you some task at least once in a week. Sorry we can't meet before you get started with work as I'm presently away on a business trip but be rest assured that you can officially get started as all communications will be through email and text. The more reason why you need to check your email and text often.

About [redacted]

[redacted] provide a full event management service as well as a full event communication service. This ranges from working with clients to ensure they are using events to best effect; achieve their overall strategic objectives through advising on the content and optimum method of message delivery for a specific event.

Duties and Responsibilities:

* Running personal errands, supervisions and monitoring.
* Collection of my commissions.
* Booking appointments with my Clients
* Handling and Monitoring some of my Financial activities
* Process Payable and Purchase orders for submission
* Receiving my Monthly Memo from my associates
* Responsible for a variety of office tasks including tracks data and source documents. Prepares and sorts source documents, and identifies and interprets data to entered.

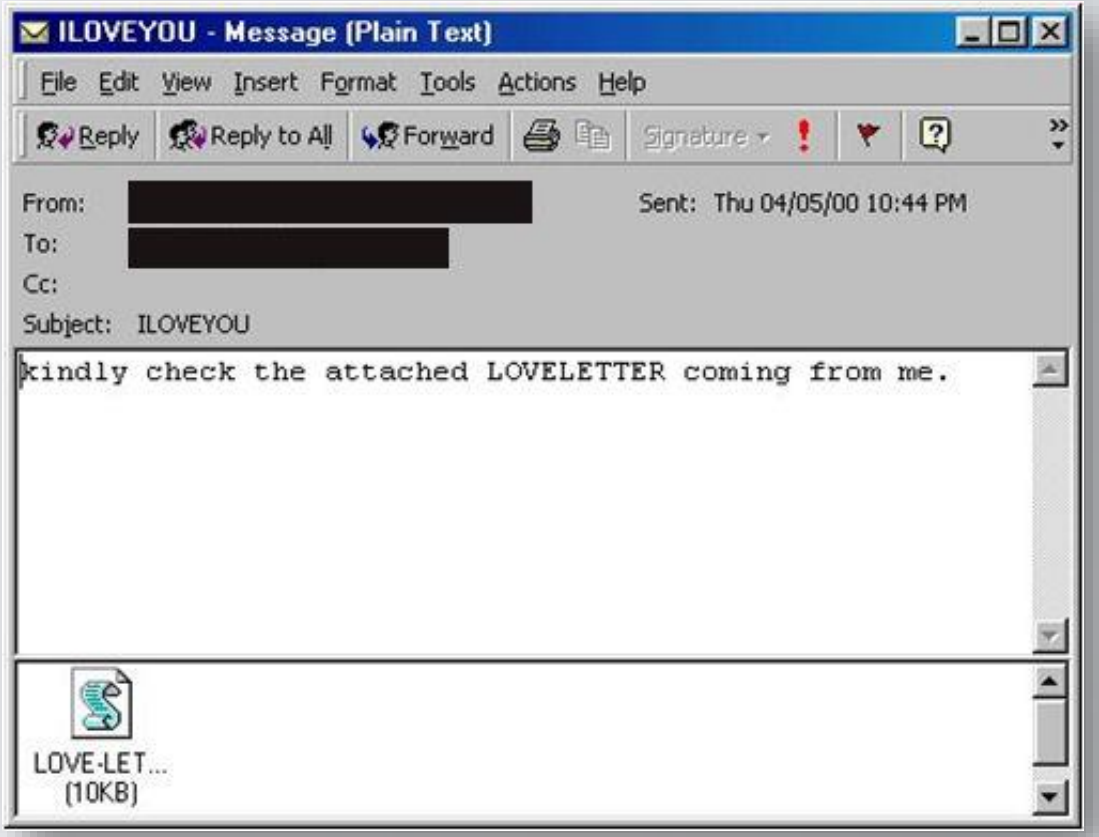
First Task:

Your first task for this week will be in charge of a monthly donations which I make to 3 Orphanage homes every month. I will provide the funds which you will use in making purchase of the stuff that will be donated to the orphanage home, The fund will be inform of a (Cashier Check) and it will be issued to you alongside your Weekly Pay of $350. As soon as you receive it, Kindly have it deposited with your bank as it clears with the next 24 hours. I will email you the list of the items to purchased at the store and all the necessary information on how to get it mailed out to the orphanage homes in my next email.

NOTE: This is a Flexible part-time job where you will determine your working time, importantly this does not disturb your other schedule both at work and at school. All the tasks are work from home/on campus job, you don't need to travel somewhere and also you don't need to have a car to get started.

Social Engineering and Malware
Love Bug worm (2000)

- Used ‘social engineering’ methods to encourage users to open (and thereby execute) a malicious attachment
- Attached Visual Basic Script file named “LOVE-LETTER-FOR-YOU.TXT.vbs”



Social Engineering and Malware
A Seasonal Striptease?

- Attacks will often attempt to exploit current events or news stories
- On Christmas Eve 2007 an email was widely distributed using a variety of message titles
- All directed users to a website claiming to contain a Santa Claus-themed striptease

Christmas Email
Cold Winter Nights
Feel the Holiday Spirit
Find Some Christmas Tail
Ho Ho Ho.s
How.s It Goin
I love this Carol!
Jingle Bells, Jingle Bells
Looking for something hot this Christmas
Merry Christmas From your Secret Santa
Merry Christmas To All
Mrs. Clause
Mrs. Clause Is Out Tonight!
Santa Said, HO HO HO
Seasons Greetings
The Perfect Christmas
The Twelve Girls Of Christmas
Time for a little Christmas Cheer.
Warm Up this Christmas
Your Secret Santa

Messages from Santa?

Yo,

Good times and holiday sheer are good, but this is great. Forget all the stress for two min and feast your eyes on these. ;-)
http://merrychristma[redacted].com/

Dude,

This Christmas, we want to show you something you will really enjoy. Hey what can 1 min from your day hurt. You wont regret it for sure. ;-)
http://merrychristma[redacted].com/

Following the links took you to the website ...

Would you trust these ladies?

Would you trust these ladies?

- Clicking on the images or the "Download for free now!" button both downloaded the W32/Dorf-AE worm
- Opens up remote access to the PC, allowing hackers to gain access to resources and data

Social engineering attacks

Source: Salahdine, Fatima, and Naima Kaabouch. "Social engineering attacks: A survey." *Future Internet* 11.4 (2019): 89.

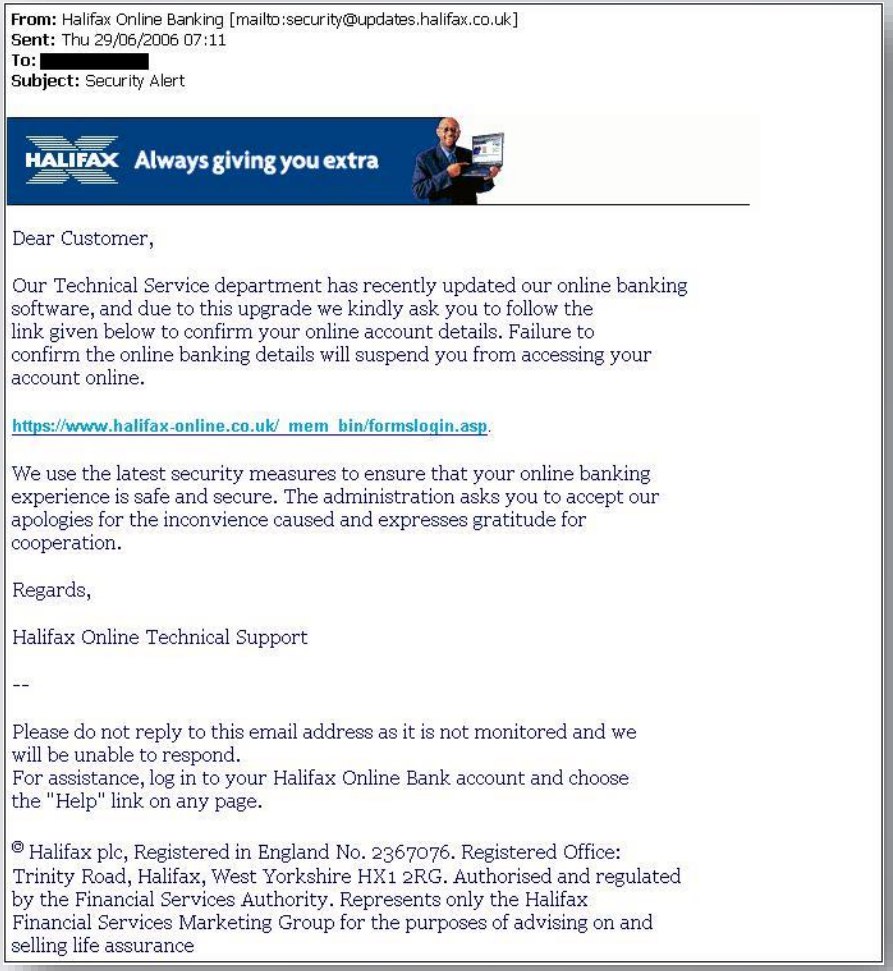
Break

- Be back at
- Check in code
- Update surgery hour (DLE updated):
  - Dr Hai-Van : 16:00-18:00 Monday, SMB101 (exception: 17:00-18:00 on Monday 14/2/2022)
- Peer Assisted Learning Scheme (PALS): information on DLE
- Cyber security research seminar series https://www.plymouth.ac.uk/whats-on/cyber-security-research-seminar-series

(next event: Wed 16/2/2022, The human factor in cybercrime by Dr Maria Bada)

Phishing

- Attempts to dupe users into divulging sensitive information
- Attacks traditionally targeted personal data relating to the user
  - e.g. bank account and credit card details
- Similar techniques also target information to compromise an employer
  - e.g. passwords and company details



From: Halifax Online Banking [mailto:security@updates.halifax.co.uk]
Sent: Thu 29/06/2006 07:11
To: [redacted]
Subject: Security Alert

HALIFAX Always giving you extra

Dear Customer,

Our Technical Service department has recently updated our online banking software, and due to this upgrade we kindly ask you to follow the link given below to confirm your online account details. Failure to confirm the online banking details will suspend you from accessing your account online.

https://www.halifax-online.co.uk/_mem_bin/formslogin.asp

We use the latest security measures to ensure that your online banking experience is safe and secure. The administration asks you to accept our apologies for the inconvience caused and expresses gratitude for cooperation.

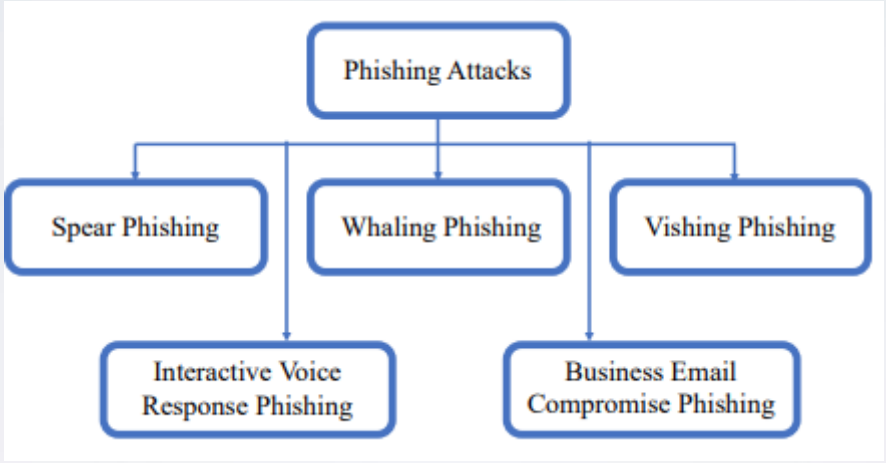
Regards,

Halifax Online Technical Support

--

Please do not reply to this email address as it is not monitored and we will be unable to respond.
For assistance, log in to your Halifax Online Bank account and choose the "Help" link on any page.

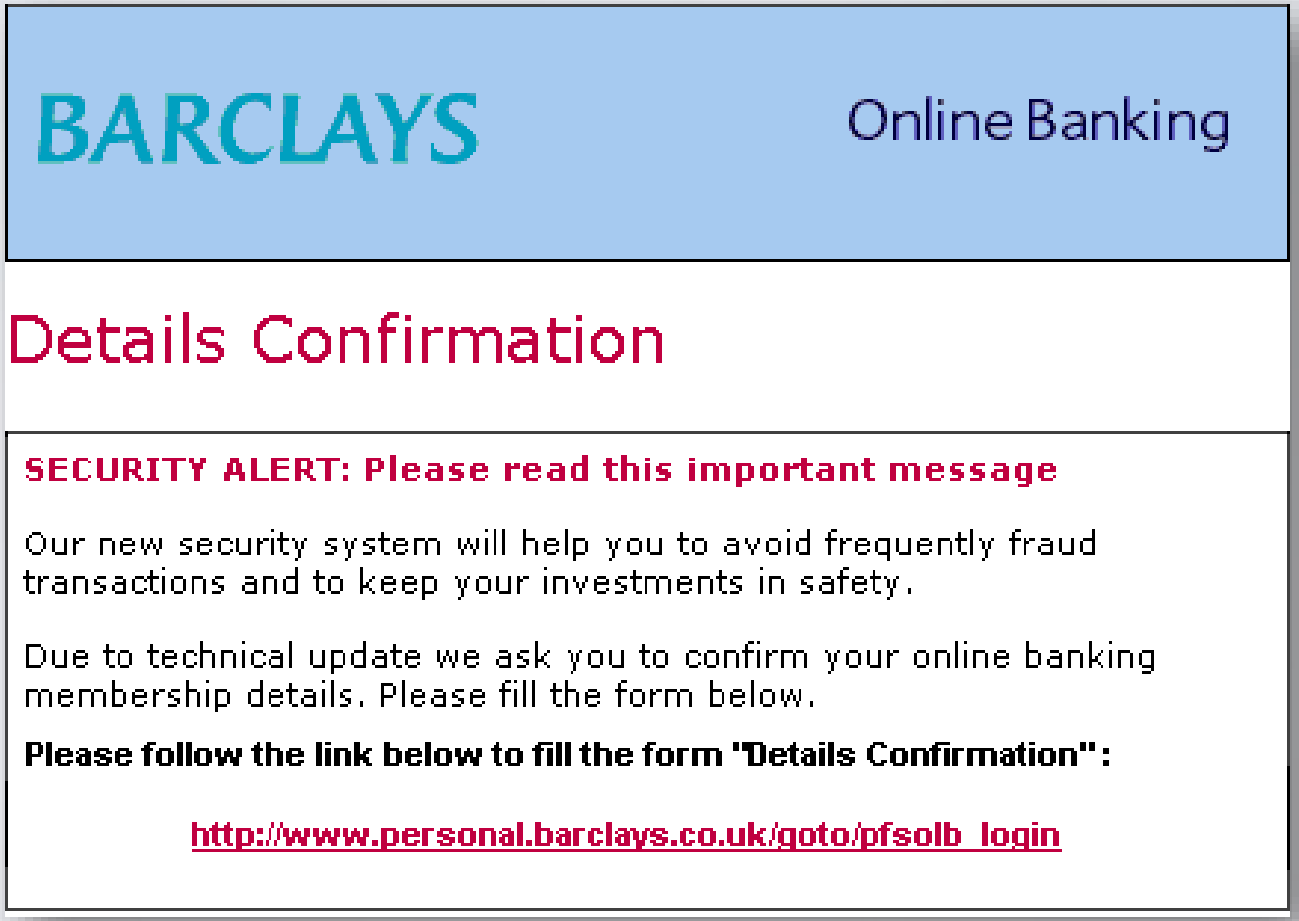
Phishing classification



Source: Salahdine, Fatima, and Naima Kaabouch. "Social engineering attacks: A survey." *Future Internet* 11.4 (2019): 89.

Phishing example

A bogus email message . . .



BARCLAYS Online Banking

Details Confirmation

SECURITY ALERT: Please read this important message

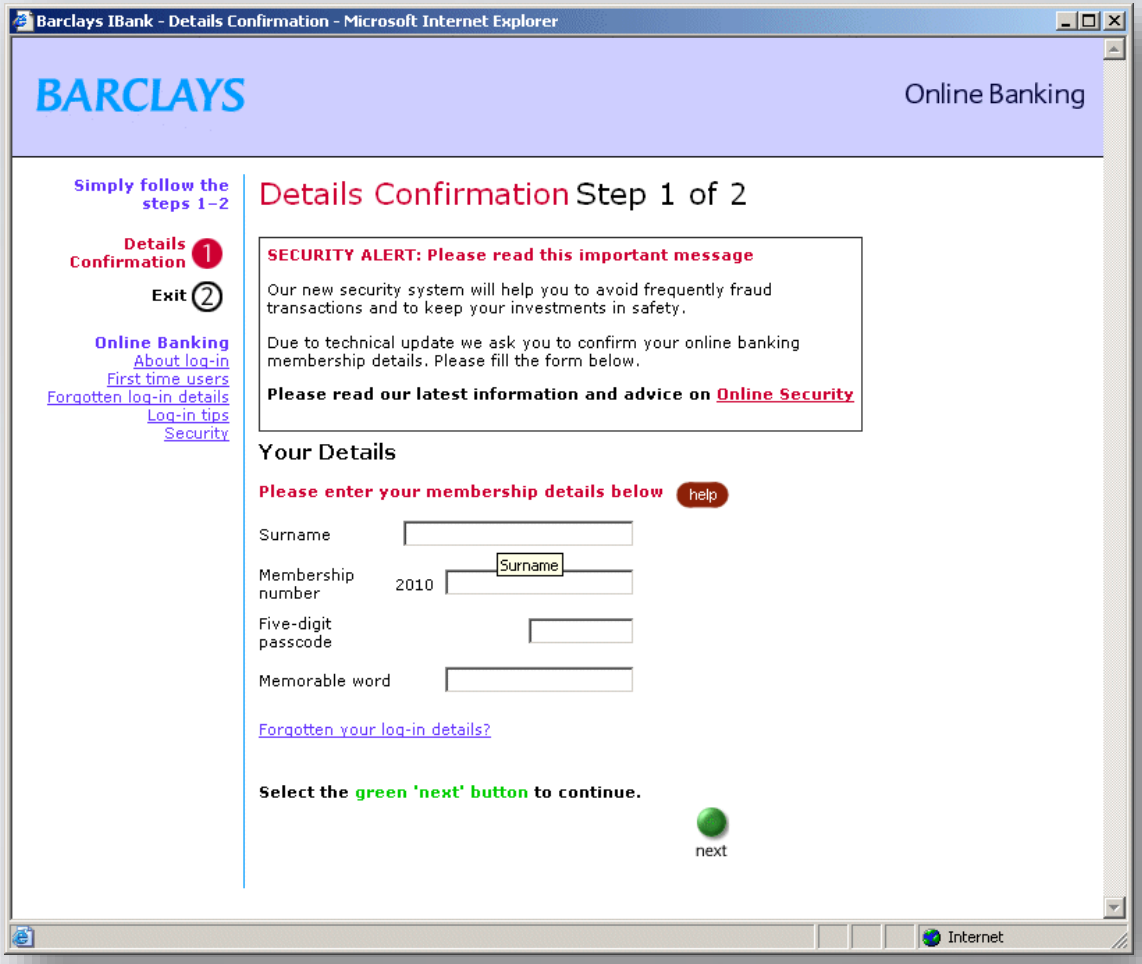
Our new security system will help you to avoid frequently fraud transactions and to keep your investments in safety.

Due to technical update we ask you to confirm your online banking membership details. Please fill the form below.

Please follow the link below to fill the form "Details Confirmation":

http://www.personal.barclays.co.uk/goto/pfsolb_login

Phishing example
. . . and a bogus website



Phishing threats

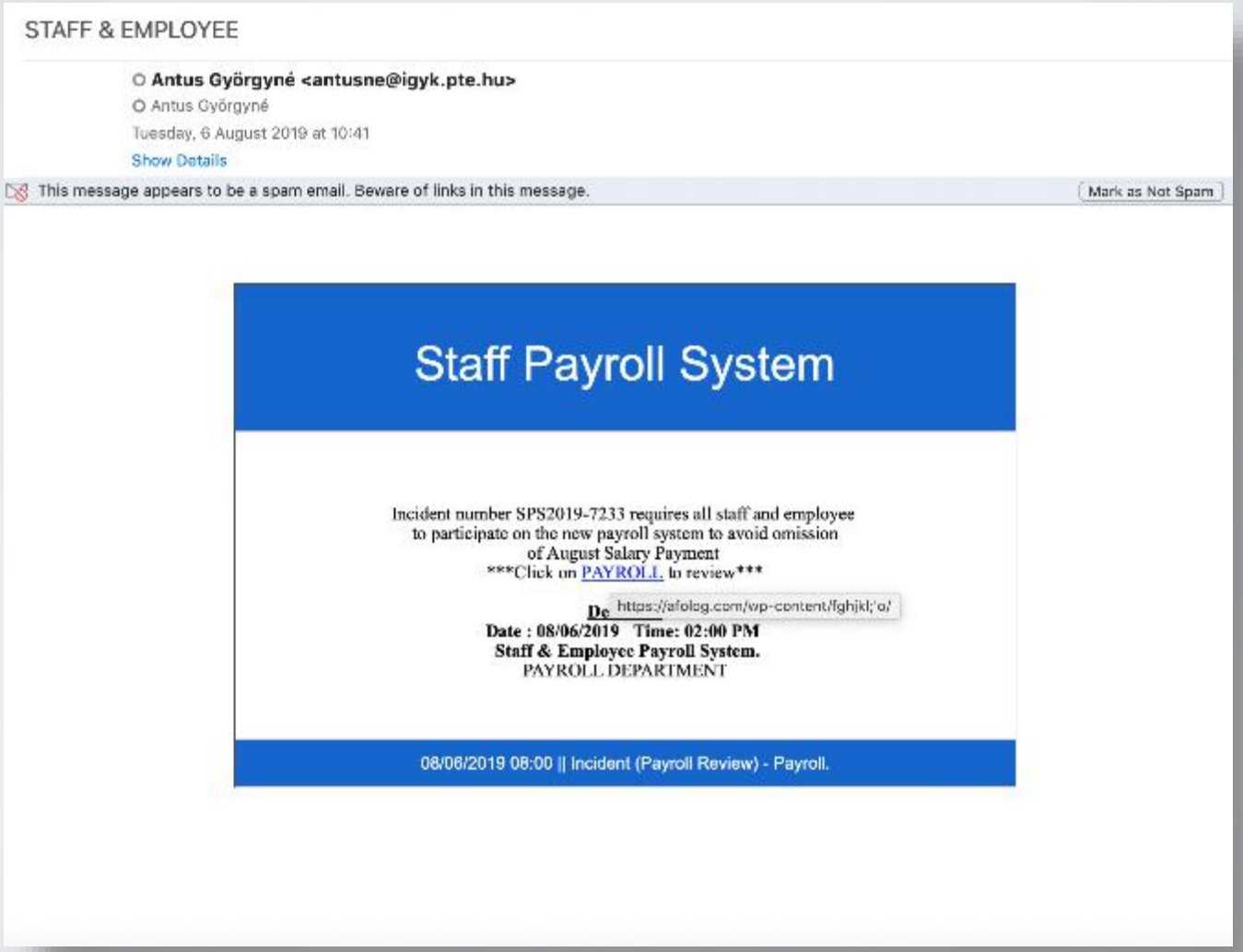
Spot (spear) phishing threats – What are the indications and triggers?

- Menti, 3 students per group

1. Go through 5 actual email messages in the following slides (you can download slide on DLE)
2. Identify the indications of the phishing emails
3. Identify the triggers (Cialdini's principles) that the attackers used
4. Agree on the answers
5. Post it to menti

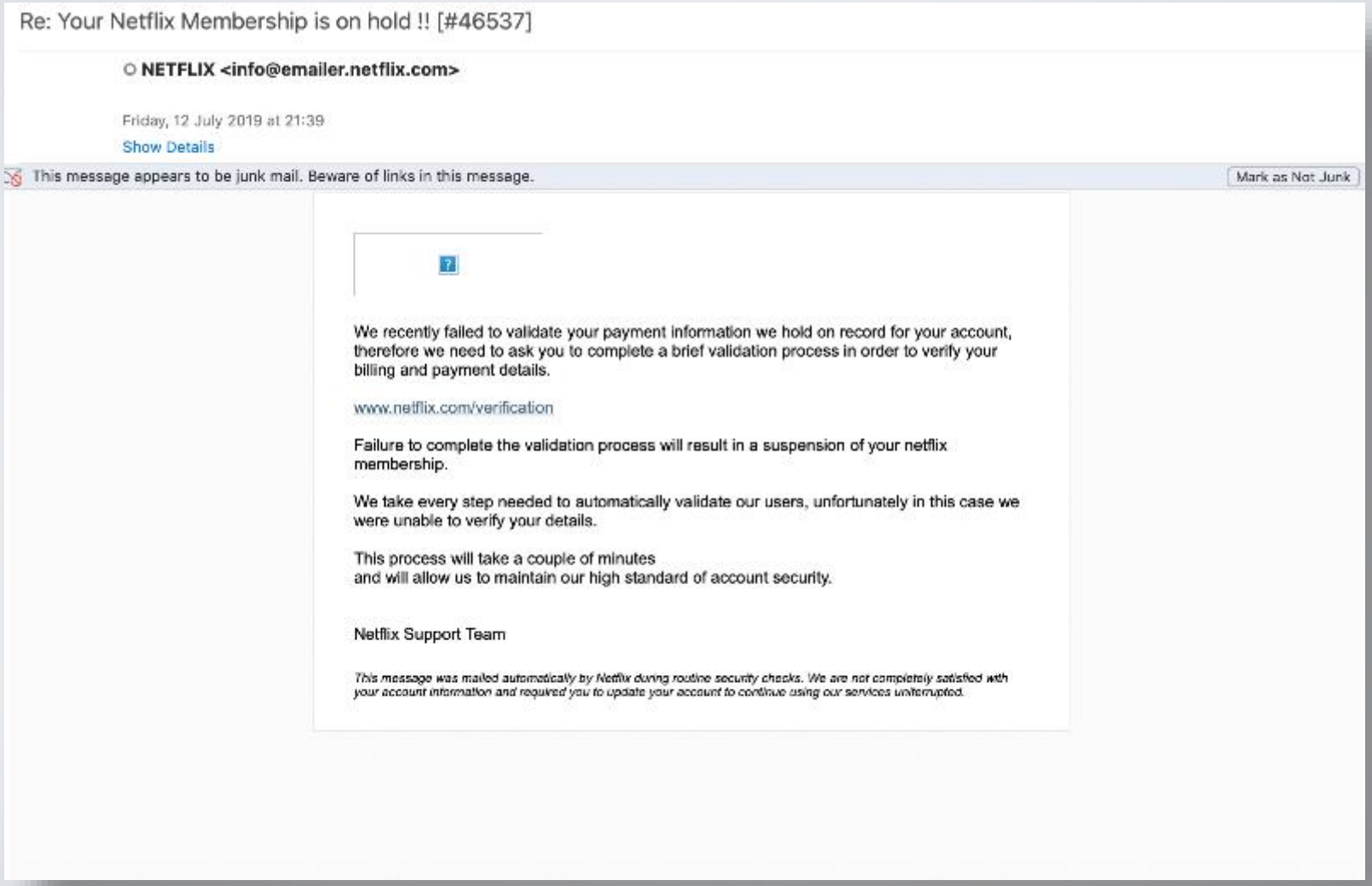
A few days in 2019

Some examples of actual messages received



A few days in 2019

Some examples of actual messages received



Re: Your Netflix Membership is on hold !! [#46537]

NETFLIX <info@emailer.netflix.com>

Friday, 12 July 2019 at 21:39

Show Details

This message appears to be junk mail. Beware of links in this message.

Mark as Not Junk

We recently failed to validate your payment information we hold on record for your account, therefore we need to ask you to complete a brief validation process in order to verify your billing and payment details.

www.netflix.com/verification

Failure to complete the validation process will result in a suspension of your netflix membership.

We take every step needed to automatically validate our users, unfortunately in this case we were unable to verify your details.

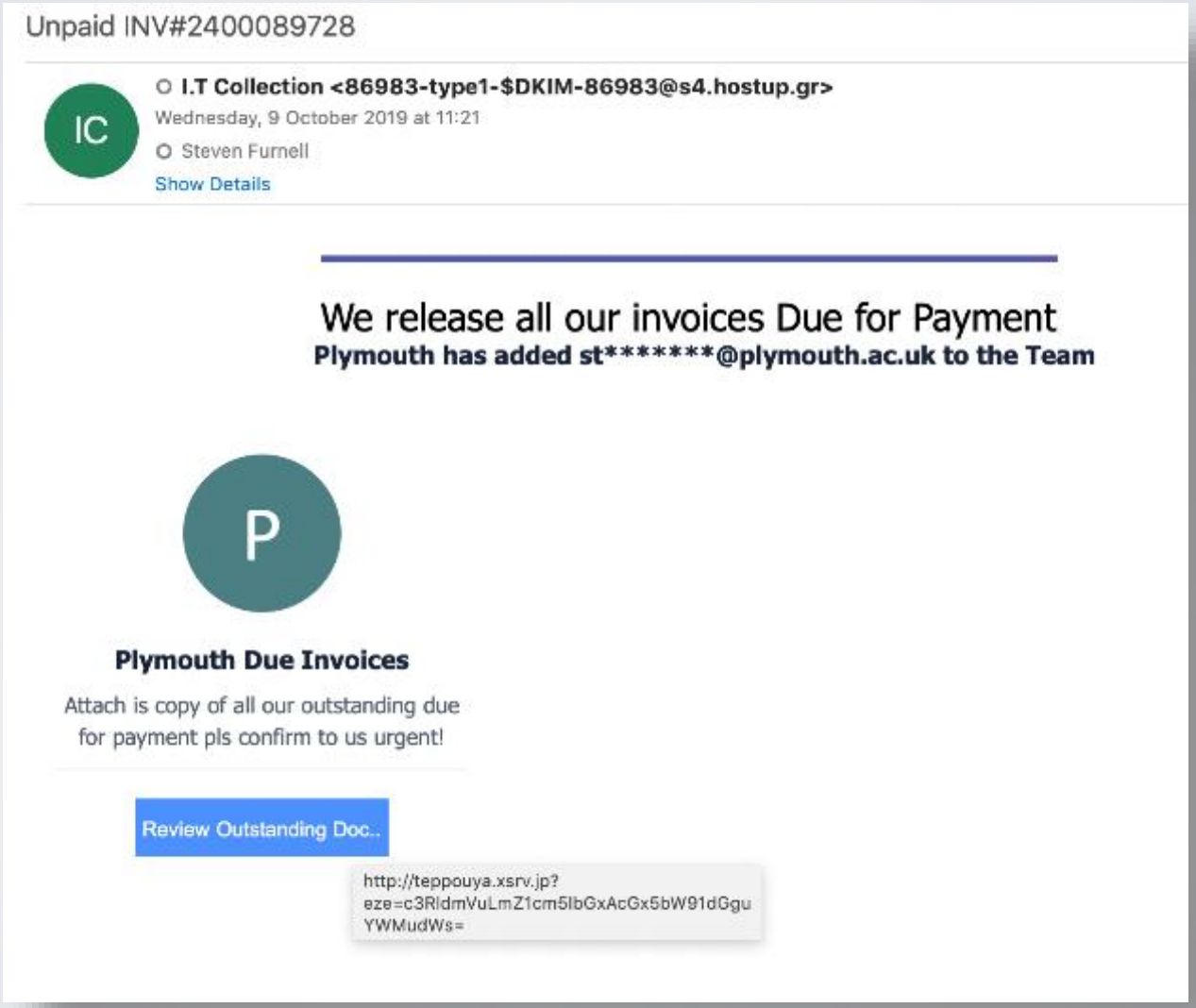
This process will take a couple of minutes
and will allow us to maintain our high standard of account security.

Netflix Support Team

This message was mailed automatically by Netflix during routine security checks. We are not completely satisfied with your account information and required you to update your account to continue using our services uninterrupted.

A few days in 2019

Some examples of actual messages received



Unpaid INV#2400089728

IC

I.T Collection <86983-type1-$DKIM-86983@s4.hostup.gr>

Wednesday, 9 October 2019 at 11:21

Steven Furnell

Show Details

We release all our invoices Due for Payment

Plymouth has added st*****@plymouth.ac.uk to the Team**

P

Plymouth Due Invoices

Attach is copy of all our outstanding due for payment pls confirm to us urgent!

Review Outstanding Doc..

http://teppouya.xsrv.jp?eze=c3RldmVuLmZ1cm5lbGxAcGx5bW91dGguYWMudWs=

A few days in 2019

Some examples of actual messages received

FW: Professional Development Opportunity

Page, Pamela <PPage@cau.edu>

Wednesday, 29 May 2019 at 13:49

Show Details

Plymouth shared do...
428 KB

Download All Preview All

This message appears to be junk mail. Beware of links in this message. Mark as Not Junk

Dear Colleagues,

The following Policy was approved by the Government Board on May 29, 2019, and have been included in this email. This policy has been developed to ensure a safe, friendly and respectful place for all staffs, students, and visitors. It outlines acceptable/unacceptable behavior required for all members, staff, students, and visitors who are expected to comply with this new policy.

All employees are required to go through the guidelines in this email, and it is also important that we all adhere to these guidelines so you will be assisting in ensuring the future success of this great institution.

Thank you all for your unflinching supporting making sure this institution continues to offer a better and reliable service.

Sincerely,

UNIVERSITY OF
PLYMOUTH

Professor Judith Petts CBE.
Vice-Chancellor
University of Plymouth

A few days in 2019

Some examples of actual messages received

Police Situation on Campus

Chaudhuri, Julian <linebegin@axion.ca>
Tuesday, 17 September 2019 at 09:01

Show Details

This message appears to be a spam email. Beware of links in this message.

Hello,

Here is a police Situation on campus, We Encourage everyone to read and follow protocol.

This message is sent Via Secured HTML Protocol Click Here to View.

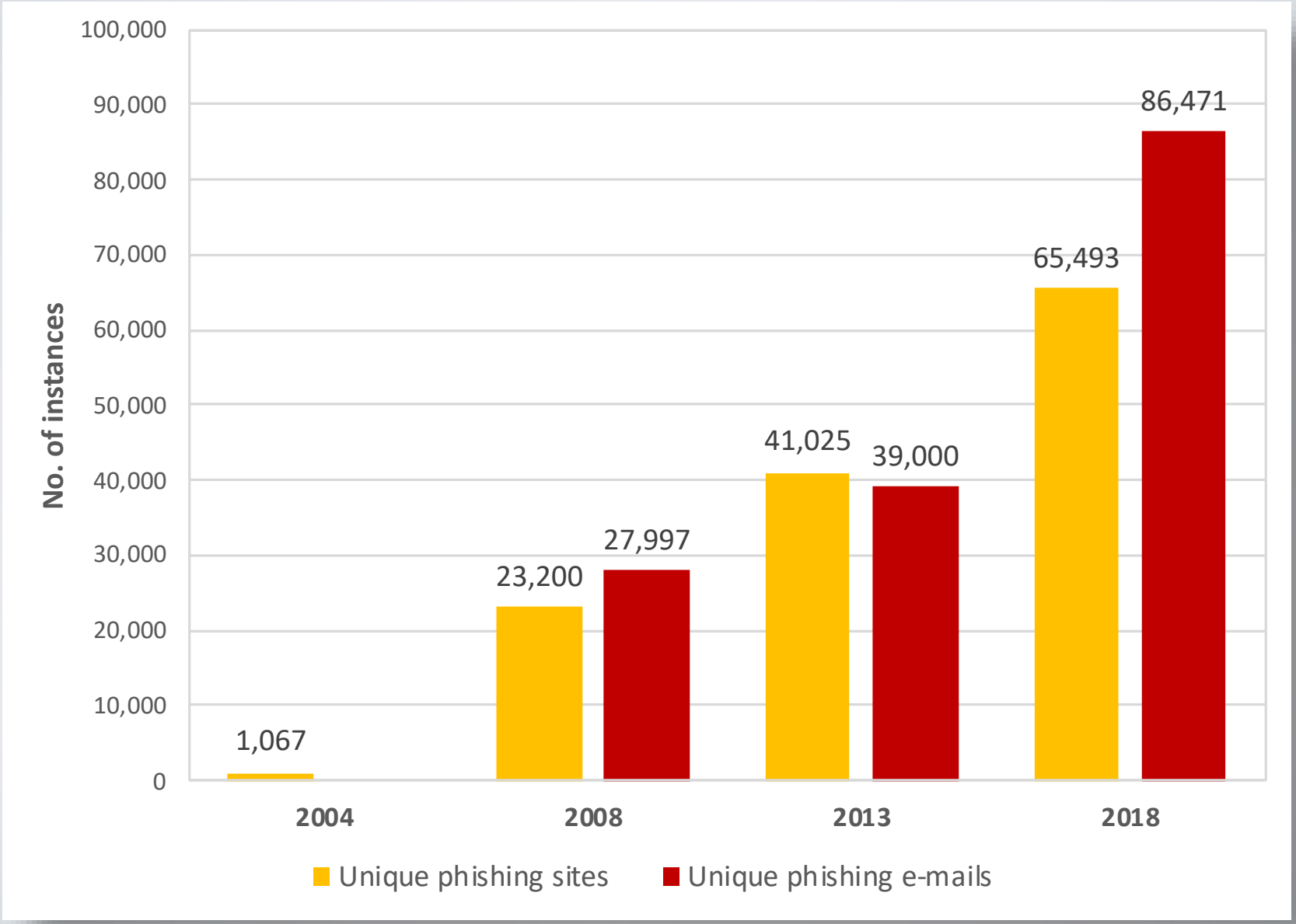
https://oagquote.wixsite.com/plymouth

Best Regards
Professor Julian Chaudhuri
Deputy Vice-Chancellor, Education and Student Experience

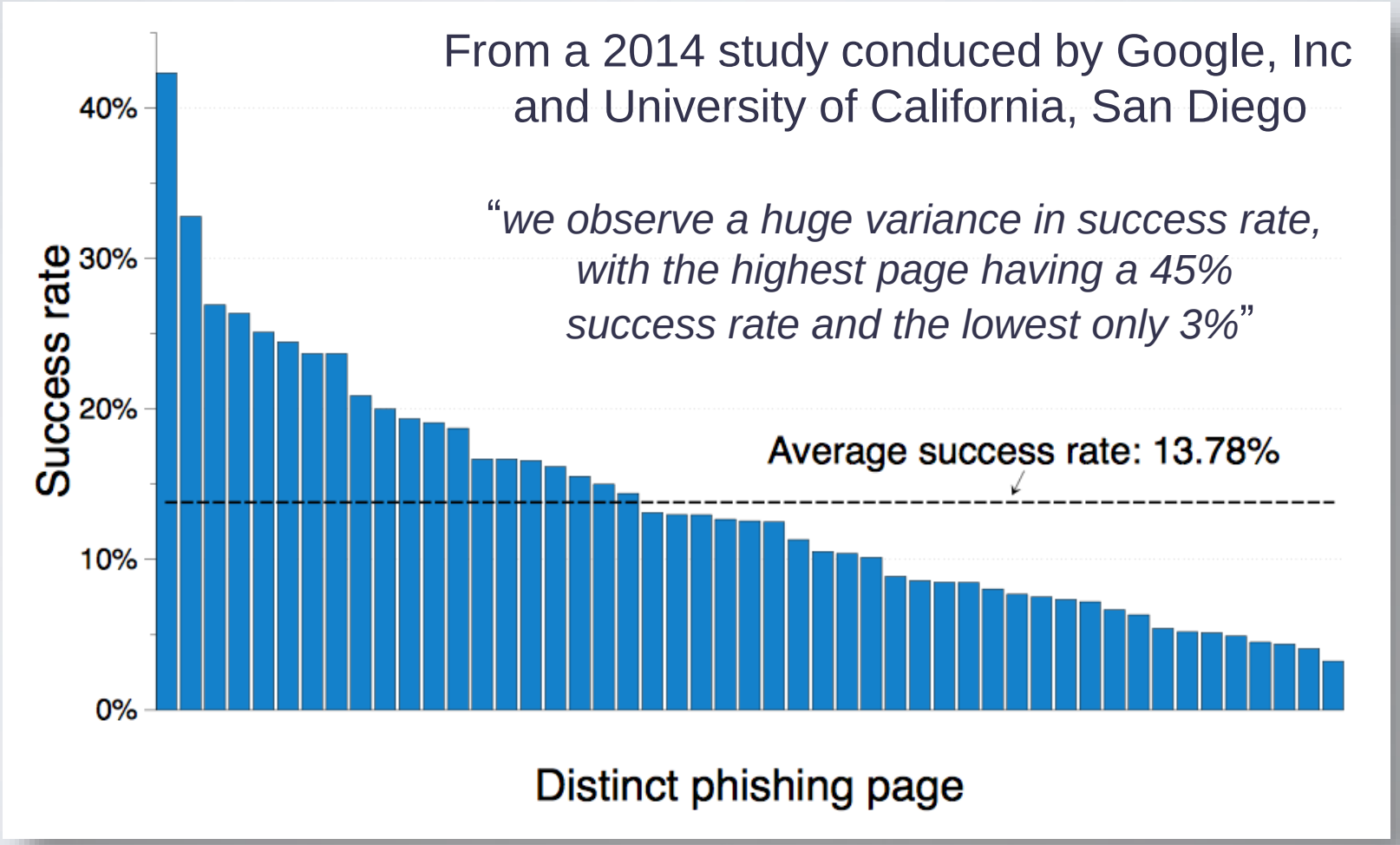
The Phishing Threat

- A combination of social engineering and technology-based deception that attempts to dupe users into divulging sensitive information
- Many phishing messages are sent in a very generic manner (i.e. indiscriminate mass-mailing, spamming)
  - e.g. banking phishing messages that are received by people who do not even have an account with the impersonated bank
- Other phishing attacks are more targeted
  - ‘Spear-phishing’ and ‘Whaling’
  - the abundance of personal and business information online already makes it easier to target the attacks

Phishing – Then and now



Phishing . . . works



(**Source:** Bursztein et al. 2014)

The Phishing Threat

- Our exposure is a function of our use of online services
  - the more benefits we get then the more risk to which we're exposed (esp. if not aware)
- Many users are unaware of the ease of spoofing a message
  - simply seeing a logo will convince many that it must be legitimate
- Convincing and persuasive message content can then be used to seal the deal …

Scammer Grammar

- For many, the poor use of grammar can be an indication that a message is bogus
- However, it can also be used as a *deliberate* technique by the scammers to filter out the more alert users
  - i.e. those that still follow the link may be less educated, and therefore more vulnerable to exploitation
  - particularly relevant to contexts such as 419 scams where further interaction with the victim may be involved

Spotting the signs?

- Phishing attacks have become more sophisticated
  - progressively more difficult for those targeted to distinguish them from genuine correspondence
  - this difficulty is directly related to advances in the social engineering and deception methods used by the attackers
- A past PU study examined the extent to which users could distinguish between legitimate emails and illegitimate messages . . .

Do they know me?

- From the APWG website:

"*phisher emails are typically NOT personalized, but they can be. Valid messages from your bank or e-commerce company generally are personalized, but always call to check if you are unsure*"

Getting speared

- Phishing tries to *gather* personal info
  - How much more can be gathered, if some personal details are already known, in order to further tailor the message?
- Increasing potential for spear-phishing based upon information available online
- Use of the psychological triggers may mean that recipients are already on the back foot
  - personalisation can only add to this

Spear phishing example

- MacEwan University in Edmonton, Alberta defrauded of $11.8 million in August 2017
- Member(s) of staff fell for an email request to change the electronic banking details held for one of the university's major vendors
  - the change was made without verifying the legitimacy of the sender
  - funds were transferred into an account controlled by fraudsters

www.infosecurity-magazine.com/news/macewan-defrauded-118mn-phishing/

1 September 2017

Does it work?

Quarter of USPS Staff Clicked on Phishing Link in Audit

A quarter of US Postal Service (USPS) employees clicked on a 'phishing email' designed to test their security awareness in an audit this year, highlighting the ongoing challenge of training staff to spot potential cyber-attacks.

The Office of Inspector General conducted the audit in May this year but the results have only just been released this week.

It claimed that the Postal Service runs one of the largest corporate email systems in the US, with over 3.5 million emails sent to more than 200,000 accounts each day.

However, disappointingly, 789 of the 3,125 employees who took part in the exercise clicked on the link in the phishing email.

What's more, 93% of those that received the email did not report it to the organization's Computer Incident Response Team, as required by policy.

The audit revealed that 95% of those who clicked on the phishing link and 96% of those who took part in the exercise didn't complete the Postal Service's annual information security awareness training.

https://www.uspsoig.gov/sites/default/files/document-library-files/2015/IT-AR-16-001.pdf

Infosecurity Magazine

9 Oct 2015

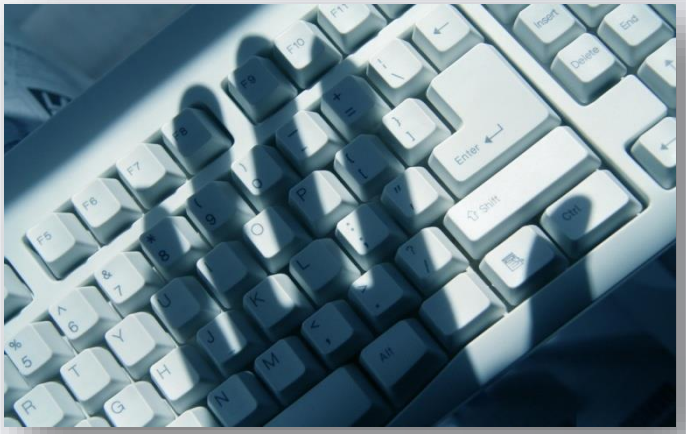
Phishing and cyber kill chain

- Menti, 3 students per group, 7 mins

1. (Individual read in 2 mins) Go to page 4 of the material "The ultimate guide to social engineering") and read the following example: "Hadnagy was once hired as an SE auditor to attempt to access the servers of a printing company whose processes … he says. "A malicious hacker would not think twice about using that information against him."
2. Identify what are Hadnagy's strategy/ means/ action in each step of Cyber Kill Chain (reconnaissance, weaponization, delivery, exploit, installation, command & control, action)
3. Agree on the answer and post to menti

Recommendations

- Use available technology
  - Phishing filters
  - Antivirus
- Improve user awareness
  - What do the attacks look like?
  - How would you legitimately be asked for information?
  - Appreciate the value of information
- Performing practical assessments
  - …without undermining trust



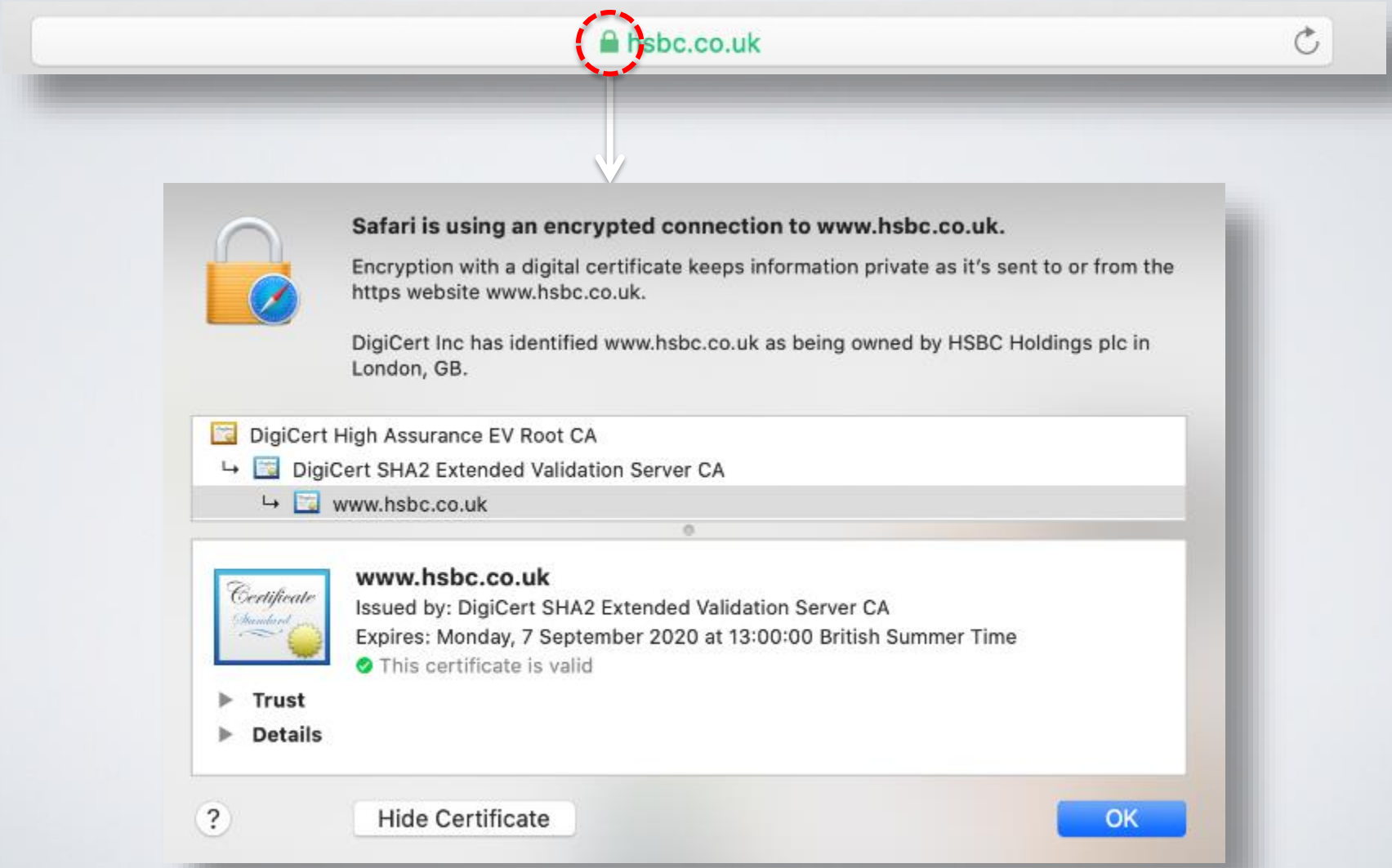
A LIST to remember

Legitimacy	Does the request seem legitimate and usual? Should you be asked for this information, and is this how you should normally provide it?
Importance	What is the value of the information you are being asked to provide or the task that you are being asked to perform, and how might it be misused?
Source	Are you confident that the source of the request is genuine? Can you find a way to check?
Timing	Do you have to respond now? If you still have doubts, take time to make further checks or ask for help.

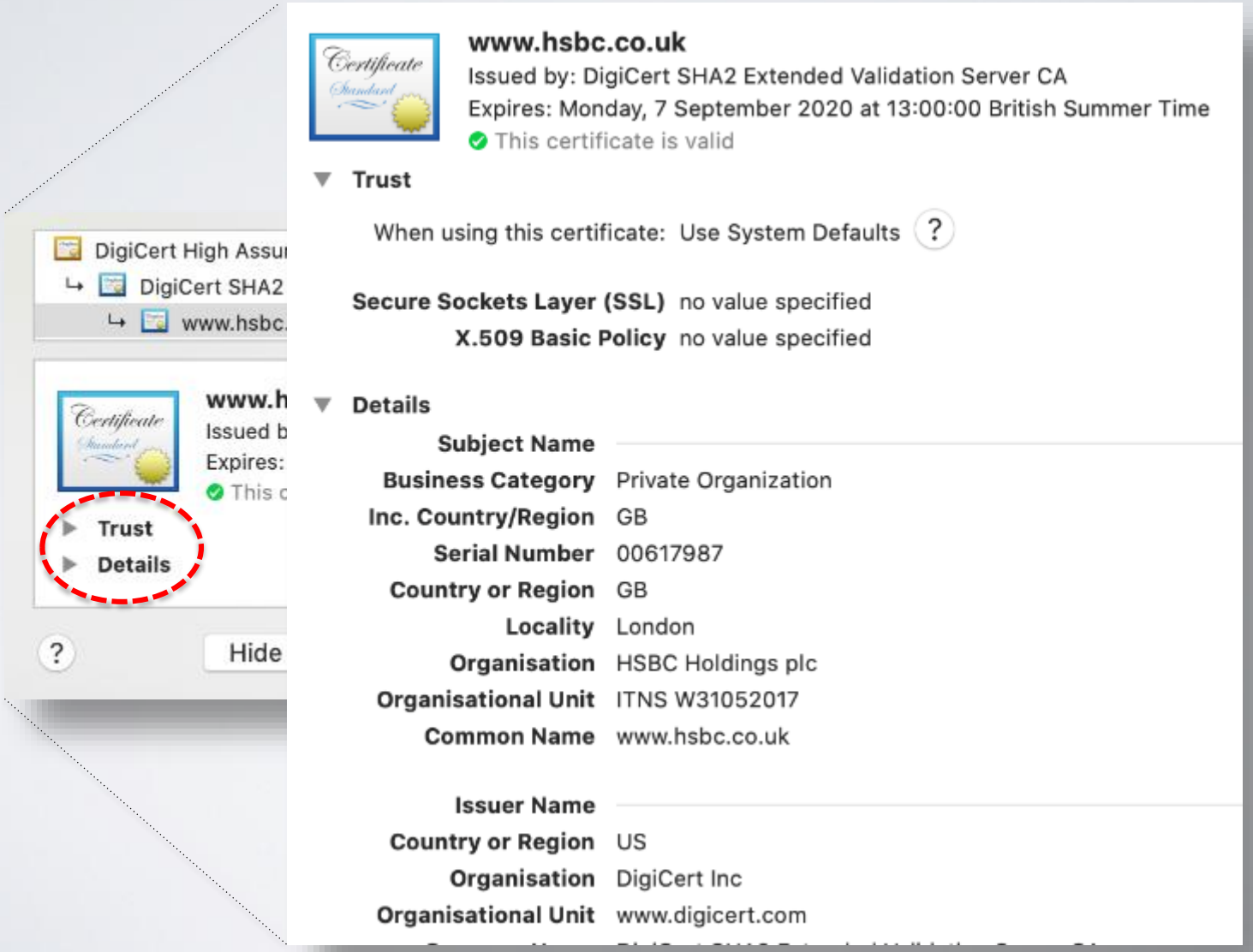
Phishing avoidance

- Think about what the message is asking for
  - use the LIST
- Avoid following links directly within emails
  - enter the expected address manually in the browser
- Look for secure sites – https, lock, ***certificate***
- Keep an eye on your key online accounts
  - logging in regularly will enable you to spot misuse

Looking for legitimacy



Looking for legitimacy



Looking for legitimacy

- Menti, individual
- Go to the university website and identify the following information from the digital certificate
  - Organization
  - Location
  - Common name
  - Organization that issues the certificate
  - Valid date time of the certificate

Reporting phishing scams

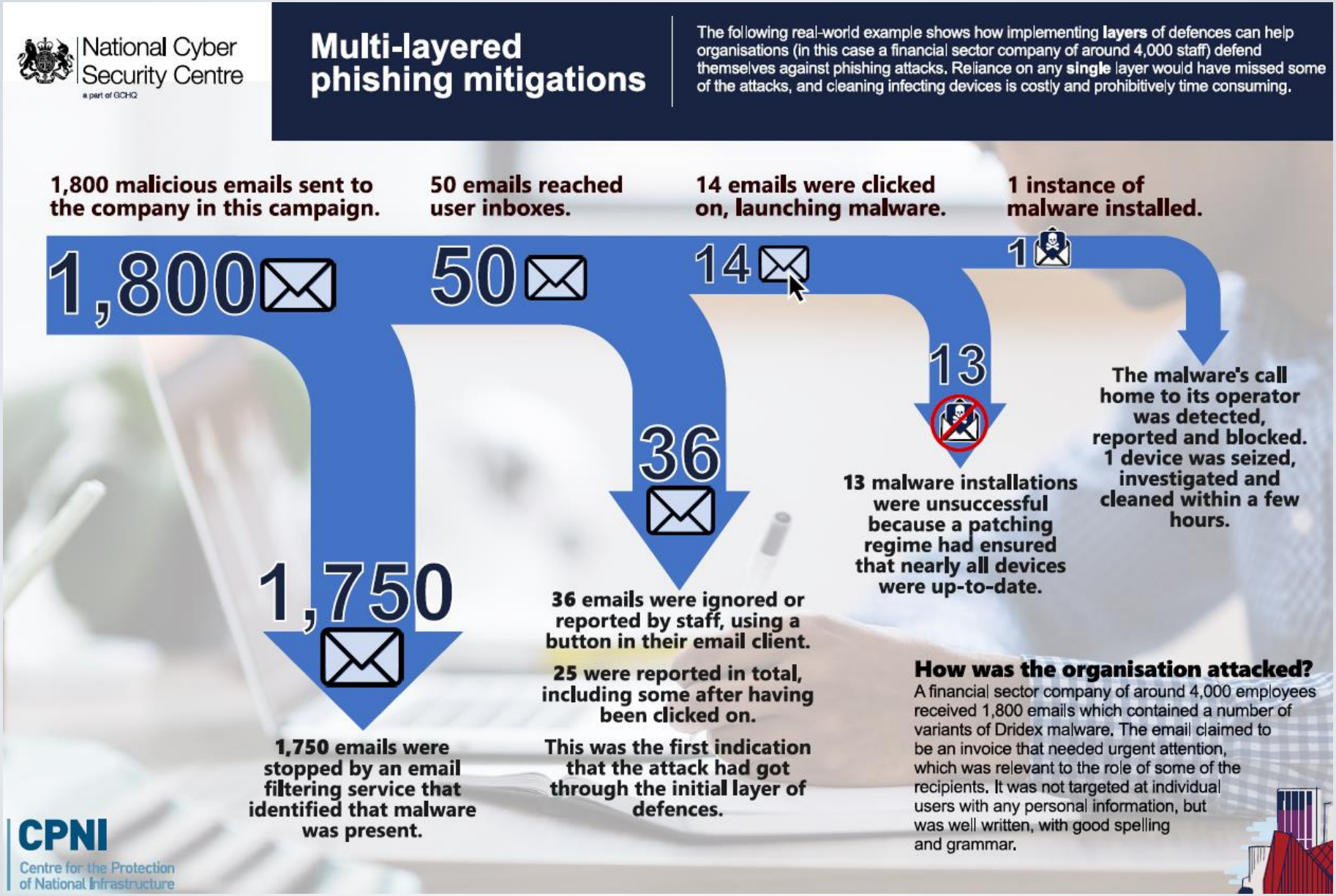
- Suspect emails can be forwarded to the APWG (anti phishing working group)

reportphishing@antiphishing.org

- and/or directly to the organisation that is being spoofed, e.g.

spoof@paypal.com

Phishing attacks – defend your organization



Phishing attacks – defend your organization

National Cyber Security Centre
a part of GCHQ

Phishing attacks:
Defending your organisation

A multi-layered approach - such as the one summarised below - can improve your resilience against phishing whilst minimising disruption to user productivity. This approach provides multiple opportunities to detect a phishing attack and stop it before it causes major harm. The mitigations included are also useful against other types of cyber attack.

LAYER 1
Make it difficult for attackers to reach users.

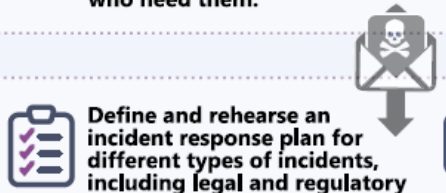
- Implement anti-spoofing controls to stop your email addresses being a resource for attackers.
- Consider what information is available to attackers on your website and social media and help your users do the same.
- Filter or block incoming phishing emails.

LAYER 2
Help users identify and report suspected phishing emails.

- Relevant training can help users spot phishing emails, but no amount of training can help them spot every email.
- Help users to recognise fraudulent requests by reviewing processes that could be mimicked and exploited.
- Create an environment that lets users seek help through a clear reporting method, useful feedback and a no-blame culture.

LAYER 3
Protect your organisation from the effects of undetected phishing emails.

- Protect your accounts: make authentication more resistant to phishing (such as setting up 2FA) and ensure authorisation only gives privileges to people who need them.
- Protect your users from malicious websites by using a proxy server and an up-to-date browser.
- Protect your devices from malware.



LAYER 4
Respond quickly to incidents.

- Define and rehearse an incident response plan for different types of incidents, including legal and regulatory responsibilities.
- Detect incidents quickly by encouraging users to report any suspicious activity.

CPNI
Centre for the Protection of National Infrastructure

Conclusions

- Phishing remains a problem and has grown in sophistication
- Targeted content makes the scam far harder to spot
  - requires more effort but may increase as easier routes are closed off
- May be the death knell for generic phishing
  - user expectation of personalised online services
  - no longer give credit to communications that don't seem to 'know' them
- Will still require the combination of technical safeguards and user awareness

2-min paper

- Menti, individual

1. Write down something you learn today that you did not know before
2. Write down something you are not still sure/ struggle with

UNIVERSITY OF PLYMOUTH

Dr Hai-Van Dang
hai-van.dang@plymouth.ac.uk

Centre for Security, Communications & Network Research
www.plymouth.ac.uk/cscan