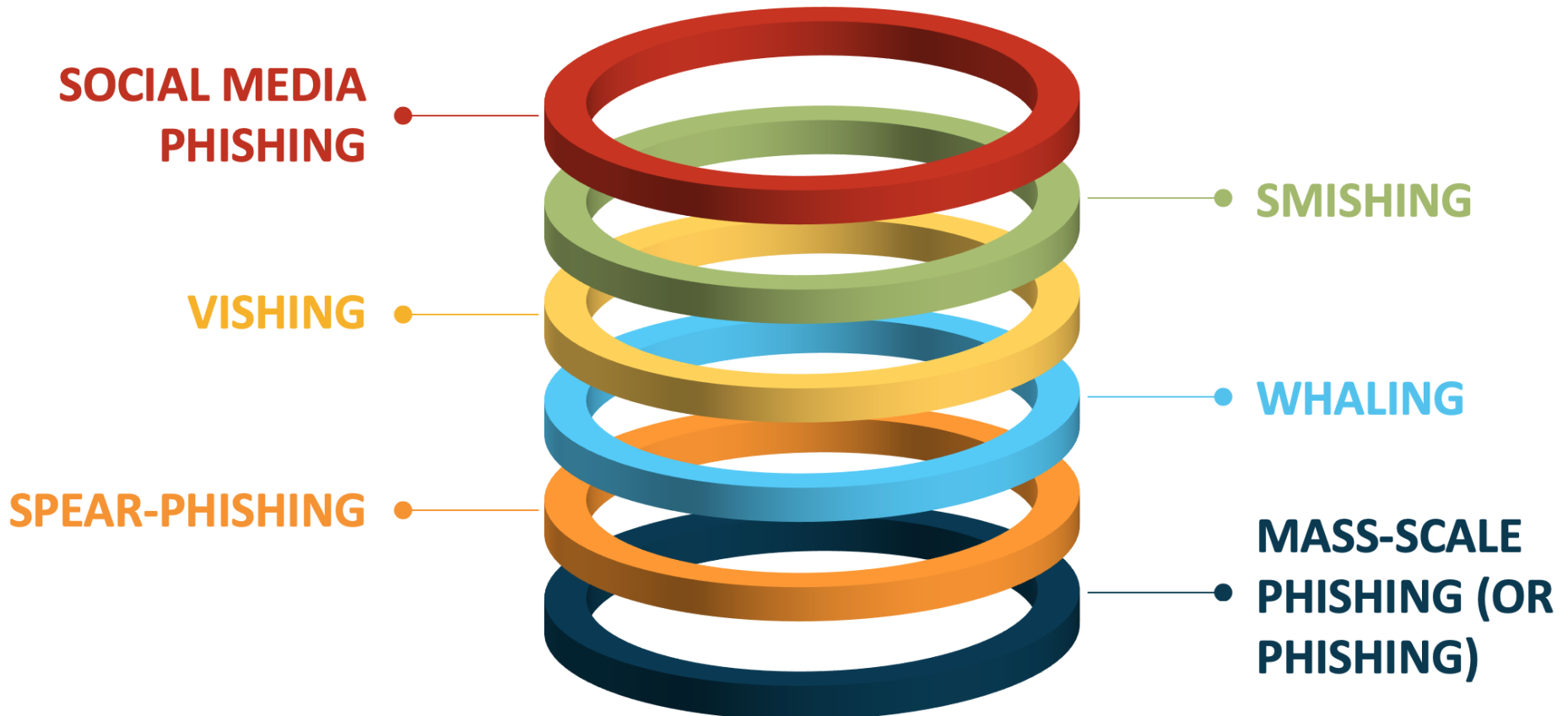


Phishing and Social Engineering Awareness



Introduction

What are we going to cover today?



What is a phishing attack

WARWICK

Phishing can be defined as *“the **fraudulent attempt or technique** to obtain sensitive information such as usernames, passwords and credit card details and many more by disguising as a trustworthy entity in an electronic communication.”*

Van der Merwe et al. (2005) and Ramzan, Zulfikar (2010)



Analysing the phishing methods

There are 3 main Phishing methods:

Whaling

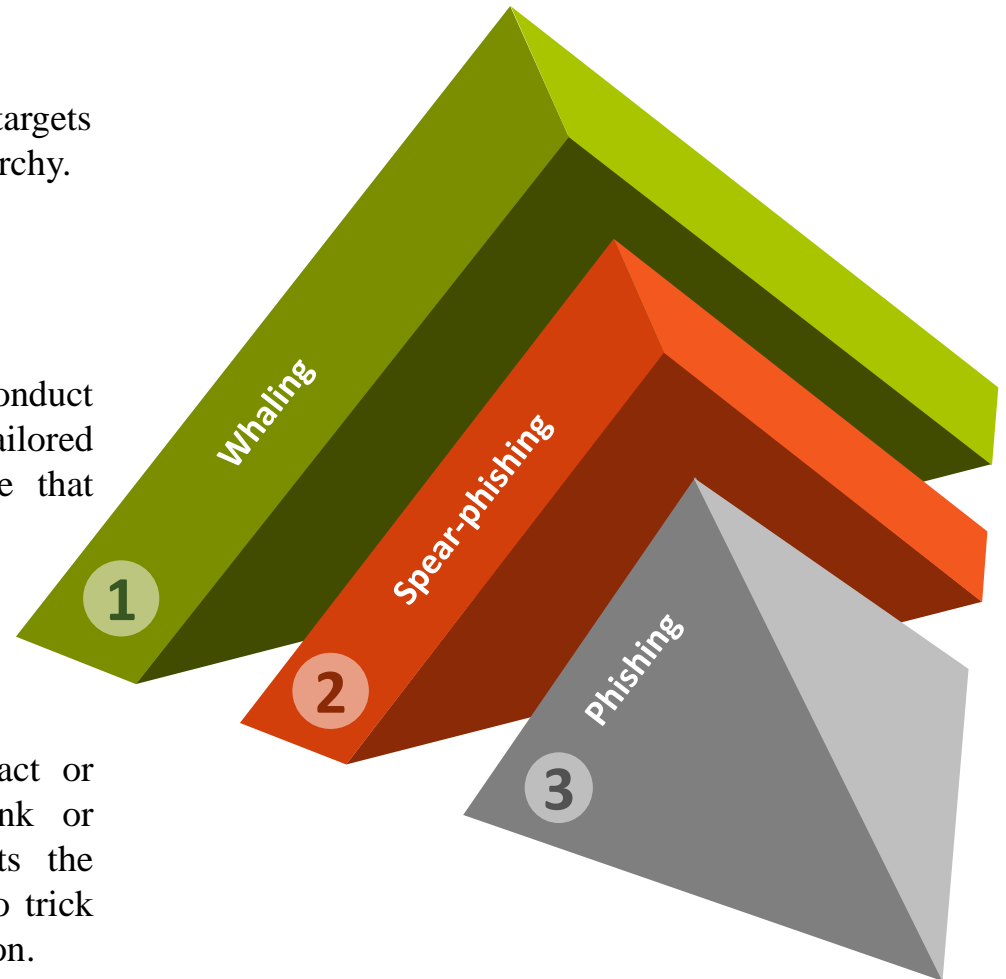
Is the same as a spear-phishing attack, but targets individuals high-up in the an organization hierarchy.

Spear-phishing

Is a form of phishing in which perpetrators conduct research on their targets first in order to create tailored emails. This method is often more effective that standard phishing.

Phishing

Are emails typically sent by a known contact or organization. These include a malicious link or attachment that installs malware or redirects the victim to a specific website that is designed to trick them into giving personal or sensitive information.



Consequences of phishing attacks

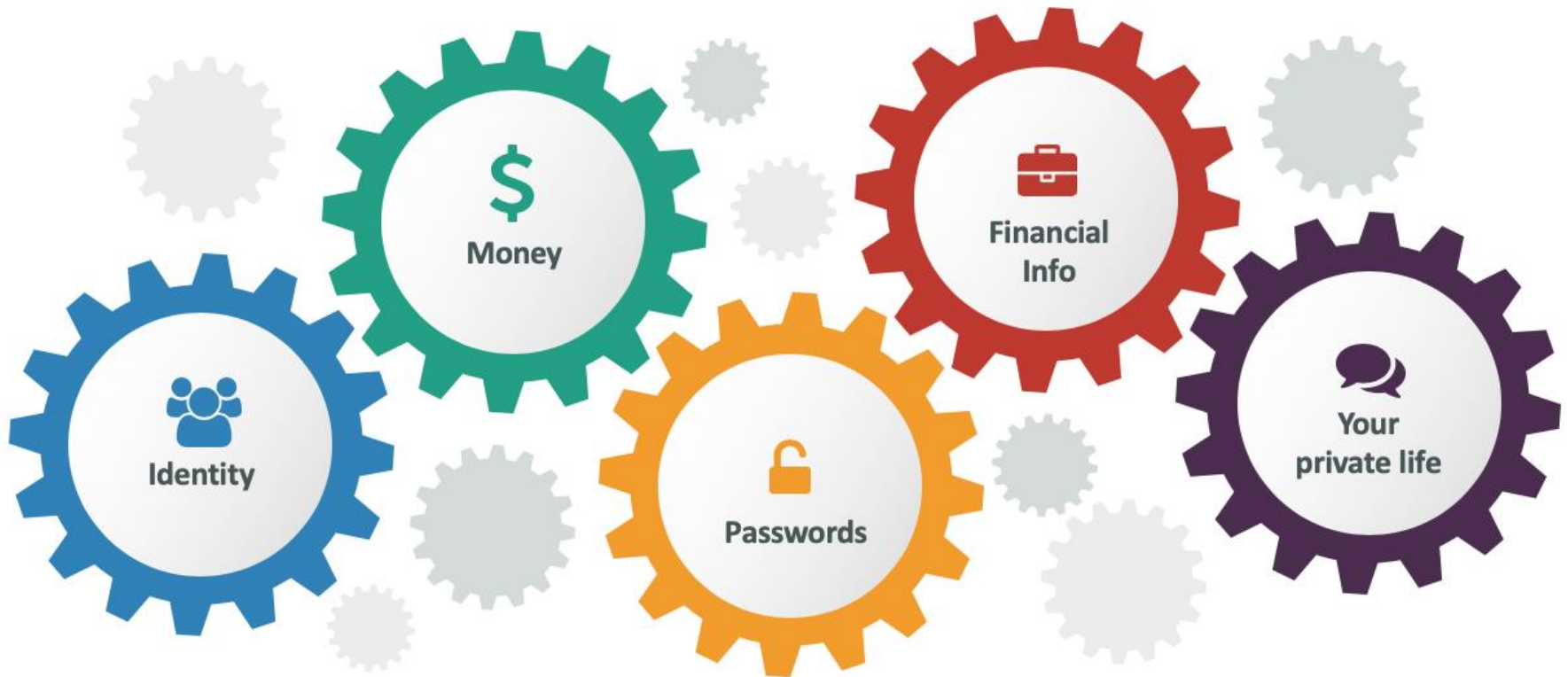


Bryan Littlefair (CEO of Cambridge Cyber Advises) said: *"If you have a breach, research suggests that 60% of your customers will think about moving and 30% actually do."*

Phishing Attacks – scammers' aims

WARWICK

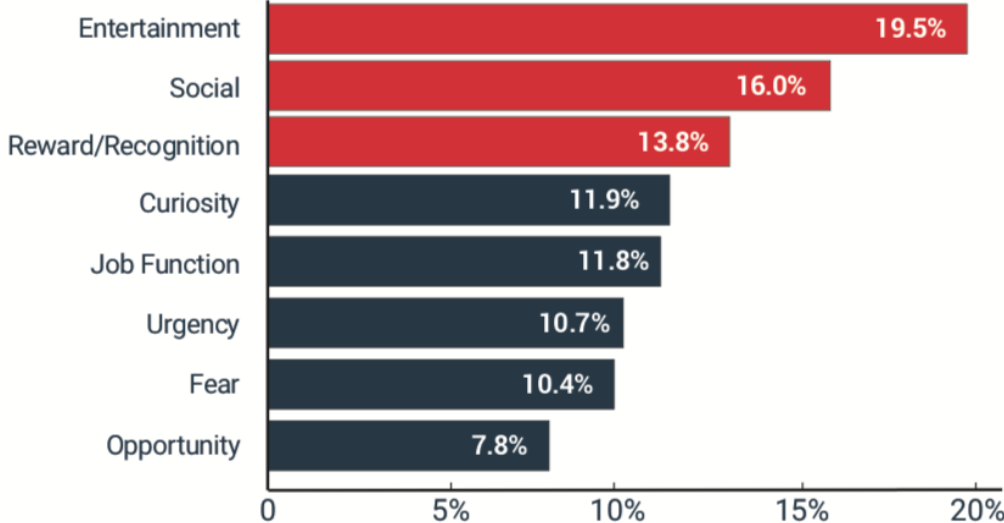
What scammers/cybercriminals want from you:



Cybercriminals methods – Why phishing works

WARWICK

It triggers you..



It gets you...

Phishing (Email)

WARWICK

Phishing or more specifically email phishing, is when fraudsters send **phony emails** that appear to come from valid sources, attempting to trick users into providing personal identifiable information, financial information or any other sensitive information.

They often utilize all the aforementioned methods (phishing, spear-phishing and whaling) depending on target and data set they want to

From: No replay Netflix@update.com [mailto:nacsafix036@1nitfix1nitfix2nitfix3.onmicrosoft.com]
Sent: Monday, July 11, 2016 10:19 AM
To: [REDACTED]
Subject: UpDaTe your PaYment MeThOd

NETFLIX

Please Update Your Payment Method

Hello,

Sorry for the interruption, but we are having trouble authorising your Credit Card. Please visit www.netflix.com/YourAccountPayment to enter your payment information again or to use a different payment method. When you have finished, we will try to verify your account again. If it still does not work, you will need to contact your credit card company.

If you have any questions, we are happy to help. Simply call us at any time on 0800 096 6380.

-The Netflix Team

Thu 21/02/2019 07:26
Bilal IQBAL <BIQBAL103@crownhills.leicester.sch.uk>
RE: Your Graduate Careers Enquiry

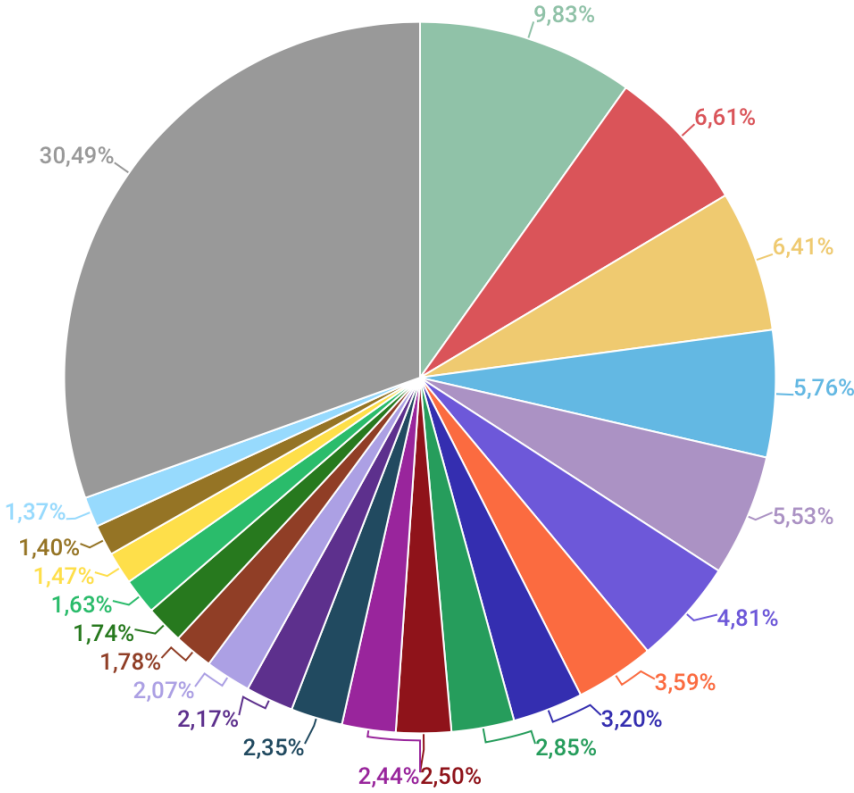
To: Marjorie Walsh

[If there are problems with how this message is displayed, click here to view it in a web browser.](#)

[Open message](#)

Marjorie Walsh
Please view this message in a separated window. Warwick
Bilal IQBAL

Countries targeted by malicious emails (2018 report)



- Germany
- Russia
- United Kingdom
- Italy
- Vietnam
- Brazil
- India
- United Arab Emirates
- Spain
- Taiwan
- Malaysia
- Portugal
- Turkey
- Hong Kong
- Japan
- United States
- Poland
- Mexico
- Bangladesh
- Indonesia
- Other

Source: Kaspersky Lab (<https://securelist.com/statistics/>)

Phishing scenarios(per emotional motivator) and percentages (2018)

Security

Scenario Name	Rate
Please Sign Online	23.6%
Internet Privileges Suspended	17.2%
Security Report	15.5%
Password Survey (Click Only)	11.8%
Data Breach (Attachment)	9.2%
PhishMe's CNBC Phish	7.8%
Password Survey (Data Entry)	7.3%
Data Breach (Click Only)	6.7%
Security Token Compromised (Data Entry)	6.5%
Security Token Compromised (Click Only)	6.5%

Employee Benefit

Scenario Name	Rate
Open Enrollment	39.2%
New Rewards Program	23.6%
HSA Customer Service Email	18.6%
Employee Satisfaction Survey	17.2%
Free Coffee	15.8%
Employee Raffle	15.5%
Cricket Big Basg Ticket Giveaway	14.6%
Free Lunch	14.3%
Cricket International Series Tickets	12.8%
Macro-Enabled Paid Time Off Request	11.9%

News and Events

Scenario Name	Rate
Ebola Outbreak	27.9%
Lunar New Year	17.8%
Halloween Costume Guidelines	16.7%
Cricket International Series Tickets	12.8%
News Alert	12.3%
Streaming Football Match	11.6%
Presidential Inauguration Live Streaming	8.9%
Brexit Impact on Operations	8.9%
Women's Euro 2017 Tickets	8.3%
Breaking News	7.9%

Computer/Software Update

Scenario Name	Rate
Browser Update Required	18.0%
Email Accounts to be Deleted	17.3%
Flash Update Required	13.4%
Email Migration (Data Entry)	11.8%
Computer Refresh Program	11.7%
Email Accounts to be Deleted (Data Entry)	7.4%
Email Migration (Click Only)	6.7%
Please Update Drivers	6.5%
Free OS Upgrade	6.3%
Required Mobile App	5.5%

Social

Scenario Name	Rate
Holiday eCard Alerts	24.8%
eCard Alerts	22.2%
St. Patrick's Day eCard Alert	19.7%
Thanksgiving Recipe	14.5%
Valentine's Day eCard	14.4%
Funny Pictures	9.7%
Brexit Forwarded Email	7.3%
Shared Folder	6.8%
New Chat App	6.2%
Forward From Manager	6.2%

Finances and Contracts

Scenario Name	Rate
Pro-forma Invoice - Indonesian	24.5%
Locky Phish	24.2%
Money Transfer Reversed	21.7%
Financial Information Review (Attachment)	20.9%
Macro-Enabled Scanned Image	19.6%
Pro-forma Invoice	18.5%
Financial Information Review (Click Only)	17.6%
Bonus Agreement	16.4%
Attached Life Insurance Policy Documents	16.0%
Macro-Enabled Attached Invoice	15.1%

Politics

Scenario Name	Rate
Rising Tensions in Korea	5.5%
Tension in the Crimean Peninsula	5.2%
Polling Center	3.8%
Election Polling (Click Only)	1.3%
Election Polling (Attachment)	0.5%

What about numbers?

UNABLE TO IDENTIFY



According to Intel, 93% of people cannot identify a sophisticated phishing email.

IMPACT



According to Wombat, 76% of businesses reported being a victim of a phishing attack in 2018.

NEW PHISHING WEBSITES



According to Webroot, nearly 1.5 million new phishing sites are created every month.

According to Aviva, Littlefair (CEO of Cambridge Cyber Advises) said: *"If you have a breach, research suggests that **60% of your customers** will think about moving and **30% actually do.**"*

Attacker techniques - Levels of Phishing attacks

Attackers will use different strategies, lets have a look:

Indicator	Level 1	Level 2	Level 3	Level 4
Expression (Receiver)	Impersonal (Anonymous)	Impersonal (Anonymous)	Personal	Personal
Links	Email contains links	Email contains links	Email contains links	Email contains links
Sender	Unknown (unrecognised email address)	Unknown (Unrecognised email address)	Email address that appears legitimate	Email address that appears legitimate
Messaging	Low intelligence message. Relying on greed, curiosity, fear, empathy.	Medium level of intelligence, relying on greed, curiosity, fear and empathy.	High level of intelligence, relying on greed, curiosity, fear and empathy.	Simple, on point email. Bradding can be used to lure the victim into clicking the link.
Vocabulary and grammar	Medium rate of misspellings.	Low level of misspellings.	Good use of grammar and vocabulary.	No mistakes regarding vocabulary and grammar.
Example	Common email, like lottery winner, inherited millions etc.	Results of assessments or health tests	Bradding email, advertising clothes or other deals.	<ul style="list-style-type: none"> Recruitment advert Payroll misconfiguration, please use that link to login

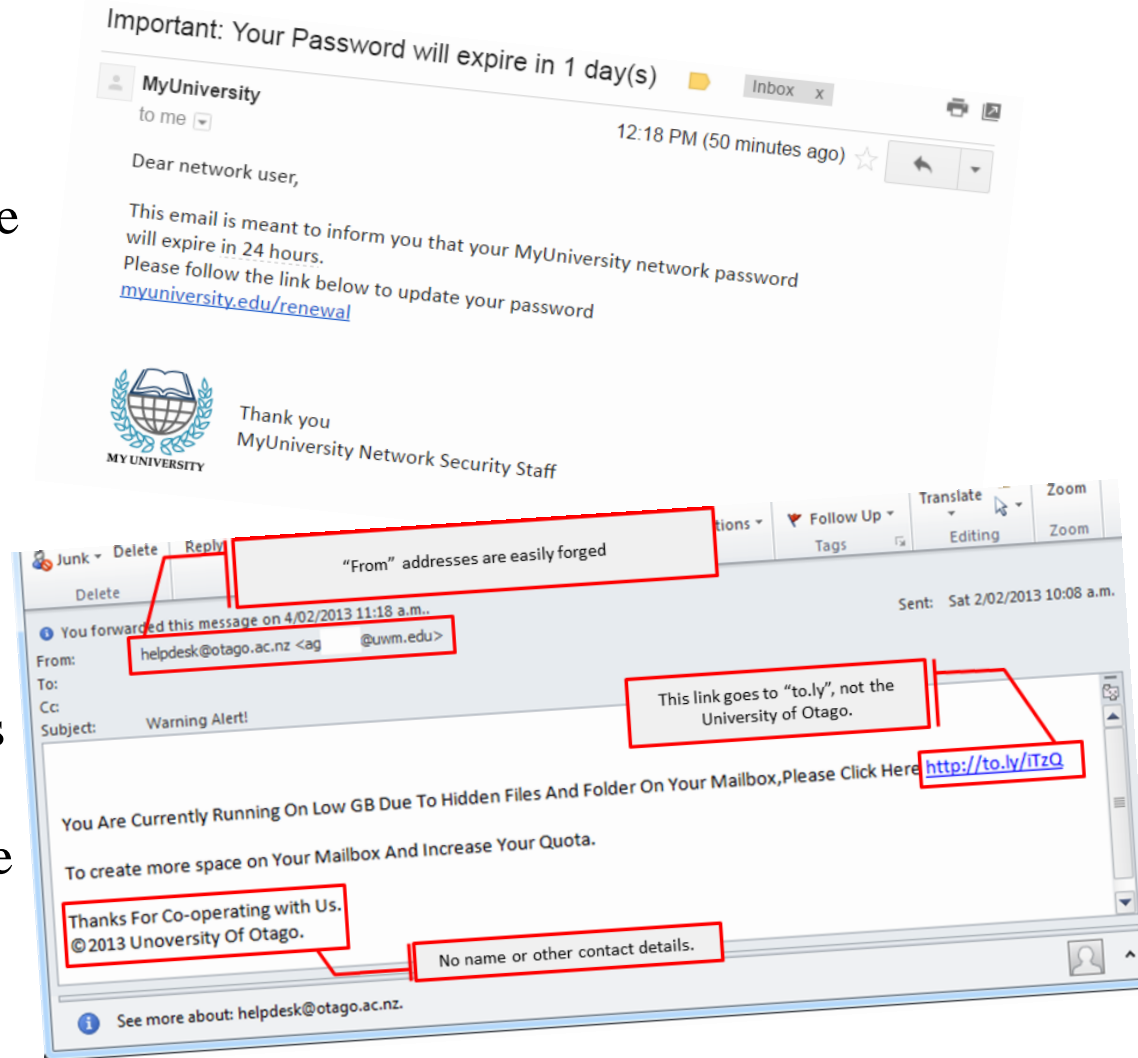
Phishing

Spear-Phishing

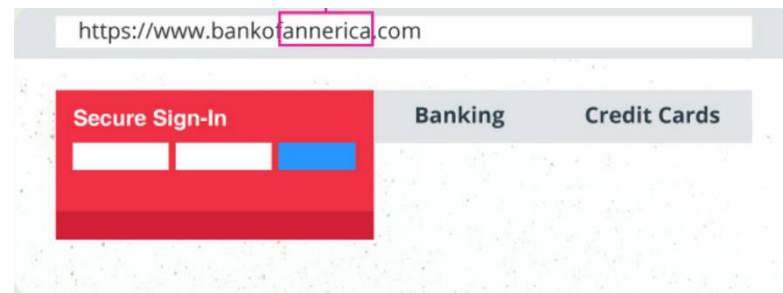
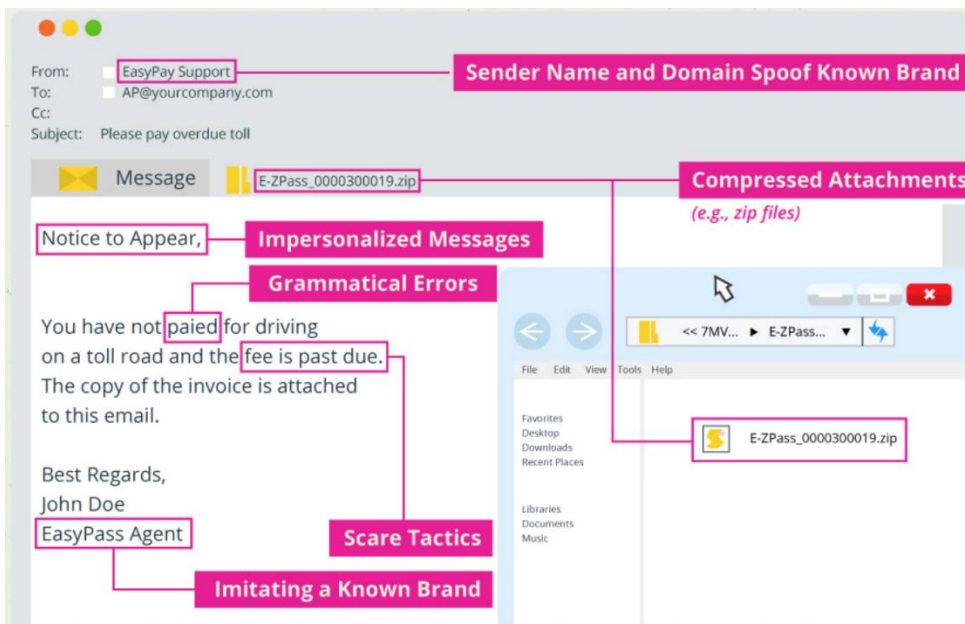
What to look for in an email

Some methods to check a phishing address:

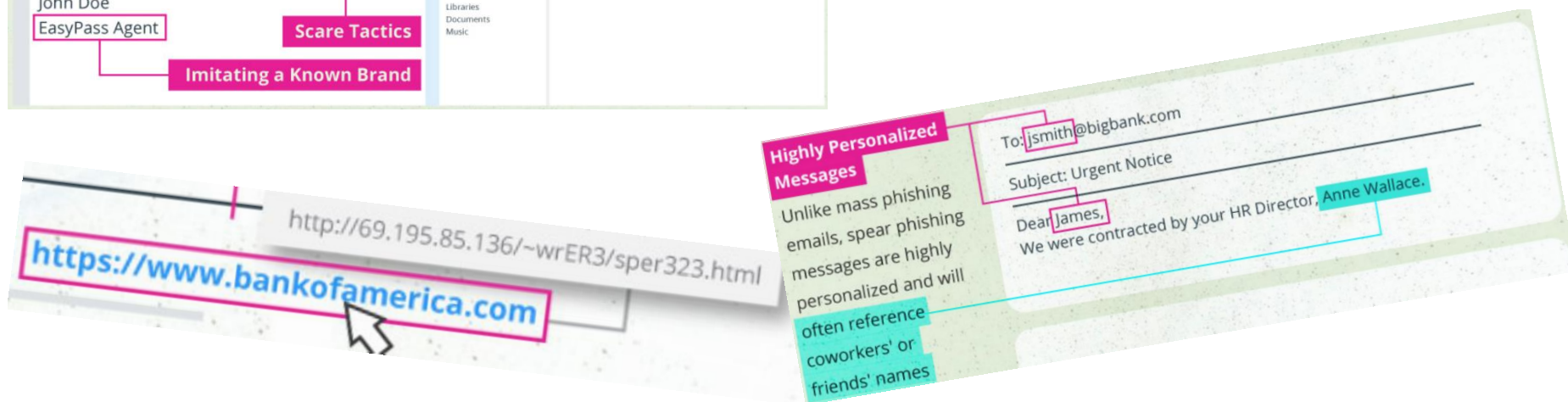
- Hover over the links to check the website.
- The email has an attachments you were not expecting.
- Might ask for personal information e.g. credit card information, passwords etc.).
- Poor email vocabulary and grammar. This might not always be the case.
- Emails that sound too good to be true (e.g. You won the lottery, a woman wants to meet you etc.).



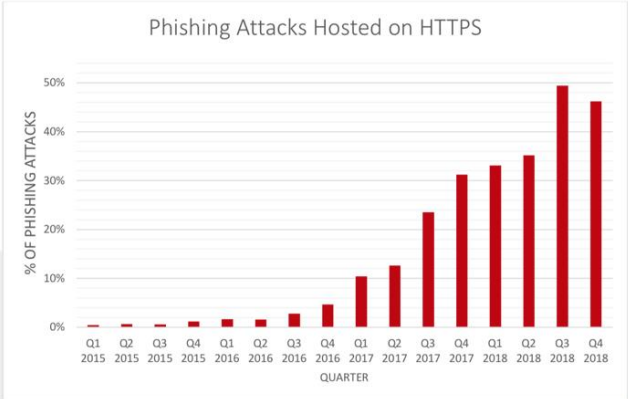
Additional examples of phishing emails



If something look suspicious, inspect it with scrutiny!



Https (Encryption) And Phishing websites



The majority of websites are using *https://* for secure communication (The locker you see behind the domain name)

1



2



Fraudsters are able to create phishing websites using digital signatures making the website looking https secure.

3



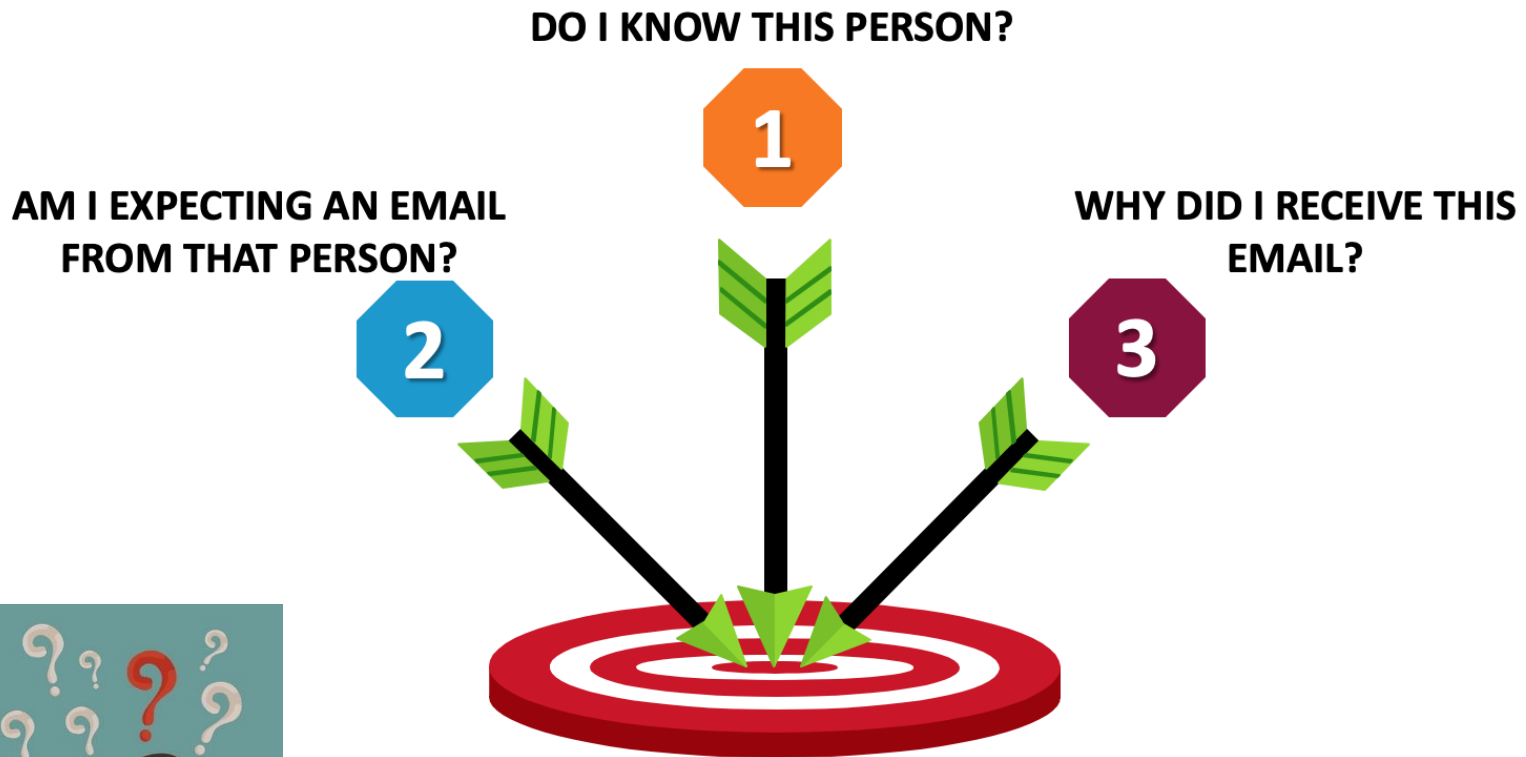
Therefore, a website being *https://* does not mean it is not a phishing website.

4



SO, WHAT CAN YOU DO?

Ask yourself (The 3Qs)



Be suspicious!

What to do when you suspect a phishing email?

- Do not click on any links in any email sent from unknown or suspicious senders.
- Do not forward an email that looks suspicious to friends, family or colleagues as this could spread a phishing attack to unsuspecting people.
- Do not download content that your browser or security software alerts you may be malicious.
- Do not give away personal information like your credit card number, home address, or social security number to a site or e-mail address you think may be suspicious. In general, any personal identifiable information.
- Fraudsters might use https to fool you into clicking a link.
- If you identify a phishing email, report it immediately to:
helpdesk@warwick.ac.uk

Can you spot why this email is a phishing attempt?

WARWICK

Reply Reply All Forward IM



Tue 02/04/2019 11:12

warwick.ac.uk - Support Team <finansije@hotelmoravica.rs>

[Reminder] Take action needed on account. Acc Id:48379biSun

To Informationsecurity, Resource

If there are problems with how this message is displayed, click here to view it in a web browser.

This email is from a trusted source.



One Time Verification

Hello informationsecurity

Please confirm e-mail password for informationsecurity@warwick.ac.uk to avoid login interruption.

Reason: (warwick.ac.uk) users email account password verification with outlook.

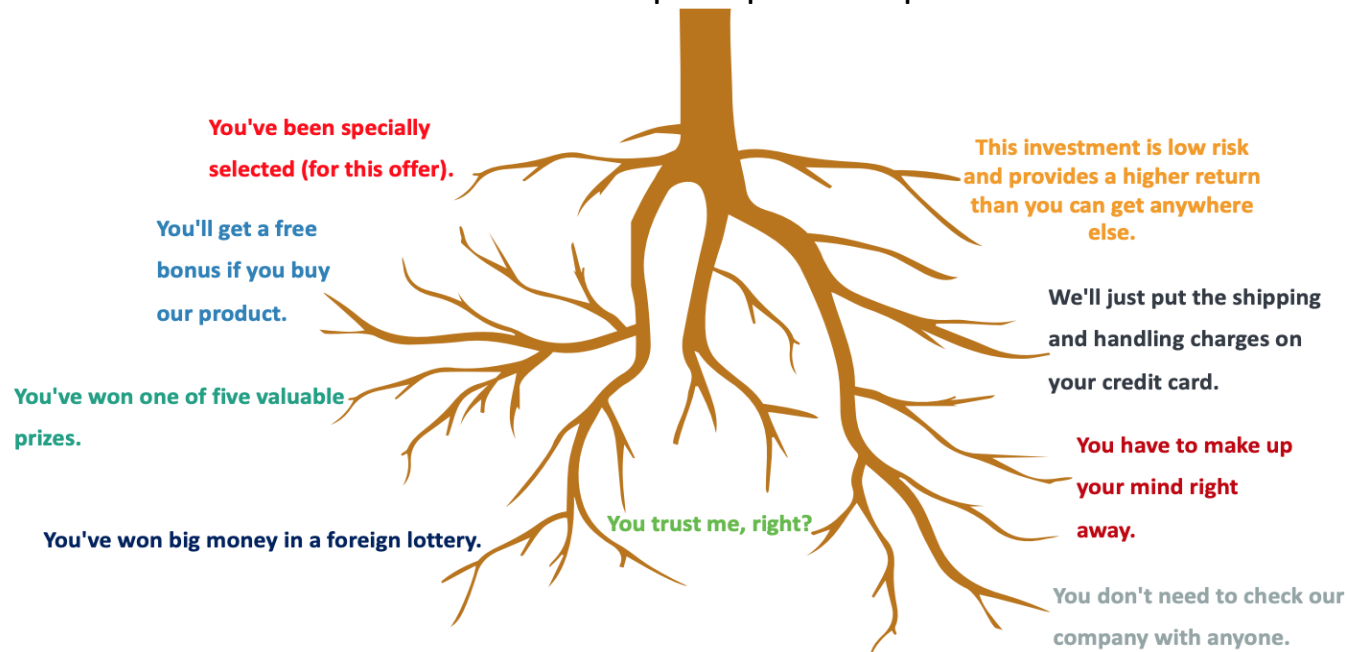
[Confirm](#)

© 2019 Office Microsoft Privacy & Terms

Vishing attacks

Vishing or “voice phishing”, tries to solicit unsuspecting people for personal or financial information. Beware because:

- They will sound very persuasive.
- They probably will know a lot about you because they gathered data from social media.
- They will use fear tactics in order to make you feel that you or your money is in danger.
- They may ask you to install software or for login credentials. **DO NOT TRUST ANY SOURCE THAT DOES THIS.** Vishers may claim they are from Microsoft, BT, IT Services or many other groups and ask for this. You will never be asked by a legitimate source for your passwords and you will never be asked by a legitimate source to install software via an unprompted telephone call.



What to do if you receive a vishing call

The logo for Warwick University, featuring a stylized white mountain peak above the word "WARWICK" in red, uppercase letters.

- Don't make a decision right away
- Personal Identifiable Information and bank information is personal. Keep it to yourself!
- Beware of offers that give you free money or offer help to recover already lost money.
- Google the number. Someone may have made a post alerting people about this number, or you might find that it indeed comes from a legitimate company.
- Some “vishers” may ask you to install software (e.g. TeamViewer), giving them access to your devices and accounts or ask for your log in information. Don't.
- If this occurs at work or relates to a work device or account, alert Information Security or ITS immediately.

“And now that I have been scammed once, I felt like it could not happen to me again.”

~ Vann Chow, Shanghai Nobody

SMShing attacks

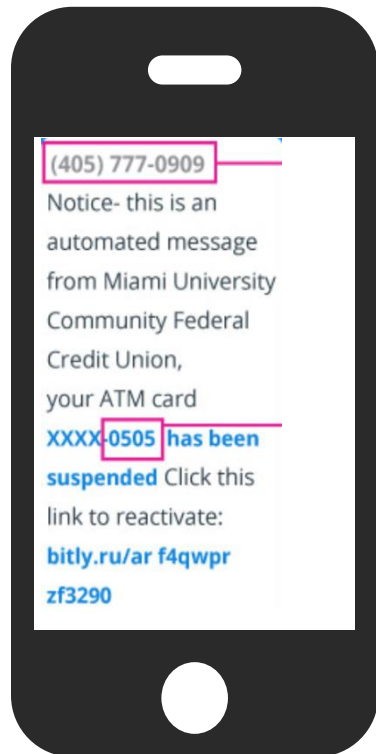
SMShing is the short form name of "SMS phishing" and refers to when SMS messages are sent by fraudsters attempting one of the following:

Steal personal and sensitive information

Inject malware in your phone

So, what to look for:

- Check for non-cell numbers (e.g.50000), most of scammers mask their identity
- Beware of links in messages, they will try to inject malware to your phone or steal information
- You should be suspicious when you receive SMS from unknown number or unsolicited messages
- They might use information to trigger your curiosity like the first digits of your debit card which is well known be everyone.



Social Media attacks

Social Media Phishing is when a fraudster use **social networking sites** (e.g. Messenger, Instagram, Twitter etc.) to obtain private and sensitive information or inject malicious software on devices.

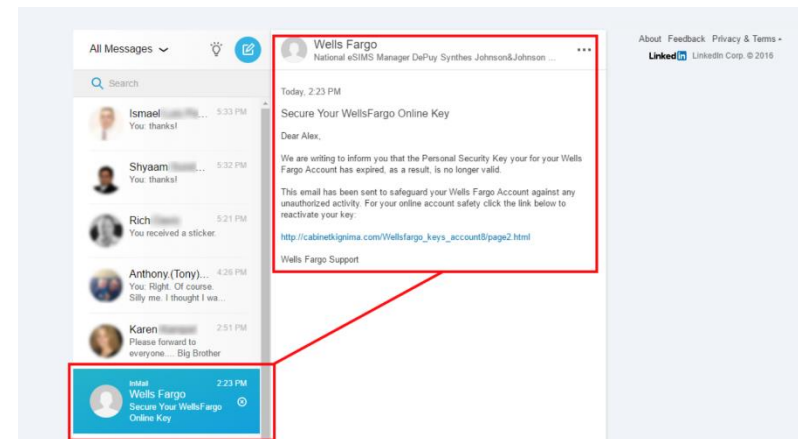
Catfishing

This involves scammers building false personalities online, building a deep relationship with targets, and ultimately scamming them in some way. Scammers will often manufacture romantic interest.

Doxxing

Your personal details like real name, address and contact information might be posted on public forums. This information is found through various means and can be exploited by scammers

An example from LinkedIn




Social Engineering (Physical engagement)

According to Dr. Robert Cialdini, there are eight principles of influence that scammers might use to achieve their goals:

- Reciprocity: People want to reciprocate to those who do kind things to us
- Obligation: Very similar to reciprocity, but it is based on social norms or expected behaviors
- Concession: To agree that something is true after first denying or resisting it
- Scarcity: When they offer something that is limited.
- Authority: When a person with the right kind of authority makes certain statements, other people may take them seriously.
- Consistency: Consistency is a sign of confidence and strength. This might make you believe the scammer.
- Liking: Scammers might say nice words to you in order to make you do what they want you to do.
- Manipulation: Scammers might use sensitive cases to make you do things you do not want to do.

Conclusion

- Be suspicious.
- Beware of unsolicited messages. Don't click on links, attachments, texts or *social media messages*.
- The University IT team will never ask for your password. Beware of any emails asking for passwords. Never send passwords, bank information or any other personal identifiable information.
- Never add personal Identifiable Information in pop-up windows opened after a clicked link.
- Look for **https** and the icon  before you consider any website safe. However, this does not mean it is not a malicious site, it just gives an extra hind.
- You can ask to contact the purported sender via a phone call to a number found on their official website.
- Last, report the incident to our ITS team.



And always be
suspicious!



THANK YOU!

References

- PhishMe Inc. 2017. Enterprise Phishing Resiliency and Defense Report [Online] Available from: <https://cofense.com/wp-content/uploads/2017/11/Enterprise-Phishing-Resiliency-and-Defense-Report-2017.pdf> [Accessed 06 March 2019]
- Pierluigi Paganini, 2015 New Intel Security study shows that 97% of people can't identify phishing emails [Online] Available from: <http://securityaffairs.co/wordpress/36922/cyber-crime/study-phishing-emails-response.html> [Accessed 05 March 2019]
- Pinsent Masons LLP, 2015, Info security professionals are business brand preservationists, says Aviva security chief [Online] Available from: <https://www.out-law.com/en/articles/2015/july/info-security-professionals-are-business-brand-preservationists-says-aviva-security-chief/> [Accessed 06 March 2019]
- Ramzan, Zulfikar (2010). "[Phishing attacks and countermeasures](#)". In Stamp, Mark & Stavroulakis, Peter. *Handbook of Information and Communication Security*. Springer. [ISBN 978-3-642-04117-4](#).
- Van der Merwe, A J, Loock, M, Dabrowski, M. (2005), Characteristics and Responsibilities involved in a Phishing Attack, Winter International Symposium on Information and Communication Technologies, Cape Town, January 2005.
- Vergelis M., Demidova N., Shcherbakova T., 2018 Spam and phishing in Q3 2018 [Online] Available from: <https://securelist.com/spam-and-phishing-in-q3-2018/88686/> [Accessed 03 March 2019]