



Credits to cathy_gig12 (2020) for creating the logo

A REPORT ON PHISHING

BY MS. NINA TUDNO JONES

ABSTRACT

In 2019, phishing scams caused a total loss of \$1.7million. After a reconnaissance, the sophisticated attacks target individuals with approaches which lie undetected until the damage is done. Accompanied with examples from genuine attacks, the report exposes these techniques and suggests methods of mitigation. The report then introduces an approach to user awareness training, in an ambition to protect Packets and Parcels from potential threats.

List of figures	2
List of tables	3
1.0) Introduction	4
1.1) Assumptions:	5
1.2) Challenges:	6
2.0) Main Part	7
2.1) Definition – What is Phishing	8
2.3) A Brief History of Phishing	10
3.0) The Penetration Test	12
3.1) Phase One, the Pre-Attack Phase.	13
3.2)Phase Two, the Attack-Phase Together with the Results.	15
4.0) The Attacks Explained	17
4.1) Social engineering	19
5.0) The consequences of Phishing	39
6.0) Awareness Training	43
Boot camp	43
The use of Games	43
The Quiz	45
Conclusion and future work.	55
References	58

List of figures

Logo: cathy_gig12, (2020)

<i>Figure 1: Person Holding Credit Card (Pixabay, 2016)</i>	<i>4</i>
<i>Figure2: The AOHELL H.L.P. file (Aolwatch.org, 1995)</i>	<i>10</i>
<i>Figure 3 Risk of attack (7 Penetration Testing Phases to Achieve Amazing Results – CyberX, 2018)</i>	<i>15</i>
<i>Figure 4: Phishing Techniques that phish explicit details (Jones, 2020)</i>	<i>17</i>
<i>Figure 5: Phishing attacks where social engineering is not required (Jones, 2020)</i>	<i>18</i>
<i>Figure 6: Social Engineering Life Cycle (Imperva, n.d.)</i>	<i>20</i>
<i>Figure 7: A Potential Tailgating Incident (Clipart, n.d.)</i>	<i>21</i>
<i>Figure 8: Post-it Note on Computer Screen (Kelleher, 2018)</i>	<i>28</i>
<i>Figure 9: Lose Weight, Spoofed Address (Jones, 2020)</i>	<i>31</i>
<i>Figure 10: Lose Weight, Original Address (Jones, 2020)</i>	<i>31</i>
<i>Figure 11: Phishing vs Spear-Phishing (KnowBe4.com, n.d.)</i>	<i>32</i>
<i>Figure 12: Red Flags in a Phishing Email (KnowBe4, 2017)</i>	<i>34</i>
<i>Figure 13: Avoid Spoofing Scams (Federal Communications Commission, n.d.)</i>	<i>37</i>
<i>Figure 14: 2 Men Standing in A Warehouse Talking. (Tiger Lily, 2020)</i>	<i>45</i>
<i>Figure 15: Woman Standing on Front of High-rise Building (Chương, 2019)</i>	<i>46</i>
<i>Figure 16: Man Cleaning the Glass of Building(Immortal Shots, 2018)</i>	<i>47</i>
<i>Figure 17: How Not to Store Your Password (Jones, 2020)</i>	<i>48</i>
<i>Figure 18: People Inside A Bus Wearing Masks (Young, 2020)</i>	<i>49</i>
<i>Figure 19: Man Sitting on Gray Pavement (Onojeghuo, 2016)</i>	<i>50</i>
<i>Figure 20: Person Resting Their Hand on Table (Magni, 2019)</i>	<i>51</i>
<i>Figure 21: Focus Photo of Yellow Paper Near Trash Can (Johnson, 2018)</i>	<i>52</i>
<i>Figure 22: Macbook Pro on White Table (Thanyakij, 2020)</i>	<i>53</i>
<i>Figure 23: Man Wearing Brown Suit Jacket Mocking on White Telephone (Moose Photos, 2017)</i>	<i>54</i>

[List of tables](#)

<i>Table 1: Definitions from various dictionaries. (Jones, 2020)</i>	<i>8</i>
<i>Table 2: Phishing Attacks Evolved (Jones, 2020)</i>	<i>11</i>
<i>Table 3: The Phases of a Penetration Test (LanFang and HaiZhou, 2012; Cyberx, 2018)</i>	<i>12</i>
<i>Table 4: Successful methods of phishing by penetration testers (Jones, 2020)</i>	<i>16</i>
<i>Table 5: Effects of Awareness Training (Kumaraguru et al., 2007, p. 911)</i>	<i>35</i>
<i>Table 6: Percentage of Stolen Information. (Field, 2016, p.7)</i>	<i>39</i>
<i>Table 7: Percentage of Trained Employees (Field, 2016, p.7)</i>	<i>39</i>
<i>Table 8: Percentages of Hacking Due to Weak Security Measures (Ponemon Institue L.L.C., 2016, p. 6)</i>	<i>40</i>
<i>Table 9: Boot Camp recommendation (Jones, 2020)</i>	<i>43</i>
<i>Table 10: Games Motivate Learning (Sheng et al., 2007, p.8)</i>	<i>44</i>

1.0) Introduction



Figure 1: Person Holding Credit Card (Pixabay, 2016)

According to the 2020 State of the Phishing Report released by Proofpoint, as high as 88% of businesses experience spear-phishing attacks worldwide. Additionally, the Federal Bureau of Investigation (F.B.I.) informs that the financial losses from business email compromises (B.E.C.) accumulated to over \$1.7 billion (Federal Bureau of Investigation, 2020).

This issue of this report follows a penetration test towards the distribution company Packets and Parcels, as per request by the company's C.E.O. In the main part, the report begins with an introduction of the company, detailing facts relevant to the material. The report continues to define phishing, discussing various viewpoints before introducing a separate definition. A presentation of the brief history of phishing follows, including an example of the first official attack and briefly displaying how the attacks evolved.

Chapter 3.0) to 3.2) reveals the exploits the penetration testers took advantage of during their assessment and briefly mentions the techniques applied during the active phase of their test. Further, the results of the test categorize from low to extreme, but the report only mentions the elevated, high, and extreme exploits. A table uncovers these results at the end of chapter 3.2).

In chapter 4.0) to 4.7c), the report analyses the techniques by utilizing relevant references such as (but not limited to) case studies, relevant attacks, research, and articles. Not all techniques display with real events, though the report makes up for this by creating fictitious events in chapter 6.0) Awareness Training.

In the paragraphs concerning mitigation, the report focuses on successful, researched techniques to discuss forms to reduce the risk. Further, the results of the penetration test conclude with approaches to user awareness training, which may benefit Packets and Parcels, and in chapter 5.0), the report explores the consequences of phishing as a whole, mentioning some techniques which the report already discussed.

The final chapter compiles the available information and suggests specific steps Packets and Parcels should consider applying to train employees.

1.1) Assumptions:

- As definitions of phishing and social engineering often are crossed, a reinterpreted definition of each phrase decides what phrase belongs in each topic covered.
- The report assumes that the C.E.O. of Packets and Parcels is aware of the results of the penetration test. There is no need to detail all the steps taken. However, as some methods are relevant to the results, the report briefly mentions some of the methods applied by the penetration testers.
- Due to the facilities floor planning, it is possible to access the building within full from the main entrance, so long one has an RFID card which grants access.
- In the cases where the report mentions "plain sight", the report is strictly referring to cases where anything visible in the office buildings can tempt employees or social engineers to release the information visible to someone who does not have the legal right to claim it.
- Dissimilar approaches to the spelling of words and phrases may confuse the reader. One example is the word "shoulder-surfing". Identical spelling remains constant for the report, though quotes and direct citations where the words present disparately (e.g. shouldersurfing/ shoulder surfing) remain identical to the author of the citations or quotes. This concept also applies to grammatical errors or other mistakes detected in quotes, phrases, and expressions.
- The company in question is purely fictional.

1.2) Challenges:

- The definition of phishing is complicated and vast. To avoid mixing terminology and methods, the report should attempt to gather the definitions and redefine them as one.
- Due to the countless definitions of what phishing is, the history portion may be challenging to reiterate. The report should focus on what the C.E.O should find interesting.
- Other definitions are unclear or do not fit the description of a cybersecurity attack. In these cases, relevant research, articles, reports, and other papers set the grounds in defining the subject.
- There are several techniques practised in phishing. It would be preferable to cover all topics, but due to shortage of time and wording, the report should decide what areas are most relevant to a company.
- Some techniques interact with each other. The report attempts to cover this in the paragraphs where the topic is most relevant.

2.0) Main Part

Packets and Parcels

Packets and Parcels is a company which specializes in domestic and international delivery and transport. The chief executive officer learned about the increase of attacks towards company's, together with reading an article claiming "4 of the 5 top causes of data breaches are caused by human or process error, (Dutton, 2018)". Considering the information, the C.E.O. hired a team of penetration testers to simulate an attack towards the company, intending to discover and harden the weakest points.

The domain registered at "*pnpp.net*". The IT department registers all employees within the domain, and they each receive a business email address such as *user@pnpp.net*.

After the results returned, the C.E.O. called all employees to a meeting, explaining where the faults were and announced that all employees should expect substantial changes in the company's policies. The C.E.O. issued no blame, and the employees were in good spirits after the meeting. Additionally, the C.E.O. agreed with the financial department to designate a substantial amount of money which would sustain all changes.

The employee count of Packets and Parcels cumulates to 80 people as of which:

- 26 employees work in the warehouse (general labourers, loaders, forklift operators et cetera).
- 54 employees work in the office (C.E.O., C.O.O., a system administrator, janitor, C.F.O., operations manager, warehouse manager, transport coordinator, purchasing manager, accountants et cetera).

It is also worth mentioning that:

- The transporters are engaged through smaller, private, offsite companies, and have clearance to enter the building on appointment.
- Packets and Parcels have never focused on user awareness training before the penetration test.

Each month the company publishes a newsletter with articles including milestones, business changes, events, big wins (bragging rights), training opportunities, reminders and a featured "employee of the month". Anyone on the company's mailing list, most employees, previous employees, and clients receive the newsletter. On Packets and Parcels website, anyone can subscribe to the mailing list by typing in their details. There are currently 14582 email addresses on the mailing list.

A Security Access System controls the employees' access to the building with radio frequency identification (RFID). The RFID also functions as the company identification card displaying a picture of the employee with a Packets and Parcels logo, the employees' full name and the employees' role in the company. Guests are not required to wear a badge.

2.1) Definition – What is Phishing

When researching what phishing is, articles, reports and reviews all appear to have different viewpoints of the concept. Some publications offer an exact explanation, others offer examples of previous attacks, and lastly, some conclude that the reader already knows what phishing is.

A variety of dictionaries define phishing as:

Source	Definition
Collins (Collinsdictionary.com, n.d.)	<i>Phishing is the practice of trying to trick people into giving secret financial information by sending emails that look as if they come from a bank. The details are then used to steal people's money or to steal their identity in order to commit crimes."</i>
Merriam -Webster (Merriam-webster.com, n.d.)	<i>"a scam by which an Internet user is duped (as by a deceptive email message) into revealing personal or confidential information which the scammer can use illicitly."</i>
American Heritage (ahdictionary.com, n.d.)	<i>"To request confidential information over the internet or by telephone under false pretences in order to fraudulently obtain credit card numbers, passwords, or other personal data."</i>

Table 1: Definitions from various dictionaries. (Jones, 2020)

The Anti-Phishing Working Group. Inc (APWG) defines phishing as:

Phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social engineering schemes use spoofed emails purporting to be from legitimate businesses and agencies, designed to lead consumers to counterfeit Web sites that trick recipients into divulging financial data such as usernames and passwords. Technical subterfuge schemes plant crimeware onto P.C.s to steal credentials directly, often using systems to intercept consumers online account user names and passwords -- and to corrupt local navigational infrastructures to misdirect consumers to counterfeit Web sites (or authentic Web sites through phisher-controlled proxies used to monitor and intercept consumers' keystrokes) (Aaron, 2018).

Although the definition varies, acquiring personal data with the intent to steal money from a bank account, is a common event during a phishing attack. The multiple definitions may create uncertainty as to what to be aware of, which is apparent in the examples of various articles and campaigns which not only define phishing attacks adversely but also contradictory. In this example from Imperva, a business whose mission is to *"protect your critical assets from the ever-changing attacks of cybercriminals"*, they explain that *"Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers"* (Imperva, n.d.).

The diverse definitions are an issue to be mindful of when creating a program whose sole purpose is to raise awareness amongst employees.

What appears to define the attack is in the way the attack plays out, and by naming and defining these adverse methods, it is easier to raise awareness on common ground.

For this report, the definition of phishing bases itself on that set by The Anti-Phishing Working Group. Inc. In short:

*"Phishing is an umbrella term which
implores several techniques to acquire
personal details in pursuance of
illegitimately extracting money from a
victim."*

Ms. Nina Tudno Jones

2.3) A Brief History of Phishing

On Thursday, September 7th, 1995, American Online president Steve Case posted an email advising their users to "change their passwords". An excerpt from the email reads *"there have been some cases where certain individuals are passing themselves off as employees or representatives of America Online and then asking members at random for their passwords. Please know that this is not our policy - under no circumstances will anyone from AOL ever ask you for your password."* The email went on to inform that a security program was in place, and that discovered problems were to be fixed by a recently installed system software.

An article written by Mike Langberg published on September 8th, 1995, reveals that a program developed by a hacker named "DaChronic", offered several tools for attacking AOL, and distributed via the internet. The program was called AOHell, and among functions, it provided a "Fisher", which enabled a user to simulate an AOL official. This way, the hackers who enabled this function could ask members for password and/or credit card numbers (Langberg, 1995).

The AOHell Documentation made available the instruction for the fisher, which referred to the AOHELL. H.L.P. file.

CC/PW Fisher

Open the People list of some room like "New Member Lounge", then on AOHell, select the Phrase you want to use, then hit "Start". AOHell will IM everyone in that room pretending to be AOL staff, asking for their PW or their credit card information (which ever you told AOHell to do) Make sure you goto File|Logging on AOL and choose "Session" logging, open up a file you want the info to go to, then click on the "Log Instant Messages" box before you start the Fisher.

****ATTENTION**** Please read the AOHELL.HLP file for complete instructions before using the Fisher! It includes vital information you need to know before you use this feature!

Figure2: The AOHELL H.L.P. file (Aolwatch.org, 1995)

The phrase "*phishing*", where the "*ph*" phenome replaces the "f", derives from several instances. An article posted to Brighthub explains that phishing comes from the practice of phreaking, which is an illegal method of exploring telephone systems (Robson, 2011). Another report from 2013 mentions an article written by Ed Stansel. The article published in Florida Times Union on March 16th, 1997, states: *"Don't get caught by online phishers angling for account information"*. The report from 2013 elaborates on the hackers' language known as "*Haxor*", also synonymous with "*Leetspeak*". In Haxor, ASCII characters replace Standard English characters, and so "f" is replaced with "*ph*". The report also backs up the theory of "*phreaking*", and, referring to an article posted to Computerworld in 2004 explains that phreaking was conceived by John Draper, aka "*Captain Crunch*", who created the Blue Box, a program which *"emitted audible tones for hacking telephone systems in the early 1970's"*. The article written by Russel Kay (2004), informed that by 1996 a hacked account

was called "*phish*", and a year later phish were considered a form of currency traded amongst hackers. Ten phish were required to trade for a piece of hacking software.

Phishing attacks evolved

The AOL phishing attacks raised awareness among the users, along with generating detection and prevention methods towards the attacks. The detection and prevention methods required new methods of scamming, and so, the methods employed to hack evolved. Some substantial attacks include:

Year	Method	Reference
2001	Spoofed URL's tricked users to enter personal details, challenging the browser security model.	(Financialcryptography.com, 2005)
2003	The first known phishing attack towards a retail bank. The Commonwealth Bank targeted NetBank users via email, with the means to steal their credentials.	(Sharma, 2010)
2004	Phishing defines as a fraudulent activity where attackers deceive people into believing the attacker is trustworthy.	Financial Services Technology Consortium (2005) as cited in Abad (2005)
2006	Banks victim-blame in attempt to dispute customers phishing losses.	(Miller, 2006)
2007	6.3 million victims of a heist reported their customer's email addresses stolen, leading to the customers receiving spear-phishing emails.	(Sophos, 2007)
2013	The first ransomware attack, Cryptolocker, infected 250,000 PC's	(Kelion, 2013)
2016	A "fake president incident" attack on the Austrian aerospace parts maker FACC resulted in a loss of 42 million euros, consequently firing C.E.O. Walter Stephan. More on this in chapter 4.7).	(Nasralla and Croft, 2016)

Table 2: Phishing Attacks Evolved (Jones, 2020)

3.0) The Penetration Test

Months before the test, the employees were informed by their respective leaders to remain alert in consideration to cybersecurity. The company withheld any information about the penetration testers, the test, and the team from the employees. Only the C.E.O. and the head of the I.T. department were aware that a penetration test was to take place. The limitation of the scope focused on the employees inside the building of Packets and Parcels, including the infrastructure of the building.

Three steps were employed to carry out the penetration test upon Packets and Parcels, and the results of these steps set the basis of the course later in the report. The steps were decided based on the research provided by Wang LanFang and Kou HaiZhou (2012), and by the methods described in the website Cyberx (2018). When placing the steps next to each other, the approach presents as such:

Pre-attack phase	Pre-Engagement Actions
	Reconnaissance
	Threat Modelling & Vulnerability Identification
Attack phase	Exploitation
Post Attack Phase	Post-Exploitation
	Reporting
	Resolution & Re-Testing

Table 3: The Phases of a Penetration Test (LanFang and HaiZhou, 2012; Cyberx, 2018)

3.1) Phase One, the Pre-Attack Phase.

LanFang and HaiZhou's Study explains that the pre-attack phase concentrates on the investigation and exploration of the target (2012, p. 1680). The penetration testers reconnaissance revealed the weakest points they planned to exploit in the attack phase.

Investigation and reconnaissance of the company:

- Research information on personnel, internal system, contact details, building infrastructure, et cetera.
- Tailgating employees to breach the building.
- Acquire secure access via the company's radio frequency identification card.
- Social engineering revealing positions, technologies, and email-addresses, including No tech hacking such as dumpster-diving, shoulder-surfing, and tailgating.

After the reconnaissance, a threat vulnerability and identification process could proceed. Those results for Packets and Parcels were:

1: Due to the warehouse facility hiring new call substitutes weekly, it was easy to act as a new employee who had not received the access needed to enter the warehouse. Entering the office area was successful via several methods, here naming the top three:

- The employees in the warehouse did not have access to the office area. Since most supervisors resided there, all they had to do was ask any office employee for help to enter, and the employee granted them access.
- The penetration testers tailgated office employees through the main entrance and entrance to the office.
- The penetration testers posed as a company's regular service provider.

Access to the building was effortless due to the weak floor- planning:

2'nd floor:

- To access the building, one enters through the main entrance on the second floor.
- There was a discontinued reception area by the main entrance.
- To the right and across the reception area, there was a small cafeteria.
- The changing rooms were to the right after the cafeteria.
- The location of the meeting rooms was on the second floor.
- Straight ahead the stairs descended to the first (ground) floor.
- To the left, empty offices were available for rent.
- One empty supply room locked off with a pin tumbler lock.
- A cleaning closet with some chemicals and cleaning supplies. Unlocked.
- Two conference rooms at the opposite of the empty office space

Ground floor:

- The stair traversing down to the first-floor lead to Packets and Parcels head offices, and to the warehouse itself.
- The offices were mainly open-plan offices, though the 7 leaders whom each retained separate offices with doors which could be locked.
- The servers were securely locked in a separate room

- At the other side of the building – directly connected to the warehousing facility, an outside area for people needing a break had been created on the ground floor. There was no security connected to this area, welcoming any intruders.
- Two rooms with office supplies, both locked off with pin tumbler locks.

An RFID card secured all doors.

The penetration testers entered the locker-room via tailgating an employee. Due to the large number of employees working in the warehouse, there were not enough lockers available, causing the employees to store their valuables openly. Not all lockers were locked, and some were damaged, but still in use. Two employees had left their RFID-cards on their outfits which were not in use, and these were taken advantage of to gain access to the warehouse and offices the following days. Employees never challenged the penetration testers presence.

2: Some computer passwords and login information were visible on notes around the open office. The private offices had pin tumbler locks, but some doors were wide open. Critical information was visible hanging on the walls, lying on the desks and written on post-it notes.

3: Nobody questioned the "unfamiliar face" in the office facility. The penetration team entered the building at several different occasions: They alternated between gender and apparel, wearing clothes typically found in a warehouse, office or as maintenance.

4: Critical information belonging to customers, accounts, banking details, phone numbers and emails were accessible via dumpster-diving, shoulder-surfing, and information available in plain sight.

5: The penetration testers sent a spoofed email from techsupport@pnp.org containing a link reading: "Are you susceptible to phishing? Take this test to find out". The link was a redirect to a spoofed site identical to the internal webserver page and prompted the employees to log on with their credentials. After entering the login information, a redirection sent them to another page stating, "An error has occurred, please contact your system administrator and close this window". Out of the 52 employees working in the office who received the email, 46 employees (88.46%) clicked the link and carried on filling out the details. A keylogger recorded the input of the login information. Later it was discovered that 31 of the passwords (59.62% were a simple password (e.g. Password123). Only one employee (2.17%) reported the email to the system administrator.

6: The six employees who did not click the link received a follow-up phone call from a spoofed number which aimed to vish the credentials from the employees. Five employees (83.33%) fell for the attempt. The same employee who reported the email also did not fall for the Vishing attempt.

7: Three employees working in finance received a Deepfake vishing call mimicking the C.E.O. The goal was to force the employees to pay an invoice of 16.499 NOK (excluding V.A.T.) to an unfamiliar account. The two first employees fell for the scam, but after learning about the call over lunch, the third employee called out the scammer. The three employees reported the incident to the boss.

8: Personal items laid strewn on and around office desks. Car keys, house keys, purses and bags were easily accessible when the employees left their desks.

3.2)Phase Two, the Attack-Phase Together with the Results.

According to LanFang and HaiZhou, this phase engages the compromise of the company where the pen-testers exploit the vulnerabilities discovered in phase one (2012, 1681).

When looking at the points mentioned in the first phase, the penetration testers set up a plan to breach the system. The following are the results which, according to the report, harvested the most success. The calculated risk of attack by the possibility of the employees falling for the scam, ranged from "Low", "Moderate", "Elevated", "High" to "Extreme".

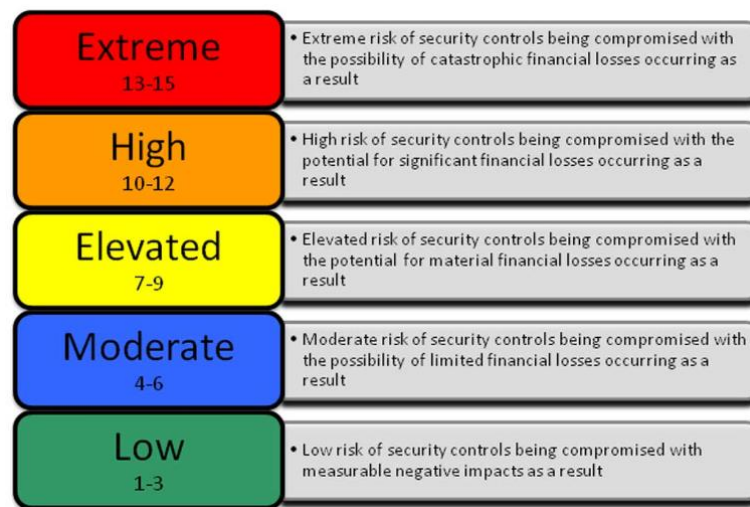


Figure 3 Risk of attack (7 Penetration Testing Phases to Achieve Amazing Results - CyberX, 2018)

Phishing Method	What medium	How	Risk of attack
Tailgating Also: No tech hacking	Physical	Tailgated employees using several excuses to gain access to the premises.	Extreme
Shoulder-surfing Also: No tech hacking	Office	While acting as maintenance, it was easy to gather information while shoulder-surfing.	High
Plain Sight Also: No tech hacking	Office	While acting as maintenance, it was easy to find information in plain sight.	Extreme
Tech Support Scam. Also: Spear phishing Also: Fake crisis notice	By a visually spoofed email	Sent an email from techsupport@pnp.org , claiming that there had been an insignificant breach, and the system needed a reset. An email requested the login and password information after the reset, to recover the user's data. The details (logo's, contact information) discovered in the office served to sign the email and make it as plausible as possible.	Elevated
Tech Support Scam 2 – Also: Vishing	By a spoofed phone number, using the information found in plain sight	Follow up phone call on the email to those who had not replied.	Extreme
Deepfake Vishing	By a spoofed phone number	Voice over Internet Protocol (VoIP) mimicking the C.E.O.'s voice, using a scare tactic to manipulate employees into paying an invoice	Extreme
Dumpster-diving Also: No tech hacking	Bins	Vital information like banking details, accounts, and unshredded documents lay strewn.	Extreme
Theft Also: No tech hacking	Physically removing personal items	Removed a bag containing personal items.	Extreme

Table 4: Successful methods of phishing by penetration testers (Jones, 2020)

4.0) The Attacks Explained

This section procures an insight of the attacks mentioned above. It also supplements explanations and consequences of the attacks, adding in examples which have happened previously. When revealing these methods, it is with the intent to implore a strategic shift to the employee's awareness. The results found in chapter 3.2) along with the following examples in chapters 4.0) to 4.7c) form the basis of the awareness program.

The Anti-Phishing Working Group. Inc mentions in their definition that social engineering is a technique used to phish. When researching social engineering, articles claim that phishing is a part of that technique. Although the definitions are contradictive, the context is the same: It is improbable that one does not come without the other. The diagram beneath illustrates that social engineering plays a significant role in phishing attacks.

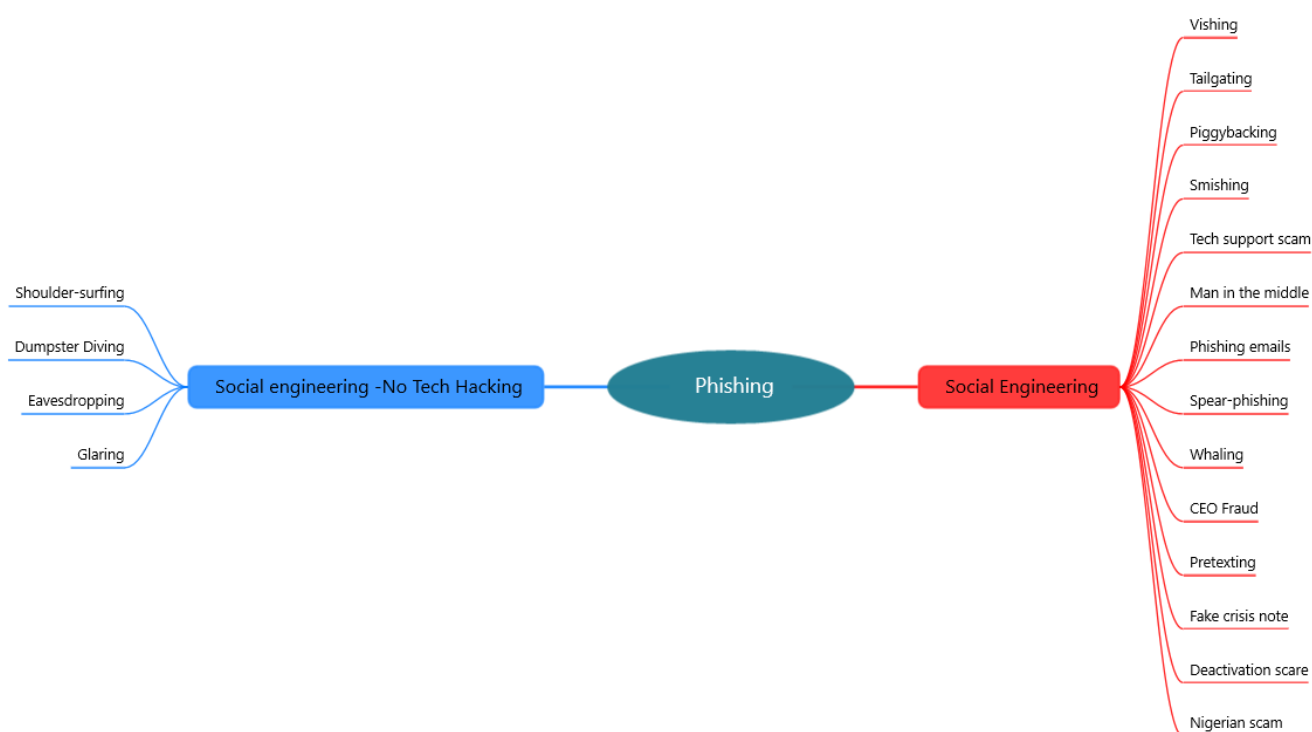


Figure 4: Phishing Techniques that phish explicit details (Jones, 2020)

In some instances, phishing attacks occur without the need to implement techniques used in social engineering, though the goal to "*...illegitimately acquire personal details in order to extract money from a victim*" remains.



Figure 5: Phishing attacks where social engineering is not required (Jones, 2020)

4.1) Social engineering

The results of the penetration test revealed that Packets and Parcels were at an extremely high risk to social engineering. According to Benny Carlsen, the first mention of the phrase "social engineer" is found in an article published in the New York Times in 1987. Two years later, another article published in the New York Times and written by William Tolman mentions "social engineering" as a verb (Carlson, 2005).

The definition of social engineering, according to the American Heritage Dictionary, is "The practical application of sociological principles to particular social problems." This definition does not appear to reveal why social engineering is essential to phishing, but CSOnline provides a more accurate description of social engineering in the context of internet security. A feature written by Josh Fruhlinger (2019) defines social engineering as "... *art of exploiting human psychology, rather than technical hacking techniques, to gain access to buildings, systems or data*".

This definition appears to be more accurate in describing the events that take place when a social engineer is at play. Additionally, Fruhlinger writes: *"Even if you've got all the bells and whistles when it comes to securing your data center, your cloud deployments, your building's physical security, and you've invested in defensive technologies, have the right security policies and processes in place and measure their effectiveness and continuously improve, still, a crafty social engineer can weasel his way right through (or around)."*

Social engineers are the greatest con-artist in modern time. They pose as bosses, leaders, colleagues, or the maintenance guy. They can call from a spoofed number, a spoofed email, or anything else they need to fake to look real. Spoofing is a threat where scammers mask a visual object on a screen, to make it look legitimate (malwarebytes.com, n.d.). A typical example is masking a phone number to make it look like the phone number is coming from somewhere else, and is a standard method used in a phishing attack. A spoofed email is another approach where the email may appear to be from a trusted source but, is sent by a scammer. The report details the methods applied to spoof in chapter 4.7a).

It may be the cute, new employee who started last week, asking "all those silly questions", or the IT-guy on the phone calling to doublecheck they have the correct information to create a "new account".

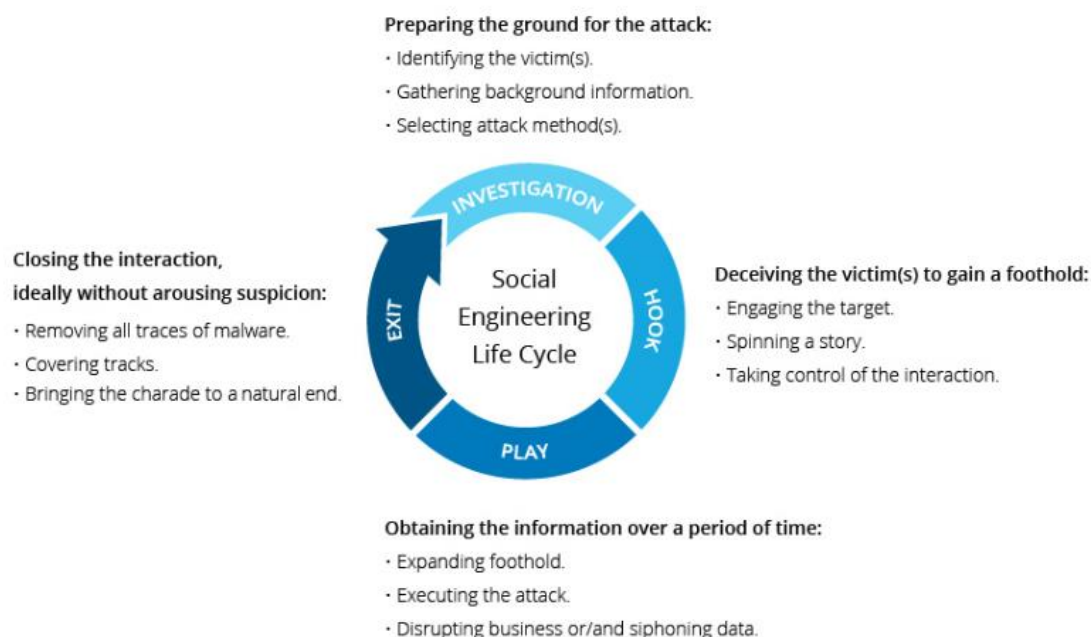
Not all social engineers are terrible people, some of them are ethical hackers, hired by a company, - for the company. No matter who, what or where they are, it is no wonder the first rule of cybersecurity is "trust no one" (Simmons, 2018).

According to Aaron Smith, Maria Papadaki, and Steven M. Furnell at Plymouth University (2013), social engineering exploits the weaknesses, the gullibility and ignorance of humans. Other techniques utilize influence and persuasion, and social engineers are masters at convincing they are someone they are not. Through manipulation, a social engineer can gain unauthorized access to personal details and systems they typically would not have access to.

The techniques used in social engineering, the manipulation and the modern-day technology make it easy for social engineers to carry out an attack. Convincing websites, emails, spoofing, redirections, and acts all play a role in an attack. Training employees to be

aware of an attack is essential, and the training must be updated and repeated continuously.

The penetration testers revealed that the employees were susceptible to techniques executed through social engineering. Imperva's image on the lifecycle of social engineering is much the same as the steps to a penetration attack as described by LanFang and HaiZhou and Cyberx, on page 12.



Social Engineering Attack Lifecycle

Figure 6: Social Engineering Life Cycle (Imperva, n.d.)

This life cycle shows the four phases of an attack which implores social engineering. Compared to a phishing attack which does not make use of social engineering (like for instance a ransomware attack), a social engineering attack revolves around what one could call a play. The attack plays out in such a manner that it would be possible to turn it into a movie. "Matchstick Men", "The Thomas Crown Affair" and "Catch Me If You Can" are three movies where social engineering plays a vital role.

In chapters 4.2a) to 4.7c), the report discusses the techniques of social engineering, uncovering incidents, examples, methodology and mitigation. Each section also recommends what the program should highlight.

4.2a) Tailgating

Risk of attack: Extreme



Figure 7: A Potential Tailgating Incident (Clipart, n.d.)

Tailgating (whatis.techtarget.com, 2017) occurs when social engineers exploit the naivety and trust of authorized personnel, to gain access to the companies' facilities. A technological security system typically distributes the levels of access, and there are several ways an intruder can acquire access to the premises. The security systems are usually guarded by a company's I.D. card, or by a radio – frequency identification card (RFID) (Salahdine and Kaabouch, 2019).

The RFID poses some risks. According to a paper written by Wang, Zhu, and Zhang (2018), the RFID programming as of today invite attacks such as replay attacks, electronic eavesdropping attacks, and denial of service (D.O.S.) attacks. They go on to further explain that many mutual authentication security protocols have been suggested, to no avail. The authentication process, according to the report, is vulnerable to SQL attacks and in conclusion, the system of today is unsuitable for the distributed systems. In their paper, Wang, Zhu, and Zhang recommend "*a new blockchain-based mutual authentication security protocol for RFID systems*". This new system guarantees the privacy of each department and company, including maintaining a secure authentication. Their suggestion excludes design flaws and satisfies the security requirements.

Please note: It is worth mentioning that piggybacking is often mentioned as a synonym to tailgating. This claim is, however, incorrect. Piggybacking is when two social engineers cooperate in gaining access to a facility. One has already acquired access, before letting the other social engineer inside. Piggybacking is therefore a terminology in itself, and must be treated as such (Newton Security Innovation, n.d.)

Some examples of tailgating are:

- Acting as a delivery driver with his or her hands full, asking for help to hold the door while they deliver a package.
- Pretending to be a new employee who has not yet received an access card to the facility.
- The social engineer may hang around the break area and gain trust by striking up a conversation with another employee, before tailgating said employee into the building, distracting said person during a conversation.

- Working as part of the company's regular service provider and gaining access through trust.
- Impersonating an employee who has lost the access card.

These are just a handful of ways a social engineer can gain physical access to a company.

4.2b) Recommendations for Mitigation

A receptionist should greet anyone entering the facility, and guests should receive a "guest badge" upon arrival. The guest badge should not have any privileges, and the guest must return the badge before exiting the building.

"Block Tailgaters"

To prevent tailgaters Long suggests no to hold the door for unauthorized personnel, do not take an identification badge too serious (ask questions!), and train employees to know when and how to notify security when they suspect tailgating.

In the survey mentioned by Diane Ritchey, more than 70% of the executives regard a barrier of some type to be the most effective way to curb a tailgater. The survey explains that more than 60% of the most preferred strategies are physical security barriers, including employee education. More than 70% believe a barrier along with a security officer and alarm was most effective in intercepting a tailgater. Less than 5% believed that a security guard alone was not enough to stifle a tailgater, according to the survey.

Prevention of tailgating is possible by imploring several techniques. Metacompliance.com (2018) suggests educating all users on the risks associated with tailgating. Enforcing specific guidelines with a clear policy on how to handle unauthorized personnel may aid in prevention. Some of the guidelines suggested are to stay vigilant if someone follows an employee through a door, alert security if someone attempts to avoid security measures, and report doors which do not shut properly.

Another step to implement, especially in the case of Packets and Parcels, is to reinstate the main entrance with a guard or receptionist. Such an employee trained in social engineering may spot a tailgater before he or she can do further damage. By stopping and asking unauthorized personnel what their business is, the company stands a higher chance of preventing an attack. A guard post near the break area to the warehouse also limits unauthorized personnel gaining access to the facility.

Chan, Yap and Soh's (2012) research paper regarding the implementation of a detection security system which strictly aims to counteract tailgating and piggybacking, explains how an access control system like the RFID card can combine with a single internet protocol camera. Their research explains how a low-cost I.P. camera in cooperation with an inexpensive embedded based control unit (known as BeagleBoard Xm) could people count, contour count and size check individuals to decide whether tailgating or piggybacking was taking place. Within certain limits, their research produced a 90.8% accuracy.

"Put That Badge Away"

Following is another method to prevent tailgating. In this paragraph, Long is referring to the company identification card, which sometimes can hold important information a social engineer can use to exploit a company. *"One look is all a no-tech hacker needs to*

memorize, duplicate, laminate, infiltrate and frustrate", he says, and tells the employees to hide the badge.

Ryan Francis, a professional penetration tester, supports this suggestion and explains in an article how he gathered username conventions and domain credentials through remote phishing and charming phone calls. The details collected also matched information found on LinkedIn and accessed the building through the main entrance using the badge details he had assembled. (Francis, 2016).

Hiding the badge is also essential when an employee leaves work.

"Check Your Surveillance Gear"

Long recommend not to hold back on the surveillance budget and investing money in good quality equipment produces a higher video quality. Quantity and quality should go hand in hand, adding that hidden cameras can detect social engineers trying to avoid detection. Cameras can record unauthorized humans during, or after tailgating, or in other instances, they have gained access to the premises.

Steven Kenny (2019), wrote an article on the cybersecurity issues regarding surveillance and suggested some best practices to mitigate risk. He explains that surveillance can lead as a back door into I.T. networks, and implementing the latest cyber defences ensures the highest level of security. Further, he proposes that insufficient coordination between the I.T. and incident response teams provide poor cyber health and that the lack or disregard of I.T. security policies, also contribute to an attack. Moreover, neglected systems which remain unpatched after a security update increases a security breach and that proactive maintenance ensures a stable and secure system.

4.2c) Suggestion for Awareness Training

As the report from the penetration test revealed that Packets and Parcels were subject to tailgating, the program should focus on raising the awareness of the employees accordingly.

4.3a) Shoulder-surfing

Risk of attack: High

Shoulder-surfing is, according to most dictionaries *"the practice of watching a person who is getting money from a machine, filling out a form, etc., in order to find out their personal information"* (Oxford Learner's Dictionary, n.d)

From the examples suggested by Oxford Learner's Dictionary, a social engineer does not need to breach security to shoulder-surf. Shoulder-surfing can happen to an employee on their commute to work, during their lunch break in the cafeteria while they are using their phones, and any other place written information is visible to the naked eye. Another way to shoulder-surf is to spy through windows, and people should always be aware of if someone has access to information via a window. Even if that means suspecting the employee in the building opposite the street.

4.3b) Recommendations for Mitigation

Implementing several measures reduces the risk of No tech hacking. Johnny Long, the author of the book "No Tech Hacking" (2008), suggests enforcing a set of practices to mitigate social engineering.

"Shut Down Shoulder-surfers"

Long advises to *"watch your angles"* when typing in passwords and digits which has the potential to reveal explicit information.

A survey posted to the CentralNic's website, which published the results of 1200 British students, was analysed by British psychologist Helen Petrie, PhD. Her reasoning was published in an article at Psychology Today and explains how passwords divided into four categories.

1, "Family Oriented": In this category which was preferred by nearly half of the students, Petrie revealed that the students used personal names such as family names, spouses, pets names, children's names and their own name to create passwords. In this category, they would also choose their birthdates to make up the password.

2, "Fans": A third of the passwords made up for the idols of the password owners, such as "athletes, artists, characters of fiction and sports teams.

3, "Fantasists": 11% of the passwords conceived of words like "sex", "stud" and "goddess".

4, "Cryptics": These fell into the last 10% and invented passwords which had no sense of meaning. Petrie also mentioned that the participants who fell into the last category appeared to be the most security-conscious group, explaining *"They tend to make the safest but least interesting choices"*.

Finally, Petrie mentions that passwords, due to being generated on an impulse, are unintentionally revealing because it is easier to choose something readily available. (Andrews, 2016).

Choosing strong passwords is also supported by an article posted to Lifelock, by Steve Symanovich (n.d), which further recommends using a VPN if an employee needs to perform a financial transaction over the Wi-Fi, and is also in a public setting. Preferably with their backs against the wall. Additionally, the article proposes to lock the computer screen at work when the employee leaves for the day (Symanovich, n.d.).

If an employee is aware that someone is watching their screen, Long suggest said employee should casually close the monitor, and pay attention to the shoulder-surfers next

steps. Alert security if needed. Another vital point Long makes is to treat any information on that screen as compromised, and act accordingly.

One study suggests implementing the protection motivation theory and suggests applying fear as a tool to persuade the employees in establishing strong passwords. Just like Helen Petrie proposes, the study explains how passwords usually are chosen spontaneously, and that "*familiar passwords, short passwords, and old passwords are often chosen primarily for the ease of later retrieval*" (Zhang and McDowell, 2009). The study hypothesized that "*Fear arousal is positively related to the intention of implementing online password protection.*" Their hypothesis bases itself on Irving L. Janis (1967), who during a study, hypothesized on the effects of fear arousal and attitude change.

One major consequence (of reflective fear), is that the aroused unpleasant emotional state gives rise to heightened vigilance, which takes the form of increased attention to threat-relevant events, scanning for new signs of danger, attending to information about the nature of the threat, and thinking about alternative courses of action for dealing with emergency contingencies. The arousal of vigilance affects not only cognitive processes of perception, attention, and planning, but also actions: The individual becomes keyed up in a way that makes him more likely to execute precautionary actions in response to any cue indicating the onset of danger. (...). During an epidemic, for example, apprehensive people not only learn about the danger signs and scan the newspaper for announcements by public health officials, but they also pay closer attention to internal stimuli from their own bodies. Sometimes they become hypervigilant, exaggerating the significance of their mild physical discomforts to the point where they become sleepless and demand prompt medical attention

(Janis, 1967, p. 171)

For further mitigation, Packets and Parcels should invest in a trusted application for their employees, which stores passwords, and implements policies which force employees to choose strong passwords and change them at least each quarter.

4.3c) Suggestion for Awareness Training

In chapter 3.2), results of the pre-attack stage demonstrated that the information gathered to attack Packets and Parcels by the penetration testers were relevant in phase two of the penetration test. With that in mind, the program should train employees to being conscious when entering passwords or scrolling through personal information on their screens. Employees should learn the benefits of creating strong passwords and changing them often. As suggested in the hypothesis by Irving L. Janis, the course should play on the emotions of the employee during the password section.

4.4a) Dumpster-diving

Risk of attack: Extreme

There are no clear definitions in dictionaries on dumpster-diving, as several definitions refer to it as searching for food out of dumpsters outside. An article posted to Computer Hope defines dumpster-diving as "*the practice of digging through a company's trash bins or dumpsters to gain information*," simultaneously explaining the reason; to retrieve passwords which allow access to a network, or to exploit personal information for social engineering (Computerhope.com, 2020).

Benji Pell, an infamous dumpster-diver who was actively selling information in the late '90s and early 2000s, explains in an interview to The Telegraph (2002), that he was running an office-cleaning business when he first began foraging through estate agents' bins. Elton John's manager, John Reid, occupied an office nearby, and a friend of Benji encouraged him to try Reid's bins. Within a week, Pell happened upon a letter with information stating that a tribute album to Princess Diana could not include "Candle in the Wind". The letter was sent to Mr. Reid and signed "Richard Branson". Benji Pell contacted public relations Max Clifford, "*who sold the story to the Sun*" (Leonard, 2002).

Piers Morgan, the former Daily Mirror and News of the World editor, also admitted to using Benji Pell to acquire information on Elton John's bank statements, adding that Piers believed the method is on the verge of unethical (BBC.com, 2011).

4.4b) Recommendations for Mitigation

"Shred Everything"

To mitigate the risk of dumpster-diving, Long proposes to purchase a micro-cut shredder, which shreds not only papers but also CD's and credit cards. Another suggestion is for the employee in charge of the incident response team to investigate discarded items in the bins. The results indicate whether the employees are satisfyingly destroying business elements.

4.4c) Suggestion for Awareness Training

Critical information was laying around the office belonging to clients, partners, individuals et. The training should ensure the employee learn how important shredding documents or concealing them is to the company.

4.5a) Plain sight and theft

Risk of attack: Extreme

Plain sight refers to stealing information which is visible throughout the building. It must not be confused with shoulder-surfing, as plain sight indicates what is visible to the naked eye, even when the employee is not there.



Figure 8: Post-it Note on Computer Screen (Kelleher, 2018)

The above photo provoked criticism when posted in an article by the Associated Press. The article was then reposted the next day without the image (KELLEHER, 2018). Yet, a screenshot of the original article resurfaced on the application Twitter, (2018) under the hashtag #warningpoint2, nodding towards the password itself. The reason for the resurfacing was the accidental false missile alert, according to Scott Saiki "*the wrong button was pushed*" (MARTINEZ and WINSOR, 2018). The image with a visible password attached to a post-it note on the computer screen initiated a debate regarding the agencies approach to information security. According to the emergency management agency spokesman Richard Rapoza, the password is legitimate, but no longer in use (HawaiiNewsNow, 2018). In the article, Rapoza also mentions "*it's not a good idea to have a password in plain sight, especially with news cameras around*".

Another relevant case worth mentioning is that of the offence committed toward Turbine Engines Technologies Corporation (TECT). An engineer formerly employed by TECT stole roughly 100 computer discs containing trade secrets belonging to TECT. Later he was employed by TECT's competitor Precision Components International (PCI), and the information stolen resulted in a loss of up to \$14 million toward TECT at the time (Salinger, 2013).

Considering the information that is available in plain sight is easily stolen, it falls naturally under the category theft, and it is the reason why the chapter mentions them at once.

4.5b) Recommendations for Mitigation

"Go Undercover".

In this paragraph, Long suggests not to work on private things in a public room. He proposes to use a privacy filter if possible, before arguing that such a filter counteracts the purpose and draws the attention of a social engineer, thus working against itself. Long goes on to advise to attach sticky notes over company stickers which are attached to private property when travelling. This practice limits the risk of losing leaked information to Plain Sight.

Although Long does not mention the theft of individual items, Jayson E. Street (referenced in chapter 5.0), emphasizes the importance of securing the employees' belongings. Packets and Parcels should consider investing in extra lockers for all employees, including the office employees.

One other concern is the rooms secured with pin tumbler locks. Several tutorials are available showing how simple it is to pick such locks (Tool, 1991). It is advisable to substitute these locks with more secure devices, such as an RFID card. The cleaning closet should also be secured; chemicals falling into the wrong hands can lead to unfortunate events.

As mentioned in chapter 4.2b), to mitigate the theft of guest identification badges, each guest should register with an I.D. and a name via the RFID. The receptionist annuls the details upon the return of the badge.

4.5c) Suggestion for Awareness Training

The penetration testers snatched a card from the locker rooms, but the information on the card could just as quickly provide information to create a false card or badge. The course should remind employees about the privacy of the identification on the RFID card.

Another issue the penetration testers commented on were the unshredded documents laying around. The course should raise awareness on the importance of concealing classified information.

In chapter 5.0) the report introduces a study performed by the Ponemon Institute L.L.C. A diagram illustrates that 49% of the retrieved information in their study was from an employee desk (Ponemon Institute L.L.C., 2016, p. 9). With that in mind, the course material should focus on training the employees to keep a neat desk, and not to hang documents on the wall for convenience's sake.

Regarding theft, the course material should instruct the employees to make conscious decisions concerning where they choose to store their belongings.

4.6a) Phishing and Spear Phishing

Classic phishing email scams are when scammers distribute the same email to possibly thousands of recipients on a mailing list, hoping someone takes the bait. The method exploits human vulnerabilities and therefore defines as a semantic attack, in which "*The use of incorrect information to damage the credibility of target resources or to cause direct or indirect harm.*" (Yourdictionary.com, 2017). The method is also the reason why it has received the nickname "spray-and-pray". These emails are impersonal and often replicate standard websites populated by regular consumers around the world. The impersonation plays on the trust of the consumer, and the goal usually is to steal the credentials and credit card numbers of unsuspecting users. Some emails are more advanced, containing infected attachments, and macros with payloads. In some cases, social media platforms such as Facebook and LinkedIn contribute to distributing malicious attachments via messages, and the perpetrators are known for spoofing website to make the scam more authentic (Phishing.org, 2019).

As mentioned in chapter 4.1), spoofing is the technique where something falsely claims to be something it is not. The retrieved sample is from the outlook application. The email appears to be from a trusted vector, and the translated heading reads: "noreply@coop.no on behalf of Website "*Lose weight efficiently*" newsletterw@xtdoestetica.asia "

noreply <noreply@coop.no> on behalf of Nettsted „Mist vekt effektivt“ <newsletterw@xtdoestetica.asia>
30/05/2020 17:31

Figure 9: Lose Weight, Spoofed Address (Jones, 2020)

The information in the header differs from that of the application when accessed via outlooks website.

Nettsted „Mist vekt effektivt“ <newsletterw@xtdoestetica.asia>
Sat 5/30/2020 5:31 PM
To: You

Figure 10: Lose Weight, Original Address (Jones, 2020)

The consequences worsen when the senders' address appears to be from a business-partner, financial institution, colleague or even a leader. Other methods of spoofing are domain spoofing, I.P. and website spoofing. All are tools used to phish details from a victim.

According to research developed by Trend Micro, 91% of cyberattacks begin with spear-phishing (Savvas, 2012). The goal, according to the research, is to lure the victims into opening malicious attachments or clicking links which redirect to a site containing exploits and malware.

During a spear-phishing attack, the criminals already know some details of the victim, as Kaspersky (2019, p.9) explains: *"The attacker may prepare by spending weeks inside the organization's network and accounts, studying the organization's vendors, billing system, and even the CEO's style of communication"*. The details assembled target the victims and produce a more authentic scam. The victims are not necessarily singular people, as companies and private people also fall victims to the spear-phishing. The differences between phishing and spear-phishing are demonstrated in this infographic by KnowBe4

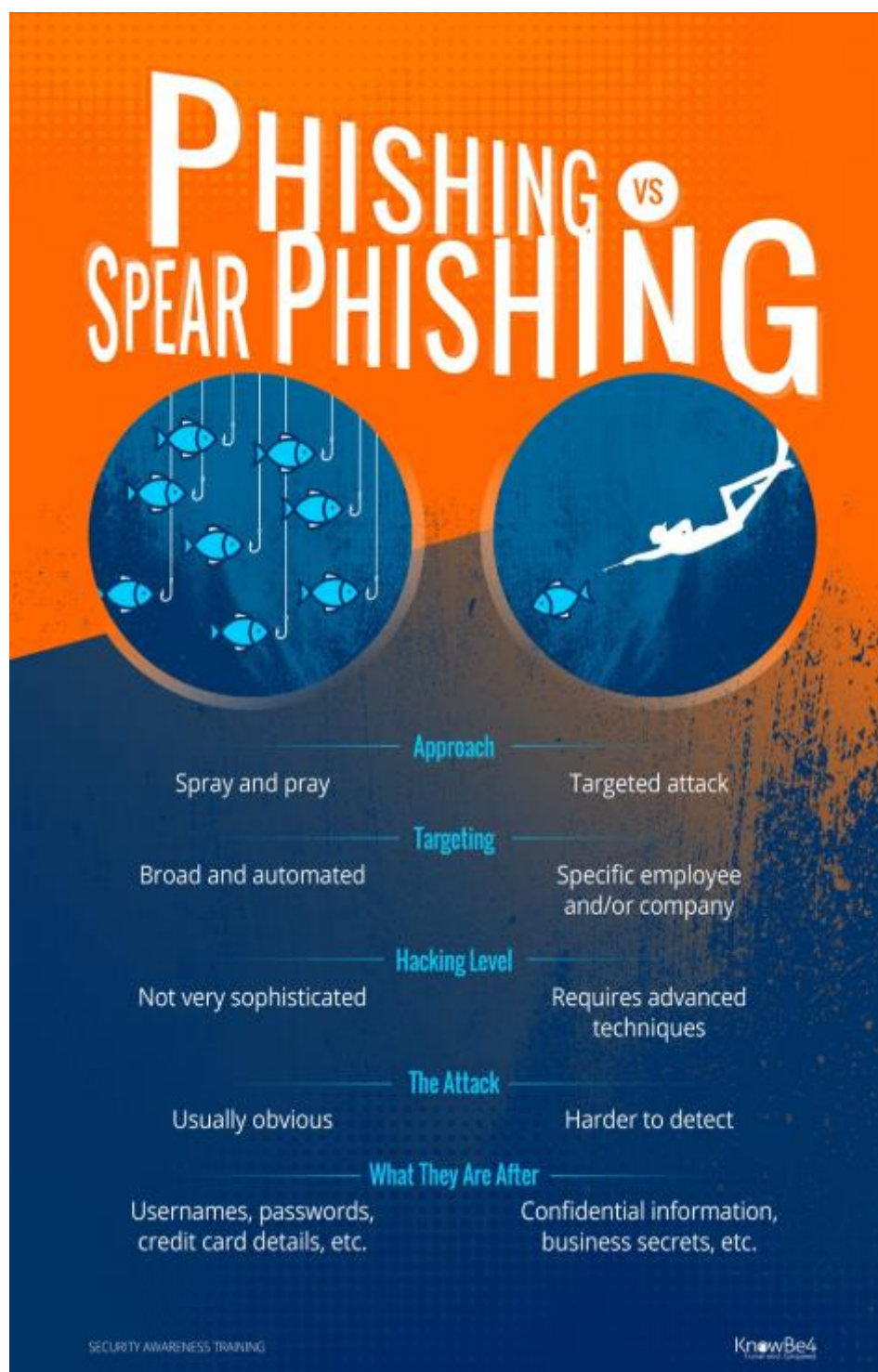


Figure 11: Phishing vs Spear-Phishing (KnowBe4.com, n.d.)

KnowBe4 reveals the method used in spear-phishing attacks, explained in six steps.

1. In the first step, the hackers gather email addresses and find the targets by deciding what data they are after, and who has access to it.
2. After the offenders have acquired the email targets, their next step is to send the email through the company's antivirus software. Advertised system administrator positions in the company may already detail the software. Another method to collect information is searching for exposed information on social media.
3. After the second phase, the attacker moves on to egress filtering. The goal is to collect the targets information unless social engineers already have acquired it.

Assuming the email can enter through the antivirus, it carries with it a malicious payload, which, according to Cloudflare is the *"component of the attack which causes harm to the victim"* (Cloudflare.com, n.d.). Some examples of payloads (but not limited to) that Cloudflare mentions are:

- To affect the behaviour of a computer, a payload can delete and edit files, and either disable the operating system or the boot process. Some payloads are known to "brick" smartphones, impairing their ability to function.
 - Once distributed, a small payload stored in a file can be activated to trigger a download of more extensive and malicious software.
 - A payload can run background processes such as cryptocurrency mining, or store data.
4. The hackers now have information on the email addresses, the antivirus software, the payload, and the details on the target. In step four, the hackers create a scenario which aims to draw the attention of the victims. The assembled details create an email with spoofed details which appear legitimate. It has the name and contact details of the recipient, and since the hacker has learned the recipients' contacts, the email signs off with a familiar name.
 5. The email is ready for distribution. To bypass the mail server, KnowBe4 recommends the free email server which comes with purchasing a valid domain, before changing the "Whois" information to match the domain target. It is also possible to set up a temporary mail server and "spray-and-pray", but the low reputation score from the hacker's mail server may block the emails entry to the company's mail server.
 6. Assuming steps 1-5 have succeeded, and a keylogger registers password hashes and credentials from the machine, the perpetrator collects the data they need to gain access to the whole network.

Learning the steps behind a spear-phishing attack is essential, and KnowBe4 has created another infographic which displays the "red flags" any consumer must be aware of when opening and reading emails.

Social Engineering Red Flags

FROM

- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization** and it's **not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- I **don't know the sender personally** and they **were not vouched for** by someone I trust.
- I **don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on** is a .txt file.

CONTENT


- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

TO

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big red flag**.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofamerica.com — the "rn" is really two characters — "r" and "n."



© 2017 KnowBe4, LLC. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.



Human error. Conquered.

Figure 12: Red Flags in a Phishing Email (KnowBe4, 2017)

In 2016 FACC fired Walter Stephan, the former chief executive officer of the Boeing and Airbus supplier, and FACC's chief financial officer after Stephan fell victim to a spoofed email from outside attackers (Pindrop.com, 2016). CSOnline reported that the attackers duped the financial controllers into wiring €52.8m throughout several transactions, and the company's share price fell 38% because of the incident. The company halted one transaction of €10.9m, and the recorded loss dropped to €41.9m. Usually, the company's operating profit accumulated to €18.6m, but after the incident, the company recorded a loss of €23.4m (Tung, 2016).

4.6b) Recommendations for Mitigation

88.46% of the employees in Packets and Parcels clicked the phishing email issued by the penetration testers. The studies show that even with user awareness training and infographics, employees still fail to report spear-phishing emails. Arun Vishwanath, Ph.D., M.B.A., is a faculty associate at the Berkman Klein Center at Harvard University. In a presentation (Vishwanath, 2017), he shares the suspicion, cognition, automaticity model (SCAM). (Vishwanath, Harrison and Ng, 2016) They developed the published peer-reviewed model which begs the question: "What is a successful attack?". Vishwanath elaborates

further that the model suggests a trust triad they call "Vishwas" (meaning "trust" in Sanskrit (Pitarau.com, n.d.)). The model consists of three parts; the trusted source (google, amazon, PayPal), a modifiable field (something the end-user does not pay much attention to, such as the URL), and the user routine or expectation. These three ingredients result in a 50% success rate, according to Vishwanath, and they are the main ingredients in his penetration attacks.

Further, he connected several processes which revealed if and how humans are susceptible to phishing – emails. A questionnaire consisting of 40 questions then evaluated the combined processes and forwarded the results to a Cyber Risk Index (C.R.I.). The score is not static, as, through awareness training, the score can improve. A higher score produces a better result. Vishwanath also compares the score to a credit score, and it establishes a risk score for the division or group in question. After awareness training, the group can be penetration tested again, before answering the same questions and hopefully increasing the risk score. Vishwanath then compares the process as to when someone receives a diagnose from a doctor. *"What our 40 questions help us do is it helps us diagnose what's ailing the patient"*. Vishwanath continues the analogy by suggesting how a patient receives one pill without really knowing what is wrong; the patient goes back to the doctor and is prescribed more pills and is still not cured. In the end, it is the patient's fault they are sick. The C.R.I. pinpoints precise answers as to why the employees fall for the scams and can then treat the "symptoms". The results from the C.R.I. aid in deciding who gets trained and how.

Once an evaluation of the C.R.I. is available, the employees training can commence. One study suggested imploring embedded training and displayed how people with little knowledge of phishing reacted to learning through a security notice intervention, text and graphics intervention and a comic strip and the results are as follows:

Method of user awareness training.	What percentage fell for the scam before the awareness training?	What percentage fell for the scam after the awareness training?	Comment from participants.
Security notice intervention.	90%	90%	<i>"Took too long to read, and the conveyed message was unclear."</i>
Text and graphics intervention.	80%	70%	<i>"Giving the steps to follow to protect from phishing was helpful" "This is definitely useful and good stuff and will remember that [to look for URLs in the status bar]."</i>
Comic strip intervention.	100%	30%	Some participants said they preferred the comic to the text/graphics intervention because it engaged them with a story.

Table 5: Effects of Awareness Training (Kumaraguru et al., 2007, p. 911)

Kumaraguru et al. (2007, p. 913), further recommend to *"Embed the training into users' regular activities so they do not have to go to a separate website to learn about phishing attacks,"* and *"Keep the training messages simple and short. One reason the security notices did not work well was too much text"*.

Another recommended form of mitigation is to integrate a "Phish Alert" button to the software's technologies. The button prompts users to report phishing attacks and reports the action to the incident response team. The instant feedback reinforces the training, and after a year, KnowBe4 claims the Phish Alert can reduce the risk of attack by 33.2%, based on 4 million users (KnowBe4, 2020).

Lastly, one article posted to psychology.jrank.org (n.d.) suggested that most people are competitive by nature, citing Sigmund Freud, who suggests *"humans are born screaming for attention and full of organic drives for fulfilment in various areas"*. The article also establishes the doctrine of natural selection, by Charles Darwin, established in his work *"The Origin of the Species"*, that it is the species who find it most natural to adapt and master the natural environment who survive. This phrase, yet never uttered by Darwin himself, is commonly known as *"survival of the fittest"*. The article does argue that some people do; however, respond better to cooperation and mentions the studies by Margaret Mead.

Regarding the identification badge, there is no need for personal details, pictures, names, or anything else revealing the identity of a person on the badge. To avoid phishing the badge should only control access to the building.

4.6c) Suggestion for Awareness Training

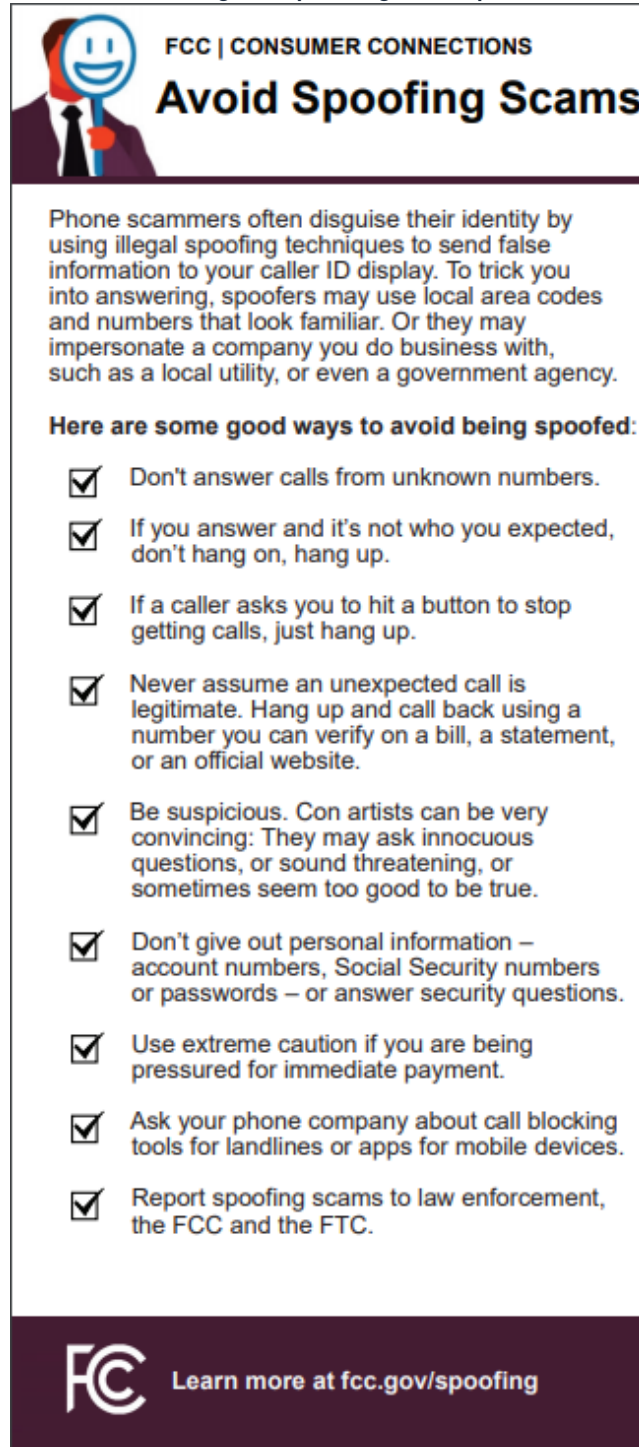
The I.T. department should consider evaluating the employees Cyber Risk Index. Based on the results, awareness training should focus on embedded training over an extended period. The I.T. department should incorporate a Phish Alert button, and decide on a method to engage the employees in a way where the employees find it natural to either not open the phishing emails, or click on redirects and attachments in the emails. A comic strip in the monthly newsletter can aid in entertaining the employee's, reminding them to remain vigilant. Further, the incident response team should entertain the idea of initiating a relaxed and fun competition which keeps a score of the employees and commend the top 10 employees with the best score in the monthly newsletter.

Also, the company should train the employees to recognize a phishing attack. As mentioned in the attack phase, the penetration testers were able to register a fake domain to send a spoofed email to the employees. The business email is registered at the "pnp.net" domain, while the penetration testers registered their domain at "pnp.org". There are ways a company can mitigate against domain spoofing, but that is outside the scope of the report.

Lastly, the company should consider cleaning up the addresses on the mailing list, and not disclose information which hackers can exploit.

4.7a) Tech Support – Vishing

"Vishing (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorized entities" (Rouse, 2008). Spoofed phone numbers contain false information in an attempt to disguise the callers' identity, in an attack known as "vishing". Scammers are known to use local area codes to avoid detection by caller I.D. They spoof numbers in an attempt to gain the trust of a victim. An infographic by Federal Communications Commission suggests following a checklist to mitigate spoofing attempts.



FCC | CONSUMER CONNECTIONS

Avoid Spoofing Scams

Phone scammers often disguise their identity by using illegal spoofing techniques to send false information to your caller ID display. To trick you into answering, spoofers may use local area codes and numbers that look familiar. Or they may impersonate a company you do business with, such as a local utility, or even a government agency.

Here are some good ways to avoid being spoofed:

- ☒ Don't answer calls from unknown numbers.
- ☒ If you answer and it's not who you expected, don't hang on, hang up.
- ☒ If a caller asks you to hit a button to stop getting calls, just hang up.
- ☒ Never assume an unexpected call is legitimate. Hang up and call back using a number you can verify on a bill, a statement, or an official website.
- ☒ Be suspicious. Con artists can be very convincing: They may ask innocuous questions, or sound threatening, or sometimes seem too good to be true.
- ☒ Don't give out personal information – account numbers, Social Security numbers or passwords – or answer security questions.
- ☒ Use extreme caution if you are being pressured for immediate payment.
- ☒ Ask your phone company about call blocking tools for landlines or apps for mobile devices.
- ☒ Report spoofing scams to law enforcement, the FCC and the FTC.

FCC Learn more at fcc.gov/spoofing

Figure 13: Avoid Spoofing Scams (Federal Communications Commission, n.d.)

Attackers may claim there is a problem with an account and asks for a money transferral to correct the issue. Other methods are to impersonate calls from banks, The Internal Revenue Service (I.R.S.) or a financial organization, where the goal is to fool the victim into providing explicit information over the phone to access a bank account or steal the victim's identity (FraudWatchInternational.com, 2019).

4.7b) Recommendations for Mitigation

The penetration test revealed that two employees at Packets and Parcels fell victim to the VoIP call.

Michael Madon (2018) suggests verifying unknown incoming phone calls and being suspicious of callers who request login information. Additionally, they implore employees to report to the incident response team if a caller asks to receive explicit information and to refuse to cooperate in changing passwords, logins, or network settings over the phone.

Quostar (2019) suggests employing a zero-trust policy so that employees only know what they need to know, which reduces the risk of compromised information. Another idea is establishing a list of names who may have access to specific details, which a zero-trust policy reinforces.

4.7c) Suggestion for Awareness Training

Senior security consultant and social engineer Jen Fox held a presentation at the Circle City Con in 2015. She recommends encouraging employees to escalate calls to a supervisor, verify the caller's story and to request a number to call back. She proposes to train employees to build a "mental script" so that they can react automatically to suspicious calls (Fox, 2015).

5.0) The consequences of Phishing

One study carried out by Agari Field C.T.O. Tom Field (2016), explains that 46% of the surveyed leaders confirm their companies were victims of a social engineering attack in 2015. Not surprisingly, 52% admitted that their organizations' defences towards a targeted attack rated as average or below. Only 5% claimed that their organizations' defences against social engineering were superior (2016, p.2).

Of the 46% of the businesses which had fallen victim to social engineering, it appeared that stolen information was that belonging to employees:

Damages	Percentage
Compromised employee credentials	65%
Breached financial accounts	17%
Breached intellectual property	15%
Negative publicity received after the attack	11%

Table 6: Percentage of Stolen Information. (Field, 2016, p.7)

Interestingly enough, the study revealed that some businesses already had attempted to train their employees.

Greatest vulnerabilities	Percentage
Ineffective awareness training	50%
Outdated anti-spam and anti-virus system	47%
Attackers always a step ahead	38%
Business partners have insufficient security	31%
Senior management does not recognize the seriousness of the issue	12%

Table 7: Percentage of Trained Employees (Field, 2016, p.7)

At the beginning of chapter 6.0,) studies suggest user awareness training is ineffective, a claim which is supported by Stefan Gorling (2006). He argues in his research as (cited in KUMARAGURU et al., 2009, p. 4) that "*security user education is a myth*" which may explain why the 50% in Filed's study claimed their efforts to train user awareness were unsuccessful. The methods are, however, vast. Research shows that various methods produce different results. The study by the Ponemon Institute briefly mentioned in chapter 4.5) on visual hacking (plain sight), explains that out of 157 trials conducted on 46 companies, 91% were successful. 27% of the hacked data was sensitive information, and the most likely documents to be hacked were those visual on vacant desks. In 49% of the hacking attempts, the first attack only needed 15 minutes to complete. Further, the research found that an open floor plan exacerbates the risk of an attack (Ponemon Institute L.L.C., 2016, p. 2).

The penetration test toward Packets and Parcels revealed that no tech hacking appeared to be uncomplicated due to a lack of physical security, which, with the open floor plan, was easy to manoeuvre. Ponemon's study exhibited the percentage frequency of the information types visually hacked after a breach.

n = 613 pieces of data; 8 countries (combined)

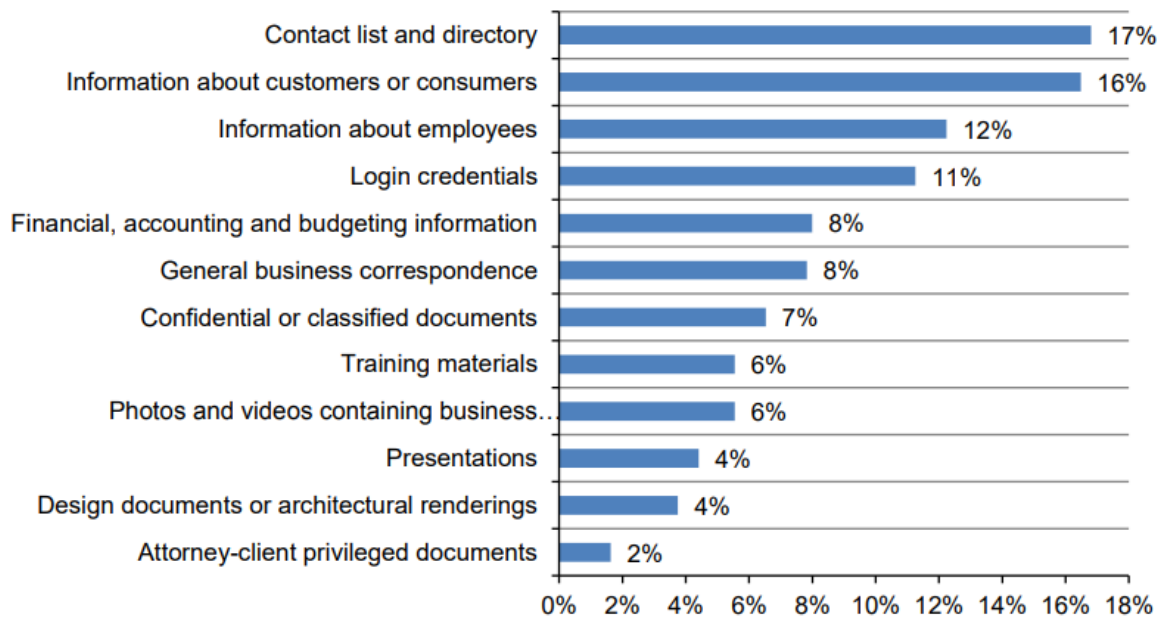


Table 8: Percentages of Hacking Due to Weak Security Measures (Ponemon Institute L.L.C., 2016, p. 6)

Several articles on Tailgating reference one specific survey conducted by Boon Edam Inc, but the access to this survey is denied without a company email. An attempt to create a domain with an email address was attempted but remained unsuccessful.

Boon Edam Inc, (cited by Ritchey, 2015), released a survey conducted on enterprise security executives. According to Diane Ritchey, author of the article in Security Magazine, the survey's results claim that a majority of the respondents assume tailgating to be on the rise, or at the same level. More than 70% of the executives suspect they or their company are vulnerable to a tailgating attack.

Over half of the respondents believe the cost of a breach to be \$150 000 and up. Over 25% believed a tailgating incident would result in costs "*too high to measure*".

Also, to be mindful of is that once a social engineer has found their way in – they are in! The damage they can cause is limitless. This fact is why it is essential to train employees to be suspicious of unfamiliar faces.

Theft, which may result in industrial espionage is "*the covert and sometimes illegal practice of investigating competitors to gain a business*" (whatistechtarget.com, n.d.)is another consequence of tailgating but does not confine only to tailgating. A case study published by Ira S. Winkler (1996, p.3) explains in the paragraph regarding "Illegal Methods" that companies frequently use insiders to gain access to information. As these people already are established within the company, they "*can typically move through the organization unchecked*". In the case study, a penetration tester was temporarily employed in a "large high technology firm", as part of a penetration test. Once inside Winkler explains that the penetration tester conducted a "*misrepresentation of responsibilities by the temporary, abuse of physical access, internal hacking, internal coordination and facilitation of external hackers, and straight external hacking*". By the end of the day, the penetration tester hypothetically stole \$1,000,000,000 worth of information. Winkler added that due to

the Smart Cards and firewall, the network and building were impenetrable (Winkler, 2016, p.6).

In a blogpost posted by The Graphus Blog (2020), the blog post mentions five other areas which are affected by social engineering attacks. Direct financial losses are the obvious consequence, and the losses usually do not go below \$25,000. The blog does not mention the open loss, but as demonstrated in the previous paragraph, the cost has the potential to ruin a company.

Another area which is affected by social engineering is the recovery cost. The cost of having to pay for a clean-up team, new software, and protect against future threats can take a significant space in the budget. The aftermath of an attack affects productivity loss and business disruption when the company needs to organize meetings, overtime shifts due to faulty equipment, loss of customers, and employee updates. Lastly, the blog mentions reputation damage. A significant security breach can lose the trust of business partners, customers, and suppliers. It can also affect the company's stocks, and the aftermath can affect its reputation for years.

In 2012, Chief Information Officer at "Stratagem 1 Solutions" Jayson E. Street, held a guest presentation at Defcon19 sharing the details of a penetration attack he had performed, detailing what he did, could, and did not do. The presentation was named "*Steal Everything, Kill Everyone, Cause Total Financial Ruin!*", and during his appearance, he demonstrated the results of actual engagements where he practised as a penetration tester. During the speech, he recalls an incident where he could have caused severe damage to the company.

I stole the purse; I stole the car keys, and yes I stole the phone (...) but let's hold on, let's cut for a second (...) I didn't go to the parking lot to find out what car it is. I unlocked the car, I go back and put her car keys back. She comes back after work; I'm in the backseat with a gun telling her that I've got her driver's license showing that I know where she lives. That I've got people there that will kill her family if she does not go back into that facility, steal all the data that I need, and then come right back out. And that we're tracing you and that we've got your phone cloned and that we can monitor it. Employees need to know that their personal belongings are theirs, but the impact can be severe for them as well as the company. That's why they need to secure their stuff

(Street, 2012)

6.0) Awareness Training

Boot camp

Before recommending awareness training, the system administrator recommends that the employees attend a boot camp. The boot camp should have two set dates so that everyone can attend. Some employees may find the idea strange, but the company should consider rewarding the attendees by paying them a regular salary for attending and offering food and drink at the event. The boot camp should offer competitions where the employees divide into teams, gathering points along the way. This method includes cooperation and winner's instinct. Hiring actors and stooges, or cooperating with the penetration testers to fabricate incidents may stimulate the learning process.

After the boot camp, the attendees receive a certificate of competition. Everyone who completes the course receives an honourable mention in the newsletter.

The system administrator recommends applying the following roleplaying approaches during the boot camp for the employees.

Tailgating:	➤ Tailgating where they act as attacker and victim.
Shoulder-Surfing	➤ Attempting to shoulder-surf each other in different situations.
Dumpster-Diving	➤ The employees could look in the bins to see if anything explicit is up for grabs.
Plain Sight	➤ The employees should take a look around their offices to see if anything explicit is visible.
Theft	➤ Attempt to "steal" belongings from actors and stooges.
Vishing	➤ A phoney vishing call from the actors may raise awareness. ➤ Train employees to escalate suspicious calls to a supervisor.

Table 9: Boot Camp recommendation (Jones, 2020)

The boot camp does not include phishing and spear phishing, as constant training can mitigate the risk of this method. The company should consider installing a "Phish Alert" button and train the employees to use it vigorously.

The use of Games

In chapter 5.0), the report highlighted the myth of training employees, as claimed by Stefan Gorling. One dissertation on the topic which asks if phishing education enables users to recognize phishing discloses the answer to the question: It appears that the most successful technique which aids in employees not only raising the awareness revolving cybersecurity but also causes the employees to exercise security measures is through the use of games (Alghamdi, p. 28, 2017). A study particularly on this subject, which Alghamdi also references, designed a game (cups.cs.cmu.edu, 2007) *"which teaches users how to identify phishing URLs, where to look for cues in web browsers, and how to use search engines to find legitimate sites"*. An analysis revealed that the participants who joined the

game excelled in identifying phishing websites, compared to the participants who only received a tutorial or read existing reading material, as the information below uncovers.

Total correctness	Existing Training Material	Tutorial	Game
Pre Test	66%	65%	69%
Post Test	74%	80%	87%
Improvement	8%	15%	18%

Table 10: Games Motivate Learning (Sheng et al., 2007, p.8)

A total of 42 people took part in the test, divided into three equal groups of 14. Screening confirmed that the participants were "non-experts" in the field, and the study concluded that interactive games are most successful in raising the awareness of cybersecurity among people who only have a general knowledge of it (Sheng et al., 2007).

The Quiz

Following is the suggestion for a quiz. The quiz can put a humorous twist to wrap up the boot camp. It must be noted that some questions offer multiple correct answers.

Scenario 1:

A man is sat smoking outside the break area. He starts eavesdropping on a conversation regarding an event which is broadcasted on the views and offers his opinion on the matter, making rapport with another employee called Lars. He asks where they're from and explains that he recently started working as a lorry driver, before changing the subject. As they get up to access the building, he approaches Lars and claims he has not previously been directed to the transport coordinators office and would like some help getting there. What should Lars do?

- A) Call the transport coordinator and ask him to come down to the floor and meet the lorry driver.
- B) Point him in the right direction and hand him his key card, explicitly telling Lars to hand it back before lunch.
- C) Follow the lorry driver to the transport coordinators office.
- D) Invite Lars to join his colleagues for a beer after work, congratulating him on his new job.



Figure 14: 2 Men Standing in A Warehouse Talking. (Tiger Lily, 2020)

Scenario 2:

A woman stands outside the main entrance claiming she is a new employee. As an employee passes her by to enter the building, she explains she is new to the facility and hasn't received an entry-card yet, and if the employee could please let her in. What should the employee do?

- A) Let the woman in.
- B) Ask the woman who hired her, before doublechecking with said person that the woman is, in fact, a new employee. If everything checks out, the employee can let her in.
- C) Nothing, it's best to stay out of it.
- D) Ask the woman out on a date.



Figure 15: Woman Standing on Front of High-rise Building (Chương, 2019)

Scenario 3: Karen is working on a business transaction. On her screen, the details of a company, their account, and contact details are visible. Behind her, a man cleaning the exterior windows has had a direct view of the transaction. What should Karen do?

- A) Ask the man who he is, then carry on working
- B) Ask to see the man's badge and check with security if he has made an appointment to clean the windows.
- C) Close her screen, regard all information as compromised, change her password and report the incidence to her superior. Additionally, Karen should ask the man who he is, what his business is and confirm this information with security.
- D) Go home, hide under a quilt, and wait for her termination notice.



Figure 16: Man Cleaning the Glass of Building(Immortal Shots, 2018)

Scenario 4: After the last incident, the company invest in a password manager app and tells Karen to create a secure password, what should she choose?

- A) Password123, Summer2020, ArianaGrande! or something else easy to remember. Preferably writing it on a sticky note and attach it to her screen should help her remember.
- B) She can close her eyes and type something on the keyboard: h4X0r34\$t3r3Gg is good enough.
- C) Write something situational: "IamWearIn90DD!socks"
- D) Nobody will notice if she reuses the last password, so she keeps it for convenience sake. She has a brain, who needs a password manager anyway?

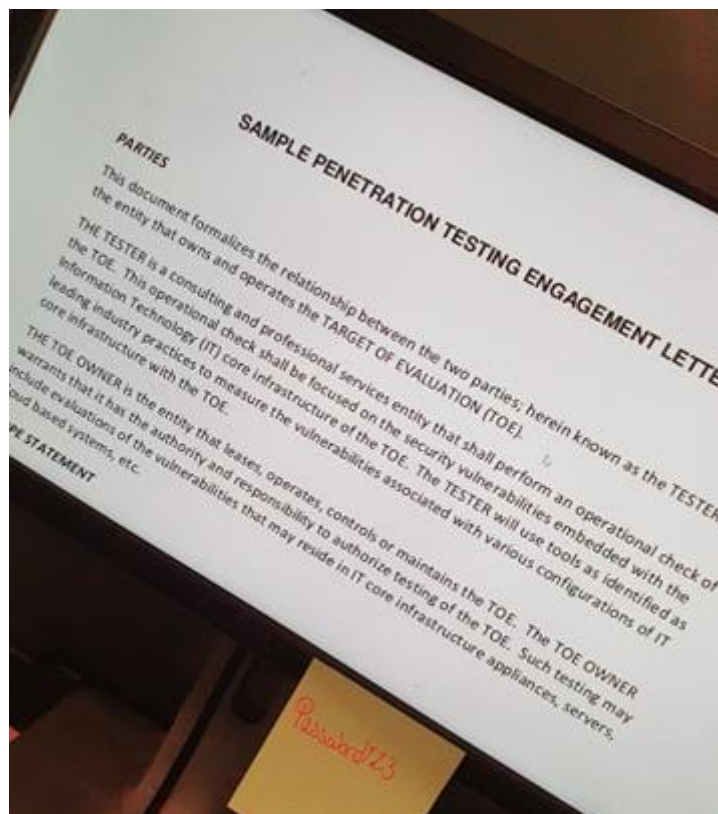


Figure 17: How Not to Store Your Password (Jones, 2020)

Scenario 5: During Peter's bus-trip home from work, he remembers a task he had not completed. He must log on to the company's intranet from his phone to finalize the project before he gets home, or the company might lose a customer by morning. What must Peter be aware of?

- A) There is no time to be aware now, customer first!
- B) Check his surroundings, and if anyone is behind him or next to him, he must hide his screen.
- C) Wait until he gets off the bus and hope it's not too crowded.
- D) Ignore it; He's sure the customer can wait until morning.



Figure 18: People Inside A Bus Wearing Masks (Young, 2020)

Scenario 6: Unfortunately, the company fired Peter because he chose to ignore the customer. The following week Peter returns and waits outside the main entrance. He asks Karen to let him in so that he can clear his desk. What should Karen do?

- A) Tell Peter to wait for his superior.
- B) Call Peter's superior and wait for further instructions.
- C) Let Peter in.
- D) Politely tell Peter to go squat in a cactus patch.



Figure 19: Man Sitting on Gray Pavement (Onojeghuo, 2016)

Scenario 7: Karen receives a document with explicit details which her supervisor places on her desk, telling her he needs the details finalized before lunch. She is busy and tells him she will get right to it as soon as she can. What should Karen be aware of in this scenario?

- A) Not much, she has said what she will do and is satisfied with her course of action.
- B) Hide the document in a safe place until she is ready to take care of the task.
- C) Drop everything and finalize the work, adding a "Yes sir"!
- D) Burn the document.



Figure 20: Person Resting Their Hand on Table (Magni, 2019)

Scenario 8: Karen has finished her work on the document, what is her next course of action?

- A) Lock it in a cabinet with the other essential documents or shred the paper.
- B) Throw it unscathed in the recycle bin.
- C) Store it in a secure folder and put the folder in the shelf behind her.
- D) Burn down the building to erase all trace of any explicit information.



Figure 21: Focus Photo of Yellow Paper Near Trash Can (Johnson, 2018)

Scenario 9: Karen returns from lunch and finds her handbag on the floor next to her desk, which she finds strange as she usually hangs it on her chair. How should Karen react?

- A) Report it to a leader, cancel all the credit cards and check the backseat of her car. She should also call home to check if everything is o.k., or have a friend follow her home in case somebody duplicated her keys and broke in.
- B) Nothing, she's probably confused.
- C) Report it to security.
- D) Complain, accuse everyone of stealing, flip out and have a panic attack. And burn the car.



Figure 22: Macbook Pro on White Table (Thanyakij, 2020)

Scenario 10: At 6.30 am on a Sunday, Karen is awoken by the ringtone on her phone. Her superior is screaming down the line, demanding her to transfer money to the account mentioned in the email she received yesterday. Her superior tells her to get a pen and write down the details. Before the call ends her superior tells her to have it done "yesterday". What should Karen do after the call ends?

- A) Complete the transaction.
- B) Log onto her email to doublecheck if the details in the email and the details received over the phone are correct, and then complete the transaction.
- C) Call her superior back to confirm if she has all the correct details. Report the incident if the superior is surprised by the call, claiming he never called her.
- D) Quit her job; no job is worth getting up at 6.30 am on Sunday.



Figure 23: Man Wearing Brown Suit Jacket Mocking on White Telephone (Moose Photos, 2017)

Conclusion and future work.

After learning how susceptible humans are to phishing, it is no surprise that 88% of businesses experience spear-phishing attacks worldwide.

This report served as a reply to the request by the CEO of Packets and Parcels, following a penetration test where the scope was to explore the users' awareness concerning phishing attacks.

To avoid confusion, the report attempted to combine the several definitions discovered in the creation of a new definition. This definition served as the base of all examples in the full report. At the end of chapter 2.3), the report shares a brief history of phishing attacks. The chapter could have been more detailed, but the decision to cut it short was because the author felt that due to the vast explanations of phishing it was challenging to find specific information which related to the topic. Neither did the history part serve as a tool in user awareness training.

The report exposed several weaknesses in the business' infrastructure, and some of the methods penetration testers utilized to perform the test. The pre-attack phase displayed the penetration testers reconnaissance of the building, and the attack-phase displayed the highlights from the test. The results demonstrated the weaknesses which identified as elevated, high, and extreme. Table 4 uncovered which methods put the company most at risk.

In chapters 4.0), to 4.7c), the report served to explain the mechanisms behind phishing attacks. The report explored each method utilizing tools such as research, case studies, and examples from relevant attacks. By breaking down the methods and techniques, it was easier to defend the recommendations for mitigation. Some topics received more attention than others. The reason for this decision was that the information on the topic was limited. The material collected in each topic, including the results from the penetration test, was then applied to suggest methods and activities for user awareness training.

In chapter 5.0), relevant information serving as consequences of phishing attacks were elaborated. The exploration of topics such as industrial espionage and theft demonstrated which Plain Sight information was at the highest risk, and the repercussions of leaked information once a penetration tester enters a building.

In the final chapter, the report compiles suggestions for awareness training to recommend a program and course of action which aims to raise the awareness of the employees. Some suggestions were a boot camp, roleplaying, Kahoot and engaging a cartoonist for the newsletter. Included in the awareness training is a quiz which plays on simplicity, humour, and the information in the report. The next newsletter plans to reveal the answers to the quiz if published.

Challenges Overcome

- In the introduction, the report gathered several definitions of "phishing" and based all examples, findings et cetera on the definition.
- In the history portion, the report directed its attention toward a short description of attacks which appeared to change the history of phishing (as described in the definition). The report avoided mentioning financial losses, as it had no relevance to user awareness training.
- In the event of unclear definitions, the author decided on a definition and wrote the following information based on the findings. One example of this was the topic of dumpster-diving.
- Among the several techniques used to phish, the methods mentioned in the report could raise user awareness through training. Due to lack of time and word count, several techniques were left out but acknowledged in figures 4 and 5 in chapter 4.0).
- The report covered the techniques which interacted with each other in the topics where they had most relevance, as in the case of spoofing, which was introduced in chapter 4.1), and elaborated in chapter 4.6a).

Future work:

There is no use in budgeting a high cost towards awareness training if the training only is enforced "here and now". Entertaining the idea of a cyber risk index to mitigate phishing attacks can motivate the employees to embed a culture of security awareness throughout the company, causing the damages from a potential threat to decrease in the long run. The index may also motivate in the long run.

The C.E.O should consider engaging a cartoonist in creating a comic strip in the monthly newsletter. The strip should display amusing situations revolved around phishing which happens in the workplace. A creative writer could also contribute to writing an intriguing update on the cybersecurity front. As mentioned in chapter 4.6), the newsletter should include the score of the employees who report phishing emails and treat them appropriately. The boot camp can also count as some amount of points.

In light of the studies performed by (Sheng et al., 2007), the system administrator recommends Packets and Parcels engages the incident response team to create a biweekly Kahoot to test the employees' knowledge with a small prize for the winner (cinema tickets, fruit basket et cetera).

Regarding awareness training revolving around phishing-emails, Packets and Parcels should consider setting a goal for the employees based on the Cyber Risk Index. When the employees together have reached the goal of lowering the risk of attack, the company should award the employees. Suggestions for rewards are a "night out" sponsored by the company or a weekend trip.

References

- Aaron, G., (2018). *Phishing Activity Trends Report*. [online] Anti-Phishing Working Group, p.2. Available at: https://docs.apwg.org/reports/apwg_trends_report_q3_2018.pdf [Accessed 1 May 2020].
- Abad, C., (2005). The economy of phishing: A survey of the operations of the phishing market. *First Monday*, [online] 10(9). Available at: <https://journals.uic.edu/ojs/index.php/fm/article/view/1272/1192>
- ahdictionary.com, (n.d). Phish. In: *The American Heritage Dictionary of The English Language*. [online] Houghton Mifflin Harcourt. Available at: <https://www.ahdictionary.com/word/search.html?q=phish> [Accessed 1 June 2020].
- Alghamdi, H., (2017). *Can Phishing Education Enable Users To Recognize Phishing Attacks?*. Masters dissertation. Technological University Dublin.
- Andrews, L., (2016). *Passwords Reveal Your Personality*. [online] Psychology Today. Available at: <https://www.psychologytoday.com/us/articles/200201/passwords-reveal-your-personality> [Accessed 22 May 2020].
- Aolwatch.org, (1995). *Aohell Documentation*. [online] Aolwatch.org. Available at: <http://www.aolwatch.org/chronic2.htm> [Accessed 19 April 2020].
- BBC.com, (2011). *Morgan: I Used Benji The Binman*. [online] bbc.com. Available at: <https://www.bbc.com/news/av/uk-16274015/leveson-inquiry-i-used-benji-the-binman-says-piers-morgan> [Accessed 24 May 2020].
- Carlson, B., (2005). *Social Engineering, 1899-1999: An Odyssey Through The New York Times*. *American Studies In Scandinavia*. 37 (1). [online] Lund: Lund University, p.70. Available at: https://lup.lub.lu.se/search/ws/files/7703618/4495_17334_1_PB_1.pdf [Accessed 11 May 2020].
- cathy_gig12, (2020). *"Packets And Parcels" Logo*. [image] Available at: https://www.fiverr.com/cathy_gig12 [Accessed 9 May 2020].
- Chan, T., Yap, V. and Soh, C., (2012). Embedded Based Tailgating/Piggybacking Detection Security System. *CHUSER 2012 - 2012 IEEE Colloquium on Humanities, Science and Engineering Research*, [online] pp.277-282. Available at: https://www.researchgate.net/publication/261054766_Embedded_based_tailgatingpiggybacking_detection_security_system [Accessed 18 May 2020].
- Chương, H., (2019). *Woman Standing On Front Of High-Rise Building*. [image] Available at: <https://www.pexels.com/photo/woman-standing-on-front-of-high-rise-building-2533287/> [Accessed 31 May 2020].
- Clipart, (n.d). [image] Available at: <https://www.clipart.email/download/6768593.html#.XsQKsaHt61U.link> [Accessed 19 May 2020].
- Cloudflare.com, (n.d). *Cloudflare*. [online] Cloudflare.com. Available at: <https://www.cloudflare.com/learning/security/glossary/malicious-payload/> [Accessed 12 May 2020].
- Collinsdictionary.com, (n.d). Phishing. In: *Collins*. [online] Collins. Available at: <https://www.collinsdictionary.com/dictionary/english/phishing> [Accessed 24 April 2020].

Computerhope.com, (2020). *What Is Dumpster Diving?*. [online] Computerhope.com. Available at: <https://www.computerhope.com/jargon/d/dumpdive.htm> [Accessed 24 May 2020].

cups.cs.cmu.edu, (2007). *CMU Usable Privacy And Security Lab (CUPS)*. [online] Anti-Phishing Phil. Available at: http://cups.cs.cmu.edu/antiphishing_phil/ [Accessed 29 May 2020].

Cyberx.tech, (2018). *7 Penetration Testing Phases To Achieve Amazing Results - Cyberx*. [online] Cyberx.tech. Available at: <https://cyberx.tech/penetration-testing-phases/> [Accessed 3 May 2020].

Dutton, J., (2018). *4 Of The 5 Top Causes Of Data Breaches Are Caused By Human Or Process Error - IT Governance UK Blog*. [online] IT Governance UK Blog. Available at: <https://www.itgovernance.co.uk/blog/4-of-the-5-top-causes-of-data-breaches-are-caused-by-human-or-process-error> [Accessed 8 May 2020].

Federal Bureau of Investigation, (2020). *2019 INTERNET CRIME REPORT*. [online] Federal Bureau of Investigation, p.9. Available at: https://pdf.ic3.gov/2019_IC3Report.pdf [Accessed 25 May 2020].

Federal Communications Commission, (n.d). *Avoid Spoofing Scams*. [ebook] Federal Communications Commission. Available at: https://www.fcc.gov/sites/default/files/avoid_spoofing_scams_english.pdf [Accessed 20 May 2020].

Field, T., (2016). *Email Security: Social Engineering Report*. [online] Princeton: Information Security Media Group and Agari. Available at: <https://dbac8a2e962120c65098-4d6abce208e5e17c2085b466b98c2083.ssl.cf1.rackcdn.com/email-security-social-engineering-report-pdf-7-w-2783.pdf> [Accessed 26 May 2020].

Financialcryptography.com, (2005). *Financial Cryptography: GP4.3 - Growth And Fraud - Case #3 - Phishing*. [online] Financialcryptography.com. Available at: <http://financialcryptography.com/mt/archives/000609.html> [Accessed 25 April 2020].

Fox, J., (2015). *113 Reducing Your Organizations Social Engineering Attack Surface Jen Fox*. [video] Available at: <https://www.youtube.com/watch?v=atlj86P9Zf8> [Accessed 8 May 2020].

Francis, R., (2016). *Ever Been In These Social Engineering Situations?*. [online] CSO Online. Available at: <https://www.csoonline.com/article/3048820/ever-been-in-these-social-engineering-situations.html#slide10> [Accessed 22 May 2020].

FraudWatchInternational.com, (2019). *What Is Vishing? Voice Phishing Scams Explained & How To Prevent Them*. [online] FraudWatch International. Available at: <https://fraudwatchinternational.com/vishing/what-is-vishing/> [Accessed 8 May 2020].

Fruhlinger, J., (2019). *Social Engineering Explained: How Criminals Exploit Human Behavior*. [online] CSO Online. Available at: <https://www.csoonline.com/article/2124681/what-is-social-engineering.html> [Accessed 11 May 2020].

HawaiiNewsNow, (2018). Yes, that is a password stuck to a screen at Hawaii's emergency management HQ. *Hawaii News Now*, [online] Available at: <https://www.hawaiinewsnow.com/story/37279882/yes-that-is-a-password-stuck-to-a-screen-at-hawaiis-emergency-management-hq/> [Accessed 21 May 2020].

Immortal Shots, (2018). *Man Cleaning The Glass Of Building*. [image] Available at: <https://www.pexels.com/photo/man-cleaning-the-glass-of-building-756883/> [Accessed 31 May 2020].

Imperva, (n.d). *Social Engineering Attack Lifecycle*. [image] Available at: <https://www.imperva.com/learn/application-security/social-engineering-attack/> [Accessed 10 May 2020].

Imperva, (n.d). *What Is Phishing / Attack Techniques & Scam Examples / Imperva*. [online] Imperva. Available at: <https://www.imperva.com/learn/application-security/phishing-attack-scam/> [Accessed 10 May 2020].

Janis, I., (1967). Effects of Fear Arousal on Attitude Change: Recent Developments in Theory and Experimental Research. *Advances in Experimental Social Psychology*, [online] 3, p.171. Available at: <https://www.sciencedirect.com/science/article/pii/S0065260108603445> [Accessed 23 May 2020].

Johnson, S., (2018). *Focus Photo Of Yellow Paper Near Trash Can*. [image] Available at: <https://www.pexels.com/photo/focus-photo-of-yellow-paper-near-trash-can-850216/> [Accessed 31 May 2020].

Kaspersky, (2020). *Phishing Activity Trends Report, 1St Quarter 2020*. [online] Kaspersky, p.9. Available at: https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf [Accessed 12 May 2020].

Kay, R., (2004). *Sidebar: The Origins Of Phishing*. [online] Computerworld. Available at: <https://www.computerworld.com/article/2575094/sidebar--the-origins-of-phishing.html> [Accessed 19 April 2020].

Kelion, L., (2013). *Cryptolocker 'Infects 250,000 Pcs'*. [online] BBC News. Available at: <https://www.bbc.com/news/technology-25506020> [Accessed 25 April 2020].

Kelleher, J., (2018). *ID: 17202791213129*. [image] Available at: <http://www.apimages.com/metadata/Index/Hawaii-North-Korea/56ab0d525e3640a9b8d7bd4f9d2e84cf/15/0> [Accessed 21 May 2020].

Kelleher, J., (2018). Hawaii prepares for 'unlikely' North Korea missile threat. *Associated Press*, [online] Available at: <https://apnews.com/687028df588f4411a1cb2a2747c43db9/Hawaii-prepares-for-%27unlikely%27-North-Korea-missile-threat> [Accessed 21 May 2020].

KnowBe4, (2017). *Social Engineering, Red Flags*. [image] Available at: <https://info.knowbe4.com/hs-fs/hub/241394/file-26212286.jpg?hsLang=en> [Accessed 12 May 2020].

KnowBe4, (2020). *Phish Alert Button / Employees Report Phishing Attacks With One Click*. [ebook] KnowBe4. Available at: <https://cdn2.hubspot.net/hubfs/241394/PhishAlert.pdf> [Accessed 12 May 2020].

KnowBe4, (n.d). *Phishing Vs Spear-Phishing*. [image] Available at: <https://info.knowbe4.com/hubfs/Phishing-vs-SpearPhishing.jpg?hsLang=en> [Accessed 12 May 2020].

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L., Hong, J. and Nunge, E., (2007). Protecting people from phishing. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '07*, [online] pp.911 - 913. Available at: https://www.researchgate.net/publication/221518419_Protecting_people_from_phishing_The_design_and_evaluation_of_an_embedded_training_email_system [Accessed 12 May 2020].

Kumaraguruk, P., Sheng, S., Acquisti, A., Cranor, L. and Hong, J., (2009). *Teaching Johnny Not To Fall For Phish*. [online] Carnegie: Carnegie Mellon University, p.4. Available at: https://www.heinz.cmu.edu/~acquisti/papers/johnny_paper.pdf [Accessed 29 May 2020].

LanFang, W. and HaiZhou, K., (2012). *A Research Of Behavior-Based Penetration Testing Model Of The Network*. International Conference on Industrial Control and Electronics Engineering. [online] Huaian: Faculty of Computer Engineering, pp.1680, 1681. Available at: <https://ieeexplore.ieee.org/document/6322734> [Accessed 3 May 2020].

Langberg, M., (1995). AOL Acts to Thwart Hackers. *Mercury News*, [online] p.1C. Available at: https://simson.net/clips/1995/95.SJMN.AOL_Hackers.html [Accessed 19 April 2020].

Leonard, T., (2002). Benji the Binman Cleans Up. *The Telegraph*, [online]. Available at: <https://www.telegraph.co.uk/news/uknews/1388476/Benji-the-Binman-cleans-up.html> [Accessed 24 May 2020].

Long, J., (n.d). *No Tech Hacking: A Guide To Social Engineering, Dumpster Diving, And Shoulder Surfing*. 1st ed. Burlington: Syngress Publishing, Inc and Elsevier, Inc, pp.274 - 277.

Madon, M., (2018). 4 Simple Tips for Stopping Vishing. [Blog] *Mimecast.com*, Available at: <https://www.mimecast.com/blog/2018/10/4-simple-tips-for-stopping-vishing/> [Accessed 8 May 2020].

Magni, O., (2019). *Person Resting Their Hand On Table*. [image] Available at: <https://www.pexels.com/photo/person-resting-their-hand-on-table-2058147/> [Accessed 31 May 2020].

malwarebytes.com, (n.d). *What Is A Spoofing Attack?*. [online] Malwarebytes. Available at: <https://www.malwarebytes.com/spoofing/> [Accessed 20 May 2020].

Martinez, L. and Winsor, M., (2018). 'This is not a drill': Hawaiians get false alert of missile attack due to worker's pushing 'wrong button'. *abc NEWS*, [online] Available at: <https://abcnews.go.com/US/drill-hawaii-residents-wake-false-alarm-imminent-missile/story?id=52328642> [Accessed 21 May 2020].

Merriam-webster.com, (n.d). Phishing. In: *Merriam-webster.com*. [online] Merriam-webster. Available at: <https://www.merriam-webster.com/dictionary/phishing> [Accessed 24 April 2020].

Miller, R., (2006). *Bank, Customers Spar Over Phishing Losses*. [online] News.netcraft.com. Available at: https://news.netcraft.com/archives/2006/09/13/bank_customers_spar_over_phishing_losses.html [Accessed 25 April 2020].

Moose Photos, (2017). *Man Wearing Brown Suit Jacket Mocking On White Telephone*. [image] Available at: <https://www.pexels.com/photo/man-wearing-brown-suit-jacket-mocking-on-white-telephone-1587014/> [Accessed 31 May 2020].

Nasralla, S. and Croft, A., (2016). *Austria's FACC, Hit By Cyber Fraud, Fires CEO*. [online] U.S. Available at: <https://www.reuters.com/article/us-facc-ceo-idUSKCN0YG0ZF> [Accessed 25 April 2020].

Newton Security Innovation, (n.d). *FAQ - NEWTON SECURITY*. [online] Newtonsecurityinc.com. Available at: <http://www.newtonsecurityinc.com/faq.html> [Accessed 17 May 2020].

Onojeghuo, C., (2016). *Man Sitting On Gray Pavement*. [image] Available at: <https://www.pexels.com/photo/adult-alone-art-blur-173299/> [Accessed 31 May 2020].

Oxford Learner's Dictionary, (n.d). Shoulder Surfing. In: *Oxford Learner's Dictionary*. [online]. Available at: <https://www.oxfordlearnersdictionaries.com/definition/english/shoulder-surfing?q=shoulder+surfing> [Accessed 21 May 2020].

Phishing.org, (2019). *Phishing / Phishing Examples*. [online] Phishing.org. Available at: <https://www.phishing.org/phishing-examples> [Accessed 3 May 2020].

Pindrop.com, (2016). CEO of FACC Fired After Firm was hit by Email Scam. [Blog] *Pindrop*, Available at: <https://www.pindrop.com/blog/ceo-of-austrian-firm-facc-fired-after-email-scam/> [Accessed 12 May 2020].

Pitarau.com, (n.d). *Vishwas - Meaning Of Vishwas / Hindu Name Vishwas / Pitarau*. [online] Pitarau.com. Available at: <https://www.pitarau.com/meaning-of-vishwas> [Accessed 12 May 2020].

Pixabay, (2016). *Person Holding Debit Card*. [image] Available at: <https://www.pexels.com/photo/shopping-business-money-pay-50987/> [Accessed 26 April 2020].

Ponemon Institue L.L.C., (2016). *Global Visual Hacking Experimental Study: Analysis*. [online] Ponemon Institue, pp.2, 6, 9. Available at: <https://multimedia.3m.com/mws/media/12542320/global-visual-hacking-experiment-study-summary.pdf> [Accessed 21 May 2020].

Proofpoint, (2020). *State Of The Phish*. [online] Proofpoint. Available at: <https://www.proofpoint.com/us/security-awareness/post/2020-state-phish-security-awareness-training-email-reporting-more-critical> [Accessed 25 May 2020].

Psychology.jrank.org, (n.d). *Competition*. [online] Psychology.jrank.org. Available at: <https://psychology.jrank.org/pages/135/Competition.html> [Accessed 12 May 2020].

Rader, M. and M. Rahman, S., (2013). Phishing Techniques and Mitigating the Associated Security Risks. *International Journal of Network Security & Its Applications*, 5(4), p.25.

Ritchey, D., (2015). *Tailgating: A Common Courtesy And A Common Risk*. [online] Securitymagazine.com. Available at: <https://www.securitymagazine.com/articles/86026-tailgating-a-common-courtesy-and-a-common-risk> [Accessed 19 May 2020].

Robson, D., (2011). *Phishing History - The Earliest Phishing Scams*. [online] Bright Hub. Available at: <https://www.brighthub.com/internet/security-privacy/articles/82116.aspx> [Accessed 19 April 2020].

Rouse, M., (2008). *What Is Vishing (Voice Or Voip Phishing)? - Definition From Whatis.Com*. [online] SearchUnifiedCommunications. Available at: <https://searchunifiedcommunications.techtarget.com/definition/vishing> [Accessed 8 May 2020].

Salahdine, F. and Kaabouch, N., (2019). *Social Engineering Attacks: A Survey*. [online] North Dakota: School of Electrical Engineering and Computer Science, University of North Dakota, p.6. Available at: <https://securitytrails.com/blog/social-engineering-attacks> [Accessed 14 May 2020].

Salinger, L., (2013). *Encyclopedia Of White-Collar And Corporate Crime*. Los Angeles, London, New Delhi, Singapore, Washington DC: SAGE Publications Inc, p.463.

Savvas, A., (2012). *91% Of Cyberattacks Begin With Spear Phishing Email*. [online] Techworld.com. Available at: <https://www.techworld.com/news/security/91-of-cyberattacks-begin-with-spear-phishing-email-3413574/> [Accessed 12 May 2020].

Sharma, M., (2010). *Commonwealth Bank Served As Training Ground For Global Phishing Attacks*. [online] Computerworld. Available at: <https://www.computerworld.com/article/3461019/commonwealth-bank-served-as-training-ground-for-global-phishing-attacks.html> [Accessed 25 April 2020].

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L., Hong, J. and Nunge, E., (2007). *Anti-Phishing Phil: The Design And Evaluation Of A Game That Teaches People Not To Fall For Phish*. [online] Carnegie: Carnegie Mellon University, p.8. Available at: https://cups.cs.cmu.edu/soups/2007/proceedings/p88_sheng.pdf [Accessed 29 May 2020].

Simmons, R., (2018). The First Rule of Cybersecurity: Trust No One, Or...?. [Blog] *Beyond Trust*, Available at: <https://www.beyondtrust.com/blog/entry/first-rule-cybersecurity-trust-no-one> [Accessed 11 May 2020].

Smith, A., Papadaki, M. and Furnell, S., (2013). *Improving Awareness Of Social Engineering Attacks*. Plymouth: Centre for Security, Communications and Network Research, Plymouth University, p.249.

Sophos, (2007). *Torrent Of Spam Likely To Hit 6.3 Million TD Ameritrade Hack Victims*. [online] Available at: <https://www.sophos.com/en-us/press-office/press-releases/2007/09/ameritrade.aspx> [Accessed 25 April 2020].

Street, J., (2012). *DEFCON 19: Steal Everything, Kill Everyone, Cause Total Financial Ruin! (W Speaker)*. [video] Available at: <https://www.youtube.com/watch?v=JsVtHqICeKE> [Accessed 24 May 2020].

Symanovich, S., (n.d). *What Is Shoulder Surfing?*. [online] Lifelock.com. Available at: <https://www.lifelock.com/learn-identity-theft-resources-what-is-shoulder-surfing.html> [Accessed 22 May 2020].

Thanyakij, B., (2020). *Macbook Pro On White Table*. [image] Available at: <https://www.pexels.com/photo/macbook-pro-on-white-table-3740741/> [Accessed 31 May 2020].

The Graphus Blog, (2020). *The "Five Agonies" Of Social Engineering Cyber Attacks - Graphus*. [online] Graphus. Available at: <https://www.graphus.ai/the-five-agonies-of-social-engineering-cyber-attacks/> [Accessed 14 May 2020].

Tiger Lily, (2020). *2 Men Standing In A Warehouse Talking*. [image] Available at: <https://www.pexels.com/photo/2-men-standing-in-a-warehouse-talking-4480798/> [Accessed 31 May 2020].

Tool, T., (1991). *MIT Guide To Lock Picking*. 2nd ed. [ebook] Cambridge, Massachusetts: Massachusetts Institute of Technology. Available at: <https://www.lysator.liu.se/mit-guide/MITLockGuide.pdf> [Accessed 29 May 2020].

Tung, L., (2016). *CEO Fired After 'Fake CEO' Email Scam Cost Firm \$47M*. [online] CSO Online. Available at: <https://www.csoonline.com/article/3502270/ceo-fired-after-fake-ceo-email-scam-cost-firm-47m.html> [Accessed 12 May 2020].

Twitter, (2018). *#Warningpoint2*. [image] Available at: <https://pbs.twimg.com/media/DTqinRxWsAEcLQF.jpg> [Accessed 21 May 2020].

Vishwanath, A., (2017). *Why Most Cyber Security Training Fails And What We Can Do About It*. [video] Available at: <https://www.youtube.com/watch?v=3L3lrAN30a4> [Accessed 12 May 2020].

Vishwanath, A., Harrison, B. and Ng, Y., (2016). Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility. *Communication Research*, [online] 45(8). Available at: https://www.researchgate.net/publication/278676335_Suspicion_Cognition_Automaticity_Model_SCAM_of_Phishing_Susceptibility [Accessed 12 May 2020].

Wang, S., Zhu, S. and Zhang, Y., (2018). *Blockchain-Based Mutual Authentication Security Protocol For Distributed RFID Systems*. 2018 IEEE Symposium on Computers and Communications (ISCC). Beijing, pp.00074-00077.

whatis.techtarget.com, (2017). *What Is Tailgating (Piggybacking)? - Definition From Whatis.Com*. [online] WhatIs.com. Available at: <https://whatis.techtarget.com/definition/tailgating-piggybacking> [Accessed 8 May 2020].

whatis.techtarget.com, (n.d). *What Is Industrial Espionage? - Definition From Whatis.Com*. [online] WhatIs.com. Available at: <https://whatis.techtarget.com/definition/industrial-espionage> [Accessed 24 May 2020].

Winkler, I., (1996). Case Study of Industrial Espionage Through Social Engineering. [online] Carlisle: National Computer Security Association, pp.3, 6. Available at: <https://csrc.nist.gov/csrc/media/publications/conference-paper/1996/10/22/proceedings-of-the-19th-nissc-1996/documents/paper040/winkler.pdf> [Accessed 25 May 2020].

Young, J., (2020). *People Inside A Bus Wearing Masks*. [image] Available at: <https://www.pexels.com/photo/people-inside-a-bus-wearing-masks-3960076/> [Accessed 31 May 2020].

Yourdictionary.com, (2017). semantic attack - Computer Definition. In: *Your Dictionary*. [online]. Available at: <https://www.yourdictionary.com/semantic-attack> [Accessed 12 May 2020].

Zhang, L. and McDowell, W., (2009). Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords. *Journal of Internet Commerce*, 8(3-4), pp.180, 186.