TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technologies

IT College

Romaine Ayoki Burrell 177783IVSB

Building Resilience to Social Engineering in Pipedrive through Awareness Training

Bachelor's Thesis

Supervisor:	Kaido Kikkas
	PhD
Co-Supervisor:	Jesse Wojtkowiak
	MSc, CISSP

Tallinn 2020

TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

IT Kolledž

Romaine Ayoki Burrell 177783IVSB

Pipedrive'i koolitusprogramm vastupanuvõime tõstmiseks sotsiaalsele manipuleerimisele

bakalaureusetöö

Juhendaja: Kaido Kikkas

PhD

Kaasjuhendaja: Jesse Wojtkowiak

MSc, CISSP

Tallinn 2020

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Romaine Ayoki Burrell

30.04.2020

Abstract

Pipedrive has implemented a basic awareness training programme and now seeks to improve on that. This thesis aims to investigate the current security awareness training programme, and document suggested improvements.

An investigation was carried out by looking at how the training is delivered, a close-ended survey, analysis of the simulated phishing emails and focus area of the training programme. The analysis showed that the training was one dimensional and used a "one-size" fits all model. Also, the training was geared towards phishing and spear phishing, while a few other topics e.g. password management was included - it does not cover other important social engineering techniques such as Business Email Compromise (BEC)...etc

The conclusion yielded was that the programme already has a good baseline structure. However, improvements such as adding a few more topics (after a risk assessment has been done and the most logical attacks are identified), making the course more engaging, and rewriting policies that are not wordy and contain mostly complex (legal) jargon.

This thesis is written in English and is 48 pages long, including 7 chapters, 13 figures and 2 tables.

Annotatsioon

Pipedrive'i koolitusprogramm vastupanuvõime tõstmiseks sotsiaalsele manipuleerimisele

Pipedrive on juurutanud elementaarse turvateadlikkuse programmi ja soovib nüüd seda paremaks muuta. Käesoleva lõputöö eesmärk on uurida praegust turvateadlikkuse koolitusprogrammi ja dokumenteerida soovitatud parandused.

Uuriti koolituse läbiviimist, viidi läbi etteantud vastustega küsitlus, andmepüügimeilide simulatsioon ja koolitusprogrammi fookusgrupi analüüs. Analüüs näitas, et varasem koolitus oli ühemõõtmeline ja selle jaoks kasutati vaid üht mudelit. Samuti oli koolitus suunatud eeskätt suunamata ja suunatud õngitsemisele ning kuigi ka mõned muud teemad (nt. paroolide haldamine), ei kajastatud mitmeid sotsiaalmanipulatsioonitehnikaid (näiteks BEC ehk ettevõtte e-posti ülevõtmine).

Autor jõudis järeldusele, et programmil on juba hea lähtestruktuur, kuid pakutavad täiendused muudavad kursuse huvitavamaks ja aitavad vältida ka keerulise juriidilise stiili kasutamist turvaeeskirjades.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 48 leheküljel, 13 peatükki, 8 joonist, 2 tabelit.

List of abbreviations and terms

B2B	Business to business
BEC	Business email compromise
CSAT	Cyber Security Awareness Training
FBI	Federal Bureau of Investigation
GDPR	General Data Protection Regulation
IC3	Internet Crime Complaint Center
InfoSec	Information Security
OSINT	Open-Source Intelligence
PII	Personally identifiable information
SE	Social Engineering
USD	United States Dollars

Table of Contents

List of figures

List of tables

1 Introduction

Phishing is an attempt to obtain sensitive information, such as usernames, passwords, and credit card details, often for malicious reasons, by disguising oneself as a trustworthy entity in an electronic communication [1]. Still regarded as one of the most effective attacks to date. Phishing works because of humans' default behaviour to trust. As further defined in chapter 3. This information is then exploited by being sold on the black market or combined with other information to get access to restricted information. Phishing can result in breaches that have a costly impact on a company's reputation or financial losses. Over the years, different variations of phishing have been created. Phishing is, however, only but one of the various social engineering techniques currently being used. Many security awareness training programmes focus mostly on Phishing because of its far-reaching effects. However, over the years, other techniques have been created due to persons being more aware of phishing.

This thesis aims to look at ways to allow Pipedrive to harden its defences against phishing attempts as well as other social engineering attacks by suggesting technical and non-technical solutions and a redesign of the current security awareness programme.

This paper will have 7 chapters. The first chapter will host the Introduction. The second chapter will look into Background - Pipedrive. The third chapter will focus on The main concept and current state. The fourth chapter looks at the Methodology. The Fifth chapter will look at the Survey Analysis. The sixth chapter deals with the Training programme improvement suggestions that Pipedrive can incorporate. Remaining chapters will give a summary and look at the references and additional details that have not been included in the main section of this paper.

2 Background - Pipedrive

Pipedrive is the first CRM platform made for salespeople, by salespeople. Founded in Tallinn, Estonia in 2010, co-founders; Timo Rein, Martin Henk, Ragnar Sass and Martin Tajur set out to build a customer relationship management (CRM) tool that helps users visualize their sales processes and get more done. Pipedrive was created around activity-based selling, a proven approach that's all about scheduling, completing and tracking activities. Pipedrive currently has over 600 employees, Over 90 million in funding, used by over 90,000 companies in over 170 countries and has 8 offices across the globe (Tallinn, Tartu, New York, Lisbon, London, Prague, Dublin and Florida).

With a user base of over 90,000 companies (small, medium and large), Pipedrive holds what most attackers want – data. As a B2B service provider, Pipedrive establishes itself as a data processor for its customers. This means Pipedrive customers use the platform to store, manage and track their customer's/client's data. Therefore, each potential or signed client of theirs is added to Pipedrive. Additionally, Pipedrive is also a data controller since it is responsible for the data it holds on its employees and data that has been shared with 3rd party service providers to aide in executing its functions.

Since Pipedrive has become a popular platform, recognised internationally as a game-changer in the CRM industry working with major global brands – an attacker will be more drawn to the platform. This increases the number of data assets that Pipedrive will have to protect, store and manage. Pipedrive could be holding millions of data on thousands of companies and hundreds of thousands of persons.

3 The main concept and current state

Before understanding how phishing impacts Pipedrive, we first have to understand what social engineering is, phishing, the different techniques of phishing and different types of phishing.

3.1 Social Engineering

Social engineering can be classified as using the art of deception to gain your trust and trick you into revealing information you would not normally share. Social engineering relies on human rational (psyche) to be able to execute. As humans are emotional beings, social engineers are skilled at tapping into those emotions and exploiting them [2]. Social engineering takes the way humans are wired to make decisions and exploits the vulnerabilities in those processes [3].

Why is this successful

We would need to understand one of the key" ingredients" of social engineering – “Psychological manipulation”. Psychological manipulation refers to the form of social influence that aims to change the perception or behaviour of people through underhanded, abusive or deceptive techniques. According to psychology author, George Simon, psychological manipulation can be successful when a manipulator manages to conceal their intentions, learn about the weaknesses of their victims and identify what technique they can use on them [4].

Some of these techniques include [5];

- Positive reinforcement
    - Praise
    - Excessive apologising
    - Approval
    - Money

    - Attention
    - Public recognition
    - Superficial empathy
- Negative reinforcement
    - Removing their victims from negative situations as a form of reward.
- Intermittent reinforcement
    - Intermittent negative reinforcement
        - Creates doubts and fears
    - Intermittent positive reinforcement
        - Encourages the victims to persist

Persons said to be most likely manipulated are those that lack assertiveness, self-reliance, self-control, self-confidence or sense of identity. Some persons are naïve, as to them, persons may not be as dubious as others portray them to be [6]. Manipulation/mind control is not a new concept and can be seen in advertisements, sales tactics…etc [1] [4].

There are several tactics encompassing manipulation/mind control and exploitation that have moved to the digital world, these include phishing (in its different varieties), clickjacking, cross-site scripting and many others. A few have been expanded on in this chapter.

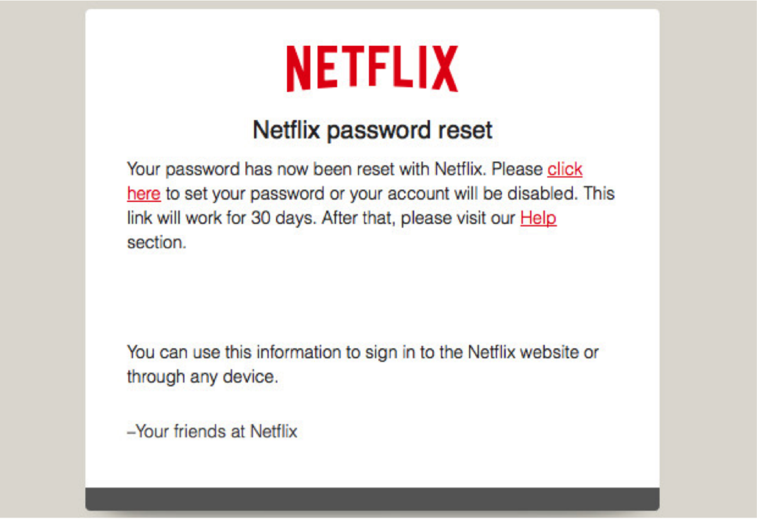
Phishing

A phishing email is a form of spam email; it's an undesirable message sent in bulk to many recipients or a particular person. While traditional spam emails are mostly a part of advertising campaigns, phishing emails are more sinister. The main goal of a phishing email is usually to obtain confidential information from the email's recipient [7]. Phishing emails try to look as real and convincing as possible, however, they have malicious intents [8]. Phishing can lead to the installation of malware, freezing of the system as part of a ransomware attack, or revealing of sensitive information [9].

According to the Infosec Institute, the below are the most common Phishing attempts and examples of different types of each.

- Link Manipulation - It is done by directing a user through fraud to click a link to a fake website [10]. Some examples of link manipulations are;

  - Hiding the URL - this is when an attacker uses words instead of the actual link. eg. using “click here” instead of “http://malicioussite.com” [11].



NETFLIX

Netflix password reset

Your password has now been reset with Netflix. Please click here to set your password or your account will be disabled. This link will work for 30 days. After that, please visit our Help section.

You can use this information to sign in to the Netflix website or through any device.

–Your friends at Netflix

Figure 1. image of a URL hidden (hyperlinked text) in an email received from Netflix

  - Misspelt URL - This is where an attacker is unable to spoof the domain of a well-known service, they will then misspell the domain and use this in their attempts to have use visit their malicious site. This technique is also referred to as type squatting or URL hijacking [11]. e.g. Original = “https://www.spoons.com” , malicious link = “https://www.sp00ns.com” . You can see from the example that both URLs look the same however, in the malicious link instead of the letter “O”, there is the number “0” (zero).

- Pop-Ups - according to the InfoSec Institute, pop-up phishing is one of the easiest to execute. A user would receive a pop-up message box that leads to a fraudulent website [10]. There are afew different tricks used to execute this.

  - In-Session Pop-up - This is when a user gets a message while browsing on a webpage. This typically occurs on banking sites where your credentials can be stolen [10].

  - Pop-up tech support - This is where a user will receive a pop-up message letting them know that there is a virus detected on their computer and they should click a link and enter their contact details to be contacted [10].

- Website Forgery - Website forgery is another phishing technique that works by making a malicious website impersonating an authentic one, to make the visitors give up their sensitive information like account details, passwords, credit card numbers, etc [10]. Website forgery can occur in different ways including;

  - Cross-site scripting -XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites [12].

Business email compromise

Carried out by transnational criminal organizations that employ lawyers, linguists, hackers, and social engineers, BEC can take a variety of forms. But in just about every case, the scammers target employees with access to company finances and trick them into making wire transfers to bank accounts thought to belong to trusted partners—except the money ends up in accounts controlled by the criminals [13].

According to the FBI's Internet Crime Complaint Center (IC3), there have been over 1,300 reported cases and identified exposed losses, now totalling over three hundred million (300,000,000) USD [13]. While no actual figures have been provided, of the roughly six hundred thousand (600,000) EUR in financial loss, a significant amount of this attributed to BEC where small companies reported losing between ten thousand (10,000) EUR and twenty thousand (20,000) EUR (according to the Estonian Information System Authority: Annual Cyber Security Assessment 2019) [14].

Attackers find a way into the network by spear-phishing and use of malware. They remain undetected, study the company's operation and then act when the CEO or relevant personnel is away. The attacker then sends a fake email to a targeted employee in the finance office—a bookkeeper, accountant, controller, or chief financial officer. A request is made for an immediate wire transfer, usually to a trusted vendor. The targeted employee believes he is sending money to a familiar account [13].

Different types of phishing

The popularity of email phishing becoming a well-known vector has raised concerns of many and rightfully so. Due to this rise in awareness and its impact persons have become more sceptical and this has impacted the growth of traditional email phishing campaigns. New types of phishing were introduced, these are;

- **Vishing** - Voice phishing is when an attacker makes contact with someone in an attempt to social engineer them via a phone call [15].

- **Smishing** - Just like phishing, smishing uses cell phone text messages to lure consumers in. Often the text will contain an URL or phone number. The phone number often has an automated voice response system. And again, just like phishing, smishing message usually asks for your immediate attention [15]. One reason why Smishing works is that it's much more difficult to see the actual link via a cell phone compared to checking this on a computer where you can hover the mouse to see the actual link [16].

- **Impersonation** - one of the most dangerous and one of the riskiest. impersonation is the physical impersonation of an employee of the target company or someone in authority who can be trusted [3].

- **Spear Phishing** - After an attacker has done deep OSINT of their target. Then they create a very personalized form of phishing [3]. This means that they have understood enough details about you to craft a malicious email that you can relate to.

3.2 Impact on Pipedrive

Pipedrive like any other company holds assets that any attacker would find useful. One such asset is data. Yes, we can say that almost every company has data, but some hold data that can be considered more important in Pipedrive's case. Pipedrive being a sales CRM holds the data of over 90,000 companies - ranging from small to large entities. Additionally, Pipedrive will also hold data belonging to the customers of those companies, this can range into the millions. Unauthorised access to the Pipedrive network can prove catastrophic as attackers can not only exfiltrate the data but sell or combine this data with other data sources. This combined data can create a profile of a person that gives threat actors information needed to conduct actions such as account takeover, identity theft...etc.

It is also important to know that apart from customers data being at risk, data of the employees themselves and Pipedrive reputation and financial standing could be affected. Pipedrive could stand to lose customers and significant financial losses. Data loss of any kind can be constituted as a breach and countries have implemented strict regulations that have large penalties, GDPR is one of the most notable ones. The General Data Protection Regulation (GDPR), is a European Union legislation that protects the data of all EU residents and citizens. Any company anywhere in the world is subjected to GDPR if they hold or process data for any EU or EEA member resident or citizens. GDPR levies fine up to €20 million (EUR) or 4% of global annual turnover, whichever is greater [17]. It is important to note that regulations such as these along with the cost associated with a data breach, according to the IBM and Ponemon institute 2019 report can range from 300,000 - 11 million (on average, not including mega breaches that can cost more than 350million) [18] can cripple a company forcing them out of business or to start over [8].

Phishing is one attack vector that Pipedrive has to look into since it is still widely regarded as one of the most successful to date. Having mentioned in chapter 2, Pipedrive as a data controller for its employees' data and its customer's data shared with 3rd party service providers, likewise being a data processor for its customers and their clients manage millions of data assets every day. These data assets can be an attractive target for threat actors and therefore persons with ill intent will use any means necessary to get to this data if they so, please. As social engineering is still ranked as the most exploitable vector, the need for resilience and hardening is a much-needed area of assessment and continual improvement.

4 Methodology

Identifying that the need for improvement on resilience to Social engineering, the current thesis aims to reduce vulnerabilities to phishing at Pipedrive and introduce other social engineering knowledge. To accomplish this, research into how other companies have designed their security awareness programme, how it is delivered and how it is structured and can any of these approaches be incorporated into Pipedrive’s training programme. Research also was done into different e-learning and teaching frameworks. Maslow’s Hierarchy (Pyramid) of needs and John Keller’s ARCS model. Understanding these models will aid in looking at the structure of the training from a psychological point of view to yield a greater impact in delivery. Delivering a training programme that keeps learners engage, is fundamental in ensuring that the learner retains the knowledge and not aim to get it done but skipping through the training.

Additionally, Pipedrive undergoes yearly security awareness training. The training involves fifteen multiple-choice questions and phishing simulation. The results from the phishing simulation were analysed. This includes how successful was the simulation, the number of people that were caught by the simulation.

A survey was also launched to gather basic knowledge from all participants to their level of understanding of phishing and social engineering in general.

The survey was delivered by the use of Google Forms. It consisted of 10 closed-ended questions taking into account respondents department and location. Data from the phishing simulation along with samples of the phishing emails can be seen in Appendix one. Admitting that this topic is not unique, what is unique is how this topic relates to Pipedrive and understanding how to limit the exposure.

Having identified the issue, I will assess the current state of the security awareness programme and provide suggestions for improvement, using the survey results.

All of the above allowed us to build a profile for each location and departments. It gave us insights about the effectiveness of the current training setup. We also learned about the training deliverability and the undesirability of persons to do the training.

We also learnt that persons would much rather click through to the end, do the questions and continue on their day. This highlighted to us a fundamental flaw that had to be addressed. These suggestions can be seen in chapter 6.

4.1 Keller's ARCS Model

This model may be perceived as a systematic problem-solving approach that instructional designers can use to create content [19]. This model takes into consideration:

- Knowing and identifying the elements of human motivation [19],
- Analysing audience characteristics to determine motivational requirements [19],
- Identifying characteristics of instructional materials and processes that stimulate motivation [19],
- Selecting appropriate motivational tactics, and [19]
- Applying and evaluating appropriate tactics [19].

The ARCS model has two main categories: first one focuses on components of motivation and the second focuses on the systematic design process [20]. The model can then be broken down into four categories (representing the acronym ARCS), these categories have their subcategories as shown below [21]:

Table 1. Categories of Keller's ARCS model [21]

Attention	**Relevance**	**Confidence**	**Satisfaction**
A1Perceptual arousal A2Inquiry arousal A3 Variability	R1 Goal orientation R2 Motive matching R3 Familiarity	C1 Learning requirements C2 Success opportunities C3 Personal control	S1 Intrinsic reinforcement S2 Extrinsic rewards S3 Equity

.

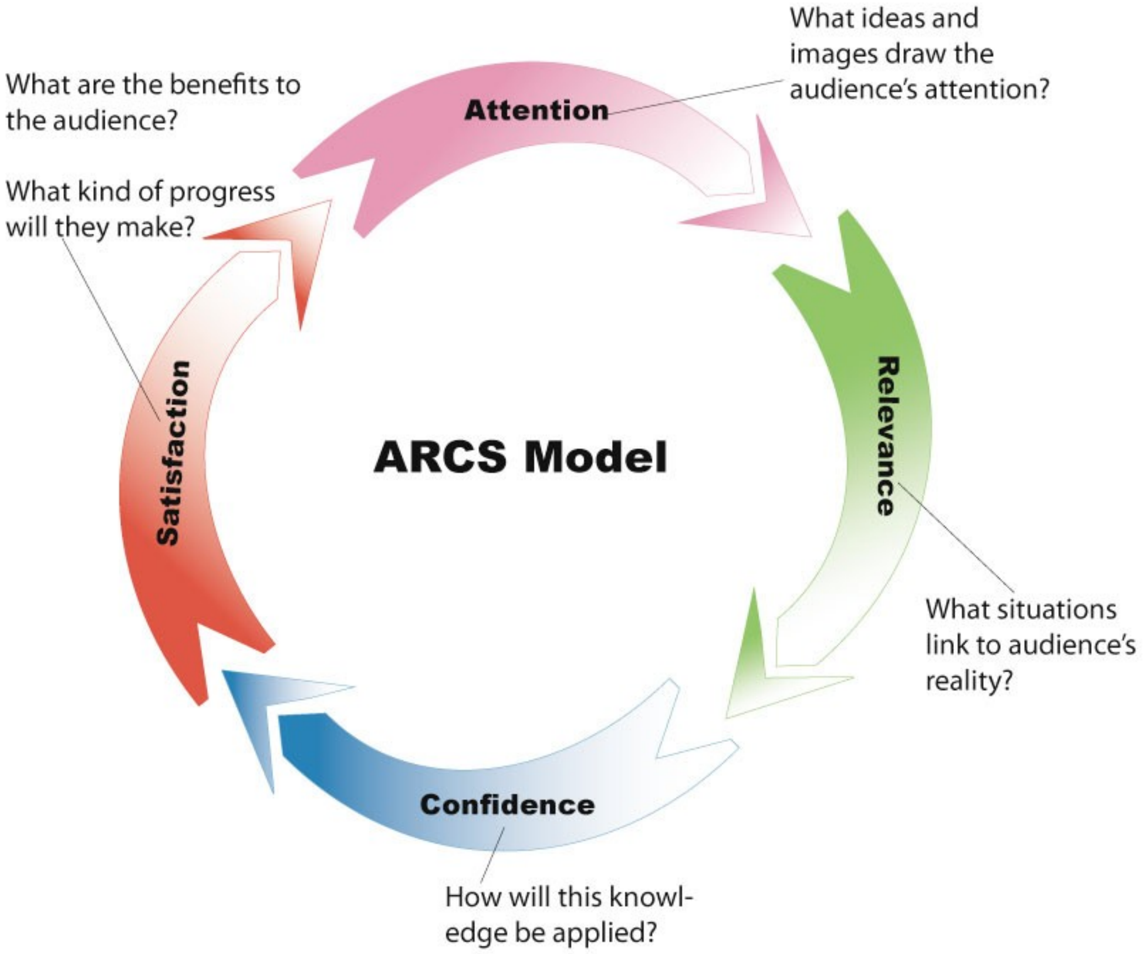

What ideas and images draw the audience's attention?
What are the benefits to the audience?
What kind of progress will they make?
Attention
ARCS Model
Satisfaction
Relevance
What situations link to audience's reality?
Confidence
How will this knowl-edge be applied?

Figure 2. diagram depicting the flow of the ARCS model [22].

What does each category mean

Attention includes (1) perceptual arousal--use of strategies to gain initial interest; (2) inquiry arousal--the use of problem-solving, questioning, a sense of mystery and progressive disclosure to increase interest; (3) variability--the use of variety (lecture with visuals, group activity, or game) for a change of pace [23].

Relevance, which is the concept of linking the content to the learner's needs and wants, includes (1) goal orientation, which may mean the outcome of learning such as obtaining a job, reward, etc. or may imply the means of learning; (2) motive matching involves the learner's choices about strategies of learning, such as by group interaction, competition, or individual work; (3) familiarity or connect to what one already believes and understands such as realistic graphics, people’s names, personal learning experiences [23].

Confidence, which provides a sense of self-worth and success ability in challenging tasks, involves strategies to (1) provide learning requirements in the form of clear objectives; (2) provide success opportunities early and often enough to establish the learner’s belief in his or her ability to achieve. (3) provide personal control over the learning with choices of content, objectives and activities. This relates success to one’s choices and effort [23].

Satisfaction includes strategies to (1) increase the natural consequences for use of the content, simulations, projects, real-life activity; (2) provide positive consequences--both intrinsic and extrinsic rewards; (3) assure equity of rewards so that they match achievements [23].

4.2 Maslow’s hierarchy of needs

Developed by Abraham Harold Maslow, an American psychologist and philosopher. Maslow’s major works focused on motivation and personality. He believes that there is a hierarchy of needs that must be satisfied, ranging from basic physiological requirements to love, esteem, and, finally, self-actualization [24].

Maslow's hierarchy of needs is a motivational theory in psychology comprising a five-tier model of human needs, often depicted as hierarchical levels within a pyramid [25].

Needs lower down in the hierarchy must be satisfied before individuals can attend to needs higher up. From the bottom of the hierarchy upwards, the needs are physiological, safety, love and belonging, esteem, and self-actualization [25].

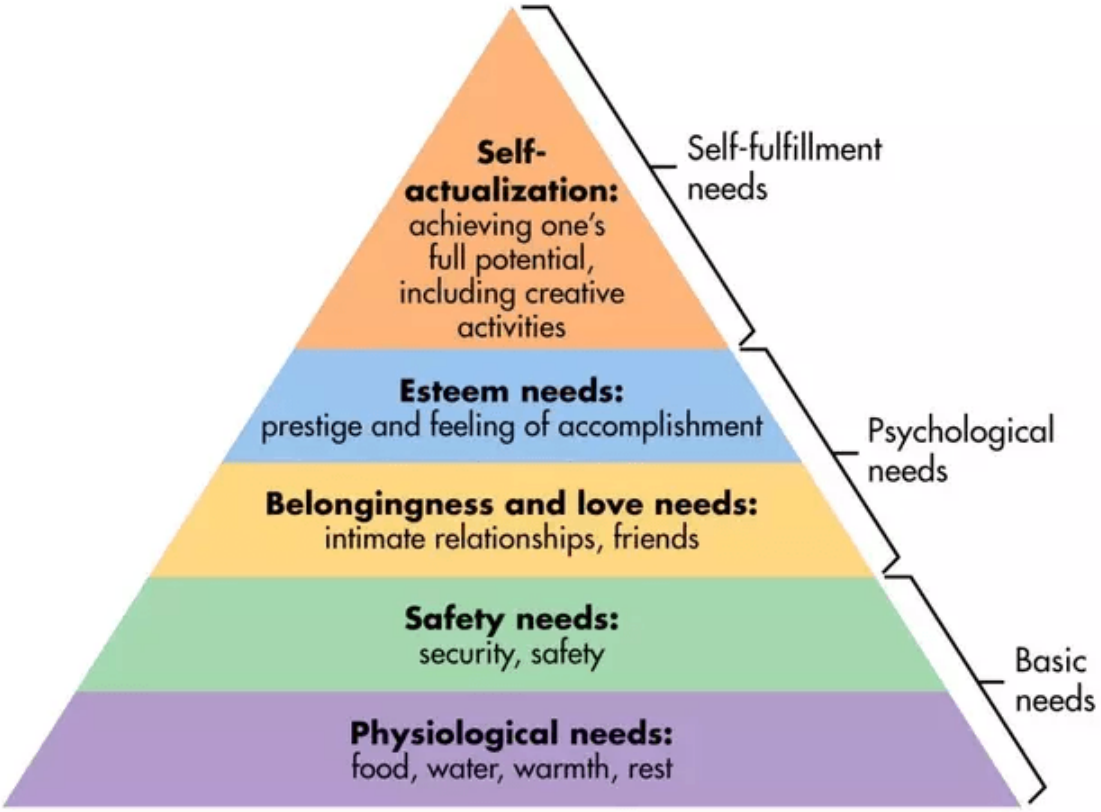

Self-actualization: achieving one's full potential, including creative activities
Esteem needs: prestige and feeling of accomplishment
Belongingness and love needs: intimate relationships, friends
Safety needs: security, safety
Physiological needs: food, water, warmth, rest
Self-fulfillment needs
Psychological needs
Basic needs

Figure 3. Pyramid depicting Maslow's Hierarchy of Needs [25].

4.3 How others are doing it

Research conducted to analyse what are considered to be the areas of social engineering that is of greatest concerns to different companies revealed that Phishing is where most security awareness programme is focused. It's not hard to see why this is so. Phishing is still the most effective vector (according to IBM cost of a data breach report). However, other attack vectors are not ignored depending on the industry and services this business may offer.

According to security and compliance firm; Security Metrics, these are the recommended areas for training;

1. Classical social engineering – This is in-person or vishing type social engineering. Persons would have been contacted or visited by someone that might be from their IT department seeking to get their credentials to debug an issue [26].

2. Email social engineering – This is your typical phishing or spear-phishing emails [7]. The attack vector relies on crafty and sometimes ingenious creation that stroke the right human emotion or catch them at a mental state of being less aware. Also, uninformed employees are a great way for social engineers to achieve their target.
3. Opportunity social engineering – This includes USB drops. AN attacker leaves a few USB drives with the hope that someone will insert these into their computers [26].

A few of these have been corroborated by Security awareness firm, InfoSec Institute. Phishing again showing up in the list, along with; Whaling, Pretexting, Baiting and Quid Pro Quo, and also tailgating.

Western Area Power Administration (WAPA)

Currently, a government organisation found in U.S. Department of Energy offers a CSAT covering efficient use of assets(computers, security badges(access cards), implications of misuse to the business, password creation and storage, browsing, remote work, physical security, email security, mobile security, use of removable media, procurement of equipment and services and PII protection. Under their social engineering section: Thwart social engineering, Phishing/Whaling/Spear phishing, Internet Hoaxes, Identity theft and Malware [27].

The training then explains why this is necessary and the policies that are involved.

Since WAPA is a government organisation, that has access to a massive amount of critical data, they are required to have a comprehensive training plan. This was created base on the risk landscape they have a discovered and requirements by federal laws [27].

University of California

Offers both a 40-minute online training where persons who are required to complete this training will be contacted from a designated email address. They will be required to login to a system and complete the training. They also offer documents for download in the form of various presentations and videos. Alternatively, persons can request an in-person training. Some topics are not relevant for certain roles and as such, there is a role-based training [28] [29].

Fitting this in with Pipedrive

The structure of Pipedrive while still lending itself to many forms of social engineering, already mitigates or lessens the likelihood of a breach due to some social engineering techniques such as:

1. Impersonation - all new employees and also persons who no longer work at the company are publicly announced. There are criteria's in place to make all employees identifiable. One such is an internal communication tool slack. There must be a photograph of the person, their profile must have their location and title. No form of IT service is supplied without validation of employee. If this a remote worker or employee in a different location, they must coordinate with the local representative, if this is not possible, a video call **must** be done. Employees are free to challenge anyone they deem to be suspicious.
2. USB drops – regular drops are done and therefore staff have been very conscious. Employees are asked to notify the Information Security Team of any suspicious devices. USBs (personal or otherwise) are also not permitted for data storage and must never be inserted in any company devices or anything attached to the company's network.

Looking at these two companies there is some take away that could be incorporated.

Role-based assessment/Training

Currently, Pipedrive's training is a general assessment that is sent to everyone (including some contractors). This lends itself to persons not having any motivation as they do not see the purpose since these do not directly correlate to their everyday tasks. An office attendant getting a BEC email will be more suspicious since they have never handled any form of payment and would flag this as strange that the "CEO" of a company would be asking them to make payments.

Introducing different attacks

Both companies have incorporated different types of SE attacks within their programme. It can be perceived that these are the identified areas that require focus and hence the programme was created to aid in mitigating the discovered risks.

5 Survey Analysis

To collect data on the basic understanding of the team a survey was created. The survey was made available to all members of the company (600+) persons. The survey was live for two weeks. A total of 50 responses were received. Responses were from the various locations of Pipedrive:

- 80% (40) Estonia
  - 12% (6) Portugal
  - 4% (2) United Kingdom (UK) and Ireland
  - 1% (1) United States of America (USA)
  - 1% (1) the Czech Republic

For the survey to be successful, no personally identifiable information was collected. Also, the survey had to be written using the easy-going tone of the company culture to spark interest. The survey comprised of 10 closed-ended questions. Questions had multiple choice answers with the option to select one or multiple answers.

After analysing the questions

- Of the 50 respondents 42% indicated that of the listed social engineering attacks, they are more aware of Phishing (see figure 4). This corroborates with the stats that phishing is still the most prominent and effective technique

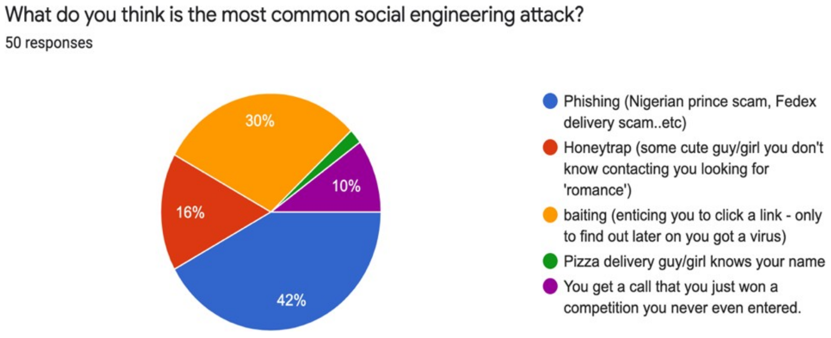


Figure 4 Pie chart: showing the response of what respondents' perception of most common social engineering attack

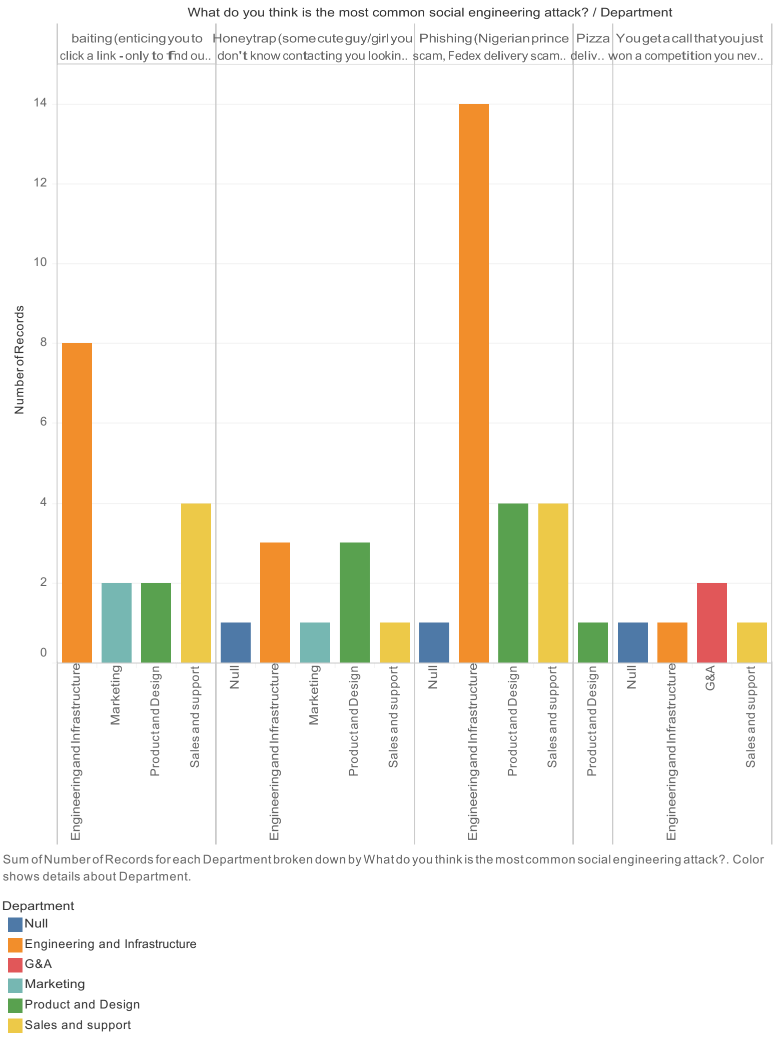


Figure 5 Chart showing comparison by the department about what the respondents perceive to be the most common social engineering attack.

- Of these 42% however, it was identified that those most aware fell into the age bracket of 29 – 35, followed by 22 -28 and above 36 respectively (as shown in figure 4).

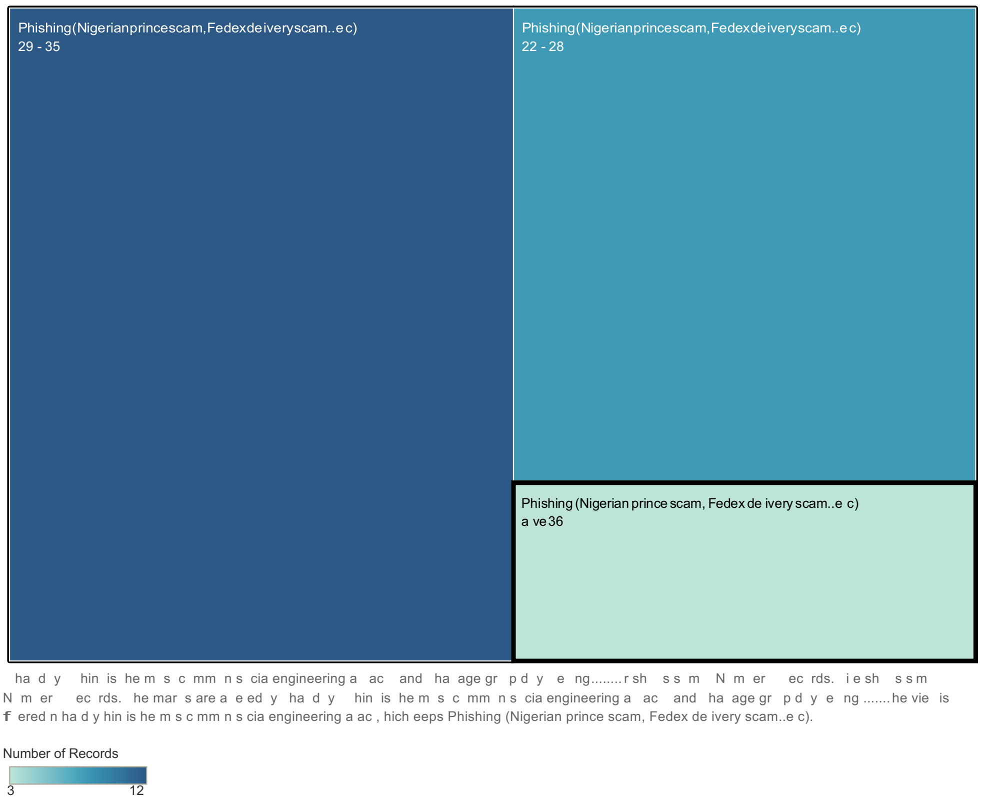
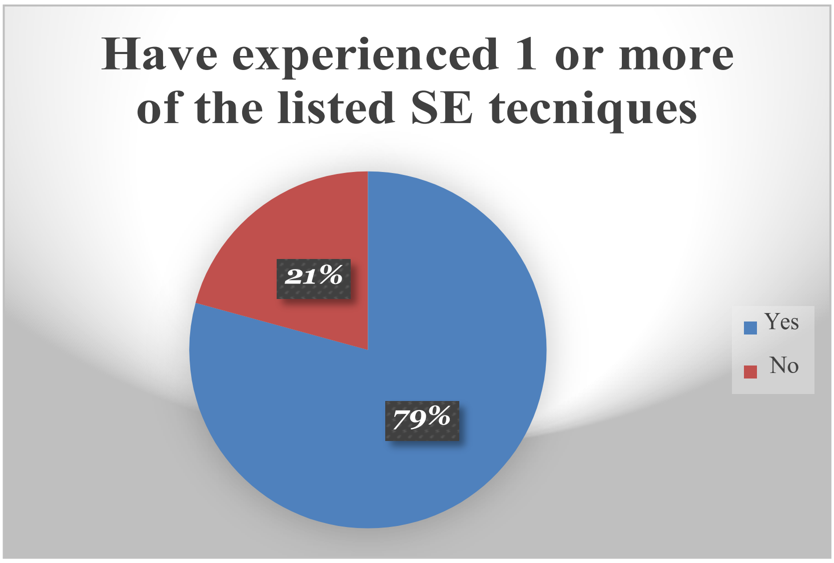


Figure 6 Graph: Awareness by age group about the most common social engineering attacks

This number, however, does highlight that those above 36 might not have an easy time identifying these attacks. The older you get the less reactive your brain becomes according to many psychologists. Hence it is expected that older persons are ranked amongst the most vulnerable and most likely to be exploited [4].

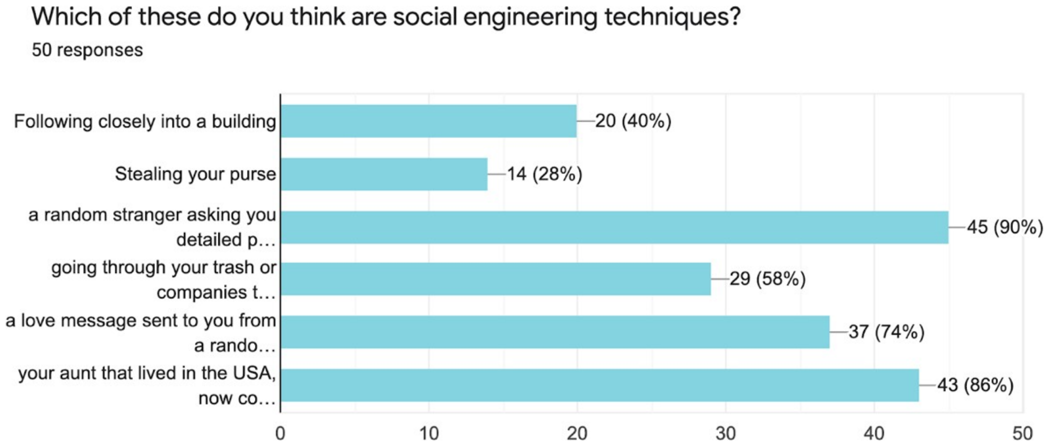
- 79% of all respondents have experienced at least one or more of these



Have experienced 1 or more of the listed SE tecniques

Figure 7 Pie chart showing persons that have experienced on or more of the mentioned attacks

- 15 persons identified the trick question “Stealing your purse” as a social engineering attack.
- Other attacks such as tailgating and dumpster diving were identified by 20 and 30 persons respectively.
- Though the survey was launched a month after the annual training was completed, Tailgating was only identified by 40% (of 100%) of respondents



Which of these do you think are social engineering techniques?

50 responses

Figure 8. Identifying social engineering techniques (each option is out of 100%)

6 Training programme improvement suggestions

After a clear analysis of the current programme and researching recommendation for the improvement of the awareness programme, the following suggestions have been determined.

Rethinking the entire training

Social engineering isn't something a video alone can teach; it needs to be hands-on. Additionally, the training should leave employees feeling empowered. Take into account Keller's ARCS model and Maslow's hierarchy of needs, grab this attention of the learner, keep them engage and ensure that they walk away with a sense of purpose or self-actualisation [23] [24] [26].

Creating a corporate policy that employees understand and support

Policies are generally written in standardize legal jargons or wordy documents [26]. These wordy documents are spark little to no interest to most employees. Documents such as these have several issues:

a. Not understood by the regular employees. Only a small subset of the employee population will understand. Make it simple, use simple terms, ensure you are speaking to the masses.
b. Lengthy. Lengthy policies tend to be skimmed over, get to the point and make it easy enough to understand (a).

Put staff to the test

Reinforced the theoretical training with some practical exercises. Have some real-life testing of some of the topics that were taught in the training. A practical reinforcement is could to show if they can apply what is learned [26].

Make this a regular occurrence

Currently, the training is delivered once per year, this number should be adjusted. There can be one overall training, however, some level of reinforced learning should be done.

For example, instead of sending several simulated emails at the end of the training. Send these simulated phishing emails at regular intervals (e.g. once per quarter…etc). Therefore, even though there was one training, the knowledge is being reinforced [26]**.**

Form a culture of questioning

Employees should feel as though they are allowed to question strangers. Or voice their concerns and feedback. These should be then taken into consideration for the next training [26].

Adjust phishing simulation from once a year to one or two emails per quarter

Adjusting the interval of the programme from once a year, to a minimum of two emails per quarter scattered out at least one month apart helps to reinforce the details of the training.

Add different types of social engineering

e.g. Business email compromise, tailgating, dumpster diving...etc. The InfoSec team can carry out checks to see if persons are applying the things learned from the training. Casually walking by a person's computer and looking at what they are working on, sending a BEC email to one of the financial controllers…etc

Tailor awareness programme to fit the language of the different departments

E.g. an attacker attempt at someone in Finance will be different from someone in HR or customer support. Tailoring the training to match unique situations of each department and issues that they would most likely face.

Gamify the awareness programme

This could reinforce self-actualisation, and confidence [23]. Offer an award (whether public recognition or a simple token) that will boost morale. E.g. persons that identify the most phishing email gets a token and/or gets acknowledge as the "phish identifier of the month" …etc

Create a lunch and learn once per quarter where one topic can be discussed

Making yourself available, a few times a year offering live sessions is one way of engaging with the team. Diversifying the way, the information is disseminated creates another avenue for reinforcement and appreciation. Different persons have different ways of learning.

7 Summary

Following the results published in this paper, we can see that there has to be diversification in how the annual training is delivered. Not only how it is delivered but the structure of the overall programme (how its written, how engaging it is…etc) and the variations in topics. Whilst phishing is still a very successful vector and one of the major costs of a data breach (IBM 2019 cost of a data breach report [18]), it is not the only social engineering tactic used. Other techniques such as BEC, for example, is on the rise. BEC (as reported by the FBI-IC3) has accounted for over 1.7 billion USD. In 2019 alone, there have been more than 1,300 reported cases. This equates to a loss in revenue of over 384 million dollars [13]. BEC was accomplished employing other social engineering tactics and use of malware [13]. The technology industry of which Pipedrive is a part of has the third-highest cost per record for a data breach at $183.00 (USD). Sixth on average cost per total breach of approximately USD 5.05 million [18]. IC3 2019 report points out that top 6 crimes are Phishing (and its relations), Non-payment/non-delivery, Extortion, Personal Breach, Spoofing and BEC. Whilst BEC is number 6, it has been ranked as the costliest exploit [13].

To understand, what improvements were needed, and what is relevant to the company. A series of observations had to be done. First, why was this training being offered? Was it only to meet regulatory and compliance requirements or was there a genuine need to offer this training to our employees (such as aid in protecting themselves and company assets). Second, it was imperative to understand the way the programme was delivered. Did the training take into consideration the effects that it might have on the learner? Did the learner walks away feeling as though they accomplished something useful, did they feel as though there is no repercussion for possibly failing the training was done and what is the next step? Did the training clearly state its relevance and usefulness? These are important points to understand. Using Maslow's hierarchy of needs pyramid, these are fundamental points that should be addressed.

Research on how to design a training programme and best practices were looked into(Keller's ARCS model and Maslow's Hierarchy of needs). A survey to get a general understanding if employees could identify any other form of SE techniques and analysing the phishing simulated emails that are sent. From the results of the survey, it is shown that a high number of persons are not familiar with other forms of SE attacks, and those that are, are generally developers/engineers. This could mean that persons are the victim of (and not yet aware) or potentially higher risk of being a victim of different SE techniques. Pipedrive is a technology company, however, not everyone has the technical knowledge and are not required to. One issue that was discovered the same training is given to everyone despite your area of work and department. This was shown to be an issue for some as they have already lost interest since they did not see the relevance of why they should be doing this training except for compliance and regulatory reasons. There was an attempt to make this training as general as possible, however, this yielded the same result of disinterests and questions from persons.

Looking at the structure of the company, recommendations were created and will be shared with the security analyst and head of InfoSec for their evaluation. A few of those suggestions entail:

- Create different content for different departments. The issues that affect finance are not necessarily the same for a developer.
- Gamify the training. At every stage of the training, there should be an attempt to keep the learner engaged. If the learner is not engaged throughout the training, then they are more like to click through to the end just to get it over with. Additionally, learners walk away with a sense of purpose and accomplishment.
- Currently, the training is delivered once per year, this number should be adjusted. There can be one overall training, however, some level of reinforced learning should be done. For example, instead of sending several simulated emails at the end of the training. Send these simulated phishing emails at regular intervals (e.g. once per quarter…etc). Therefore even though there was one training, the knowledge is being reinforced.
- Diversifying the awareness training programme using the results of a risk assessment that looks at the structure of the company and what are some of the issues that could affect Pipedrive, could be better in limiting the likelihood of exploitation. Include topics such as dumpster diving and tailgating just to name a few.

- It is imperative also for employees to understand that things such as OSINT both non-technical and technical have made recognisance of information far easier to get. The rise of social media is one such non-technical form of OSINT.
- In delivering this training, there one should take into consideration the different learners and the style of learning. Training should clearly state the benefits (what knowledge the learner will get from doing this training), its relevance to their work and everyday life.

In concluding, not everyone responds to indirect attacks such as phishing, why? they are aware and if the attempt is a topic that this potential "victim" is a subject matter expert in, then this has a lesser chance of being effective. Others need to be courted personally and face to face. This is exactly what a determined attacker might do. If their targets warrant the time and resources, they will try as many different techniques as possible. The more resilient and aware the team becomes, the lesser the chance of exploitation and by extent acts that could comprise data security, confidentiality and availability.

Using the techniques given by Maslow and Keller, it is possible to create a more engaging and robust programme that employees will find rewarding.

References

[1] D. E. Ozkaya, Learn Social Engineering: Learn the art of human hacking with an internationally renowned expert, Birmingham: Packt Publishing, 2018.

[2] M. Qadir, “Whatis Social Engineering? Attacks Examples & Prevention,” Pure VPN, 17 October 2017. [Online]. Available: https://www.purevpn.com/blog/social-engineering-attacks/. [Accessed 02 January 2020].

[3] C. Hadnagy, Social Engineering: The Science Of Human Hacking, Indianapolis: John Wiley and Sons, Inc, 2018.

[4] A. Brown, Persuasion: Dark Psychology - Secret Techniques To Influence Anyone Using Mind Control, Manipulation And Deception (Persuasion, Influence, NLP), Zen Mastery, 2019.

[5] H. Braiker, Who's Pulling Your Strings?: How to Break the Cycle of Manipulation and Regain Control of Your Life, 1 ed., New York, New York: Mcgraw-Hill, 2004.

[6] . C. Taylor, J. Larssen and K. Janvee, Dark Psychology: Manipulation, Abuse, Body Language, Influence People, Analyze People, Persuasion, Mentalism, Hypnosis, Alpha Male, and Sociopath Details, A to Z Publishing Audio, 2018.

[7] “Phishing and its Impact on Businesses and Employees,” Defintel, 02 2017. [Online]. Available: https://defintel.com/blog/index.php/2017/02/phishing-and-its-impact-on-businesses-and-employees.html. [Accessed 01 01 2020].

[8] Retruster Ltd, “Phishing:The True Cost of a Phishing Attack - Retruster,” Retruster Ltd, [Online]. Available: https://retruster.com/blog/phishing-attack-true-cost.html. [Accessed 01 January 2020].

[9] "Understanding phishing techniques - Deloitte," December 2019. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-part10.pdf. [Accessed 01 January 2020].

[10] T. Appleby, "Phishing Definition, Prevention, and Examples," Infosec Inc, [Online]. Available: https://resources.infosecinstitute.com/category/enterprise/phishing/. [Accessed 01 January 2020].

[11] S. Moramarco, "Link Manipulation - Infosec Resources - InfoSec Institute," Infosec, Inc, [Online]. Available: https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-tools-techniques/link-manipulation/. [Accessed 01 January 2020].

[12] "OWASP Top Ten," Open Web Application Security Projec, 2020. [Online]. Available: https://owasp.org/www-project-top-ten. [Accessed 09 February 2020].

[13] Federal Bureau of Investigation, "2019 Internet Crime Report," Federal Bureau of Investigation, 2019.

[14] Estonian Information System Authority, "Estonian Information System Authority: Annual Cyber Security Assessment 2019," Estonian Information System Authority, Tallinn, 2019.

[15] "Phishing,Pharming, Vishing, and Smishing - Intuit Security," Intuit Inc, [Online]. Available: https://security.intuit.com/index.php/protect-your-information/phishing-pharming-vishing-and-smishing. [Accessed 02 January 2020].

[16] "What is Cross-Site Scripting (XSS)? Prevent XSS Attacks - Rapid7," Rapid7 LLC, [Online]. Available: https://www.rapid7.com/fundamentals/cross-site-scripting/. [Accessed 01 January 2020].

[17] THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, “REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free,” *Official Journal of the European Union,* p. L 119/83, 04 May 2016.

[18] Ponemon Institute, “IBM Security Cost of a Data Breach Report,” Ponemon Institute LLC, North Travese, 2019.

[19] J. Keller, “ARCS Design Process,” [Online]. Available: https://www.arcsmodel.com/arcs-design-process. [Accessed 27 April 2020].

[20] J. Keller, “What is the ARCS Model?,” [Online]. Available: https://www.arcsmodel.com/arcs-model. [Accessed 27 April 2020].

[21] J. Keller, “What Are the ARCS Categories?,” [Online]. Available: https://www.arcsmodel.com/arcs-categories. [Accessed 27 April 2020].

[22] M. L. Sisley, “MOTIVATIONAL DESIGN FOR LEARNING PERFORMANCE: ARCS,” Neurobox, 30 November 2016. [Online]. Available: https://neurobox.ca/motivational-design-for-learning-performance-arcs/. [Accessed 30 April 2020].

[23] B. J. Shellnut, “John Keller: A motivating Influence in the Field of Instructional Systems Design,” Detroit, 1996.

[24] The Editors of Encyclopaedia Britannica, “Abraham Maslow,” Encyclopædia Britannica, 28 March 2020. [Online]. Available: https://www.britannica.com/biography/Abraham-H-Maslow. [Accessed 27 April 2020].

[25] S. A. Mcleod, “Maslow's hierarchy of needs,” Simply Psychology, 20 March 2020. [Online]. Available: https://www.simplypsychology.org/maslow.html. [Accessed 28 April 2020].

[26] SecurityMetrics, “White Paper: How to Train your Workforce on Social Engineering,” [Online]. Available: https://info.securitymetrics.com/white-paper-train-employees-against-social-engineering. [Accessed 03 March 2020].

[27] Western Area Power Administration, “2020 Annual Cyber Security Awareness Training,” 2020. [Online]. Available: https://www.wapa.gov/jobs/Documents/annual-cyber-security-training-new-hire.pdf. [Accessed 29 April 2020].

[28] University of California Santa Cruz, “Security Awareness Training,” University of California Santa Cruz, [Online]. Available: https://its.ucsc.edu/security/training/index.html. [Accessed 20 April 2020].

[29] University of California Santa Cruz, “UC Cyber Security Awareness Training 2019,” University of California Santa Cruz, 2019. [Online]. Available: https://its.ucsc.edu/security/training/infosec.html. [Accessed 29 April 2020].

Appendix 1 – Non-exclusive license

Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Romaine Ayoki Burrell

1. grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis
Building Resilience to Social Engineering in Pipedrive through Awareness Training
supervised by Kaido Kikkas and Jesse Wojtkowiak ,

1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

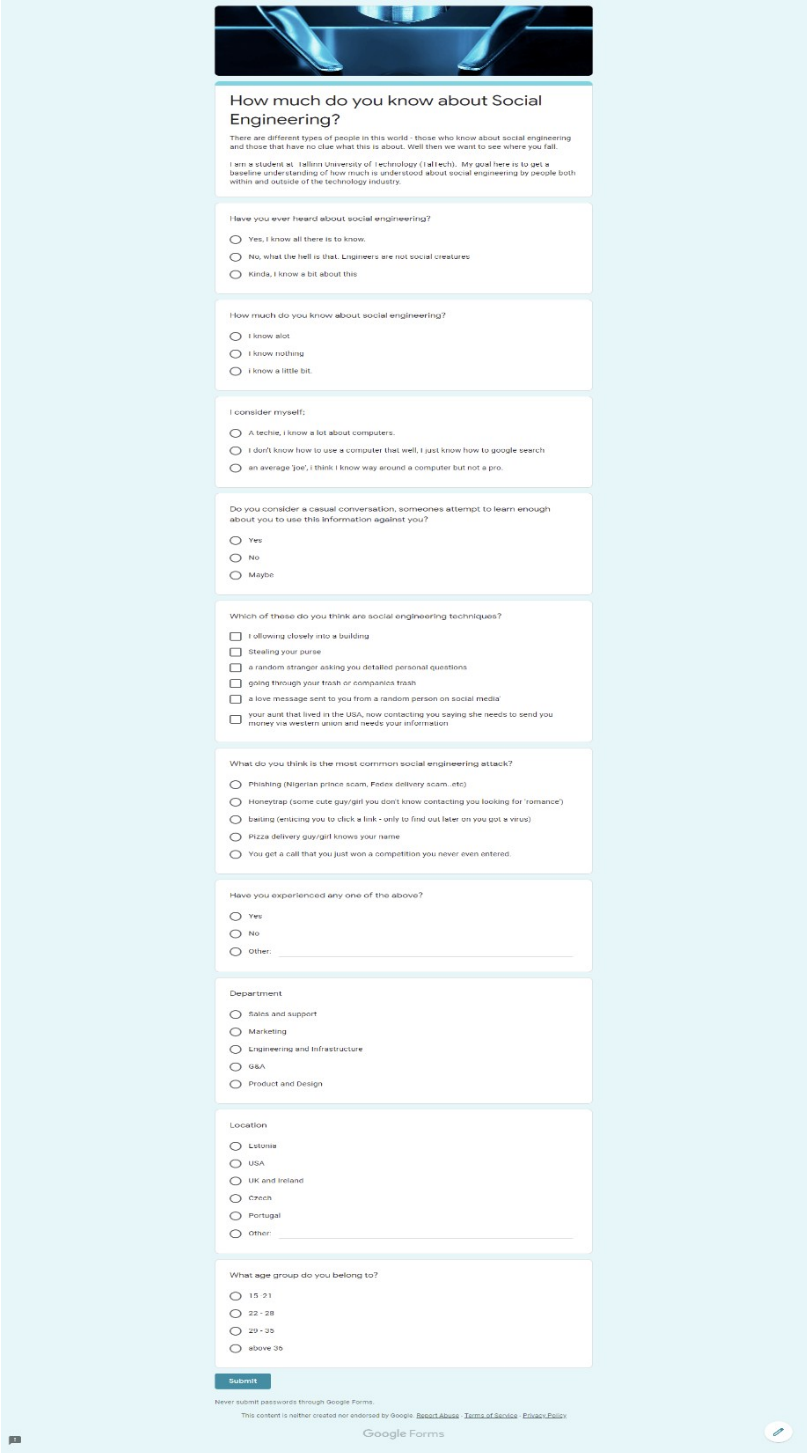
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

January 7, 2021

[1] *The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.*

Appendix 2 – Screenshot of survey questions



How much do you know about Social Engineering?

There are different types of people in this world - those who know about social engineering and those that have no clue what this is about. Well then we want to see where you fall.

I am a student at Tallinn University of Technology (TalTech). My goal here is to get a baseline understanding of how much is understood about social engineering by people both within and outside of the technology industry.

Have you ever heard about social engineering?

- ○ Yes, I know all there is to know.
- ○ No, what the hell is that. Engineers are not social creatures
- ○ Kinda, I know a bit about this

How much do you know about social engineering?

- ○ I know alot
- ○ I know nothing
- ○ i know a little bit.

I consider myself:

- ○ A techie, i know a lot about computers.
- ○ I don't know how to use a computer that well, I just know how to google search
- ○ an average 'joe', i think I know way around a computer but not a pro.

Do you consider a casual conversation, someones attempt to learn enough about you to use this information against you?

- ○ Yes
- ○ No
- ○ Maybe

Which of these do you think are social engineering techniques?

- □ Following closely into a building
- □ Stealing your purse
- □ a random stranger asking you detailed personal questions
- □ going through your trash or companies trash
- □ a love message sent to you from a random person on social media'
- □ your aunt that lived in the USA, now contacting you saying she needs to send you money via western union and needs your information

What do you think is the most common social engineering attack?

- ○ Phishing (Nigerian prince scam, Fedex delivery scam..etc)
- ○ Honeytrap (some cute guy/girl you don't know contacting you looking for 'romance')
- ○ baiting (enticing you to click a link - only to find out later on you got a virus)
- ○ Pizza delivery guy/girl knows your name
- ○ You get a call that you just won a competition you never even entered.

Have you experienced any one of the above?

- ○ Yes
- ○ No
- ○ Other: ________

Department

- ○ Sales and support
- ○ Marketing
- ○ Engineering and Infrastructure
- ○ G&A
- ○ Product and Design

Location

- ○ Estonia
- ○ USA
- ○ UK and Ireland
- ○ Czech
- ○ Portugal
- ○ Other: ________

What age group do you belong to?

- ○ 15-21
- ○ 22 - 28
- ○ 29 - 35
- ○ above 36

Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. Report Abuse - Terms of Service - Privacy Policy

Figure 9 Screenshot of survey questions

Appendix 3 – Extract of questions from annual training

Table 2 Extract of questions and answers from 2019 security training

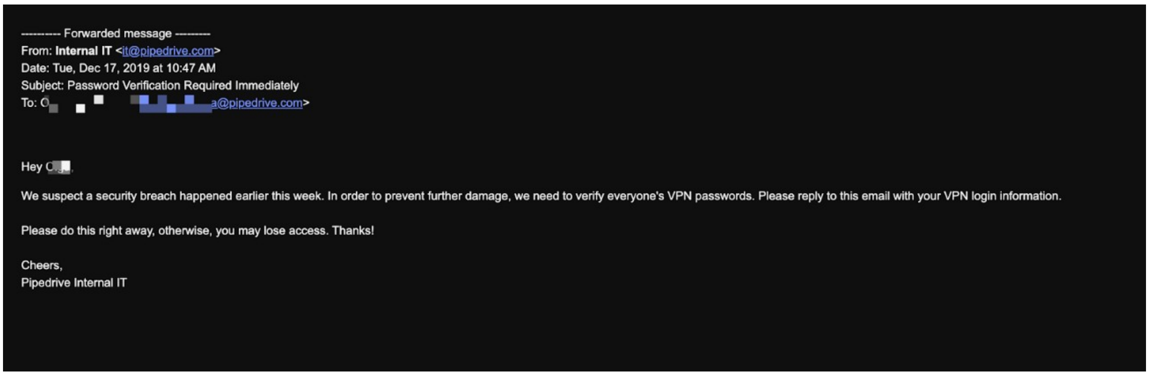
Question	Answers
Who is responsible for data security at Pipedrive?	**a) Everyone** b) The security department c) The executives
You believe that someone knows your password in the application A. You should immediately:	a) Contact your manager b) Wait for the IT person to contact you c) Change your password in the application A **d) Change your password in the application A and any other application, where a similar password is used**
Is it a good idea to use a 2FA (2-factor authentication)?	**a) Yes! If someone steals my password, they still can't log into my account without access to my phone or mailbox** b) No! I want to log into applications faster and 2FA wastes my time. It is an unnecessary requirement that the security team put in place
You work in Pipedrive and want to create a password that is hard to brute-force (try millions of combinations) using English dictionary but is easy to remember. Which password fits the description?	a) Pipedrive123 b) xT&V-4]U6R>9Vvhp **c) _Pipedrive's initial name was Growty** d) salesforceFTW*123
True or False: The safest way to keep a copy of your password is to email it to yourself	**a) FALSE** b) TRUE
Which word is common enough to make a weak password?	a) Hippopotamus b) Salamander c) Monkey

	d) gibbon
Someone from the security team writes to you in Slack and says that your password has been leaked and you should change it immediately. You ...	a) Thank for the message, but ignore the suggestions. The security team is always paranoid and makes things worse than they really are **b) Follow the instructions and actually change the password immediately. Also, think where else you used a similar password, and change it there too** c) Don't change the password, because you are using a 2FA (2-factor authentication) and therefore are not affected by hackers
Common password practices aren't as secure as people think, due to the fact that people tend to think in patterns. Knowing this, why would changing "diamond1" to "diamond2" be unsafe?	**a) Incrementing a number is a common behaviour** **b)** The word "diamond" is a commonly breached password **c)** People commonly use short passwords **d)** Trick question. It's safe
You enjoy playing Playstation and one morning receive the following email to your Pipedrive mailbox. What do you think happened and what you should do?	a) Someone clearly tried to break into my PlayStation account. I click on the link to change password b) This is a phishing email. I see the sender is "sony@techsoupstore.org", which can't be real Sony. Also, I never signed up for PlayStation account with my Pipedrive email address. This email should be forwarded to phishing@pipedrive.com
You receive an unexpected email from a co-worker asking you to review a document. There is a file attached. What should you do?	a) Reply to the email in order to confirm that the attachment came from your co-worker b) Without replying to the email, use another channel to confirm that your co-worker sent the attachment

	c) Open the attachment and review it immediately Download the attachment and wait to open it until you can confirm with your co-worker that it is safe
"Spear phishing" is when:	a) A phishing attack involves a sophisticated, tailored message that appears to know specific information about you b) A phishing attack involves an unusually aggressive or threatening message c) A phishing attack involves a sophisticated, tailored message that is very polite and gives the impression of being important d) A phishing attack is not actually a phishing attack
Most browsers allow you to inspect links by:	a) Pasting the link in a private browser session. b) Clicking the link. c) Sending the link to your manager. d) Hovering over the link with your mouse pointer.
Spearphishing emails may reference supposedly private details such as:	a) All of these b) Project names c) Co-workers' titles d) Names of family members
You are trying to access Pipedrive's main website (www.pipdrive.com), but get a message, that your Mac is infected with a virus. What do you think happened and what should you do?	a) No idea what happened. You click OK and close the browser tab just in case b) There was a typo in the website address. You investigate the error message carefully and close the browser tab without clicking OK c) Pipedrive started providing antivirus services. You click OK and then Scan Now, because maybe your Mac is indeed infected
Who is responsible for protecting organizational information?	a) My supervisor b) HR department

	c) Each employee d) IT department

Appendix 4 – Simulated phishing email samples



---------- Forwarded message ---------
From: **Internal IT** <it@pipedrive.com>
Date: Tue, Dec 17, 2019 at 10:47 AM
Subject: Password Verification Required Immediately
To: O[redacted]a@pipedrive.com>

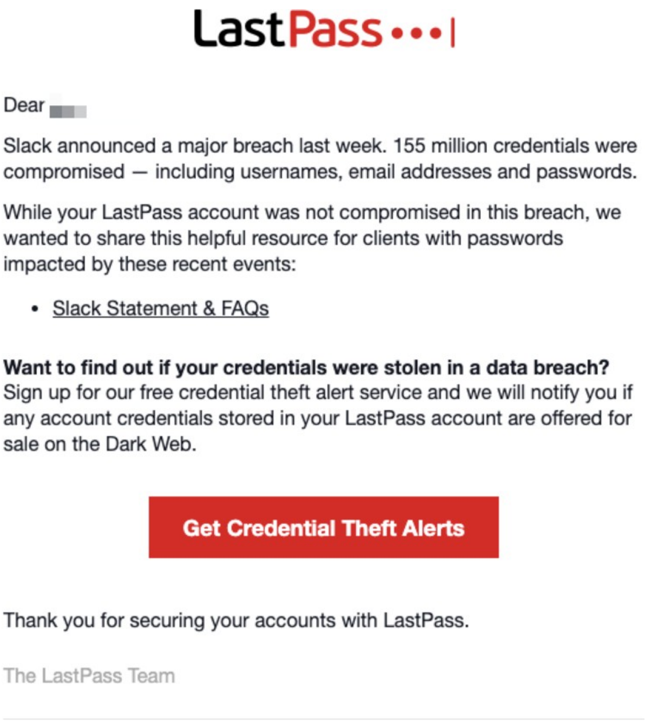
Hey C[redacted].

We suspect a security breach happened earlier this week. In order to prevent further damage, we need to verify everyone's VPN passwords. Please reply to this email with your VPN login information.

Please do this right away, otherwise, you may lose access. Thanks!

Cheers,
Pipedrive Internal IT

Figure 10 Simulated phishing email - Password verification



LastPass •••|

Dear [redacted]

Slack announced a major breach last week. 155 million credentials were compromised — including usernames, email addresses and passwords.

While your LastPass account was not compromised in this breach, we wanted to share this helpful resource for clients with passwords impacted by these recent events:

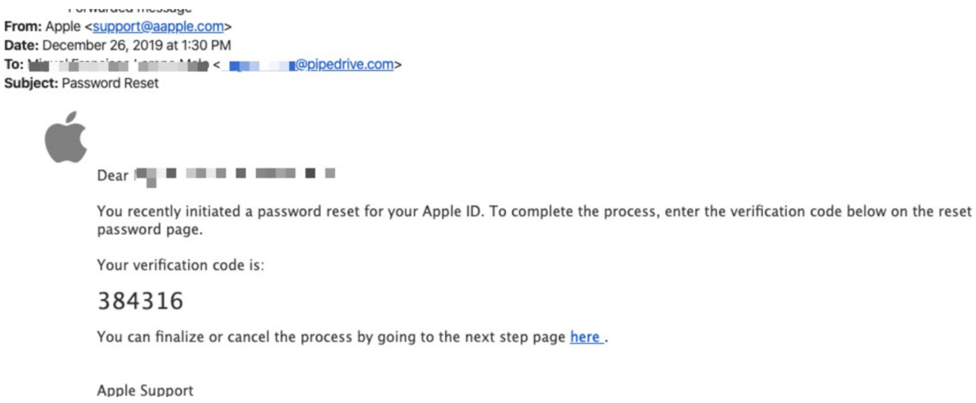
- Slack Statement & FAQs

Want to find out if your credentials were stolen in a data breach? Sign up for our free credential theft alert service and we will notify you if any account credentials stored in your LastPass account are offered for sale on the Dark Web.

Thank you for securing your accounts with LastPass.

The LastPass Team

Figure 11 Simulated phishing email- LastPass - Credential Theft Alerts



Forwarded message

From: Apple <support@aapple.com>
Date: December 26, 2019 at 1:30 PM
To: [redacted] < [redacted]@pipedrive.com>
Subject: Password Reset

Dear [redacted]

You recently initiated a password reset for your Apple ID. To complete the process, enter the verification code below on the reset password page.

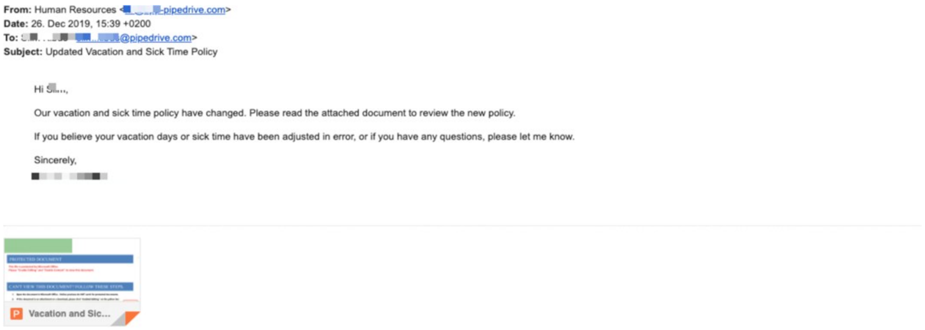
Your verification code is:

384316

You can finalize or cancel the process by going to the next step page here .

Apple Support

Figure 12 Simulated phishing email- Apple ID password reset



From: Human Resources <[redacted]-pipedrive.com>
Date: 26. Dec 2019, 15:39 +0200
To: [redacted]@pipedrive.com>
Subject: Updated Vacation and Sick Time Policy

Hi [redacted],

Our vacation and sick time policy have changed. Please read the attached document to review the new policy.

If you believe your vacation days or sick time have been adjusted in error, or if you have any questions, please let me know.

Sincerely,
[redacted]

Figure 13 Simulated phishing email- Vacation request