Cyber security in customer support: training needs analysis

Jiri Kucera

2024 Laurea

LAU
REA

Laurea University of Applied Sciences

Cyber security in customer support: needs analysis and training outline

Jiri Kucera
Business Information Technology
Thesis
April, 2024

Laurea University of Applied Sciences	**Abstract**
Business Information Technology	
BBA	

Jiří Kučera

Cyber security in customer support: needs analysis and training outline

Year	2024	Number of pages	74

The subject of this thesis project was the needs analysis and outline for cyber security awareness training in a customer support department. The client was a company working in the mobility sector.

The first part of the report reviews the relevant threats to such a department based on current trends. Next, training frameworks, teaching methods and quiz creation methodologies are discussed and their relevancy towards the training being designed. A survey regarding cyber security awareness, which included both quantitative and qualitative questions, was proposed and tested with a general audience to be utilized for prioritizing the training topics and testing learners' awareness before and after the training.

The outcome of the thesis project was a training outline with relevant topics, suggested training frameworks, methods, and a quiz which will be used by the client to create the training. The aim was to assist the client with the creation of a new cyber security awareness training which will increase their protection against cyber security threats.

Keywords: Cyber security training, Customer support cyber security, Cyber security awareness

Contents

1 Introduction

For companies operating in the digital space, data is essentially their currency – both in terms of their internal information and customer data, this can often be the most valuable asset they own. Therefore, it is only logical that just like with physical assets, criminals around the world have been trying to steal companies' information, with purposes varying from getting ransom to abusing personal information as such. Additionally, the processing of personal data is generally heavily regulated, such as by the General Data Protection Regulation in Europe.

This thesis is based on an agreement with the training team for a customer department of a larger company, for whom a training needs analysis will be conducted based on recent trends in both cyber security and training, in order to find the best methods to pass this information to the department's employees.

According to the IBM Corporation Cost of a Data Breach Report, the average cost of a data breach in 2023 was USD 4.45 million (IBM Corporation 2023, 5). The report also claims that phishing and stolen or compromised credentials were the two most common ways that attackers gained access to a company's data and ultimately led to a data breach. This is specifically relevant to my client as these are two vectors where it can be reasonably assumed that they could target the customer support department which communicates externally.

The focus on customer support as a department is an important factor in this thesis and the analysis as such. Since the customer support department will typically handle a majority of the external-facing communication and especially be the first in line to receive incoming messages, they are at a high risk of becoming targets of different types of cyber-attacks transmitted through these.

This thesis will initially describe the most common cyber-attacks that are relevant to workers within the customer support department, including the potential risks of these and past cases where companies were exploited. Next, it will describe possible training methods and frameworks which could be used for a training within the cyber security field. Then, it will discuss the results of a survey which asks the respondents about people's awareness of various types of cyber-attacks and the countermeasures they can take against them. Finally, the thesis will be concluded by the finalized product – a training needs analysis including the specific topics and their importance, as well as the training methods that should be used for an efficient delivery.

1.1 Aims

The overall aim of the finalized product is improving the cyber security awareness (and by extension, the overall security) of the client's customer support department. This will be achieved by the following objectives:

- Providing the client with a training outline/training needs analysis to increase cyber security awareness within the customer support department.
- Providing the client with a knowledge base of relevant cyber security threats for the customer support department.
- Providing the client with a way to test cyber security awareness within the department through a survey.

This thesis aims to gather sufficient theoretical background and then produce these results for the client.

1.2 Scope

This section defines the topics that are in the scope of this thesis and the topics that are out of it.

The following is in scope of this thesis:

- Literature review and compiling information regarding threats relevant to a customer support department.
- Literature review and compiling information regarding useful training methods for a cyber security awareness training for a customer support department.
- Review of training frameworks provided by the client to relate them to this training.
- Definition of a survey that can be used for cyber security awareness measurement within the client company and its test to see general public's awareness of the defined threats.
- Creation of a training outline with suggested topics and methods for a cyber security awareness training.

The following is out of scope of this thesis:

- Creation of the training.
- Utilizing the survey in the client's company.
- Providing client-specific data.

2 Theoretical background

The literature review will include a discussion of resources in four areas – firstly, looking at cyber security threats relevant to a customer support department to find the most relevant topics for its workers as content for the training, secondly, looking at training frameworks that the client utilizes, thirdly, looking at usable online training methods and lastly, looking at quiz creation methods. The thesis will consider both recommendations in terms of cyber security training, as well as online training in general.

2.1 Cyber security threats

This section of the literature review will focus on security threats, going from broader trends within cyber security attacks in the recent years, further narrowing down to threats specifically relevant to customer support workers and finally looking at specific threats and research regarding what makes them efficient, in order to select the most relevant topics for a training.

2.1.1 Cyber security threat landscape

As mentioned in the introduction, cyber threats have a significant potential impact on any organization and with the average cost of a data breach being USD 4.45 million (IBM Corporation 2023, 5) and as such, they should be an organization's top priority. The report further elaborates that phishing was responsible for 16% of the leaks analyzed and stolen and compromised credentials were responsible for another 15% (IBM Corporation 2023, 20).

These claims are further supported by Verizon's 2023 Data Breach Investigations Report, which claims that "74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering" (Verizon 2023, 8). Verizon also reports that "External actors were responsible for 83% of breaches, while Internal ones account for 19%. It is worth reminding our readers that Internal actors are not only responsible for intentional harm in these cases, but they are also just as likely [actually, twice as likely] to be responsible for Error actions" (Verizon 2023, 12). What this means for the purposes of this thesis is that even though an external actor is most likely to initiate a breach, an internal actor is often at fault and more likely accidentally than on purpose – this means that it can be inferred that through proper training and education, the likelihood of these attacks can significantly decrease.

It is important here to note the difference between attack *vectors* and the exploitation itself, as they may be different. An attack vector is "a path, method or means by which cybercriminals penetrate a target system" (Kaspersky 2024), but what they do once they find it can be completely different – as one of the most common attack vectors per both reports is phishing, it can be used as an example here. With a phishing email as the attack vector, an attacker can exploit their target in multiple ways, for instance, they can simply ask for information they need to know and pretend to be somebody from within the company, but they can also send a fake website tricking the user to enter their credentials or they can trick them into opening a file containing malware.

Further attack vectors mentioned by IBM (2023) include cloud misconfiguration, unknown (zero-day) vulnerability, business email compromise, social engineering, malicious insider, accidental data loss or lost or stolen device, known unpatched vulnerability, system error and physical security compromise, with only unknown vulnerabilities and cloud misconfiguration reaching over 10% of the analyzed cases.

Looking at what follows after the attack vector is successfully utilized, Verizon (2023) mentions the use of stolen credentials, as well as other actions, ransomware, phishing, and pretexting, with the use of stolen credentials exceeding 40% of the attacks analyzed.

Ransomware is also mentioned as one of the top threats by the IBM report, with Verizon placing it at 15.5% for all reported incidents and at 24% of breaches, and IBM putting it at 25% in the breaches it reports on.

To proceed with the selection of topics for the learning needs analysis, the attack vectors and actions mentioned will be further analyzed below by their relevance towards the customer support department workers and then further defined with past examples, in order to examine why they can be successful and what knowledge is necessary to include in the training in order to prevent a data breach due to them.

2.1.2 Threats towards a customer support department

Within this section, the thesis aims to select the relevant threats for a customer support department within the clients' company based on the overall threat scenario outlined above.

To select the most relevant topics for a training aimed at a customer support department, simple criteria were used: the threats that workers in customer support should be educated about are those threats that require a user interaction in order to function successfully, as opposed to threats that attackers use independently to target vulnerable systems, meaning that the attack vector needs to include a human element. The reason for this criterion is simple – customer support workers' main job is to work with external communication and as such, they can encounter malicious messages. For this reason, threats that do not need user interaction (and rather depend on system configuration or application security) will be excluded from the training as they are relevant to other departments of the company. At the same time, the thesis and analysis will not be limited to social engineering attempts and will also include attacks that require user interaction in combination with a vulnerable system, as these may occasionally also be relevant to the workers of a customer support department.

Using these criteria, the following can be said about the attack vectors mentioned previously:

- Phishing – as a department closely working with external communication, there is certainly a possibility for the workers of the customer support department to get phished via email or other means, hence this is a topic that should be included.
- Stolen/compromised credentials – this is relevant to any employee with access to internal systems, as they can be compromised in a multitude of way, inside or outside of work and especially in case of reusing the same credentials. Hence, this is another relevant part of the training.
- Cloud misconfiguration – this attack vector relates to system configuration, rather than user interaction, hence it will be excluded from the training.
- Unknown (zero-day) vulnerability – this attack vector is dependent on application security, not user interaction, so it will not be included in the training.
- Business email compromise – like mentioned above with phishing, this is relevant to external communication and user interaction and so it should be included in the training.
- Social engineering – this vector is also related to communication and external communication and should be included in the training.
- Malicious insider – though a malicious insider threat is by definition not caused by accident, it should be mentioned in the training for the employees’ caution.
- Accidental data loss or lost or stolen device – just like any other employee, this issue can happen to an employee to the customer support department and hence should be included in the training.
- Known unpatched vulnerability – this is related to application security and hence out of scope for the training.
- System error – this is related to system configuration and hence out of scope for the training.
- Physical security compromise – this is a threat to any employee regardless of their position, hence this should be included in the training.

Regarding the attack actions, as mentioned previously, they can be caused by various actors including those that were deemed necessary to include in the training and therefore, they will all be further mentioned, defined, and prepared for the training.

2.1.3 Attack vectors

In this section, the attack vectors necessary to include in the training will be mentioned. To avoid confusion, some of these methods are both vectors and actions and will be mentioned separately for that reason (for instance, phishing can be a method to gain access to a user's data through pretending to be somebody else, i.e., a vector, but it can also be an action in case data accessed by another vector is then further utilized in a phishing attack).

2.1.3.1 Social engineering, business email compromise and phishing

This section will discuss the details of social engineering attacks, the sub-categories of business email compromise and phishing and the relevance of these attacks to the customer support department, in order to gain sufficient information for the final training.

According to Krombholz, Hobel, Huber and Weippl (2015), "Social engineering is the art of getting users to com- promise information systems. Instead of technical attacks on systems, social engineers target humans with access to information, manipulating them into divulging confidential information or even into carrying out their malicious attacks through influence and persuasion" (Krombholz et al. 2015, 2). In context of the thesis' topic, this is a key attack vector, since as mentioned previously, the customer support workers are often communicating externally as their main work. Hence, it is important to describe the different methods falling under the umbrella of social engineering and document them in the training needs analysis.

Before separating social engineering attacks into different types, Salahdine and Kaabouch (2019) describe a similar 4-step path all attacks falling under this umbrella typically take: "(1) collect information about the target; (2) develop relationship with the target; (3) exploit the available information and (4) exit with no traces" (Salahdine & Kaabouch 2019, 2). This is a crucial piece of information to our training, as recognizing this common path for any type of social engineering attack is going to be key for a customer support worker in order to avoid falling into the trap of the attacker.

Salahding and Kaabouch (2019, 3), as well as Aldawood and Skinner (2020, 2) provide two ways to distinguish social engineering attacks. Both of these papers mention a divide firstly based on whether a human is directly executing them or whether they are done by a computer (meaning it can rapidly target many users at once). The second divide looks at whether the attacker is physically gaining the information, they use technology to do it or they use a social relationship with the users. From the perspective of a customer support worker, all of these types of social engineering can be relevant, however, for the purposes of this training, the main focus is on online threats and hence lower priority will be put on physical threats. On the other hand, both human based and computer based threats are viable in the environment – customer service workers may be targeted by an automated scam email just as much as an individual specifically sending them messages. While the specific names and taxonomy of social engineering may not be relevant in its entirety to the workers, it is important for them to recognize that these attacks may take on very different forms and be able to realize this before revealing any information.

When it comes to the specific types of social engineering attacks, Salahdine and Kaabouch (2020) offer the following overview:

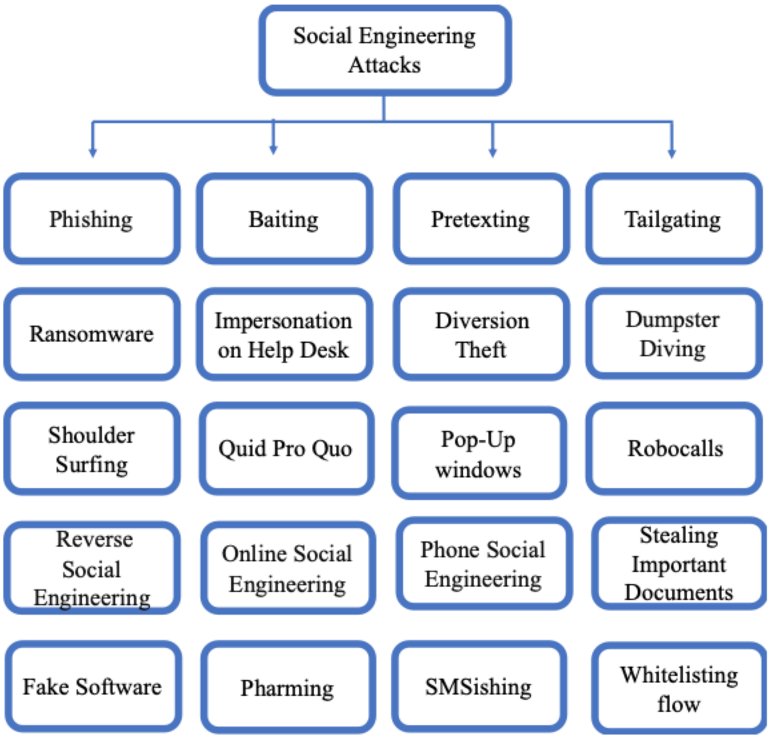


Figure 1: Different kinds of social engineering attacks (Salahdine & Kaabouch 2019, 4)

For the purposes of this thesis, some of these types would be considered actions, rather than attack vectors (such as ransomware) and overall, it is not key for the customer support workers to know every single type of social engineering attacks, but rather it is important that they are aware of the general process of a social engineering attack and how to avoid it.

However, based on the previous parts of the thesis, there are two specific types of social engineering attacks that need their own explanation as they are present as some of the most prevalent attack vectors in the Verizon and IBM reports on the most common threats: specifically, that is phishing and business email compromise. Kaspersky IT Encyclopedia says that “a typical phishing attack involves sending emails or messages in the name of a real organization with some “bait” in the subject line or message body and a link to a page asking for data” (Kaspersky 2024), also placing it under the umbrella of social engineering, and defines business email compromise as an attack “in which the attacker uses social engineering to gain access to a corporate email account. Once inside, the cybercriminal can send phishing messages, spam, or malicious programs to recipients on behalf of the compromised company” (Kaspersky 2024). Hence, the further explanations of social engineering will include an elaboration on the general social engineering process and then further explanations of phishing and business email compromise with more detail and examples.

In order to elaborate on the general stages of the social engineering process, Christopher Hadnagy’s book on social engineering provides useful insight in combination Salahdine and Kaabouch’s general four steps. Hadnagy (2010) takes the perspective of a social engineer trying to use this skill in order to gain information, which is helpful to imagine in this situation.

For the information collection stage, Hadnagy (2010) talks about planning, information collection and storing and overall, gaining good insight on the target before attacking the target as such. This phase would typically happen before customer support workers come into contact with the attacker, but the key insight in here is that they should be aware of the fact that the attacker will often not come empty-handed: they will have overall information about the company, perhaps with some details they managed to find publicly and they will be able to use that to gain the trust of workers within the company.

The second and third stage from Salahdine and Kaabouch (2020) both belong under the term elicitation in Hadnagy (2010) and from his tips to an aspiring social engineer, there are several learnings that can be useful in order to counter a social engineering attack

Hadnagy (2010), says that information that is seemingly useless can form a very useful picture in the head of a social engineer combined with other data points. For customer support workers, the learning here is that they should not share even seemingly harmless information with third parties if not required. Further, he claims that a natural conversation is key in order to successfully perform a social engineering attack – an unnatural sounding message may be easy to uncover for workers, but they need to be on the lookout for much more professional work. One of the other key tips he shares is that the attacker needs to be well-educated to know who they can pretend to be – a worker will easily recognize somebody pretending to be the CEO, but they may fall for somebody pretending to be a researcher. Finally, Hadnagy (2010) says it is important to not be greedy with the information you are trying to learn – if an attacker asks for secret information all at once, it is likely they will be discovered. But tying back to the first point, if they ask for seemingly harmless information, they are more likely to succeed. The final part of Salahdine and Kaabouch’s (2020) process is an unseen exit – Hadnagy (2010) does not describe a specific stage for this, however, the previous tips do suggest that a social engineer needs to know when to stop the conversation and the key learning for a customer support worker is that there will not always be an immediate effect after a social engineering attack, but the results can be seen after a longer period of time.

Going further into specific types of social engineering, phishing is responsible for 16% of all the analyzed leaks and hence the training should put explicit focus on it in order to ensure workers' understanding of the topic and mainly the typical strategies employed, including specific case studies.

Stojnic, Vatsalan and Arachchilage (2021) tested the presence of keywords in phishing emails to find out what methods are the most common among such messages. By performing this analysis, the paper has found that a typical phishing message will follow a similar pattern:

"1. Get victim to open the email with a short catchy email subject header that creates a feeling of urgency and intrigue.

2. Keep the victim's attention and gain trust by establishing a sense of authority (by claiming to be from a bank, wealthy individual, or lawyer) and leveraging this to offer the victim a reward.

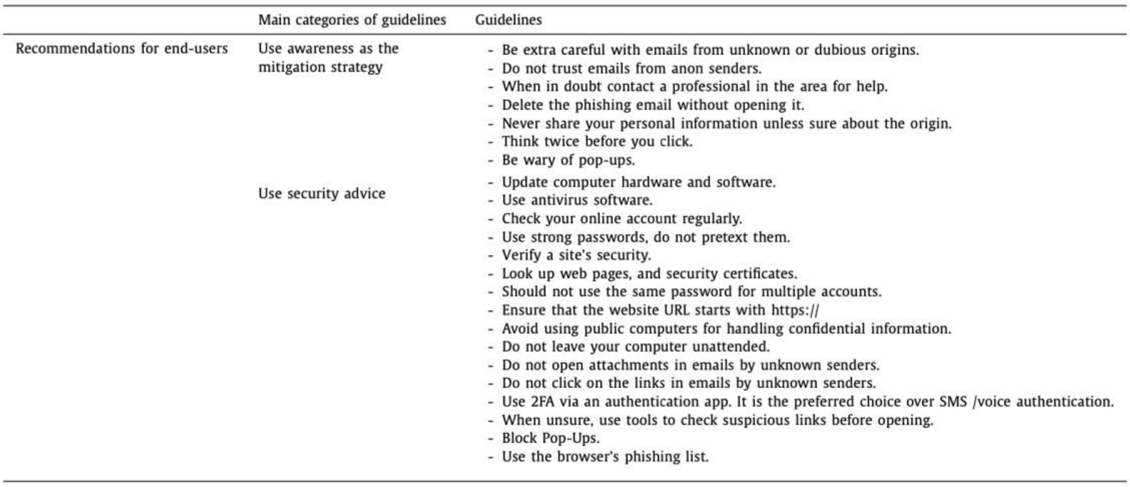
3. Give the victim a call to action in order to gain a response (often asking for the victim to provide personal information with the promise of a large sum of money)" (Stojnic et al. 2021, 12). Hence, carefully considering the emotions an email is trying to appeal to and the calls to action it may provide is an important part of being able to avoid being caught via a phishing attack.

Another important factor to consider – and going back to the division of social engineering attacks overall – is that the strategies of phishing do not have to rely exclusively on the users simply responding to an email, but also using unverified links under a false pretense – Desolda, Ferro, Marrella, Catarci and Costabile (2021) actually define the typical form of a phishing attack as consisting of "sending a message (e.g., an email), which appears as from a reputable organization (e.g., a bank), sounds urgent, claims to enclose important information, and invites the victims to open a website that is a clone of the original one (e.g., a clone of their own bank website). In the message, the victims are invited to provide personal information on the website, for example, they are required to login to the website for updating their profile information. In most cases, the victims are unlikely to check or question the website validity; thus, they open it providing the required information that, unfortunately, is stolen by the attackers who can use it, for example, to enter on the bank account on behalf of the victims to steal their money"(Desolda et al. 2021, 4), meaning that in order to gain the victim's trust, the attackers provide a deceptive website, as opposed to simply asking for the information. In these types of messages, it is hence important to provide the agents with information and examples on recognizing correct URLs for the websites they are visiting, in order to avoid visiting one of the falsified pages and providing their information.

Phishing attacks are well illustrated by examples – the New York Times reported in 2019 on a case of a man impersonating a supplier for Google and Facebook who managed to scam these companies for around USD 100 million simply by crafting an email and asking to be transferred these sums of money (Fortin 2019). This example shows that even such a low-tech approach, where the importance was rather on the message itself than a complicated technological approach, can be a very efficient way for scammers to successfully attack their target.

In another example, FOX reports about a scam where "scammers e-mailed the accounts payable coordinator at Upsher-Smith Laboratories, a drug company in Maple Grove, and pretended to be the CEO. The thieves instructed the employee to follow directions from the "CEO" as well as a lawyer's name they provided. Over the course of three weeks in 2014, the employee asked the company's bank, Fifth Third Bank, to make nine wire transfers totaling more than $50 million" (FOX9 Minneapolis-St. Paul 2016). This illustrates a similar case where by crafting efficient, believable emails and targeting the correct employees can be an efficient way to attack a company, as opposed to needing a complicated technical setup to achieve this.

Multiple sources also report on the most efficient ways to combat phishing attacks. Naqvi, Perova, Farooq, Makhdoom, Oyedeji and Porras (2023) mention strategies on mitigating phishing attacks from various perspectives, however, their research on end-user strategies is most relevant for the purposes of this thesis and training needs analysis. The following table illustrates their main recommendations for end-users, encompassing different perspectives that an end-user may need to consider when evaluating the legitimacy of an email they receive:



	Main categories of guidelines	Guidelines
Recommendations for end-users	Use awareness as the mitigation strategy	- Be extra careful with emails from unknown or dubious origins. - Do not trust emails from anon senders. - When in doubt contact a professional in the area for help. - Delete the phishing email without opening it. - Never share your personal information unless sure about the origin. - Think twice before you click. - Be wary of pop-ups.
	Use security advice	- Update computer hardware and software. - Use antivirus software. - Check your online account regularly. - Use strong passwords, do not pretext them. - Verify a site's security. - Look up web pages, and security certificates. - Should not use the same password for multiple accounts. - Ensure that the website URL starts with https:// - Avoid using public computers for handling confidential information. - Do not leave your computer unattended. - Do not open attachments in emails by unknown senders. - Do not click on the links in emails by unknown senders. - Use 2FA via an authentication app. It is the preferred choice over SMS /voice authentication. - When unsure, use tools to check suspicious links before opening. - Block Pop-Ups. - Use the browser's phishing list.

Figure 2: Phishing recommendations for end-users (Naqvi et al. 2023, 13)

Looking at these recommendations, they are split into two categories – the first, "Use awareness as the mitigation strategies", includes relevant information for the purposes of this training as it talks of the different tactics an attacker may use with phishing – from simply looking at the sender to exercising overall caution over messages received. The second category, "Use security advice", rather goes towards more technical aspects of a potential phishing attack and the websites a user is linked towards which goes back to falsified websites that can steal users data. It also opens up the topic of reused passwords which will be further important in the part of this thesis regarding use of stolen credentials – the relevance for phishing is to limit potential breach in case one password is revealed, other platforms with the same password can also be breached by the attacker if they use the same password.

Tally, Roshan and Van Vleck (2004) share a similar set of recommendations – both for corporations (from the perspective of this thesis, though, those are more relevant for the system admins) and for consumers – these ones are relevant for customer support workers as well. These recommendations. Like Naqvi et al. (2023), it mentions exercising caution, specifically in looking at hyperlinks and verifying the authenticity of websites that users are visiting and the specific addresses.

To summarize, there are three main themes that seem to be especially relevant for end-users (and as such, customer support workers) throughout the literature mentioned above and which should be key parts of the training in this section:

1. Users need to pay attention to messages trying to evoke certain emotions and urgency.
2. Users need to pay attention to the legitimacy of a request and whether it is reasonable for them to follow it through.

3. On the more technical side, users need to pay attention to URLs/senders of messages to ensure they have not received messages with slightly mistyped links trying to get them to enter sensitive information.

Finally, the third attack vector related to social engineering is business email compromise. In order to avoid confusion between phishing and business email compromise, the definition by Bakarich and Baranek (2020) shall be used for the purposes of this thesis: “These scams usually involve the compromise of legitimate business email accounts to conduct unauthorized transfers of funds, although other variations include requesting Personally Identifiable Information, W-2 forms, real estate information, or gift cards” Bakarich & Baranek 2020, A1). In other words, the key difference from phishing is that business email compromise uses a legitimate (albeit compromised) email address, while phishing uses an unknown email address or an email address pretending to be somebody else – though notably, some other literature, such as Cross and Gillett (2020), talks about both attack vectors almost as synonyms (or rather, as business email compromise being a subset of phishing). However, according to Cross and Gillett (2020) there is a common pattern where phishing and business email compromise cross over: specifically, this reports says that in many cases, phishing is first utilized as an attack vector in order to gain access to a legitimate email account, while this account is then used in a business email compromise attack for another goal (for instance, financial gain).

To illustrate the severity of this issue, Verizon’s Data Breach Investigations Report (2023) says that the occurrence of this type of attack has nearly doubled, meaning it is becoming an even larger threat and hence its mitigation is key to ensure information security in companies. One of the largest examples of a successful business email compromise attack is the Belgian Crelan Bank: according to O’Donnell (2023), “The hacker was able to successfully gain access to the email account of a high-level executive. They managed to spoof the email account of the CEO by masking the sender as the CEO. The attacker then instructed the company’s employees to transfer money into a bank account controlled by them, all while posing as a high-level executive” (O’Donnell 2023). This is a prime example of how a business email compromise functions – through other means, the attackers managed to successfully gain access to the email address of the CEO in order to appear legitimate, then this was used as the attack vector for their true final goal.

However, in terms of this thesis’ main purpose of finding key topics for a cyber security training and the fact that in some ways, business email compromise can be considered a subset of phishing utilizing a very similar approach, with the main difference being where the scam email comes from (the legitimacy of the sender), the strategies for defense will overlap with phishing as well. The key difference, however, is that as defined previously, the sender will appear legitimate and the email will come from a legitimate email address, so on the side of an end-user, any technical inspection for the email would not work. However, the two points mentioned in defenses against phishing are key in here: the users should consider the emotions and urgency that the message is trying to evoke and they should also consider the request itself – especially how reasonable it is for them to follow through with what the attacker is asking.

To conclude the section that talks about social engineering and its two subsets most important for a training for customer support workers, these are some of the threats that according to the presented reports are most common in data breaches and hence the knowledge of how to protect against them is a key security measure. At the same time, these attacks can be aimed at anyone in the company and for a large part, the non-technical defense is extremely important – this means that the users need to be aware of the typical signs of a social engineering attack and the fact that they can be victims of it as well. Hence, this will be added as one of the key parts of the training needs analysis.

2.1.3.2 Stolen/compromised credentials

The second threat to be discussed are stolen and compromised credentials that were mentioned by the reports above as one of the most common threats. Shah et al. say that compromised user credentials "represents the legitimate user login information that the cyber-criminal took over" (Shah, et al., 2019). Through this definition and the previous definition of business email compromise from the previous section, there is a certain crossover, though the difference for the purposes of this section is that with compromised credentials attacks, the malicious users already gain access to their target, while with business email compromise, the gain of the email is simply a means to utilize it in order to gain access to the target.

The IBM Cost of a Data Breach report (2023) puts stolen/compromised credentials as the second most common initial attack vector, right after phishing, with a 15% representation among the sample collected. It is therefore important for end users to know how to deal with such a threat and what are some ways to protect themselves from it.

According to Okta (2022), there are a few tactics that users can use in order to protect themselves from password leaks or to minimize the damage of a leak:

- In order to track whether one of the users' passwords has been leaked, the free "Have I Been Pwned" service can be used – it tracks existing password leaks and this way, users can find out about their passwords that may have been compromised.
- In case a password leaks, the user should update their password on the given platform and check for suspicious activity (a password leak does not mean their specific account has been used by an attacker, so it should be investigated whether this is the

case or not). In case of this thesis, the users should also learn of a potential escalation procedure within the company to make the relevant team aware of a potential leak.

- Unique passwords should be used across platforms – especially relevant advice for business users, where a leaked password from a personal account could then cause a breach of their business account as well.
- Users should use a secure way to store their passwords – such as a password manager.

In addition to this general advice, the training should also inform the customer support workers about company policy when it comes to passwords and password managers, as well as escalation procedures.

However, the essential part of preventing leaked credentials is actually using a secure password. An example how insecure users' passwords can be a news article about the Czech police from last year by Vítková and Pošmura (2023): in a picture posted on official social media, viewers could see a sticky note with a password written down on it: "Police123". While this may seem like an entertaining exception, statistics show otherwise: a study by Jaeger et al. which analyzed passwords from a set of various password leaks showed that these were some of the most common passwords:

- 123456 (or based on other password lengths, counting further)
- 11111
- password
- iloveyou

This means that users are still commonly setting easy passwords for themselves, making their accounts susceptible to password breaches – while a strong password will not protect the users if a leak of a password database is shared, it can protect them from other types of attacks. For instance, brute-force attacks are "a method for guessing a password (or the key used to encrypt a message) that involves systematically trying all possible combinations of characters until the correct one is found" (Kaspersky 2024), while dictionary attacks are a sub-set of brute-force attacks which is "based on selecting potential passwords from a preprepared list. The attacker creates a 'dictionary' of the most likely sequences of characters and uses a malicious program to check them all in turn in the hope of finding a match" (Kaspersky 2024). Both of these attacks make users with easily guessed passwords easy targets, plus social engineering can be used to figure out other parts of a password if the attacker knows other facts about the user (their pet names, children's/partner's names, birthdays and so on). Google (2024) and Microsoft (2024), as some of the largest technology companies, have both designed guidelines on creating strong passwords and they include the following information:

- Both companies suggest a password of at least 12 characters, with Microsoft suggesting that 14 or more is even better.
- Microsoft suggests to use a “combination of uppercase letters, lowercase letters, numbers, and symbols” (Microsoft, nedatováno).
- Both companies suggest to make passwords unique and different from previous passwords.
- Microsoft says that a passwords should not be “a word that can be found in a dictionary or the name of a person, character, product, or organization” (Microsoft, nedatováno).
- Google, on the other hand, suggests to use the following ideas as the basis for a password:
    - “A lyric from a song or poem
    - A meaningful quote from a movie or speech
    - A passage from a book
    - A series of words that are meaningful to you
    - An abbreviation: Make a password from the first letter of each word in a sentence” (Google 2024)
- Microsoft also suggests it is good for a password to be easy to remember, but difficult to guess (providing the example of “6MonkeysRLooking^” (Microsoft 2024).

In addition to these tips, the client company likely has a specific password policy of their own, which should certainly be included in the training as well.

To summarize, in order to protect themselves from breached credentials, users need to ensure they are safely stored, different across platforms, not a part of a data leak yet and adhering to the best practices of passport creation.

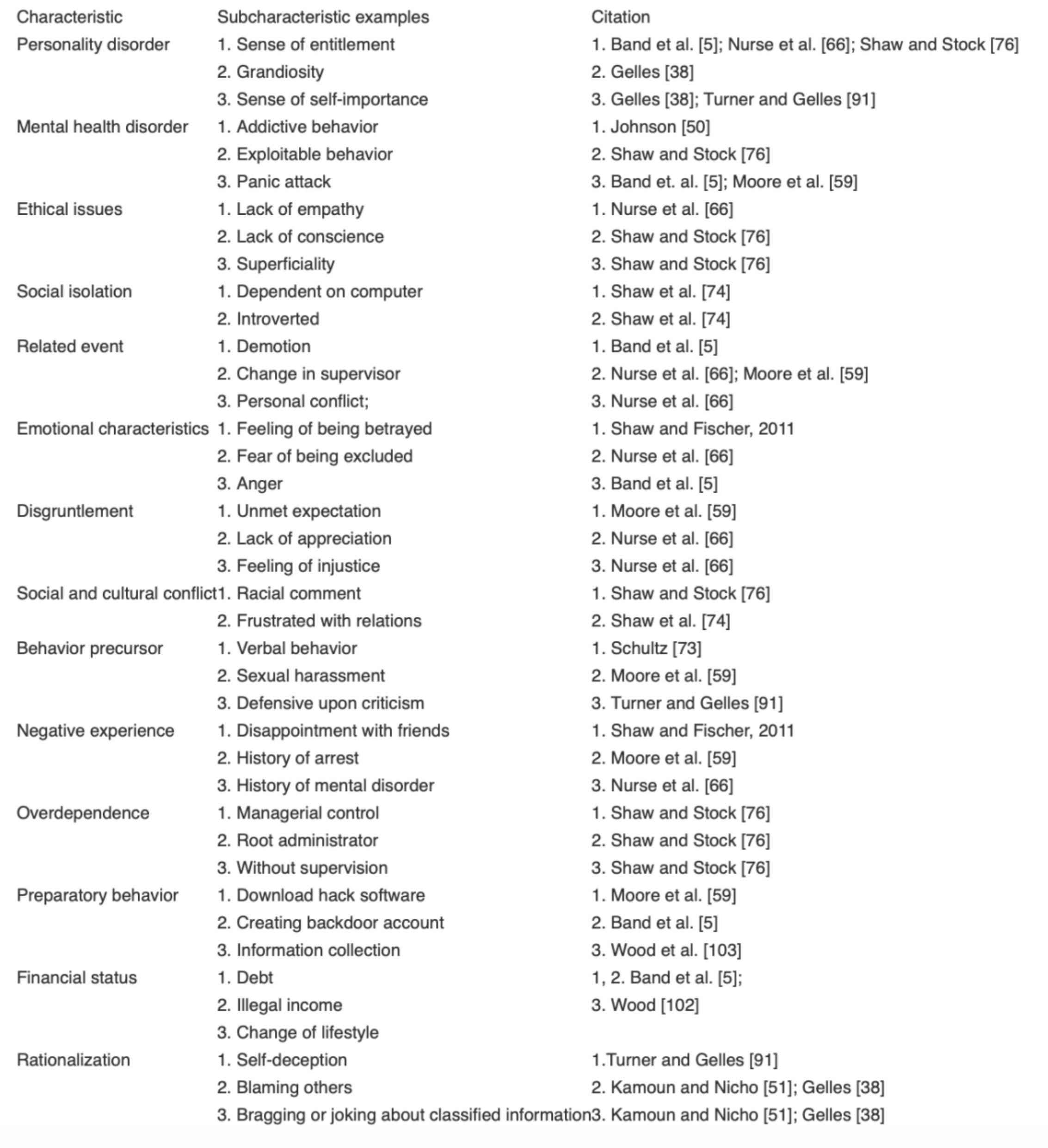
2.1.3.3 Malicious insider

Next, the threat of a malicious insider needs to be examined as it also caused a significant number of leaks based on the reports above. According to Kaspersky (2024), an insider threat “is a risk for an organization that comes from people inside the security loop. These people, known as insiders, can include either current or former employees of the company, as well as contractors or partners — that is, anyone with access to the company’s confidential information or critical infrastructure” (Kaspersky 2024). While Kaspersky (2024) goes on to mention that this can be caused by intention or by accident, the point of a malicious insider is that this attack is done on purpose.

A case that ran through the media a few years ago was that of a contractor for the American National Security Agency, who, according to Savage and Blinder (2018) leaked an important document regarding the Russian influence on American elections. This demonstrates how an insider with malicious intent can influence not only a company and its internal information, but even governmental bodies.

As such, there is little point in telling the users how to not become a malicious insider (as this would be done on purpose), but a warning can be shown about the consequences of such breach. However, what is a potentially more valuable lesson is to teach the workers of the customer support department how to recognize potential malicious insiders around them.

Liang, Biros and Luse (2016) publish the following table with characteristics found regarding malicious insiders in previous research:



Characteristic	Subcharacteristic examples	Citation
Personality disorder	1. Sense of entitlement	1. Band et al. [5]; Nurse et al. [66]; Shaw and Stock [76]
	2. Grandiosity	2. Gelles [38]
	3. Sense of self-importance	3. Gelles [38]; Turner and Gelles [91]
Mental health disorder	1. Addictive behavior	1. Johnson [50]
	2. Exploitable behavior	2. Shaw and Stock [76]
	3. Panic attack	3. Band et. al. [5]; Moore et al. [59]
Ethical issues	1. Lack of empathy	1. Nurse et al. [66]
	2. Lack of conscience	2. Shaw and Stock [76]
	3. Superficiality	3. Shaw and Stock [76]
Social isolation	1. Dependent on computer	1. Shaw et al. [74]
	2. Introverted	2. Shaw et al. [74]
Related event	1. Demotion	1. Band et al. [5]
	2. Change in supervisor	2. Nurse et al. [66]; Moore et al. [59]
	3. Personal conflict;	3. Nurse et al. [66]
Emotional characteristics	1. Feeling of being betrayed	1. Shaw and Fischer, 2011
	2. Fear of being excluded	2. Nurse et al. [66]
	3. Anger	3. Band et al. [5]
Disgruntlement	1. Unmet expectation	1. Moore et al. [59]
	2. Lack of appreciation	2. Nurse et al. [66]
	3. Feeling of injustice	3. Nurse et al. [66]
Social and cultural conflict	1. Racial comment	1. Shaw and Stock [76]
	2. Frustrated with relations	2. Shaw et al. [74]
Behavior precursor	1. Verbal behavior	1. Schultz [73]
	2. Sexual harassment	2. Moore et al. [59]
	3. Defensive upon criticism	3. Turner and Gelles [91]
Negative experience	1. Disappointment with friends	1. Shaw and Fischer, 2011
	2. History of arrest	2. Moore et al. [59]
	3. History of mental disorder	3. Nurse et al. [66]
Overdependence	1. Managerial control	1. Shaw and Stock [76]
	2. Root administrator	2. Shaw and Stock [76]
	3. Without supervision	3. Shaw and Stock [76]
Preparatory behavior	1. Download hack software	1. Moore et al. [59]
	2. Creating backdoor account	2. Band et al. [5]
	3. Information collection	3. Wood et al. [103]
Financial status	1. Debt	1, 2. Band et al. [5];
	2. Illegal income	3. Wood [102]
	3. Change of lifestyle	
Rationalization	1. Self-deception	1.Turner and Gelles [91]
	2. Blaming others	2. Kamoun and Nicho [51]; Gelles [38]
	3. Bragging or joking about classified information	3. Kamoun and Nicho [51]; Gelles [38]

Figure 3: Characteristics of a malicious insider (Liang et al. 2016, 7-8)

Further work by Glancy, Biros, Liang and Luse (2020) also elaborates on different motivations for becoming a malicious insider based on personality disorders and suggests the following:

- Insiders who cannot hold a job and are not financially responsible often launch attacks that make them achieve their personal goals (such as financial).
- Arrogant and haughty insiders rather launch expressive attacks, as opposed to achieving a goal of their own.

It is important to note that ethically, there are some parts of this research where the customer support department workers should not automatically consider somebody a threat based on one of these precursors, plus they would be invasions of privacy of the person they may suspect, hence it is important to carefully consider which of these characteristics to mention in the training. Everything that is an employee's private information should be excluded from the context of the training (such as disorders or changes of financial status).

However, there are a few characteristics included in the research which are possible to detect for a typical worker and should be raising red flags:

- Behavior precursor: even regardless of a social insider threat, these are events that should be escalated according to the internal procedures.
- Social and cultural conflict: similarly to the previous section, in case of any issues in this category, this should be resolved even outside a social insider threat.
- Preparatory behavior: this part is especially relevant – if a worker sees another worker doing any of the actions mentioned in Figure 6 under this category, they should be aware of the escalation process in order to stop a potential threat in the making.

In summary, for the purposes of the training, the workers should be educated on the consequences of causing a malicious insider threat, of the precursors they may see around them and of the escalation process if they detect a similar issue.

2.1.3.4 Accidental data loss or lost or stolen device

Accidental data loss or stolen device is another scenario causing significant losses based on the reports above. According to Sullivan (2024), “Common unintentional causes of data loss include hardware malfunction, software corruption, human error, and natural disasters. Data can also be lost during migrations and in power outages or improper shutdowns of systems” (Sullivan 2024). This simply means that data is lost through an accidental action without a possible recovery. Rock (2024) then elaborates on the specific ways that a human can cause accidental data loss (and hence ways in which workers can be educated in order to avoid such incidents) – specifically, she mentions accidental data deletion, social engineering (which is already covered under another point within the thesis), mishandled migrations (i.e., any sort of moving data from one place to another), bad integrations (data is lost while being transferred from one tool to another) and general mishaps due to lack of IT knowledge.

These are important to know for the users, but the way to protect against this threat is dependent on the policies of the client – it depends on whether users keep a lot of files locally, or typically back them up in the cloud and what these files may contain. Hence, this section needs to be adjusted to the client's needs based on their own policies. Additionally, for the purposes of this thesis, accidental data loss does not include accidental data leaks or protecting and recognizing sensitive data.

Similarly, very little can be done to educate users about preventing loss or theft of a device: besides a general advice to always pay attention to the device and making sure not to leave it unattended, the important part is rather to know how to proceed in case such a loss were to happen, so that a potential malicious user does not gain to the data stored on the device. Hence, in this section, the client needs to adjust the education based on their own internal procedures.

2.1.3.5 Physical security compromise

With physical security compromise, the topic is straying away from purely digital threats: these threats simply require the malicious actor to be present physically at the victim's location and this allows them to breach their data.

Mackay (2024) defines a few different types of physical security breaches:

- Tailgating, which he defines as "a type of cyber attack where fraudsters follow authorised personnel into a restricted area of an organization" (Mackay 2024).
- Theft of documents
- Theft of organizational devices (already covered by the previous part of the thesis)
- Theft of identification

For tailgating, he suggests the following protective measures:

"1. Never permit anyone to tailgate you into the workplace, especially in restricted areas.
2. Be confident enough to ask or challenge suspicious individuals for their credentials.
3. Be cautious around third parties, delivery drivers and other outsiders, as they could be potential hackers.
4. Report any suspicious individuals to the relevant personnel" (Mackay 2024).

This also means that the workers should be educated on the public and private areas of their workplace based on the internal policies and should ensure they never let any unauthorized people into the private areas.

When it comes to theft of documents, devices or identification, the important information is the same as previously in device theft: employees should always be aware of the location of all of their belongings and they should know the procedure for reporting theft or loss in case it does happen according to internal rules.

Breda, Barbosa and Silva Morais (2017) further add types of physical security compromises:

- Piggybacking: similar to tailgating, but in this case, the attacker uses a more sophisticated ruse then simply entering the building with a worker – they come up with a backstory or persona that makes the worker trust them (this involves social engineering as well - protection falls into that category, too).
- Eavesdropping: simply listening to employees speak in public can be efficient to find out confidential information. The protection in this case is simple – employees should not discuss confidential materials if they are not sure they are not being listened to.
- Shoulder surfing: if an employee works in a public area, their screen should not be visible to others, if it is, it can easily be read by an attacker.
- Dumpster diving: if employees simply throw out confidential documents, these can be found in the trash by malicious users.

Workers should be made aware of all these types of physical security attacks in order to then recognize them and avoid behavior that makes their exploitation easy.

2.1.4 Attack actions

As previously defined, for the purposes of this thesis, attack actions are defined as what happens once an attack vector is successfully executed and the attacker gains access to the target’s data.

Hence, as opposed to prevention that was largely the focus of the previous section, this section will focus rather on remediation in case of a successful attack. It is also important to note that in some cases, there are topics mentioned in both attack vectors and attack actions and the difference is purely semantic, but the protection measures are essentially the same, in which case these sections will refer to what has been written previously.

2.1.4.1 Use of stolen credentials

Protection against stolen credentials was mentioned along with remediation previously: firstly, the user can learn about the fact that their credentials were breached through suspicious activity in their account or through a website, such as Have I Been Pwned. If they realize they have, in fact, been hacked, this needs to be escalated internally in order to assess the possible damage and their credentials need to be changed so they can no longer be abused.

2.1.4.2 Ransomware

Ransomware is one of the key attack actions based on the reports above. Kaspersky (2024) defines ransomware as “malicious software that encrypts data or blocks access to it, demanding that the user pay for unlocking or decrypting the data” and IBM (2023) claims it was responsible for 24% of the overall malicious attacks over the time period the report analyzed. Malwarebytes (2024) talks about one of the most infamous ransomware attacks in history: WannaCry. It says that within hours of releasing the virus, an approximate 230,000 devices were infected with the virus, despite Microsoft having released a fix patching the security issue months prior to it. After infection, the victim's device had files encrypted and they were asked for a ransom of USD 300, which was later increased to USD 600.

Hence, if such an attack were to occur to the customer support department workers, they need to be equipped to react accordingly.

Anghel and Racautanu (2019) distinguish 4 types of ransomware:

- Encrypting
- Non-encrypting
- Leakware
- Mobile

While encrypting ransomware encrypts files on the target machine and then asks for ransom to unlock these files, non-encrypting ransomware rather locks the machine overall and asks for ransom so that the user can access it at all. Leakware works differently from the other two types, where instead of blocking access to files or machines, it collects information from the computer and threatens with its publication to the user. Mobile ransomware is then run on mobile devices and the key difference the authors mention is that since the information is less likely to be valuable and more likely to be backed up, the ransomware relies on the value of the device overall (and it being worthless without being able to access it), rather than the value of data.

Razaulla, Fachkha, Markarian, Gawanmeh, Mansoor, Fung and Assia (2023) do not separate out mobile ransomware in their classification, but they add scareware, which they say "tricks users into downloading or buying malicious or sometimes useless software by displaying startling messages, often done using pop-up ads. Users who take the bait inadvertently install ransomware on their devices. This type of ransomware does not necessarily pose a real threat to its victim" (Razaulla 2023, 2). This is an especially interesting type of ransomware for the purpose of the training needs analysis, as its also important to recognize a legitimate pop up from a scareware – in a very similar way to how legitimate emails and phishing need to be distinguished.

Both articles then go to explore the technical side of ransomware and the prevention from this perspective, however, for the purposes of this training, it is mainly key to explore how users should behave in case they are infected with malware and presented with the ultimate decision – to pay or not to pay.

Per the Cybersecurity & Information Security Agency (2020) based in the US, it is not recommended to pay the ransom since there is no guarantee to get the data back. In fact, Sophos (2021) reports that according to their analysis, 92% of companies do not get all their data back regardless of paying the ransom.

The key part to explain in here, however, is that in case of a ransomware attack, users should escalate this issue internally and then have the responsible teams decide on the future course of action, as opposed to trying to deal with the situation on their own due to fear of the consequences of being the cause of such a data breach.

In summary, the users should be educated on how a ransomware attack should look like, why it is not a good idea for them to pay the ransom themselves and hope for the best and on the escalation procedure for this type of attack.

2.1.4.3 Destructive attacks

The report from IBM (2023) puts destructive attacks at 25% of the sample analyzed, specifically saying that this is the percentage of attacks in the sample which rendered the target systems inoperable. One of the most famous examples of such an attack was NotPetya – according to HYPR (2024), this attack - which masked itself as ransomware, but damaged data in such a way that even after paying the ransom, there was no way to decrypt it -, caused damages in the value of USD 10 billion.

For the workers in customer support departments, however, the learning is very similar to ransomware – they should be aware of the existence of such viruses and beware of the attack vectors that could infect their computers, but in case they do get such an infection, they should not try to fix it themselves but rather escalate according to internal workflows in order to minimize potential damages and stop its spread.

2.1.4.4 Phishing and pretexting

Phishing and pretexting are two largely related terms: according to Fortinet (2024), pretexting is a tactic used to “gain access to information, systems, or services by creating deceptive scenarios that increase the success rate of a future social engineering attack”. As per the article, the tactic of pretexting is then often utilized as a part of a phishing email.

However, to take phishing/pretexting purely as an action, is difficult – rather, this will be an action that is also a vector (for instance, the attacker gets information through a data leak – the attack vector – and utilizes it for a phishing attack, which is the action in the first step, but an attack vector for another step). Hence, the defense from a user’s perspective is the same in this case as well, perhaps with one exception – if a user sees an email pretending to be from them or from a colleague, they once again need to know the proper escalation procedure.

2.1.5 Limitations

While the literature presented presents a solid theoretical background necessary to design a training on the topic of cyber security awareness, there are the following potential limitations to it:

- The statistics of common attacks from last year, to be as recent as possible, are both based on reports from private companies. While both highly reputable businesses, it is still necessary to acknowledge that this is not research done by an independent academic institution. At the same time, the topics discussed, and conclusions derived from these documents mainly focus on statistics and numbers of common attacks and as such pose little threat to the legitimacy of those claims.
- There is essentially no literature specifically focused on cyber security in customer support, so to identify these threats, this thesis has to take the overall landscape and then filter out threats relevant to the nature of customer support work. However, this is a synthesis that is quite reliable as it simply needs to define the customer support work and how threats can relate to it.
- The cyber security world develops in a very fast pace, meaning that research only few years old could already contain somewhat outdated information. However, for statistics on common threats, this thesis mostly relies on the two reports released at the end of last year, for the other papers, they are mostly used for defining the threats and necessary knowledge, which will not be as strongly changed throughout the time.

2.2 Training frameworks

To successfully design the training needs analysis, the client provided 4 frameworks that are utilized within the organization to ensure alignment with the other trainings created by their team.

These frameworks need to be applied within the context of a self-paced online training focused specifically on cyber security awareness. The applicability of their specific parts will be evaluated in this section in order to select focus areas for the training itself.

The frameworks provided are:

- The nine events of instructions based on Gagné, Briggs and Wager (1992).
- Learning styles and the experiential learning cycles based on Kolb and Kolb (2013).

- The cognitive theory of multimedia learning based on Mayer (2005).
- Theory of intrinsically motivating instruction by Malone (1981).

After evaluating these general instructional design frameworks and concepts, they will be put into conversation with recent research on the specific efficient methods of online learning and specifically online learning within the cyber security field.

2.2.1 Gagné's nine events of instructions

The first framework utilized by the client is the nine events of instructions which are mentioned in the book Principles of Instructional Design, written by Gagné et al. in 1992.

While the whole book focuses on instructional design as a field overall, the nine events of instructions specifically are “designed to make it possible for learners to proceed from "where they are" to the achievement of the capability identified as the target objective” (Gagné et al. 1992, 189). The book specifies that these do not necessarily need to be followed in the same order every time (but the book puts them in the most likely one) and some of them do not need to be mentioned explicitly as they are obvious to the learner, so they may not always be needed; notably, the authors also mention that these steps are applicable for self-guided study as well, which is necessary for this use case (Gagné et al. 1992, 189-190).

The authors define the following steps of instructional design:

1. Gaining attention
2. Informing the learner of the objective
3. Stimulating recall of prerequisite learned capabilities
4. Presenting the stimulus material
5. Providing learning guidance
6. Eliciting the performance
7. Providing feedback
8. Accessing performance
9. Enhancing retention and transfer

During the first stage of gaining attention, instructors may use various methods to achieve this – for example, the authors suggest employing appeal to learners' interests by asking questions or using changing stimuli (Gagné et al. 1992, 190-191). In the context of the training being designed using this thesis, this is especially key as it is a self-paced training, and the learners need to stay engaged throughout as opposed to simply try clicking through the training to complete it as an obligation.

In the second stage of informing the learner of the objective, the authors suggest to explicitly describe to the students how they will know they were successful with their learning, but also describe the usefulness of the learning and how they can apply it (Gagné et al. 1992, 191-192). For this cyber security awareness training, an example of describing the objective would be to name the threats they will be able to recognize and for the usefulness, knowing how much money this knowledge and awareness can save in the result.

In the third step, the authors suggest appealing to previous knowledge – this helps to synthesize the new information with knowledge learners may have had before and expand on concepts they are already aware of (Gagné et al. 1992, 192-193). For this training, this is slightly difficult as different learners will be on a completely different level of knowledge (as opposed to, for instance, school courses where the expectation is that everyone should have similar pre-requisite knowledge). However, an appeal to previous practical experience with security attacks would likely be a good use of this step – it is likely that the learners have experience a phishing scam or a similar campaign, even if nothing more serious.

To present the stimulus material, a course should review its objectives again – this stage is nothing more but presenting the materials a learner needs in order to learn the needed skill or knowledge (so it can be guidance on how to complete a skill or simply presenting the knowledge to memorize) (Gagné et al. 1992, 193-194). In this training, that means mostly describing the different threats, ways to recognize them and protect against them, as well as the practical escalation process in case of any security issues.

The following step is less relevant to an online self-paced learning experience – to guide learners, the authors mainly put emphasis on communication within the learning environment (Gagné et al. 1992, 194-196), which is limited in this scenario. However, to substitute this step, learners' questions should be anticipated in order to provide better understanding and explained in the training itself.

In eliciting the performance, the learners simply need to demonstrate the skills they have learnt (Gagné et al. 1992, 196). In this training, that could mean utilizing a practical exercise or a quiz for their skills in order to ensure that the knowledge was transferred successfully.

After the performance, there should be feedback provided to the learner in order to determine whether their performance was correct – this is either automatic (the learner sees that they applied the skill correctly) or it needs to be externally provided (an actual evaluation of the performance) (Gagné et al. 1992, 196-197).

When feedback is provided, this should be expanded on by a further evaluation of the skill: where the previous step focused on evaluating a singular performance, this one requires more input to evaluate – the authors specifically highlight that it is important to figure out whether the student has learnt how to apply the skill, or they simply memorized the potential answer (Gagné et al. 1992, 197). In a training of this sort, these two steps will likely be intertwined and similar, for example, by providing a question/practice situation after each unit and then testing the overall knowledge at the end of the course itself.

Finally, the last step takes place rather after the training itself and helps to increase retention and transfer longer term. The authors suggest refresher trainings or similar practices in the time period after the training to ensure that the students keep the knowledge (Gagné et al. 1992, 198). This could be achieved for the cyber security awareness training as well, by creating smaller units with the topics from the training as small refreshers on a regular basis after the base training is completed.

To summarize this framework, it seems that it is quite applicable for this sort of training, as it is agnostic of any specific methods and does not require any specific type of delivery (e.g., meetings or any in-person activities). Hence, it will be considered together with the other suitable frameworks to create the training needs analysis for the client.

2.2.2 Kolb’s learning styles and experiential learning cycles

The second part of this section discusses two models designed by David A. Kolb – his idea of learning styles and experiential learning cycles, both detailed in Kolb and Kolb (2013) – a fourth revision of the original documentation from 1971.

The experiential learning cycles need to be defined first, as they are a basis for the learning styles based on this model. The cycle is designed as following:

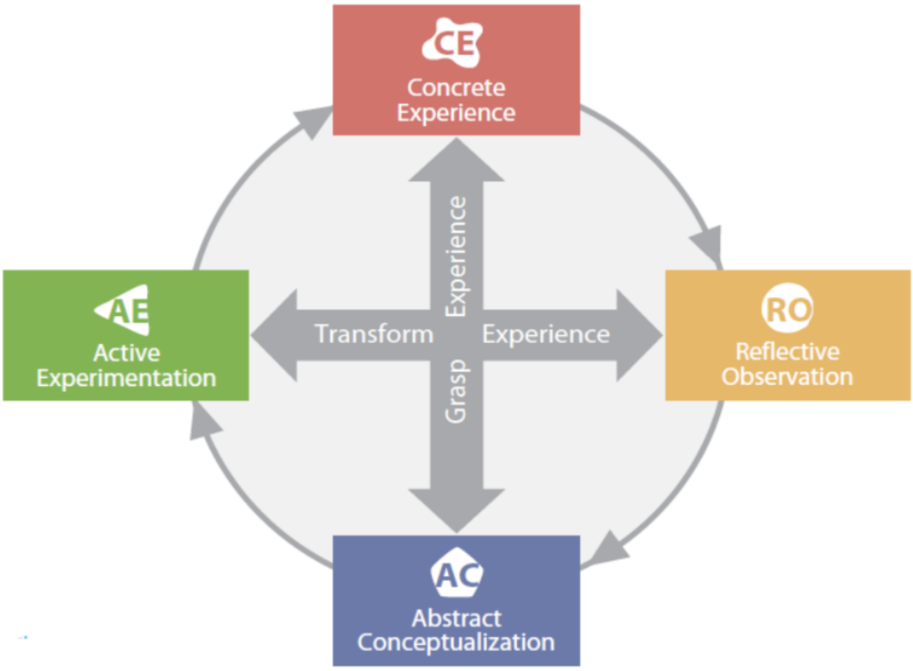


Figure 4: Kolb's learning cycle (Kolb & Kolb, 2013, p. 8)

To describe it, the authors say that “the ELT model portrays two dialectically related modes of grasping experience—Concrete Experience (CE) and Abstract Conceptualization (AC)—and two dialectically related modes of transforming experience—Reflective Observation (RO) and Active Experimentation (AE). Learning arises from the resolution of creative tension among these four learning modes. This process is portrayed as an idealized learning cycle or spiral where the learner “touches all the bases”—experiencing (CE), reflecting (RO), thinking (AC), and acting (AE)—in a recursive process that is sensitive to the learning situation and what is being learned” (Kolb & Kolb 2013, 7-8). What this means in practice is that a training should utilize a combination of training methods which allow the learners to get to each stage of this cycle – with some of the parts of the cycle focused rather on observing and having experiences and others on performing actions.

The authors then go on to categorize learners into different learning styles. As they mention, “Previous research with KLSI versions 1-3.1 has identified four learning style groupings of similar kite shapes that are associated with different approaches to learning —Diverging, Assimilating, Converging, and Accommodating” (Kolb & Kolb 2013, 10) which were based on which part of the cycle was the most beneficial for the learning of a specific learner and which they believed would make them learn the most.

However, the biggest distinction in the new version of the learner styles is that the authors actually now recognize 9 of them, as per the following graphic:

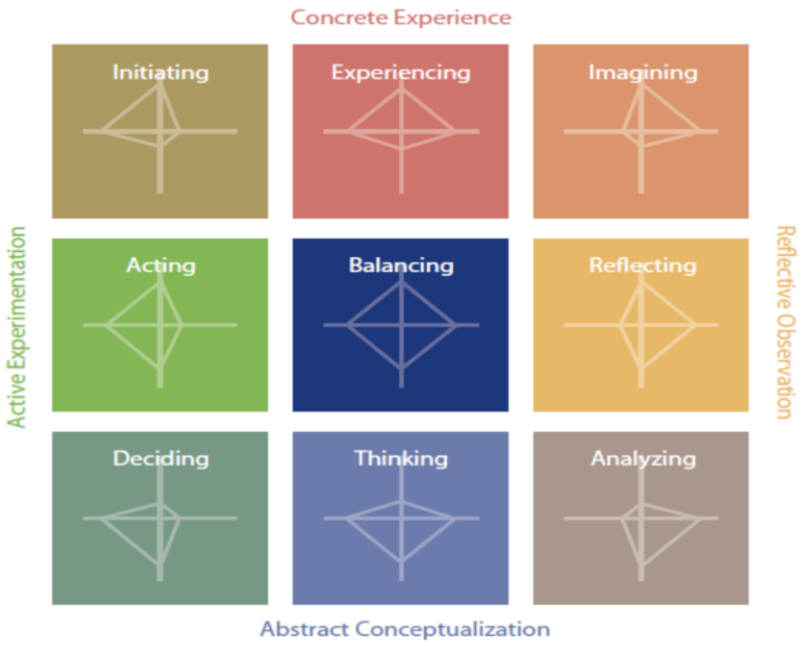


Figure 5: Kolb's learning styles (Kolb & Kolb 2013, 14)

As visible from the figure above, the model recognizes both learners who are specifically focused on one part of the cycle, while drawing also on the two surrounding ones, and learners who are in between two steps (this is where the styles defined by previous versions belonged), plus a learning type in the middle that combines all of these steps.

The styles are defined by what each of them needs to do in order to facilitate most efficient learning (for example, the Experiencing style mainly focuses on deeply involving themselves within experiences and also drawing on experimentation and reflective observation, while the Analyzing style combines reflective observation and abstract conceptualization).

The relevance of this framework for this thesis' output is mainly that in order to engage all 9 of these types of learners, all of the parts of the learning cycle have to be employed within the training, which will be considered when finalizing the suggested training outline and training needs analysis.

2.2.3 Richard Meyer's cognitive theory of multimedia training

The cognitive theory of multimedia training proposed by Meyer (2005) is based on the dual-channel assumption which says that people process visual and auditory materials using different channels and this needs to be incorporated into any kind of multimedia training.

The author then presents two ways this can be perceived:

- Based on presentation modes: focus is on whether the material is verbal (spoken or written words) or non-verbal (pictures, sounds).
- Based on sensory modalities: focus is on whether the information is perceived through sound or through visual aids, rather than on whether it is verbal or non-verbal.

Besides this, the author presents two more important assumptions:

- Limited capacity assumption: each of the channels has a limited capacity for information to process at the same time.
- Active processing assumption: people actively engage in mental processes to create a representation of the newly learnt topic in their mind.

Based on these assumptions, the author proposes the cognitive theory of multimedia learning as presented by the following figure:

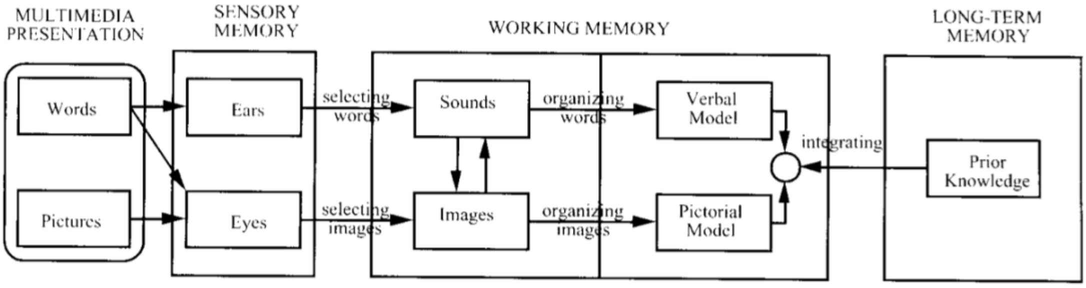


Figure 6: Cognitive theory of multimedia learning (Mayer, 2005)

Summarizing the theory, the author says that a learner can retain the materials as the exact copy of the original (i.e., as the exact words, sounds, images or other types of materials) for a short time using their sensory, but then the main part of multimedia learning takes part in working memory, which the author divides into five steps:

1. Selecting relevant words: in this step, the learner selects the most relevant words from the presented material itself which will later help them learn them concept presented.
2. Selecting relevant images: in this step, the learner selects the most important aspects of the visual aid provided to them in order to then be able to generalize them into an overall concept.
3. Organizing selected words: once a learner has selected the words, they organize them into what the author calls a “verbal model”, essentially building a connection between the different words selected.

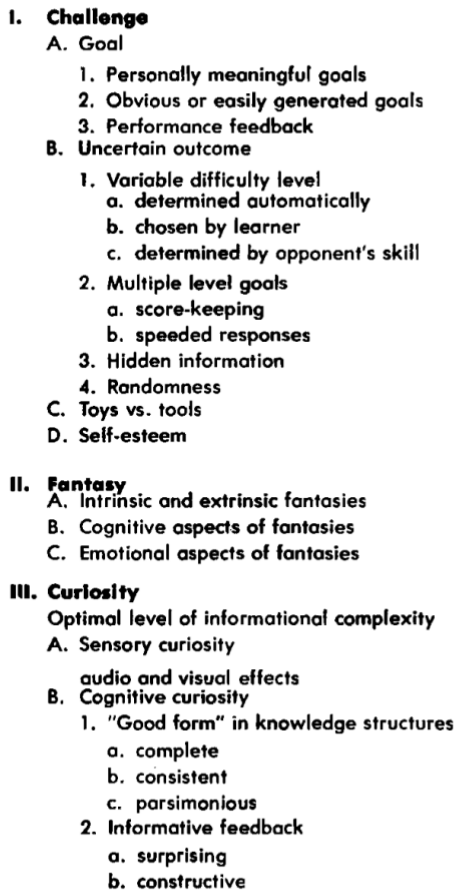
4. Organizing selected images: parallel to what happens with words – the learner connects different visual aids to each other in order to generalize the concept.
5. Integration of word-based and image-based representations: in this last stage, the author suggests that the learner finally combines the concepts they have processed visually and the concepts they have processed auditorily, integrating them into the final concept before passing it into their long term memory.

The relevance of Mayer's points towards the training proposed by this thesis comes in the following two ways:

- The training needs to ensure that the auditory and visual channels are equally utilized and yet not overwhelmed at any point.
- The training needs to ensure a good connection between auditory and visual materials in order to maximize the retention with the learner.

2.2.4 Malone's theory of intrinsically motivating instruction

The last framework for training creation which was provided by the client is the theory of an intrinsically motivating instruction written by Thomas W. Malone (1981). In this theory, the author reviews knowledge about intrinsic motivation and constructs a framework of how an intrinsically motivating training should look like. Specifically, the author proposes the following framework:



I. **Challenge**
- A. Goal
  - 1. Personally meaningful goals
  - 2. Obvious or easily generated goals
  - 3. Performance feedback
- B. Uncertain outcome
  - 1. Variable difficulty level
    - a. determined automatically
    - b. chosen by learner
    - c. determined by opponent's skill
  - 2. Multiple level goals
    - a. score-keeping
    - b. speeded responses
  - 3. Hidden information
  - 4. Randomness
- C. Toys vs. tools
- D. Self-esteem

II. **Fantasy**
- A. Intrinsic and extrinsic fantasies
- B. Cognitive aspects of fantasies
- C. Emotional aspects of fantasies

III. **Curiosity**

Optimal level of informational complexity
- A. Sensory curiosity

  audio and visual effects
- B. Cognitive curiosity
  - 1. "Good form" in knowledge structures
    - a. complete
    - b. consistent
    - c. parsimonious
  - 2. Informative feedback
    - a. surprising
    - b. constructive

Figure 7: Framework for a Theory of Intrinsically Motivating Instruction (Malone 1981, 357)

As visible in the figure above, the three main parts necessary for creating an intrinsically motivating training are that it needs to encompass a challenge, a fantasy and stimulate curiosity.

To create a challenge, the author suggests that first, the training needs to have a goal for the user (while also defining some types of these goals) – this comes hand in hand with the training having an uncertain outcome (if the outcome is known from the start, it's less likely to spark intrinsic motivation). To achieve an uncertain outcome, they should also be designed with a variable difficulty level (like video games – though this is not necessarily applicable for a training with the same exact outcome in mind). The goals should also stretch across multiple levels in order to remain motivating throughout the process. The author also suggests that not revealing all of the information at once and rather keeping some of it hidden and selectively revealing it makes a training more engaging – just like a game would. Finally, another way to achieve an uncertain outcome is implementing a level of randomness into the training. Another way the author describes to create a goal is to think about the distinction of toys vs. tools (by toys he means systems used with no external goal, such as video games, while tools are defined as systems used for achieving external goals, such as text editors). An example the author provides is that some users start considering complex systems more as a toy than a tool and that makes them more motivated to learn its most complicated functionalities. Finally, the author suggests working with the learners' self-esteem is key as it requires a balance between the boost in self-esteem that success can have and the decrease (and lowered motivation) stemming from failure, hence the difficulty should be carefully considered.

The second piece of the framework relates to fantasy: the author claims that by including fantasies into a training, it is likely to become more interesting and intrinsically motivating for the learners. The author defines that there can be extrinsic fantasies (overlaying a fantasy over existing curriculum) and intrinsic fantasies (where the learners are completing the tasks within the fantasy world and being provided immediate feedback thanks to it). The author suggests intrinsic fantasies to be the more efficient method.

The third piece of the framework relates to curiosity. In this part, the author distinguishes between sensory curiosity (brough on by change of sensory stimuli, such as change in light and color) and cognitive curiosity (which the author describes as the want to bring more structure to the learner's knowledge – such as wanting to find out the ending of a thrilling book). The way the author suggests to utilize this is to present their existing knowledge to be incomplete, inconsistent or unparsimonious in order to catch the learner's attention.

In summary, the framework presents valid ideas to utilize in the cyber security training that will be designed as a result of this thesis, namely:

- Setting goals for the training while keeping in mind the criteria for it which the author mentions.
- Utilizing fantasy in the training (and especially trying to focus on intrinsic fantasies).
- Trying to utilize both types of curiosity that the author mentions.

Finally, there are some limitations from this article that would be difficult or impossible to implement, such as the changing difficulty or uncertain outcome (as this training needs to be standardized for all learners), but the principles guiding the framework are applicable for the training overall.

2.2.5 Summary

Through the discussion of these frameworks, it is apparent that they are largely relevant to the creation of this training and shall be used in the learning needs analysis. They bring principles that are compatible with each other and hence can be used in tandem without the need of only selecting one or the other and they bring useful guidelines for the training itself.

2.3 Training methods

A key aspect of the cyber security training needs analysis designed for the client are, besides the topics themselves and the overall training framework, the training methods used. This part of the thesis aims to discuss suggestions for possible training methods that will then be paired with suitable topics in the training needs analysis.

The client has requested these methods to be suitable in an online environment, without any need for human intervention, i.e. to design a self-paced online course, which will be reflected in the methods selected.

This section will be split into two parts: the first will review literature on online training overall and suggested efficient methods in online training, while the other one will review literature specifically focused on cyber security training methods.

2.3.1 Training method overview

Lister (2014) put into conversation various papers written on the topic of online learning and identified multiple areas considered key for the success of an online training. Some of these were rather general tips for training design (such as the need to identify a pedagogical approach ahead of time and having a clear course structure from the start), but some are factors that need to be considered within this training as well:

- Including authentic tasks
- Active learning through reflection
- Providing feedback for tasks

The paper included studies focused on longer courses (such as college courses) as well, hence some of the tips are not fully applicable for this method of training, however, it provides a good initial basis for what needs to be included.

The benefit of authentic/practical task is further accented by Tirziu (2015) who says that “pedagogies which privilege collaboration, communication, sharing, problem-solving and risk-taking appear to lead to greater student engagement and sustained concentration – elements which are key aspects of achievement” (Tirziu 2015, 379), meaning that actively involving the students in some way is an important aspect of training success.

One of the ways to include practicality into a training is to utilize gamification. This is one of the trends in e-learning mentioned in Bezovski and Poorani (2016) and essentially entails adding gaming elements into a training for increased training engagement and success.

Iacono, Vallarino and Vercelli (2020) discuss the potential of gamification within the context of corporate training. The authors have explored various resources on the topic and found the following methods especially useful for corporate training:

- Going beyond a simple element of a leaderboard or coin collecting – including an overarching story in the training.
- Utilizing the self-determination theory for making “players” more curious – this theory states that there are 4 types of extrinsic motivation and the more the user identifies with the goal, the more motivated they will be with the activity itself, even if the activity itself isn’t the motivation.

Gamification was further reviewed as a training method by Wang, Hsu and Fang (2022) and their study suggested the following, based on interviews with learning experts:

- Proper integration of gamification with the curriculum.
- Providing learners with immediate feedback (and tying back to what Lister (2014) said about learning methods overall).
- Team-based competition mechanisms.
- Gradual increase in difficulties of the tasks.

Bezovski and Poorani (2016) also mention two more interesting trends in learning which could be beneficial for the purposes of the training needs analysis. Specifically, they mention micro learning as a trend of short and easily digestible trainings which are then easily memorable for the learners and do not take too much of their time to complete. Within this training needs analysis, this could be a suitable suggestion: after having a full comprehensive training completed, its smaller units could be used (potentially with small changes) as micro learning units and refreshers for the customer support department employees. This also fits with another trend from the study which is the idea of continuous learning, as opposed to a one off training.

One more trend within the study is personalized learning where learners would be able to become co-producers of a training in one way or another (essentially by working on a task they made themselves, as opposed to simply following instructions), which also ties back to ensuring the practicality of a given training.

2.3.2 Cyber security training recommendations

This section aims to discuss the expert opinions on cyber security trainings and the potential suggested methods of delivering such trainings. The requirement is the same as with the general training methods – these should be applicable in a self-guided online training – and additionally, these methods should be applicable to the topics written in previous sections, rather than only to advanced technical topics.

Bada and Nurse (2019) analyzed the design of cyber security awareness trainings for small and medium businesses and they found the following to be important for increased efficiency of these trainings that will also be relevant for the customer support department:

1. Alignment with company culture – a singular cyber security training cannot be the end of security efforts, and this has to be nurtured throughout the organization instead. Such a claim ties back to the trend of micro learning and sharing these topics on a regular basis instead.
2. Alignment with company resources/internal workflows – the company needs to make the training practical and include real life scenarios that could happen to the employees, as opposed to only including definitions.
3. Asset and harm-based approach – the company needs to create the training based on what harm could be caused to them and the learners, rather than just put all information down even if the risk of it happening is low.

Furthermore, Van Steen and Deeleman (2021) explored the previously mentioned idea of gamification specifically for a cyber security training and in particular, they checked for participants' self-reported future behavior and perceptions with a game in terms of cyber security and then the same game with another topic as a control – according to their findings, the game had positive effect on the participants perceptions and perceived future actions within the field (more so than the game based on another topic did). This further supports the idea of gamification being an effective component within the training needs analysis.

Abu-Amara et al. (2021) also explored the idea of a gamified cyber security training, as this seems to be a common pattern among cyber security awareness trainings. This training includes a specific framework with ideas that could be easily replicated and useful within the training needs analysis, specifically:

- Utilizing a game level where the user interactively evaluates their password strength and complexity.
- Another level is focused on social engineering, specifically through checking what the user would do in different situations that can occur to them on a regular basis.
- Similarly, the user's reaction to phishing and physical security attacks is evaluated.

In the provided game, the authors give the learner a few option with different points they can receive based on the option correctness, which also allows for feedback. According to the study, the results suggest that the awareness of the learners had improved in the threat categories monitored through the game.

Finally, Alhashmi, Darem and Abawajy (2021) summarized the options that can generally be utilized in a cyber security awareness training – these mostly include basic types of units in online trainings, including some of the options that were found to be especially efficient in the studies mentioned in the last two sections:

- Videos (specifically mentioning 2-5-minute-long videos explaining the threat)
- Game-based delivery (relating to gamification as described above)
- Text-based delivery (explanation in written form)
- Web-based training (including resources from external websites)

On top of these typical self-directed delivery methods, the paper also mentions a “teachable moment” delivery method, which is essentially a practical phishing simulation to test the audience’s reaction. All these methods can be utilized to a certain extent in the training needs analysis.

2.3.3 Training method limitations

The previous two sections discuss ideal training methods for a cyber security awareness training; however, it is necessary to note that there are a few limitations based on the intention of the training to be self-paced individual learning that need to be taken into account when designing the training needs analysis:

1. As this is self-paced and independent, feedback (which was named as one of the important factors to success) must be pre-defined and automatic as per the client’s requirements, rather than individual.
2. Similarly, there is no option for learners to interact with each other through discussion or other means, hence this would need to be simulated if necessary.
3. Gamification (as well as any other solution) must be designed with technical limitations in mind (ideally, through a non-technical solution with the possibility to later adjust to the client’s specific platform).

These limitations are to be taken into consideration when producing the final training needs analysis and suggesting training methods; then, these can be adjusted post-thesis with the client’s additional ideas and needs in mind and considering their internal setup.

2.3.4 Training method summary

The previous sections discussed the different concepts and methods for learning that will be beneficial for a cyber security training, such as the one being drafted through this thesis. To summarize, the training will utilize the following methods and concepts:

- An overall gamified experience with an overarching story throughout.

- A combination of videos, written articles, practical exercises, and study materials from external sources (articles etc.).
- Learners will be provided with feedback to their answers in interactive units (quizzes…).
- The training needs analysis will require the client to assess the company landscape in terms of cybersecurity and then design specific examples to suit the situations described.

3 Quiz methodology

The last part of the literature review will provide theoretical background on creating quizzes, as this is a part of the final product per the client's wish. Hence, this section aims to briefly review the best practices for quiz creation. The client needs specifically quizzes with closed questions in order to be able to evaluate them automatically.

Surip, Som, Palanisamy and Mohamad (2021) reviewed existing literature on quiz creation and suggest two types of quizzes exist and need to be considered when implementing an educational program: performance-based quizzes which evaluate performance and practice-based quizzes which aim to provide immediate feedback to students. The training designed based on this thesis will implement both methods: each unit will contain a few practice-based questions to ensure students' understanding and at the end of the course, it will contain a final quiz which will be performance-based. The authors also suggest utilizing a test specification table, which specifies the objective and focus of each question in a quiz.

Furthermore, Piontek (2008, 3-4) suggests best practices for creating multiple-choice questions. Suggestions by the author include the following:

- The "stem" (main description of the problem or question) needs to be a clearly described problem, description of task, needs to include all necessary information and be as brief as possible and not include anything besides the relevant information.
- Negative terms should be avoided (unless specifically testing the skill of detecting these) as they will likely distract and confuse learners.
- Incorrect options should be plausible, yet obviously not correct, so the correct option needs to be carefully designed in order to be the only correct one, without irrelevant clues.
- All of the above and none of the above should not be used unless testing for strictly factual information with no option of having two or more correct options.

This information is further corroborated by Boland, Lester and Williams (2010, 315), who agree with the specifications of the stem as focused and clear, containing the majority of information, leading to only one possible answer and being positively phrased. Furthermore, they specify distractors (the incorrect answers) should be short and to the point, independent, not include vague quantifiers and, like the previous paper suggests, avoid “all of the above” and “none of the above”. Plus, all answers should be similar in content, length and grammar.

The quizzes within the designed training outline will be utilizing the tips suggested above to design valuable questions, both for practice and for testing the learners’ knowledge.

4 Cyber security awareness survey

As part of the training needs analysis process, a survey was conducted regarding questions of cyber security awareness survey concerning the cyber security topics mentioned in previous sections.

The survey informed some of the focus areas in the training needs analysis itself, however, its secondary purpose is to test the suitability of these questions so that the client can then perform this survey internally (which is not possible as a part of this thesis due to this information being confident) and potentially adjust the focus areas inside the final version of the training.

4.1 Survey setup

The survey focuses solely on the cyber security topics and the awareness regarding them (i.e., the training frameworks and methods are not in the scope). The survey aims to find out the following:

1. What threats are the users aware of, especially in terms of what different terms mean (taking into account information from the findings regarding most relevant cyber security topics).
2. What are some cyber security threats they have encountered themselves.
3. Introduce model situations and see the users’ reactions to check how they would react to a threat (3 situations described – regarding phishing, leaked credentials and ransomware).

Through this, it is a combination of quantitative (asking about general awareness of threats) and qualitative (asking for specific examples of situations and asking to describe the reaction in a given situation). In addition to the actual survey questions, three demographical questions were asked: the users' age (bucketed), type of profession (mainly focusing on whether the user is working and if so, whether it is an office job) and gender. The survey was released through Microsoft Forms and shared through social media to gain replies; the survey also had an English and a Czech language version to gather more replies.

The full survey can be found in Annex 1.

4.2 Survey demographics

The survey was answered by 51 participants. Out of those, 32 were aged 18-24, 14 were aged 25-34, 2 people were aged 45-54 and 3 people were above 55 years. This means that 90.1% of participants were aged under 35 – this is important information to evaluate for the client when seeing whether this is an applicable sample to generalize for their population. In terms of work, 24 respondents were full-time students, 18 were office workers, 8 employed in other than office work and 1 respondent was unemployed. While office work is the most applicable for the workers the training is targeting, in today's day and age it is presumable that an average adult student should also work with a computer on a regular basis, hence making this likely well-applicable to the population as well. Finally, most of the respondents were female (74.5%) and it is once again dependent on the client whether this is a sample corresponding to their population.

4.3 Survey results and discussion

This section will shortly discuss the results of the survey as such and whether it validates the topics suggested by literature review. The next section will then discuss whether the survey questions were suitable for this purpose and whether this can be replicated internally by the client to be able to adjust the training or check security awareness before and after the training.

The first question asked "Have you heard of these cyber security threats?" and these were the results:

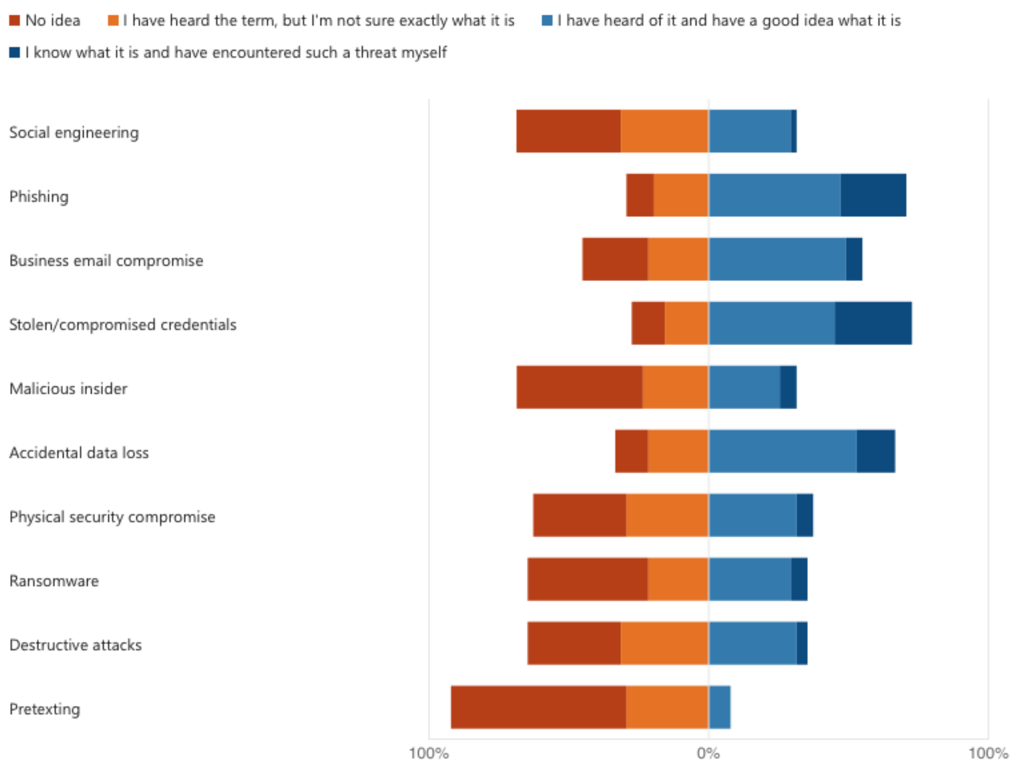


Figure 8: Survey - awareness results

Looking at the results, there were four threats that a majority (>50%) of people had a good idea about or even encountered them: phishing, business email compromise, stolen or compromised credentials and accidental data loss. It seems that people generally are aware of what phishing is and 23.5% of the respondents knowingly encountered it themselves, however, this is the only special term among these known threats – all of the other three are self-explanatory, hence possible to figure out what they are without much previous knowledge.

On the other end of the spectrum, 92.1% of people never heard of or have only a vague idea of what pretexting is (though it may be speculated that they would group this idea under phishing as it often is a part of phishing email strategies) and social engineering, malicious insider, physical security compromise, ransomware and destructive attacks all have between 60-70 people not having a good idea of what they are.

From threats that people have actually knowingly encountered, it seems that stolen or compromised credentials are most prevalent: 27.5% of the respondents say they have had this situation happen to them, followed by phishing which was encountered by 23.5% of people.

However, even with the threats with highest awareness, all had over 25% of people not knowing exactly what they are, suggesting that it is not obvious knowledge for everyone and hence a needed topic for the training. From the data in the survey, it hence looks as though all the topics mentioned should indeed be included in the final training.

From specific examples of attacks that people were targeted by (and which could hence be used as illustrative examples in the training), these were the most common answers:

- Credentials breach – mentioned 14 times – and specifically talking about bank account credentials, social media credentials or credentials breach through a public WiFi network.
- Phishing – mentioned 15 times – both in terms of asking the user to send them information (such as a 2 factor authentication code) or clicking a suspicious link; multiple times a scam involving a fake package and asking to pay for it was mentioned.
- Notably, 21 people mentioned they have not had any experience with a cyber security attack – considering all the relevant statistics above about the prevalence of these attacks, that likely also speaks to their awareness of what perhaps was an attack but they did not notice it as such.
- There were no other repeated patterns, only one singular mention of ransomware.

The next part were the situational questions. The first one related to phishing and how would the respondents react to a situation of being emailed by a person in an authority position for them to perform an action – what would they check to see it is legitimate. These were the common patterns:

- Checking the email address itself: 32 people said they would validate if the email address is correct.
- Tone and style of the message: 6 people would check the tone or style of the message (incl. e.g. calls for urgency).
- Language and grammar: 16 people would check the email for strange grammar mistakes.
- Links: 4 people mentioned that links in the email would raise their suspicion.
- Using other means of communication: 12 people would use some other means of communication to get in touch with the person directly and 1 person would verify with their IT department.
- Nature of the request: 8 people would consider whether the request itself is reasonable.
- No other overall patterns emerged.

From these patterns, it is visible that besides the email address which would be checked by 62.7% of the respondents, all of the other means of checking the validity of an email were significantly lower and hence describing typical traits to recognize a phishing email would be a welcome part of the training.

The second part of the training asks about ransomware and how would people react to getting infected and being asked to pay in order to unlock their computers:

- Escalation: 34 people said they would escalate (either to IT inside their company, asking an IT specialist friend or bringing it for repairs, some mentioned calling the police).
- Not paying: 18 people explicitly said they would not pay any money.
- None of the responders said they would pay.

It seems that in this case, people are aware or suspect that paying the ransom is unlikely to have the effect they would like. Hence, while reiterating this is important, it is key to include the information on how to escalate such cases to the relevant department in this training.

The final question asked the users how they would deal with having one of their passwords leaked:

- Change the password: 27 people said they would change their password and/or add additional security to their account (like 2 factor authentication).
- Escalation: 19 people said they would escalate such an issue – some mentioned customer support of the platform in question, others, similarly to the previous question, to their IT specialist friends or IT departments of their companies.
- Other options were rather individual – one person said they would not do anything, two people mentioned they would let others using the platform know not to trust the old account.

While changing a password and escalating is advisable, it was still only 52.9% doing the former and 37.3% doing the latter out of the respondents. Hence, educating people on how this needs to be handled and the escalation procedures is crucial in this situation as well.

Overall, the survey in this format provided good insight for the training and validated the topics included as some of those that the audience has a knowledge gap in.

4.4 Survey improvement suggestions

Besides informing the topics of the suggested training outline, the secondary purpose of performing this survey was to examine whether it yields useful information, so that it can be revised and utilized by the client to understand cyber security awareness in the department before and after the training. For the most part, it did yield useful information and asked questions in a way that prompted users to share insight, but there were two points that could be improved if it were to be released within the client's organization:

- Some users commented that they had a cyber security experience with an attack for which they marked that they did not know what it was – this likely means they were not aware of the terms. Hence, the option of "I know what it is and have encountered such a threat" could be removed, making the Likert scale only three point and then asking a separate question about whether they encountered threats where they are explained using simpler terms.
- The question regarding ransomware could be split into two parts – one free-form (as it is now) and one yes/no question asking whether the learners would pay the ransom, as this was only written in some cases.

With these, the training outline designed based on this thesis' could be updated with some additional knowledge the client may find missing and after completing the training, the users could take the survey again to see whether their knowledge has improved.

5 Implementation

The implementation of this thesis and its final product is the actual training needs analysis prepared for the client. This analysis is supposed to be utilized in tandem with the information presented in the remainder of the thesis where these topics are discussed at greater lengths – where the outline suggests to include a certain topic, the details should be included from the discussion of threats. This training needs analysis will include the following information:

- Necessary topics to cover, with details about the information that needs to be shared and a suggested order of the topics.
- Suggested methodology for each unit, i.e. the complete outline of each session saying how it should be presented.
- Suggested quiz questions for each unit and a final quiz, including suggested passing criteria.
- Questions/gaps that need to be answered using the client's internal information which cannot be a part of the thesis.

The analysis will then be shared with the client in its publishable form, however, based on the client's interest it can be further developed using internal information which is not a part of this thesis.

5.1 Training overview

Based on the research above, a training containing 8 units of content (one for each of the important threats, where ransomware and destructive attacks are merged as the learning is essentially the same) plus an introduction to the course overall and a final quiz.

In order to implement the gamification aspect to the training, it will include an overarching story about a worker named Bob who is encountering the threats that the learners are being taught about and they will get descriptions of situations that Bob has to decide about – based on this, they will then be able to see how Bob did, making the experience a bit more interactive. With each of the decisions, they can also keep a track of their points to see how they do throughout as a game (utilizing a practice-based quiz, as opposed to the performance-based final quiz).

Each unit will also include a description of the specific methods and frameworks that it utilizes from the research above in order to achieve the best possible effect in learning.

5.2 Unit 1: Introduction to the training

This unit does not include any specific training topics, but rather introduces the learner to the concept of the training as such and should help them understand the structure of it, as well as the gamified story inside.

5.2.1 Content

The unit has three topics to introduce: the point and goal of the training, the overarching storyline and the list of topics.

The learners are first introduced to the importance of cyber security education and prevention – the average cost of a data breach per IBM ($4.45M) can be shared and then to add value for the learners, they should be aware that these practices will not only help in their working life, but also in their personal lives to protect their social media accounts, as well as their internet banking and other platforms.

For the story, Bob is introduced as a customer support worker who has been working in the department for a while now, but he seems to be getting lost in the dangerous world of internet threats. It is then said that Bob will be included in all the units throughout the training to help the learners practice.

Finally, the learners go through the list of units that will be mentioned throughout the training.

5.2.2 Training outline

The unit is introduced by emphasizing the importance of cyber security and providing real life evidence of this and adding a captivating real-life story of how much financial impact cyber security attacks had recently and how much companies lost due to not being prepared – this explains to the learners the point of the training and the reason they should learn about this. Next, the story of Bob is introduced and after it, the list of units with short introductions. Finally, the quiz question is shown.

5.2.3 Quiz

There is no new topics introduced in this unit, however, in order to familiarize the learners with the overall layout of the training and to make them work within the frame of the fantasy, a simple question regarding Bob's work can be introduced with a joke to make the training more entertaining, for example:

Bob's computer stopped working out of nowhere. What should he do about this?

a. Contact the IT department.
b. Throw the computer out of the window.
c. Pretend that he is working while staring into an empty screen.

This can make the learners understand how the quizzes will look, how they will see correct and incorrect answers and finally, they can get the first point for the overarching game and consider the unit more interactive.

5.3 Unit 2: Social engineering attacks

Social engineering was determined as one of the key areas for customer support workers and it is also one of the most content-heavy units. The unit will discuss the concept of social engineering, as well as some of its most common types. Theoretical background is included in sections 4.1.3.1 and 4.1.4.4.

5.3.1 Content

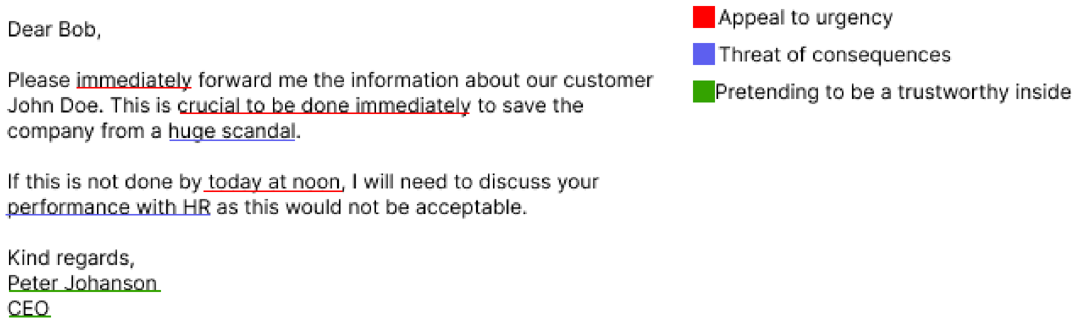
This unit focuses on social engineering attacks, including the important subtopics of phishing, business email compromise and pretexting. As such, it should cover the following knowledge:

- Introduction and definition of social engineering as an attack type where attackers try to gain access to information through a person with the required authorization, through various techniques.

- Discussing phishing emails (including the method of pretexting which is often intertwined with phishing emails as such) and how attackers typically try to gain the users' trust – the feelings they try to appeal to and the sense of urgency present. For pretexting, it is important to discuss what sort of scenario the attacker may create and who they may pretend to be – this should ideally be adjusted to company context.
- Lastly, business email compromise should be discussed and explained as the use of a legitimate email address (or seemingly so) in order to gain trust and then exploit the users.

5.3.2 Training outline

The unit should start by captivating the attention of the learner by using a real-life story of a phishing attack and its impacts, then describing the objective of what the learner should be able to recognize by the end of the unit. Then, they should be asked to think of a situation they encountered with a phishing email/social engineering overall, which due to the prevalence of these attacks should be feasible. After, they return to the overarching story of Bob who comes to work to find a phishing email in his mailbox. On this example, they are asked to identify how they may realize that it is indeed a phishing email. After, it is examined what some of the most common patterns and methods within these emails are – this can look as in the figure below:



Dear Bob,

Please immediately forward me the information about our customer John Doe. This is crucial to be done immediately to save the company from a huge scandal.

If this is not done by today at noon, I will need to discuss your performance with HR as this would not be acceptable.

Kind regards,
Peter Johanson
CEO

🟥 Appeal to urgency
🟦 Threat of consequences
🟩 Pretending to be a trustworthy inside

Figure 9: Phishing email example

This example should also have more company context added to appear more practical to the learners (e.g., changing the CEO to another person that could be contacting them). From a concrete example, the learners then move to actual definitions of the topics discussed and the concepts of phishing, pretexting, social engineering and business email compromise are described – ideally as a video to engage the auditory aspect as well. After this, they are asked to think back to the experience they had with an email or other attack and identify themes in it that relate to the definitions introduced in order to apply the knowledge. Finally, the learners complete the situational quiz for Bob.

5.3.3 Quiz

Bob receives an email from the IT department that says he needs to change his password using the link in the message. How should he validate the legitimacy of the request?

a) He should click the link and see where it leads, then evaluate it.
b) He should check with the IT department whether they have sent such a message.
c) He should just delete the email and ignore it.
d) He should run an antivirus scan of his computer.

Correct answer is B.

Feedback for the learner: If the email is allegedly coming from an internal actor, it is best to directly check with them if they sent such a message. You should never click links in emails you are not entirely sure about as they may lead to malicious websites. Deleting the email does guarantee you will not get a virus from the email or leak your information, but in case the request was valid, you will not follow the proper policy, plus if it was not, the phishing attempt will not be reported later. Finally, an antivirus scan will not be able to verify a phishing email as such unless you already downloaded a virus from it.

5.4 Unit 3: Stolen and compromised credentials

Stolen and compromised credentials are the second topic, introducing the general concept, but mainly how the users should protect and set up their passwords and what to do in case of a password leak. Theoretical background is included in sections 4.1.3.2 and 4.1.4.1.

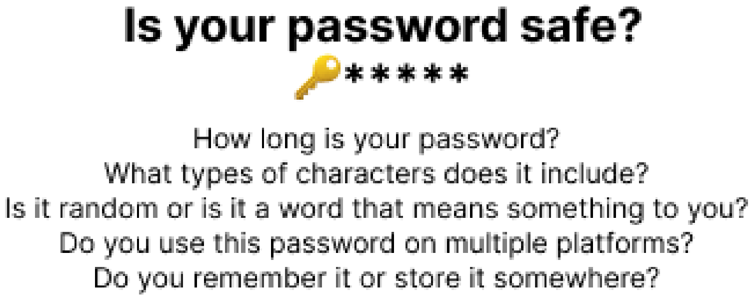
5.4.1 Content

This unit should introduce the learner to the following concepts:

- What stolen and compromised credentials are – simply that it means the attacker gaining access to the system through legitimate credentials that were leaked or they gained from someone.
- What are the best practices for creating passwords and storing them.
- How they can proceed If they believe their passwords have been compromised.

5.4.2 Training outline

Similarly to previous units, the unit starts by including a real-life related story (the story of the Czech police with an easy password written on a piece of paper is suitable here) and discussing the impact credential issues could have. Then, the users move to a practical exercise and they are asked the following questions to determine if their password is safe:



Is your password safe?

🔑*****

How long is your password?
What types of characters does it include?
Is it random or is it a word that means something to you?
Do you use this password on multiple platforms?
Do you remember it or store it somewhere?

Figure 10: Password safety exercise

The users are asked these questions about their password to consider the safety of it and then a material is presented regarding the best practices for password creation and storing, based on the materials presented from Microsoft and Google and also adjusted to company policies, which may determine the overall requirements for the passwords, as well as e.g. which password manager is allowed – ideally, this should be presented in a video or audio form to appeal to the auditory channel as well. This is accompanied by the list of most common passwords to illustrate how weak people set their passwords to be sometimes. Finally, there is a situation involving Bob in this section as well – in this case, Bob found out that one of his online passwords leaked and this is the same password that he used for his work accounts. On this example, the internal escalation policies of such incidents are explained as well as the best practices on what to do about this if it happens with a personal account (changing the password, checking for suspicious activity, checking password leaks with Have I Been Pwned).

5.4.3 Quiz

Bob was born on 1 May 1995, has a cat named Portia and lives in Oslo. Which of the following would be a suitable password for him?

a) Porti@1995
b) 10854!BrPL
c) OsloTheBest!01051995
d) 12Pi@noZf@llinG!

Correct answer is D.

Feedback for the learner: The first option includes the name of the cat (even if a bit change) and Bob's birth year, plus is is too short. The second option would be suitable as it is random, but it's also a bit short. The third option utilizes too many recognizable facts about Bob. The last option is suitable, because even though it uses a phrase that is rememberable (12 pianos falling), it changes the a's into @'s, the s into Z and capitalizes some of the letters, plus it is quite a random phrase.

5.5 Unit 4: Malicious insider

Further, the topic of a malicious insider is introduced to the learners, talking mainly about how to recognize one, but also the consequences of it. Theoretical background is included in section 4.1.3.3.

5.5.1 Content

This unit should introduce the following ideas:

- What is a malicious insider (i.e., somebody on the inside of the company trying to cause harm to it).
- What are the consequences if somebody were to become a malicious insider.
- Behaviors that a malicious insider demonstrates so that the learners can be vigilant about this.

5.5.2 Training outline

The unit starts by describing a situation to demonstrate what a malicious insider is – to make it easier for learners to relate, it can be a situation that could happen within the company itself. After the initial situation is described, the term of a malicious insider is defined (ideally, explained through video or audio). After, it is explained what the consequences for such a behavior may be (both in terms of the work contract, but also legal implications). Finally, we go back to Bob who explains that one of his colleagues has been acting a bit strange and he is not sure what to do about it. From here, the learners are asked to think what the traits of a malicious insider could be in their opinion and how this behavior would be demonstrated. Then, the traits of a malicious insider and the activities are described based on the research in the relevant section (e.g., seemingly copying company data to portable drives or sending themselves some files to personal accounts, generally strange behavior etc.) and the escalation procedure is described based on internal policies.

5.5.3 Quiz

Bob noticed that one of his colleagues has been using a portable drive a lot at work and downloading some files on it. He’s not exactly sure what files, but it’s not a typical thing for his job to be downloading files like this. What should he do?

a) Call the police
b) Escalate to the relevant team (based on internal policy)
c) Nothing, it’s none of his business
d) Just ask the colleague

Correct answer is B.

Feedback for the learner: Calling the police is a severe solution for something where Bob cannot be sure of any malicious acts just yet. Not acting would, however, also not help in case something malicious is happening. Asking the colleague in a situation where he thinks that something nefarious is going on could, on the other hand, just make that person more careful. Hence, it is best to escalate according to internal procedures – the responsible team has the expertise to check what is happening and advise Bob what to do next.

5.6 Unit 5: Accidental data loss and lost or stolen devices

This unit shows the users how they should deal with cases of lost or stolen devices and data – mainly, this should include internal escalation procedures. Theoretical background is included in section 4.1.3.4.

5.6.1 Content

This unit should teach the learners the following:

- What accidental data loss means (i.e., that it’s simply accidental deletion or other way to lose data)
- What are the escalation procedures if the learners accidentally lose some data or their laptops.

5.6.2 Training outline

The unit starts with Bob describing a situation where he managed to lose his laptop at the airport when traveling for a business trip and how he was not sure what to do. In this unit, the quiz comes after this to test whether already, the users would be able to say where to escalate such an incident. After this, the users are explained briefly how to escalate cases of losing their device or data by accident.

5.6.3 Quiz

In this section, the quiz needs to be adjusted to the company procedures, but it should look similar to this:

Who should Bob turn to first if he lost his computer at an airport (you can assume he is able to communicate with anyone through his phone)?

a) His manager
b) The office assistant
c) The IT team
d) Airport security

Correct answer depends on internal procedures, as does the final feedback.

5.7 Unit 6: Physical security compromise

The next unit talks about what constitutes a physical security compromise – as customer support workers also need to follow security principles when in the office, this topic introduces them to the potential threat of tailgating and ensuring security of documents they are handling. Theoretical background is located in section 4.1.3.5.

5.7.1 Content

This lesson should educate the learners regarding the threats of physical security compromise, specifically this entails:

- What is tailgating and how to avoid it (being careful to not let strangers into the office, ask them for credentials if uncertain).
- Being mindful of any important documents or work ID and knowing the escalation procedure if any of these were to get lost.

5.7.2 Training outline

The unit starts with a description of a situation that happened to Bob – he was going to the office one day and realized that another person tried getting into the office with him. However, he did not remember seeing that person beforehand, so he is unsure what to do. This is where the quiz in this section comes up – to test and see what the learners would do. Then, the term tailgating is explained and the way that it should be handled. Afterwards, the learners are reminded to take care of their belongings, such as important documents or ID cards and are told where to escalate in case they realize any of these are missing.

5.7.3 Quiz

What should Bob do about the person trying to get into the office with him if he's unsure who it is?

a) Nothing, most likely it's just someone new, he should just let them in.
b) Run inside the office quickly and close the door.
c) Ask the person for some identification that they work in the same company.
d) Call the security in the building.

Correct answer is C. Feedback for the learner: You should never let a stranger into the office – even if it is somebody new, you should verify this and the little moment of awkwardness to ask is better than having somebody compromise the security of the office. At the same time, there is no reason to run to the office and close the door unless you feel like there's an imminent threat to you in some way. Similarly, there is no reason to call security unless you feel unsafe. Hence, the best resolution for this situation is to calmly ask the person for some sort of identification that they work in the company (can be adjusted to company context).

5.8 Unit 7: Ransomware and destructive attacks

In the last unit before the recap, ransomware and destructive attacks are mentioned – both terms are explained and learners also learn how they should go about a computer that was already infected. Theoretical background is located in sections 4.1.4.2 and 4.1.4.3.

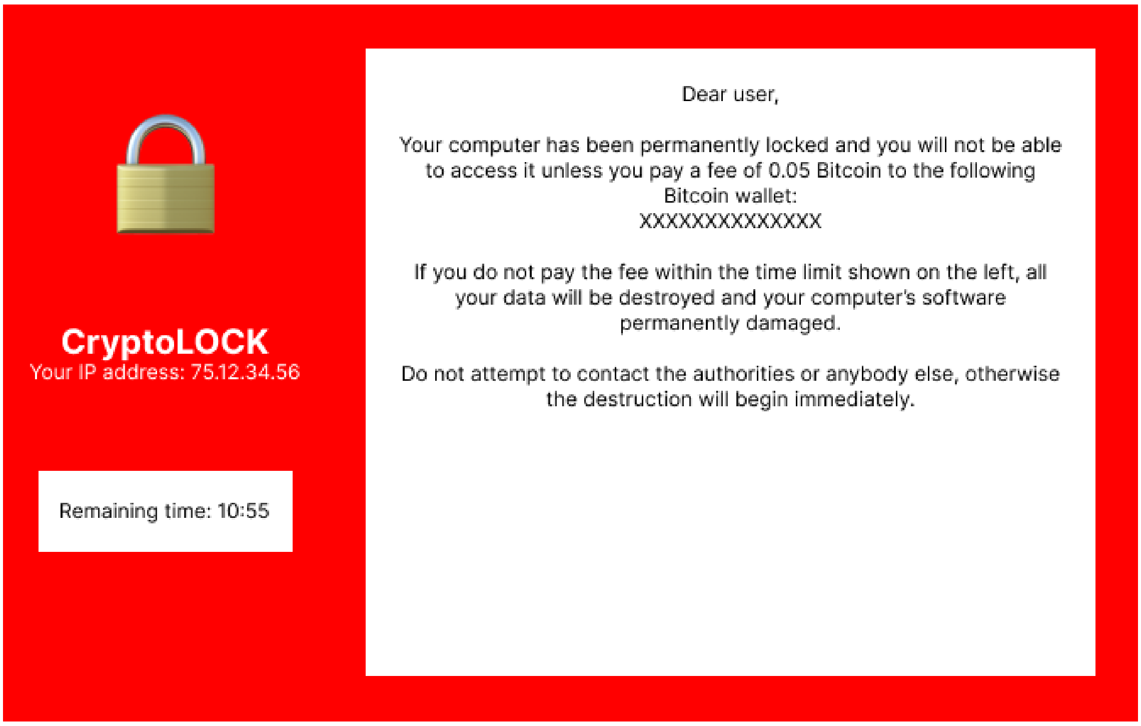
5.8.1 Content

This unit needs to explain the following topics:

- What are ransomware and destructive attacks overall and what are some types of it.
- How the learner's computer can get infected by ransomware.
- How to react in case a ransomware infects the learners' computers.

5.8.2 Training outline

The training starts by one of Bob's encounters again – this time, he came to his computer to realize that it is asking him to pay for money to unlock it, otherwise it will not let him in. The screen can be mocked, such as in the following way:



CryptoLOCK
Your IP address: 75.12.34.56

Remaining time: 10:55

Dear user,

Your computer has been permanently locked and you will not be able to access it unless you pay a fee of 0.05 Bitcoin to the following Bitcoin wallet:
XXXXXXXXXXXXXX

If you do not pay the fee within the time limit shown on the left, all your data will be destroyed and your computer's software permanently damaged.

Do not attempt to contact the authorities or anybody else, otherwise the destruction will begin immediately.

Figure 11: Mock ransomware screen

Based on this example, the learners are explained what ransomware is and what are some types of it (encrypting, non-encrypting, leakware, mobile and scareware). From this basic definition, they are asked how they believe they should protect themselves and what they should do in case they see their computer infected by these threats. They are also told of how prevalent this type of attack is (24% of all malicious attacks according to the IBM report) and some of the most infamous examples, such as NotPetya – all of this should ideally be done in a video. After the video, they are explained how ransomware can infect their computers (typically through an infected download or a link, like other malware), what destructive attacks are and lastly, they are told how to escalate – here, the statistic of 92% of paying victims not receiving all their data back can be used in order to dissuade the users from considering to pay the fee and rather escalate to the correct team. Finally, they are asked to advise Bob what to do in the quiz. After the quiz, they learn that the IT department was successfully able to remove the threat from Bob’s computer without the need to pay.

5.8.3 Quiz

How should Bob proceed with dealing with the virus?

a) Attempt to get rid of it himself.
b) Pay the ransom so nobody learns of his mistake.
c) Escalate to the relevant department.
d) Claim his laptop isn’t working and ask for a new one.

Correct answer is C. Attempting to get rid of the ransomware on his own could be putting his data in danger if he’s not an expert, paying the ransom will not necessarily have the right effect and the last option is just a bad attempt at covering his tracks. Escalating it to the right department is the only right option in here – they will know what to do about it and will also be able to determine if perhaps a larger-scale attack is at fault.

5.9 Unit 8: Recap

This unit simply reviews what has been talked about – once again shuffling through the types of attacks mentioned to reinforce the knowledge. After this, it is time to evaluate the learner’s success in Bob’s story. Depending on the learning platform, either the learner should count points themselves through the units or it will be done automatically and as there were 7 total Bob questions, this can be the evaluation for the game:

- 7 points – Bob has managed to get through the threats presented with no problem and he’s safe and sound from any criminals, great job!
- 5-6 points – Bob has made a few mistakes but has remained mostly safe in the world of cyber threats. After reviewing this training, you will definitely be able to navigate these with no problem.
- 3-4 points – Bob has had a rocky journey with the cyber threats presented for him. Make sure to remember what the training talked about and revise the trickier topics.
- 1-2 points – Bob is in a bit of a hot water with the IT team, unfortunately. However, if you carefully review the training, you can still do great!

5.10 Final Quiz

The final quiz consists of 10 questions with a 90% pass criterion (i.e., one mistake allowed). The questions do not have any specific order and both the questions and possible answers can be randomized if possible to prevent cheating as much as possible. The questions test the learners’ knowledge based on all preceding units, while adhering to the research done regarding quiz design. The full question list can be found in Annex 2.

5.11 Follow-up actions

A suggestion in Gagné’s nine events of instructions as well as generally to keep up awareness of these issues high is to follow up a training later after completion. Hence, a suggestion to this point would be to, in addition to this one large training, create small trainings from the separate units within the large one. These can then be assigned to learners as reminders on a regular basis to keep the awareness levels high.

5.12 Methodology evaluation

This section provides a brief evaluation of adhering to the frameworks and methods previously introduced.

- Gagné’s nine events of instruction: at the very beginning of the training, the units try gaining attention of the learners by describing real-life situations or introducing the stories of Bob and his encounters with cyber security. The learners were then also at the beginning informed of the objective. In the relevant units (such as phishing), they were also asked to recall previous knowledge or experience to see how this is relevant to them. Most of these steps were then repeated in each unit if applicable and finally, at the end, performance was elicited in the final quiz. For the ninth step, the suggestion of follow up reminder trainings is applicable.
- Kolb’s model: the main requirement for Kolb’s model and including as many types of learners based on it as possible was to apply each of the steps of the learning process based on his model. Hence, in each unit, a concrete experience was typically described, where the learner had the chance to reflect on what happened and then the concept was derived from the experience or situation. Finally, if possible, the learner was asked to experiment, or rather apply, this knowledge, such as when thinking about phishing emails they received or whether they apply the principles for password creation in their passwords as well.
- Meyer’s theory was mainly utilized by trying to combine both visual and auditory aids in the more complex units, so that the learner’s receive both types of input.
- The relevant parts of Malone’s theory were also utilized – mainly, it was generating a fantasy that accompanies the entire training. It also utilizes the types of curiosity that the author describes – different types of guiding materials trigger sensory curiosity, while cognitive curiosity was utilized when trying to describe stories of different cyber security experiences.
- Gamification was utilized with an overarching story and counting points from each unit as a minigame for the entire training.
- A variety of methods, such as describing real cases, including videos and other material was utilized.
- Learners were provided with feedback in the possible extent (i.e., detailed explanation of each question in quizzes, as there is a limitation on not being able to deliver personalized feedback through this sort of mass learning).
- The training needs analysis suggested parts where the client should slightly adjust it for company specifics.

6 Results

The evaluation of the results of this thesis' outcomes is based on two parts: client feedback on the finalized product and comparison of the finished thesis with the aims set out at the beginning.

The client is satisfied with a comprehensive training plan that they believe does not require tweaking from their side in order to turn it into a training. They are also satisfied with the fact that all of the methodologies they provided to be utilized were thoroughly covered, including steps that are often overlooked (they mention the example of Abstract Conceptualization in Kolb's cycle as one that is often not implemented). They also noted that feedback provided through the design of the training plan was taken into consideration and changes were made based on the suggestions from their side.

This ties back to the first and main aim of the thesis which was to provide the client with a training outline to increase cyber security awareness within the customer support department. Based on client feedback, this goal was satisfied and they can utilize this outline for its intended purpose.

The second aim, a sub-aim of the creation of the outline as such, was to create a knowledge base of relevant cyber security threats for the customer support department. This was done through a comprehensive literature research and evaluation of the relevancy of these threats for a customer support department and was then utilized to build up the training outline. Hence, this aim was also satisfied.

The final aim was to provide the client with a way to test cyber security awareness within the department through a survey. The survey was designed and tested with a general audience and based on this, improvements to the survey were also suggested for the client's use. On top of that, the data generated through the survey carried out within a general population can be used as a benchmark for the client.

Overall, all three aims of this thesis were satisfactorily met and it can be provided to the client as a finalized product.

7 Conclusion

To conclude, based on the initial aims, it was determined that three parts of the thesis need to be defined and then synthesized in order to create the desired final product – a review of cyber security threats, training frameworks, methods and quiz methodologies, as well as a survey with a test of its implementation.

The part of cyber security threats outlook showed that most methods relevant to a customer support department are related to different sorts of social engineering, but that customer support workers should also be aware of threats, such a ransomware, and not only how to prevent it, but also how to proceed in case their computer is infected through such a threat. These threats were found and evaluated as relevant based on two recent reports of most dangerous threats for a business.

The second part discussed training methodologies and framework, as well as quiz creation guidelines, and it showed training frameworks based on the client's request as very valuable to create a comprehensive training outline in the final product of the thesis. It also showed methods that have been shown to be efficient with cyber security in particular, such as gamification, which were then also implemented into the final product.

The survey itself was designed based on the relevant cyber security threats and aimed to find overall awareness of these threats in the general population, but within the thesis, it was mostly included in order to test the relevancy of its results so that it can later be used by the client themselves.

Finally, the product of the training outline was synthesized using the previously researched information and included suggested content, training methods, as well as full quiz questions and a final quiz to the training as such.

For future research in this area, this thesis implies the usefulness of utilizing comprehensive training frameworks, such as the four utilized inside of it, while these need to be combined with practical information on cyber security threats as such.

7.1 Limitations

As per the thesis limitations, the company context was not available to utilize as the thesis will be public, meaning internal information cannot be written inside the paper itself. However, a cooperation with the client after the thesis project can fill this gap. Similarly, this limitation meant a survey could not be carried out to analyze the final impact of the finished training and published, as it would contain internal information. However, this can be to a certain degree substituted by the feedback of the client who is a subject matter expert on training matters and can evaluate the efficiency of a training based on its outline.

References

Abu-Amara, F., Almansoori, R., Alharbi, S., Alharbi, M. 2021. A novel SETA-based gamification framework to raise cybersecurity awareness. International Journal of Information Technology, 13(10), 1-10. Article from ResearchGate. Accessed 10 March 2024. https://www.researchgate.net/publication/353954369_A_novel_SETA-based_gamification_framework_to_raise_cybersecurity_awareness

Aldawood, H. & Skinner, G. 2020. An Advanced Taxonomy for Social Engineering Attacks. International Journal of Computer Applications, 177(30), 1-11. Article from ResearchGate. Accessed 4 March 2024. https://www.researchgate.net/profile/Hussain-Aldawood/publication/338623330_An_Advanced_Taxonomy_for_Social_Engineering_Attacks/links/5e20357b458515ba208aea83/An-Advanced-Taxonomy-for-Social-Engineering-Attacks.pdf

Alhashmi, A. A, Darem, A. & Abawajy, J. H. 2021. Taxonomy of Cybersecurity Awareness Delivery Methods: A Countermeasure for Phishing Threats. International Journal of Advanced Computer Science and Applications, 12(10), 30-35. Article from Google Scholar. Accessed 10 March 2024. https://dro.deakin.edu.au/articles/journal_contribution/Taxonomy_of_Cybersecurity_Awareness_Delivery_Methods_A_Countermeasure_for_Phishing_Threats/20627445/1/files/36832002.pdf

Anghel, M. & Racautanu, A. 2019. A note on different types of ransomware attacks. Cryptology ePrint Archive. Article from Google Scholar. Accessed 9 March 2024. https://eprint.iacr.org/2019/605.pdf

Bada, M. & Nurse, J. R. C. 2019. Developing cybersecurity education and awareness programmes for small-and medium-sized (SMEs). Information & Computer Security, 27(3), 393-410. Articles from ProQuest. Accessed 10 March 2024. https://www.proquest.com

Bakarich, K. M. & Baranek, D. 2020. Something Phish-y is Going On Here: A Teaching Case on Business Email Compromise. Current Issues in Auditing, 14(1), A1-A9. Article from EBSCOHost. Accessed 7 March 2024. https://search.ebscohost.com

Bezovski, Z. & Poorani, S. 2016. The evolution of e-learning and new trends. Information and Knowledge Management, 6(3), 50-57. Article from Google Scholar. Accessed 10 March 2024. https://eprints.ugd.edu.mk/15692/1/The%20Evolution%20of%20E-Learning%20and%20New%20Trends.pdf

Boland, R. J., Lester, N. A. & Williams, E. 2010. Writing Multiple-Choice Questions. Academic Psychiatry, 34, 310-316. Article from ProQuest. Accessed 20 March 2024. https://www.proquest.com

Breda, F., Barbosa, H., Silva Morais, T. 2017. Social Engineering and Cyber Security: proceedings of International Technology, Education and Development Conference. Accessed 30 March 2024. https://www.researchgate.net/publication/315351300_SOCIAL_ENGINEERING_AND_CYBER_SECURITY

Cross, C. & Gillett, R. 2020. Exploiting trust for financial gain: An overview of business email compromise (BEC) fraud. Journal of Financial Crime, 27(3), 871-884. Article from ProQuest. Accessed 7 March 2024. https://www.proquest.com/index

Cybersecurity & Infrastructure Security Agency. 2020. Ransomware guide. Accessed 9 March 2024. https://www.cisa.gov/resources-tools/resources/cisa-multi-state-information-sharing-and-analysis-center-ms-isac-joint-ransomware-guide

Desolda, G., Ferro, L., Marrella, A., Catarci, T. & Costabile, M. F. 2021. Human Factors in Phishing Attacks: A Systematic Literature Review. ACM Computing Surveys, 54(8), 1-35. Article from EBSCOHost. Accessed 6 March 2024. https://search.ebscohost.com

Fortin, J. 2019. He Tried To Bilk Google and Facebook Out of $100 Million With Fake Invoices. New York Times. Accessed 6 March 2024. https://www.nytimes.com/2019/03/25/business/facebook-google-wire-fraud.html

Fortinet. 2024. What Is A Pretexting?. Accessed 9 March 2024. https://www.fortinet.com/resources/cyberglossary/pretexting

FOX 9 Minneapolis-St. Paul. 2016. 'CEO Spoofing' costs drug company $50 million. FOX 9 Minneapolis-St. Paul. Accessed 6 March 2024. https://www.fox9.com/news/ceo-spoofing-costs-drug-company-50-million

Gagné, R. M., Briggs, L. J. & Wagner, W. W. 1992. Principles of Instructional Design. 4th Edition. New York: Holt, Rinehart & Winston.

Glancy, F., Biros D. P., Liang, N., Luse, A. 2020. Classification of malicious insiders and the association of the forms of attacks. Journal of Criminal Psychology, 10(3), 233-247. Article from ProQuest. https://www.proquest.com/index

Google. 2024. Create a strong password & more secure account. Accessed 9 March 2024. https://support.google.com/accounts/answer/32040?hl=en#zippy=%2Cmake-your-password-longer-more-memorable%2Cavoid-personal-info-common-words%2Chide-written-passwords%2Cmanage-your-passwords-with-a-tool%2Cmake-your-password-unique

Hadnagy, C. 2010. Social Engineering: The Art of Human Hacking. Hoboken: John Wiley & Sons

HYPR. 2024. Five Facts to Know About History's Most Destructive Cyberattack. Accessed 9 March 2024. https://www.hypr.com/security-encyclopedia/notpetya

Iacono, S., Vallarino, M. & Vercelli, G. V. 2020. Gamification in Corporate Training to Enhance Engagement: An Approach. International Journal of Emerging Technologies in Learning (iJET), 15(17), 69-84. Article from ProQuest. Accessed 10 March 2024. https://www.proquest.com

IBM Corporation. 2023. Cost of a Data Breach Report 2023. Accessed 4 March 2024. https://www.ibm.com/reports/data-breach

Jaeger, D., Graupner, H., Cheng, F. & Meinel, C. 2016. Analysis of Publicly Leaked Credentials and the Long Story of Password (Re-)use: proceedings of the 11th International Conference on Passwords (PASSWORDS'16). Accessed 8 March 2024. https://www.researchgate.net/publication/327623664_Analysis_of_Publicly_Leaked_Credentials_and_the_Long_Story_of_Password_Re-use

Kaspersky. 2024. Kaspersky IT Encyclopedia. Accessed 4 March 2024. https://encyclopedia.kaspersky.com/

Kolb, D. A. & Kolb, A. Y. 2013. The Kolb Learning Style Inventory 4.0: Guide to Theory, Psychometrics, Research & Applications. Kaunakakai: Experience Based Learning Systems.

Kolb, D. A. 1984. Experiential Learning: Experience As The Source Of Learning And Development. Englewood Cliffs: Prentice-Hall.

Krombholz, K., Hobel, H., Huber, M. & Weippl, E. 2015. Advanced Social Engineering Attacks. Journal of Information Security and Applications, 22, 113-122. Article from Google Scholar. Accessed 4 March 2024.

https://www.academia.edu/download/44296089/Advanced_social_engineering_attacks20160401-20471-12e5dbw.pdf

Liang, N. (P.), Biros, D. P., Luse, A. 2016. An Empirical Validation of Malicious Insider Characteristics. Journal of Management Information Systems, 33(2), 361-392. Article from EBSCOHost. Accessed 9 March 2024. https://search.ebscohost.com

Lister, M. 2014. Trends in the Design of E-Learning and Online Learning. MERLOT Journal of Online Learning and Teaching, 10(4), 671-680. Article from ProQuest. Accessed 10 March 2024. https://www.proquest.com

Mackay, J. 2024. Protecting Against Physical Security Threats. MetaCompliance. Accessed 9 March 2024. https://www.metacompliance.com/blog/cyber-security-awareness/physical-security

Malone, T. W. 1981. Toward a Theory of Intrinsically Motivating Instruction. Cognitive Science, 4, 333-369. Article from Google Scholar. Accessed 13 March 2024. https://onlinelibrary.wiley.com/doi/pdfdirect/10.1207/s15516709cog0504_2

Malwarebytes. 2024. WannaCry. Accessed 9 March 2024. https://www.malwarebytes.com/wannacry

Mayer, R. 2005. Cognitive theory of multimedia learning. The Cambridge handbook of multimedia learning, 41, 31-48. Article from APA PsycNet. Accessed 13 March 2024. https://psycnet.apa.org/record/2006-00633-003

Microsoft. 2024. Create and use strong passwords. Accessed 9 March 2024. https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb

Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S. & Porras, J. 2023. Mitigation strategies against the phishing attacks: A systematic literature review. Computers & Security, 132. Article from ScienceDirect. Accessed 7 March 2024. https://www.sciencedirect.com/science/article/pii/S0167404823002973

O'Donnell, B. 2023. Three of the world's most expensive phishing attacks… and how they could have been prevented. Betanews. Accessed 7 March 2024. https://betanews.com/2023/06/29/worlds-most-expensive-phishing-attacks-2/

Okta. 2022. Tactics to Avoid Password Leaks. Accessed 8 March 2024. https://www.okta.com/identity-101/password-leak/

Piontek, M. E. 2008. Best practices for designing and grading exams. Occasional Paper, 24, 1-12. Article from Google Scholar. Accessed 20 March 2024. https://crlt.umich.edu/sites/default/files/resource_files/CRLT_no24.pdf

Razaulla, S., Fachkha, C., Markarian, C., Gawanmeh, A., Mansoor, W., Fung, B. C & Assi, C. 2023. The age of ransomware: A survey on the evolution, taxonomy and research directions. IEEE Access. Accessed 9 March 2024. https://ieeexplore.ieee.org/iel7/6287639/6514899/10105244.pdf

Rock, T. 2022. 75% of data loss is from human error. Here's how to deal with it. InvenioIT. Accessed 30 March 2024. https://invenioit.com/continuity/data-loss-from-human-error/

Salahdine, F. & Kaabouch, N. 2019. Social Engineering Attacks: A Survey. Future Internet, 11(4), 89. Article from Google Scholar. Accessed 4 March 2024. https://www.mdpi.com/1999-5903/11/4/89

Savage, C., Blinder, A. 2018. Reality Winner, N.S.A. Contractor Accused in Leak, Pleads Guilty. New York Times. Accessed 29 March 2024. https://www.nytimes.com/2018/06/26/us/reality-winner-nsa-leak-guilty-plea.html

Shah, S., Shah, B., Amin, A., Al-Obeidat, F., Chow, F., Moreira, F. J. L. & Anwar, S. 2019. Compromised user credentials detection in a digital enterprise using behavioral analytics. Generation Computer Systems, 93, 407-417. Article from Google Scholar. Accessed 8 March 2024. https://zuscholars.zu.ac.ae/cgi/viewcontent.cgi?article=2004&context=works

Sophos. 2021. Ransomware: don't expect a full recovery, however much you pay. Accessed 9 March 2024. https://news.sophos.com/en-us/2021/04/27/ransomware-dont-expect-a-full-recovery/

Stojnic, T., Vatsalan, D. & Arachchilage, N. A. G. 2021. Phishing email strategies: Understanding cybercriminals' strategies of crafting phishing emails. Security and Privacy, 4(5). Article from Wiley Online Library. Accessed 6 March 2024. https://onlinelibrary.wiley.com

Sullivan, E. 2024. Data loss. Techtarget. Accessed 9 March 2024. https://www.techtarget.com/searchdatabackup/definition/Data-loss

Surip, N., Som, Z. M., Palanisamy, M. B. & Mohamad, M. 2021. Ideas for Designing Better Quizzes: A Literature Review and Suggestions. International Journal of Academic Research in Progressive Education and Development, 10(8), 190-201. Article from Google Scholar. Accessed 20 March 2024. https://www.academia.edu/download/95515608/ideas-for-designing-better-quizzes-a-literature-review-and-suggestion.pdf

Tally, G., Roshan, T. & Van Vleck, T. 2004. Anti-phishing: Best practices for institutions and consumers. Accessed 7 March 2024. https://docs.apwg.org/sponsors_technical_papers/Anti-Phishing_Best_Practices_for_Institutions_Consumer0904.pdf

Tirziu, A.-M. & Vrabie, C. 2015. Education 2.0: E-Learning Methods. Procedia - Social and Behavioral Sciences, 186, 376-380. Article from ScienceDirect. Accessed 10 March 2024. https://www.sciencedirect.com/science/article/pii/S1877042815024738/pdf?md5=6eaa753dfbe849c51bcace574c418683&pid=1-s2.0-S1877042815024738-main.pdf&_valck=1

Van Steen, T. & Deeleman, J. R. A. 2021. Successful Gamification of Cybersecurity Training. Cyberpsychology, Behavior and Social Networking, 24(9), 593-598. Article from Google Scholar. Accessed 10 March 2024. https://scholarlypublications.universiteitleiden.nl/access/item%3A3247541/download

Verizon. 2023. 2023 Data Breach Investigations Report. Accessed 4 March 2024. https://www.verizon.com/business/resources/reports/dbir/

Vítková, K. H. & Pošmura, L. 2023. Policisté představili technologickou novinku. I s heslem ke služebnímu počítači. iDnes. Accessed 8 March 2024. https://www.idnes.cz/hradec-kralove/zpravy/policie-heslo-notebook-merici-tyce-gps.A230831_144200_hradec-zpravy_kvi

Wang, Y.-F., Hsu, Y.-F. & Fang, K. 2022. The key elements of gamification in corporate training – The Delphi method. Entertainment Computing, 40. Article from ScienceDirect. Accessed 10 March 2024. https://www.sciencedirect.com/science/article/pii/S1875952121000604

Figures

Appendices

Appendix 1: Survey questions

- Section 1: Demographical information
    - How old are you?
        - 18-24
        - 25-34
        - 45-54
        - 55+
    - What is your primary occupation right now?
        - Full-time student
        - Office work (incl. government officials)
        - Other than office work
        - Unemployed
    - Gender
        - Male
        - Female
        - Non-binary
        - Other (open question)
- Section 2: Cyber security awareness
    - Have you heard of these cyber security threats?
        - List of threats: Social engineering, Phishing, Business email compromise, Stolen/compromised credentials, Malicious insider, Accidental data loss, Physical security compromise, Ransomware, Destructive attacks, Pretexting
        - List of options: No idea; I have heard the term, but I’m not sure what exactly it is; I have heard of it and have a good idea what it is; I know what it is and have encountered such a threat myself
    - Do you have any specific examples of a cyber security attack that ever targeted you? (Open question)
- Section 3: Situational examples
    - If you receive an email claiming to be your boss or the CEO of your company (or another person in a position of authority for yourself) and asking you to perform an action, what would you check to see the validity of the email and what would raise some red flags? (Open question)
    - If you were asked to pay money to attackers to unlock your computer which was attacked by malicious software, how would you resolve the situation? (Open question)
    - If you found out the credentials for one of your platforms were leaked, how would you resolve the situation? (Open question)

Appendix 2: Quiz questions

A message that appeals to your urgency or threatens with consequences under false pretenses is called:

a) A phishing email
b) Ransomware
c) Malware
d) Shoulder surfing

Correct answer: A (No other answer fits the description)

Through social engineering generally, what is the attacker trying to do?

a) Use viruses to gain access to the victim's machine.
b) Gain access to their target through an authenticated person.
c) Steal the victim's machine.
d) Use stolen credentials to log into the victim's machine.

Correct answer: B (A is not a standard approach for social engineering, C and D could technically be a part of some social engineering scenarios, but they do not describe the concept of social engineering itself)

Which one of these is a good practice when setting a password in order to remember it easier?

a) Using one from other platforms so that you need to remember fewer of them.
b) Using a name of a close person, pet or city important to you.
c) Using a phrase and modifying it by adding some characters or numbers.
d) Not using more than 8 characters so that it's not overly long.

Correct answer: C (A phrase from a book or one that you remember easily is a good start, then including some special characters, numbers and capitalizing some letters can make this a good password. Others are not recommended to do as they are then much easier to guess.)

What do we mean by pretexting?

a) A cyber security attack with a political motivation (subtext).
b) Messaging multiple users before an attack to see who's most susceptible.
c) Emailing a user just before an attack to give them a warning and ask for money.
d) Creating a fake scenario e.g. in a phishing email to increase trustworthiness.

Correct answer: D (None of the others are applicable)

What is a malicious insider?

a) Somebody who gets into the company premises by e.g. tailgating and then uses this as a way to cause harm.
b) Somebody with legitimate access (e.g. an employee) who wants to harm the company or steal data.
c) Somebody who has long-term access to the company's systems that they gained through a virus.
d) Somebody who gets their information through asking malicious questions to a person who works at the company under false pretenses.

Correct answer: B (None of the others are applicable)

If you lose your office access card, what should you do?

a) Contact the relevant department immediately (to be adjusted to company context).
b) Try copying one of your colleagues' cards.
c) Wait and see if you can find it somewhere.
d) Share one with your colleagues for the meantime.

Correct answer: A (All the others increase the risk of somebody finding it and using it)

If a person that doesn't seem familiar to you starts chatting with you near the entrance to the office and then walks with you, what should you do?

a) Clearly, they are new to the company – you should let them in.
b) You should tell them to stop bothering you – you have no idea who they are.
c) You should ask them to identify themselves somehow if they are to walk in with you.
d) You should scream for help – you are clearly being attacked.

Correct answer: C (The others either enable a possible attacker into the office or they are actually exaggerated and could result in an awkward situation if they are in fact just a new employee.)

If you receive an email claiming to have an important document attached to it, what should you do?

a) Open it but be cautious in case it looks strange – if it doesn't look right, just close it.
b) Delete it immediately in case it's a virus.
c) Report a possible phishing attack and let the responsible team have a look.
d) Open it and follow the instructions.

Correct answer: C (A and D put you at the risk of an infection, while B doesn't give the responsible team a chance to analyze the possible attack.)

Why is paying the money asked by a ransomware on your own a bad idea?

a) There is no guarantee you will get your data back.
b) Using cryptocurrency is always dangerous.
c) It should be paid, but by the accounting team for tax reasons.
d) These payments are usually difficult to do – you should have some help.

Correct answer: A (The rest is not true)

What should you do if a destructive virus damages some of your files?

a) Try working without them – if you can, no need to do anything.
b) Immediately reset your computer just in case.
c) Report this to the responsible team.
d) Take some overtime to recreate the deleted files.

Correct answer: C (This should always be reported – without reporting, there can be remainders of the virus still in the computer and damage the computer further, plus it takes away the change to investigate this issue)