LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Perceived versus Actual Phishing Detection

An analysis between IT and Non-IT Students

Kandidatuppsats 15 hp, kurs SYSK16 i Informationssystem

Författare: Isac Palenryd
Johannes Palm
Jonathan Claesson

Handledare: Umberto Fiaccadori

Rättande lärare: Nam Aghaee
Markus Lahtinen

Perceived versus Actual Phishing Detection: An analysis between IT and Non-IT Students

FÖRFATTARE: Isac Palenryd, Johannes Palm och Jonathan Claesson

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Osama Mansour, Docent

FRAMLAGD: Maj, 2026

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 53

NYCKELORD: Email-phishing, Phishing susceptibility, University students, User behavior

SAMMANFATTNING:

This study investigates the relationship between students' perceived confidence in handling phishing emails and their responses to simulated phishing attempts, with a particular focus on differences between IT and non-IT students. Using a primarily quantitative survey consisting of seven simulated email scenarios, the study examines how students distinguish between legitimate and potentially malicious emails.

The findings indicate that participants generally adopted cautious behavior, often choosing to ignore or report suspicious messages. However, unsafe behaviors remained present across all groups. A notable finding was the mismatch between confidence and decision accuracy, as several participants expressed high certainty in decisions that were objectively unsafe, suggesting the presence of overconfidence bias. The results also revealed only limited differences between IT and non-IT students, indicating that technical background alone does not eliminate phishing susceptibility. In addition, situational factors such as perceived urgency and personal relevance were found to influence participant behavior.

The study concludes that phishing susceptibility is shaped by a combination of psychological, behavioral, and contextual factors, highlighting the importance of cybersecurity education that addresses both technical awareness and human decision-making.

Content

Figures

Tables

1 Introduction

1.1 Background

The increasing reliance on digital technologies has transformed how individuals communicate, study and access information. At the same time, this development has led to a significant increase in cyber threats, both in frequency and sophistication, as malicious actors continuously adapt their methods to exploit new technological opportunities (Rohan et al., 2021). Among these threats, attacks targeting individual users have become particularly prominent, highlighting the importance of understanding human behavior in cybersecurity contexts.

A substantial proportion of cyber incidents can be attributed to the human factor. Individuals are often described as the weakest link in cybersecurity, as their actions may unintentionally compromise otherwise secure systems. For example, users may fail to recognize malicious messages, reuse passwords or handle sensitive information in insecure ways, thereby enabling attackers to gain unauthorized access (Rohan et al., 2021; Mwangala et al., 2023). Furthermore, it has been suggested that a large majority of cyberattacks involve some form of human error, emphasizing the importance of user awareness and behavior (Tech Accord, 2021).

One of the most common methods used to exploit human vulnerabilities is phishing, a form of social engineering where attackers attempt to deceive individuals into revealing sensitive information or interacting with malicious content. These attacks are typically carried out through emails or messages that appear legitimate, often creating a sense of urgency or trust to manipulate the recipient (Workman, 2007; NCSC, 2018). Despite increased awareness and technological safeguards, phishing remains highly effective largely because it targets human behavior rather than technical weaknesses in systems.

At the same time, individuals often perceive themselves as capable of identifying and avoiding such threats. However, research indicates that individuals may lack sufficient awareness of risks and may behave in ways that increase their vulnerability, particularly when interacting with unfamiliar or complex digital environments (Corradini, 2020). This suggests a potential mismatch between individuals' perceived cybersecurity competence and their actual ability to detect phishing attempts, raising concerns about overconfidence in digital environments.

Within this context, students, and particularly those studying information technology, represent an interesting group to study. IT students are expected to possess higher levels of technical knowledge and awareness compared to other individuals, yet it remains unclear whether this translates into a greater ability to identify phishing attacks in practice, or merely increases confidence without improving actual performance. This creates a practical problem, as users may believe they are capable of identifying phishing attempts while still engaging in unsafe behaviour. As a result, traditional approaches to improving cybersecurity awareness

may be insufficient, particularly in environments where attacks are becoming increasingly sophisticated.

Therefore, this study aims to investigate how aware IT students are of email phishing and to examine whether their perceived cybersecurity competence corresponds to their actual ability to identify phishing attempts, particularly in a context where increasingly sophisticated, AI-generated attacks challenge traditional detection strategies.

1.2 Research Question

The research question is:

To what extent does perceived cybersecurity competence correspond to actual phishing detection ability among students, and how does this differ between IT and non-IT students?

1.3 Purpose

This study is relevant to the field of informatics as it examines the interplay between humans, technology, and information systems within digital environments. Informatics is concerned, among other aspects, with how users interact with technology and how digital systems shape behavior and decision-making processes. Phishing attacks exploit these human factors within digital communication. Consequently, it is essential to understand how different groups of users perceive and respond to such threats.

The relevance of this problem to informatics lies in the role of technical knowledge and digital competence in shaping users' ability to identify and manage security risks in information systems. By comparing IT students with students without an IT background, this study seeks to contribute to a deeper understanding of how education and technical experience influence cybersecurity-related behavior.

The expected contribution to the field of informatics is an enhanced understanding of how users' technical competence affects their susceptibility to AI-generated phishing attacks. The findings may inform the development of more effective security education, the design of more user-centered security solutions, and the improvement of strategies aimed at mitigating the risks associated with social engineering attacks in digital information systems.

1.4 Delimitations

A clear delimitation of this study is that we have chosen to only look at and compare students. The study could have looked at people with IT knowledge compared to people without any particular in general, but is limited to students. Students represent tomorrow's workforce, and understanding their susceptibility has predictive value for organizational security later. A general population study would also require far greater resources, time and ethical clearance complexity compared to limiting it to students. Thus this limitation is more realistic for a bachelor's thesis.

1.5 Terminology

Phishing

Phishing is a common cybersecurity threat that is characterized by deceiving individuals into revealing sensitive information or private credentials through fraudulent emails, websites or messages. The people behind phishing attacks often pretend to be trusted companies as a methodology for stealing data and information, and modern phishing often uses social engineering tactics to bypass security systems and exploit human trust. Phishing is one of the most persistent cyber threats in the digital age (Shahbazi, Jalali & Molaeevand, 2025).

Spear Phishing

Spear phishing differentiates from normal phishing in the way that it is a highly personalized version of phishing. It is aimed at specific individuals or organizations, and involves carefully crafted emails and other personalized tricks that have the intent to make the message more genuine and believable. Because these attacks are so specific and appear more authentic, they are significantly harder to detect and there is a higher risk they slip past normal security systems (Shahbazi, Jalali & Molaeevand, 2025).

Social Engineering

Social Engineering attacks use a range of techniques to manipulate an individual into providing attackers with unauthorized access to systems or data. Social engineering emphasizes the human elements of the digital ecosystem rather than the technical ones. Social engineering can often involve psychological manipulation. Phishing is a core technique in social engineering and a primary method in attacks (Thomson et al., 2025).

STEM-Students

Stands for students pursuing studies in Science, Technology, Engineering and/or Mathematics.

2 Literature Review

2.1 Characteristics of Phishing Emails and Attacks

The most common in phishing emails is the attacker crafting the email to look as though it comes from a trusted source, mimicking everything from that company. Trusted sources such as banks and known service providers are often chosen. The emails rely on cues to trick the recipient into acting quickly without thinking twice. A lot of emphasis is placed on urgency and importance, and things like urgent invoices, verifying your account and changing your password because it has expired are used, since it grabs people's immediate attention. When people's attention is won, phishing emails often include immediate call to action, for example buttons or links to trick the recipient to fix the issue, but instead direct them towards a malicious link or attachment. The terms "Click here" and "Verify now" are found to be some of the most influential in this context. This flow of a phishing attack can be described as the hook, the redirection and finally the theft (Tallapally et al., 2025).

Cybercriminals are now using Artificial Intelligence (AI) to a great extent to enhance the emails and the attacks. AI-generated phishing content can closely mimic human-authored messages and can increase the personalization of the emails, making detection even harder (Shahbazi, Jalali & Molaeevand, 2025). The rapid development of artificial intelligence (AI) has therefore further increased the complexity of phishing attacks. In addition, techniques such as deepfakes can be used to imitate trusted individuals, making it increasingly difficult for users to distinguish between authentic and malicious content (Barney, 2023; Alotaibi et al., 2024). As a result, traditional indicators of phishing, such as poor grammar or suspicious formatting, are becoming less reliable, further increasing the challenge for users to accurately identify malicious communication.

2.2 Theoretical Framework

2.2.1 Protection Motivation Theory and Technology Threat Avoidance Theory

2.2.1.1 Protection Motivation Theory (PMT)

PMT was originally proposed by Roland W. Rogers and is a widely used framework for understanding the cognitive processes people go through when facing a threat. The theory originated in health and safety research, but has been adopted to cybersecurity to explain why or why not users adopt protective behaviours. The theory posits that threats are evaluated through a threat appraisal process and a coping appraisal process. These appraisal processes are the same as in the Technology Threat Avoidance Theory, with the difference that PMT also considers the intrinsic or extrinsic rewards gained from continuing dangerous behaviour during the threat appraisal. These assessments then lead to a coping strategy, which is either called adaptive or maladaptive coping. Adaptive behaviours are the recommended responses

to counter the threat, and maladaptive behaviours happen when a person chooses to avoid the recommended response (Jamil et al., 2024).

In the context of this study, PMT is useful for understanding how students evaluate phishing emails as potential threats and how this evaluation influences their decision to act safely (e.g., avoiding interaction) or unsafely (e.g., clicking links).

It is stated that PMT in cybersecurity research has yielded inconsistent and contradictory results. An explanation could be that the theory was originally designed for health contexts, where threats more often are directly related to a person's physical well-being. In comparison, threats in cybersecurity often target files or assets rather than an individual directly. Another explanation could be that in organizational settings, individuals can feel very little psychological ownership over data they use, which decreases the perceived relevance of the threat (Jamil et al., 2024).

While PMT provides a useful foundation for understanding how individuals cognitively evaluate threats, its limitations in cybersecurity and phishing contexts suggest that it may not fully capture how users respond to digital threats in practice.

This highlights the need for more context-specific models, such as TTAT, which build on PMT while addressing its limitations in explaining user behaviour in cybersecurity environments.

2.2.1.2 Technology Threat Avoidance Theory (TTAT)

TTAT can be described as an extended version of PMT, and both theories share the same structure. TTAT integrates PMT with other frameworks, for example risk analysis research, in order to investigate factors specifically related to avoiding IT threats. In comparison to PMT which is widely adopted by information security researchers, TTAT may lack some empirical support (Jamil et al., 2024).

TTAT is an indigenous Information Systems theory designed to explain the voluntary threat avoidance behaviour of computer users. The basic premise of TTAT is that users are motivated to avoid malware if they believe it is a genuine threat and that the threat can be avoided by using safeguards. Just like in the PMT, TTAT presumes that when users encounter a potential threat or malware attack, they engage in two dynamic cognitive appraisal processes, before they decide on how to act. The first one is Threat Appraisal. Here users assess the level of danger posed by the malware. This is determined by the perceived susceptibility meaning the probability the threat will occur, as well as the perceived severity, meaning the seriousness of the negative consequences. The second cognitive appraisal process is Coping Appraisal. Here users determine whether the threat can be avoided using available safeguards. This evaluation is based on three different factors: The effectiveness of the safeguard, the cost of implementing it and the user's self-efficacy (Chen & Liang, 2019).

From these appraisals, the user then chooses between two main coping mechanisms. The first is problem-focused coping, that consists of taking concrete and objective actions to change the situation, such as installing antivirus software, updating passwords, backing up files and so on. It is found that a high degree of perceived avoidability increases the likelihood of a user engaging in problem-focused behavior. When a user feels that something constructive can be done, a problem-focused response is more likely. TTAT has been developed to include a second coping-strategy that users adapt. That is emotion-focused coping, and consists of taking subjective measures to manage the emotional distress caused without changing the

objective reality. This coping strategy functions as a defense mechanism used by people to protect their feelings of safety. It is usually used when a person doubts their own competence to maintain personal safety, which causes emotional imbalance. Unlike other strategies, this is considered a passive strategy and more likely to be used when a person sees a situation as difficult to change or control. Forms of coping include distancing (forgetting the threat), denial, acceptance, self-blame and wishful thinking. Wishful thinking is classed as a desirability bias. The user fantasises that the threat will go away, leading to inflated optimism about the outcome no matter the objective evidence. A critical finding is that these types of emotion-centered coping strategies can weaken a user's motivation to take actual safeguard measures. Users who are emotionally eased by their own fantasies may feel less urgency to employ actual security tools, even if they have the knowledge of those tools' effectiveness (Chen & Liang, 2019).

This is particularly relevant in phishing contexts, where users who rationalize away threat cues through wishful thinking may be precisely those most at risk. Then they are not at risk from lack of knowledge, but from emotionally motivated avoidance.

It should be noted that the two different coping strategies can very much coexist in a person's response, and they function in 98% of stressful encounters. (Chen & Liang, 2019).

2.2.2 Overconfidence Bias

Overconfidence is a particularly dangerous vulnerability in phishing detection because it creates a false sense of security that discourages careful inspection. It occurs when a person's confidence in their judgments exceeds their actual accuracy. Confidence can be divided into two different types. Retrospective confidence is the degree to which an individual believes a judgment they made is accurate and prospective confidence (self-efficacy), is an individual's belief in their ability to perform a task beforehand. Important to notice is that merely having high confidence is not the same thing as being overconfident. This means that a person with generally low confidence can still be overconfident, as long as the actual accuracy is lower than the confidence level. When examining overconfidence in email phishing detection, it is stated that overconfidence can be measured using two metrics, since overconfidence is operationalized using these: Overprecision and overestimation. The first one means that there is a difference between the average subjective probability assigned to judgments and the actual proportion of correct answers. The second stands for the difference between a person's self-estimated frequency of correct answers and their actual performance (Wang, Li & Rao, 2016).

Several factors shape how overconfidence develops in email contexts, either for the better or worse. The only identified factor that reliably reduces overconfidence is spending more time and effort analyzing an email. The factors that increase overconfidence are a few more. Familiarity with a sender's brand, such as recognizing a bank's name, inflates confidence without improving detection, making it one of the strongest drivers of overconfidence. Heuristic shortcuts and a general expectation of positive outcomes have a similar effect, boosting perceived accuracy while leaving actual performance unchanged (Wang, Li & Rao, 2016).

Generally, overconfidence in the form of overprecision was prevalent in a big majority of participants. Overconfidence also appears to scale with difficulty. The more difficult the email was to detect, the more overconfident the participants felt, suggesting that the most dangerous

phishing attempts are also those most likely to go unrecognized by the victim (Wang, Li & Rao, 2016). This pattern is especially clear among younger users, who often provided incorrect responses while still maintaining high levels of confidence, leaving them unaware of having been deceived (Das, Nippert-Eng & Camp, 2022). Together, these findings conclude that a person's confidence belief is a very poor indicator of the actual prediction accuracy, and relying on one's own confidence is an unreliable strategy for detecting phishing (Wang, Li & Rao, 2016).

2.2.3 Signal Detection Theory (SDT)

SDT offers a quantitative lens through which phishing behaviour can be analyzed. SDT complements PMT and TTAT by providing a framework for evaluating the accuracy of users' decisions, rather than only explaining the cognitive processes behind them. SDT fills in the gap by evaluating whether users are actually distinguishing threats from non-threats, or merely acting on biased expectations (Martin, Dubé & Coovert, 2018).

SDT is a statistical and cognitive framework that is used to model decision-making when there is uncertainty and risk present in the picture. SDT is used to model and understand how individuals distinguish between signals and noise. In the context of phishing emails, signal distribution represents threatening emails, and noise distribution represents normal emails. The criterion is where an individual sets a threshold for action. If the signal strength is perceived as exceeding the threshold, the individual responds safely, for example by deleting the email. If the perceived signal is below the criterion, the response is unsafe, for example clicking on a link or downloading an attachment (Martin, Dubé & Coovert, 2018).

A big advantage of SDT over other metrics is the theory's ability to unravel two factors that are distinct. That is sensitivity and response bias. Sensitivity is a person's ability to detect a threat, and this is represented as the distance between the means of the signal and noise distributions. Response bias is the observer's expectation of risk, or their tendency to favor one response over the other. Are they being over-cautious, or taking many risks? The response bias is determined by the placement of the decision criterion. Based on what the response is, the theory categorizes the responses into four types:

A hit is correctly identifying a threat, which leads to responding safely to the signal. A miss is failing to identify a threat, leading to an unsafe response to the signal. A false alarm is when a person mistakenly identifies a safe email as a threat, leading to unnecessary safe behaviour such as deleting normal emails or not clicking on valid links. Lastly there is a correct rejection where a safe email is identified as safe. This leads to interacting with the email, which is totally appropriate behaviour (Martin, Dubé & Coovert, 2018).

2.2.4 Summary of Theories

In the context of this study, these theories are used to examine both how students perceive phishing threats and how they actually respond to them, allowing for a comparison between perceived ability and real behaviour. Together they provide a comprehensive framework for understanding phishing behaviour from multiple perspectives. PMT and TTAT explain how individuals cognitively evaluate and respond to perceived threats, while overconfidence bias highlights the potential mismatch between perceived competence and actual performance.

Signal Detection Theory complements these frameworks by enabling the analysis of how accurately individuals distinguish between phishing and legitimate emails.

2.3 Phishing Susceptibility and Detection

2.3.1 Phishing Susceptibility in General

Research on demographic factors suggests that susceptibility to phishing is not simply determined by familiarity with technology. For instance, a 2020 high school study found that older participants (35–54) were less susceptible to spear phishing and more accurate at identifying threats than younger users, challenging the digital native theory that assumes younger generations are more competent online due to lifelong exposure of technology (Das, Nippert-Eng & Camp, 2022). Gender differences have been observed, with women generally showing lower overconfidence and greater ability to detect malicious emails compared to men (Wang, Li & Rao, 2016).

2.3.2 Phishing Susceptibility Among Students

Phishing susceptibility is something that is affected by a variety of factors, such as age, culture and education, as is shown in Diaz, Sherman and Joshi (2020) and Butavicius *et al*. (2017). Which discuss an individual's susceptibility to phishing with universities and based on cultural factors respectively. For this thesis the results and subjects discussed within Diaz, Sherman and Joshi (2020) will weigh heavier due to its closer relevance to the topic of the thesis.

Education is an extremely important factor in mitigating the phishing susceptibility of an individual. Students in STEM fields have shown a lower rate of clicking on phishing links than in non-STEM fields by fifteen percentage points (Diaz, Sherman & Joshi, 2020). And within the same study it was also noted that STEM students also clicked less the further into their education they were. Furthermore students with relevant scholarships, or members of relevant clubs were even less likely to click on the phishing links than those who had neither scholarship, nor were members of such clubs (Diaz, Sherman & Joshi, 2020). Along with this Butavicius *et al.* (2017) also shows ISA, or Information Security Awareness, was one of the stronger variables in affecting how well an individual detected phishing attempts. It has however in a different study been shown that a student's level of education did not impact their likelihood of clicking a malicious link. Neither did having prior knowledge about what phishing is necessarily make someone better at avoiding it. What could be seen as having an impact was if an individual generally had higher technology competencies, and engaged in more leisure-related activities online (Ribeiro, Guedes & Cardoso, 2023). What also does matter, not completely unexpected, is exposure to cybersecurity education in the form of formal university courses and specific training programs, that positively affects a student's ability to identify phishing correctly, which is true regardless of what major a student pursues. A pattern is shown that younger students who are digitally active, but not formally trained against phishing often demonstrate clear overconfidence, increasing their susceptibility to social engineering (Shahbazi, Jalali & Molaeevand, 2025).

For the cultural side, Butavicius *et al*. (2017) shows that the most important part in someone's national culture when it comes to how susceptible they are to phishing attempts was individualism. Which they believe is due to people of cultures with low individualism generally wanting to help others and are more inclined towards doing what others requested, even if it is malicious in nature. While those with higher individualism were less likely to act upon these malicious requests.

3 Research Methodology

3.1 Literature Review Method

When searching for literature for the thesis the main search engines that have been used were Google Scholar and Lund University's search service Finn. Google scholar was selected as it is an easily accessible search engine for scholarly papers, along with having a vast number of such papers. Though, as stated in Kolata (2017), Google Scholar has been known to not vet the articles that it indexes, meaning that it can lead to articles with faulty information ending up within it. Finn was used in addition to Google Scholar as it provides access to Lund University's library databases and academic resources, allowing for more targeted searches and access to peer-reviewed research

To ensure the reliability and relevance of the selected literature, articles were evaluated based on both their relevance to the research topic and the credibility of the journals in which they were published in. The Norwegian Register of Scientific Journals was utilized to see if the journal that the article is from was peer reviewed. An article not being peer reviewed does not mean that the article is completely untrustworthy, but generally a peer reviewed article is a more reliable source of information rather than one that is not.

Literature searches were conducted using keywords related to phishing and user behavior, including terms such as "email phishing", "phishing susceptibility", "phishing detection", and "students phishing". Priority was given to studies relevant to phishing behavior among students, as those were the target group of this research.

3.2 Research Approach

Quantitative data refers to data expressed in numerical form and is the primary type of data generated through surveys. This aligns with the majority of the data collected in this study, meaning that the study predominantly adopts a quantitative approach, with most of the questions being closed. However, qualitative elements are also present. Qualitative data includes all data that is non-numeric, such as text-based responses (Oates, Griffiths &

McLean, 2022). As further explained in section 3.3, the survey includes open questions that allow participants to elaborate on their reasoning. The research approach can therefore be described as primarily quantitative, with qualitative elements. While quantitative data is used to identify patterns in behaviour, qualitative responses provide deeper insight into why participants acted as they did. The qualitative components aim to provide context and explanation for the quantitative findings.

This approach is particularly suitable for this study, as it enables the measurement of both perceived cybersecurity competence and actual behaviour in response to phishing scenarios. By collecting standardized responses, it becomes possible to compare participants' self-assessed ability with their actual performance, which is central to the research objective.

The study uses a survey approach, where data is collected through a structured questionnaire. The questionnaire serves as the data collection instrument and consists of standardized questions presented to all participants, allowing for consistent measurement and comparability across responses. As the questionnaire is distributed via email, it is self-administered, meaning that no researcher is present when participants respond.

A survey using a questionnaire was selected as the most appropriate method, as it enables the collection of data from a larger number of participants within a limited timeframe. This is particularly relevant for this study, which aims to compare responses across groups (IT and non-IT students). Surveys are also well suited for identifying patterns and differences in behaviour across a broader population.

Alternative methods, such as interviews or qualitative approaches, were considered less suitable, as they focus on in-depth understanding rather than measurable behavioural differences. Since this study aims to compare perceived competence with actual performance across groups, a structured survey design is more appropriate. While interviews could have provided deeper insights into individual reasoning, they would not allow for the same level of comparability or generalizability across participants.

While the concepts of exploratory, descriptive, and explanatory studies are illustrated through case studies in literature (Oates, Griffiths & McLean, 2022), they refer to the purpose of a study rather than the method itself. Despite employing a survey approach, this study can be described as partly explanatory, as it seeks to explain students' behaviour in relation to phishing, and partly descriptive, as it measures how students act, what they perceive, and how they assess their own ability.

3.3 Design of Questionnaire

In the planning phase of this study, the original plan was not to have a questionnaire at all. Instead the plan was to send out "real" phishing emails to students, with the hope of the institution helping us to distribute the emails. The thought was to construct a fake email with a clickable link. Nothing would happen when someone clicks the link, except that we would keep track of how many and what types of students click the link. However after consultation with a supervisor, it was concluded that this would not be possible to implement within the framework of this work, and it was decided that a questionnaire would be a better and easier option to go forward with.

The questionnaire starts with section one, consisting of four demographic questions, asking about age, gender, education and the amount of IT the education contains. These are closed questions, except for one open question where respondents can write freely what they are studying.

After that, respondents can move on to section 2 of the questionnaire. Here respondents will view 7 fabricated e-mails, and have to choose how they would interact with each one. The description at the beginning of section 2 is "*Imagine that you are quickly checking your email between lectures. How would you handle the following messages?*". Each email has a closed question attached, with alternatives on what one would do with the email. The alternatives are tailored to each email, but it can be summarized as the respondent choosing between interacting, ignoring or reporting the mail to your email provider. The emails in the questionnaire are:

- Email from DHL (Legit)
- Email from Netflix (Phishing attempt)
- Email from Swedbank (Phishing attempt)
- Email from Spotify (Phishing attempt)
- Email from Försäkringskassan (Legit)
- Email from CSN (Phishing attempt)
- Email from Postnord (Phishing attempt)

Example of one of the emails, asking to scan a QR-code to update your payment details. The question translates "What would you do with this email if you have an active netflix subscription?":

Figure 1: Netflix phishing email.

Artificial intelligence tools, specifically ChatGPT, were used to assist in the creation of email examples included in this study. The tool was used to generate both phishing-style and legitimate email messages intended for the research material. All generated content was carefully reviewed and adjusted by the researcher to ensure that the emails were realistic, relevant and appropriate for the context of the study.

Each email is followed by a scale question (Oates, Griffiths & Mclean, 2022), asking how sure the respondent is in their decision, enabling the study to look at overconfidence bias.

Then the DHL, Netflix and Swedbank-email also have the follow up question about how urgent the email feels, while Försäkringskasssan and CSN have the follow up question about how important the email feels. Both the urgency and importance questions are scale questions. These questions are included for two reasons. The first reason is that it can be useful to measure if respondents are more likely to interact with a phishing email if they perceive it as more urgent or important, since the nature of phishing attacks often is to stress that something is urgent and needs to be fixed now (Tallapally et al., 2025). The second reason is to not make the respondents completely sure that the survey aims to test phishing susceptibility. By including questions about urgency and importance, respondents may not directly think about phishing but rather email handling in general. Questions like “How likely is this email a phishing attempt?” would immediately raise the suspicion towards the other emails, and increase the risk of the respondent answering like a critical reviewer. Something that is not

desired, as it is wanted that they respond as students going through their inbox. This is also why the title of the questionnaire is "*How students manage everyday digital communication*" and not something in the lines of "How susceptible students are to phishing emails". The word "phishing" is not mentioned at all in the first two sections of the questionnaire. The more prepared the respondents are to review phishing beforehand, the more bias will the answers have.

The DHL, Swedbank and CSN email also have an open follow-up question, where respondents can write freely why they chose the option they did. This is to get an insight into how students resonate, identify possible coping strategies and if patterns are found draw connections to the Technology Threat Avoidance Theory (TTAT).

After section 2, respondents move to a new and final page which is section 3. This section is introduced with a short description of what phishing is. More precise it says:

> *Phishing is a form of online fraud in which attackers impersonate a legitimate entity, often through email or text messages, with the aim of tricking individuals into disclosing sensitive information such as passwords, card details or bank credentials.*

This description is included because even though phishing is a well known concept, it can not be taken for granted that everyone knows its meaning. Since the following questions will be about phishing, it is important that everyone has the same understanding of what the word means.

First out is a Yes/No question if the respondent ever has fallen victim to phishing. Thereafter follows a scale question of how the respondent assesses the risk of becoming a target for phishing attempts themselves. This is followed up by another scale question, asking how serious consequences the respondent thinks a phishing email can result in for them personally. This is interesting to ask since the premise of TTAT is that users are motivated to avoid threats and malware if they believe it is a genuine threat. It is also interesting since the cognitive process called threat appraisal, which is central in TTAT, consists of the user determining the perceived probability and seriousness of the threat (Chen & Liang, 2019). The scale question "How burdensome do you find it to carefully check emails in order to avoid phishing" is justified to include with the same reason. The open question"Do you have any strategies or rules of thumb for avoiding phishing attempts", can be linked to PMT and TTAT, to see how strategies and actual susceptibility are linked together. The last and final question is an open question and asks how the respondent thinks their education has influenced their answers, since the study aims to compare the behavior of IT-students and non-IT students.

To ensure that the questionnaire is of good quality and up to expected standards, several things were thought of when designing it. Each question is kept brief and all questions are kept under 20 words. All questions are relevant to the purpose of the study and to the overall questionnaire. No words with multiple meanings are used, and when words are used that could be unfamiliar to the respondent, such as phishing, the word is explained. The overall language in the questionnaire as well as the questions are unambiguous. No leading questions are included that could direct the respondent towards a specific answer, and the questions are of objective nature (Oates, Griffiths & Mclean, 2022).

3.4 Data Collection

3.4.1 Empirical Data

The method of collecting data was by implementing and distributing the questionnaire using Google Forms, which enabled efficient data collection and automatic recording of responses. The data that we are collecting is a mix of different types of quantitative data. The main data that we are collecting is whether people choose to interact, ignore or report the emails presented. This data is nominal, since it describes categories and has no actual numeric value. Interacting with the mail is not inherently higher or lower than ignoring it. The analysis possible with this data is the frequency, which is what we will be looking at carefully. When the data about how people choose to interact with the emails is translated into what type of behaviour it is, i.e. safe or unsafe behaviour, it is still nominal data (Oates, Griffiths & Mclean, 2022).

We are also collecting ordinal data with the quantitative scales that come as follow up questions after the emails. That is, when we are asking about the perceived importance and urgency of the emails, which is measured with Likert scales when the respondents answer by selecting a number between one and five. There is a clear order with the ordinal data, but it is hard to tell the differences between each answer, for example how much of a difference is there between selecting importance 4 to importance 5 (Oates, Griffiths & Mclean, 2022).

The qualitative data that is collected is strictly textual data, and no type of audio or pictorial data is present (Oates, Griffiths & Mclean, 2022).

3.4.2 Visualization of Data

The responses of the first three demographic questions are compiled in pie charts. It is thought that pie charts can be hard to read, since when segments are close in size it is very difficult if not impossible to tell which one is bigger. They are also criticized for asking the audience to compare angles and areas instead of something simpler than a bar chart. One unique thing a pie chart has however is the concept of there being a whole, and parts of the whole (Knaflic, 2015). To get over the problem of the visual difficulty of pie charts, data labels were added in all the fields showing the percentage, for example how many % of the respondents that were in the ages 18-22 as seen in Figure 2.1. The justification for using pie charts is it is visually fitting to visualize the demographic questions are there being whole, where the respondents are parts of that whole. It can also be argued that it is not of equal importance to visualize the demographic data as carefully as the data about phishing susceptibility, although that can be considered a subjective thought and not a fact.

All the closed questions in section 2 and 3 are visualized using bar charts, more precisely multiple series vertical bar charts. Bar charts with more than one series should be used with caution, since as you add more series of data it becomes more difficult to focus on one at a time. Visual grouping also happens as a result when bar charts have more than one data series. It therefore needs to be clear what you want the audience to be able to compare (Knaflic, 2015). Bar charts of this kind are used in this study because the results when presented are grouped by what people with low, medium and high IT education answered, and therefore every option has three data series in the charts. To make differentiating between the different

perceived educational levels easier, the bars are color coded with low IT education being red, medium being yellow and high IT education being blue.

3.4.3 Participant Selection and Sampling

The target population of this study consists of university students. The final sample consisted of 43 participants who completed the questionnaire, including both IT and non-IT students. Participants were recruited through student networks, social media channels, and participant referrals. The aim was to collect as many responses as possible within the available time frame while ensuring participation from both IT and non-IT students, and no fixed sample size was determined beforehand.

In the decision between comparing students or broadening the study beyond students, the reasoning was that university students form a well-defined accessible population that is easier to recruit systemically. This improves the reliability of our sample compared to a diffuse general population.

Our sampling technique is clearly non-probabilistic, as we cannot determine whether the sample is representative of the overall student population. Participants were recruited through accessible student networks, meaning the sample may not form a representative cross-section of the overall student population. More specifically, the study uses a combination of convenience and purposive sampling, with elements of snowball sampling. Our sampling can be classified as purposive since we in a way deliberately hand-pick the participants. When we are sending out the survey, we will know if we send it out to an IT student or non-IT student in order to make sure we get answers from both groups. We are purposely targeting groups with specific characteristics, and in our case that characteristic is field of study. It would be faulty to claim that that is our only sampling technique, since other sampling techniques are present. One of them is convenience sampling. We are sending the survey out to students that are available to us via our networks. The participants are to a degree included because they are easy for us to reach, and one way of distributing the survey is through our own contacts and social channels. For example, the survey will be sent to friends and acquaintances that are both IT and non-IT students. This very much classifies as convenience sampling. These people are also told that they can forward the survey to people they know, with the requirement of them needing to be students. This is snowball sampling, and is not done because we do not know how to gain access to the target group, but rather as a way to increase the sample size (Oates, Griffiths & Mclean, 2022). The snowball sampling goes against our purposive sampling since it is harder to control what type of student someone forwards the survey to. One way to control it is to have knowledge of who you ask to forward the survey. If we for example ask a student studying law to forward our survey, we can predict that more law students are going to be participating, i.e. non-IT students.

These sampling techniques were chosen for this study because it is a challenge to get access to something that could be interpreted as a representation for the whole student population, for example students representing the different universities across the country. This limited access to the student population, as well as a time constraint, made these sampling techniques a viable option for this study.

The limitations identified as a consequence of our sampling technique are that the sample may not be representative of all students. Since we are convenience sampling, there is a risk for a bias from the sampling being present, since many of the participants will be students with the

same background. First of all it is estimated beforehand that most of the students will come from the university we are attending, Lund University. This means many participants will be a part of the same university culture, and it is hard to predict to what extent that will affect the result. There is also a possible risk that many participants will study the same program. If we take the group of IT-students, we can not guarantee that the majority of IT-programs in Lund University will be represented by the respondents in the study. The reason for this is that snowball sampling can contribute to the study being sent out to the same circle of people, as stated before with the law student example. Furthermore, we ourselves are IT-students, meaning that other students attending the same program as us are easier to reach via social channels. Then there is also the factor of self-selecting which must be considered. We are sending a survey out to selected people, but at the end of the day it is those students that decide themselves if they want to answer or not. The students deciding to answer may or may not be systematically different from those who do not, it will be very difficult to know. The students deciding to answer may for example be more interested in digital communication and cybersecurity, or suspect that it is about phishing making them more eager to answer. Even among the non-IT students, the students deciding to answer may be more tech-interested, which may skew the result.

These factors stated are limiting the generalizability of the results and the study. Despite these limitations, the sampling method allows for meaningful comparisons between subgroups within the sample, such as IT and non-IT students. This means that the findings of the study should be interpreted with caution, particularly when generalizing beyond the sample. However, the sampling approach remains suitable for identifying patterns and differences within the studied groups.

3.5 Data Analysis

The collected data was analyzed using a primarily quantitative approach, supported by qualitative elements. Responses from the closed questions were compiled and analyzed to identify patterns in participants behaviour, perceptions and decision making related to phishing emails. Descriptive statistics, such as frequencies and percentages, were used to summarize the results and compare response patterns between participants with different levels of IT education.

The quantitative analysis focused on how participants interacted with the fabricated emails presented in the questionnaire. Particular attention was given to whether participants chose to interact with, ignore or report phishing emails, as well as their reported confidence levels and perceptions of urgency or importance. Comparisons were also made between participants with different educational backgrounds in order to identify possible differences between IT and non-IT students.

In addition, the results were interpreted using concepts related to Signal Detection Theory (SDT), where responses could be understood in terms of correct identifications and different types of decision errors, such as false alarms and misses. This allowed for a more nuanced interpretation of participants' decision-making under uncertainty.

The open-ended questions included in the questionnaire were analyzed qualitatively through thematic interpretation. Responses were reviewed in order to identify recurring patterns, reasoning strategies and attitudes related to phishing awareness and email handling. These

qualitative responses were primarily used to complement and contextualize the quantitative findings rather than serve as the primary source of analysis.

The results were presented through tables and figures in order to visualize response distributions and facilitate comparisons between different groups and questionnaire items.

3.6 Validity & Reliability

3.6.1 Validity

Validity in research means that an appropriate process has been used for the research, that the findings come from the data collected and that the findings do answer the research question (Oates, Griffiths & Mclean, 2022).

3.6.1.1 Construct Validity

Construct validity concerns whether the questionnaire actually measures the intended concepts (Oates, Griffiths & Mclean, 2022). To support construct validity, the questions were designed using clear and neutral wording in order to reduce ambiguity and misunderstandings. In this study, construct validity is particularly important as the questionnaire aims to measure both participants' ability to identify phishing attempts and their perceived confidence in doing so. The use of realistic email scenarios contributes to capturing behaviour that reflects real-life decision-making. However, the simulated nature of the survey environment may limit the extent to which responses reflect real-world behavior.

3.6.1.2 Content Validity

Content validity concerns whether the questions are a well-balanced sample of the domain to be covered. In this study, content validity was addressed by designing the simulated email scenarios based on common characteristics of phishing attacks identified in existing literature. Elements such as urgency, impersonation, requests for immediate action, and suspicious links were incorporated in order to resemble realistic phishing attempts. Furthermore, the questionnaire measured multiple aspects related to phishing susceptibility, including behavioral responses, perceptions, and participant reasoning. This helped ensure that the questionnaire captured relevant dimensions of the phenomenon under investigation.

3.6.2 Reliability

Reliability regards whether the questionnaire would yield the same result if it were to be given several times to the same respondents, which is very hard to assess since you only view the questionnaire for the first time once (Oates, Griffiths & Mclean, 2022). Reliability was supported by using a standardized questionnaire distributed under the same circumstances to all the respondents. Responses were collected digitally and recorded automatically, reducing the risk of manual errors and inconsistencies in data collection.

There is a conflict between anonymity and the reliability of the data in the way that Google Forms is designed. As will be discussed in 3.7, respondents' E-mail addresses are not collected when they send in their response. This means that the response is submitted completely anonymously, which brings the issue of respondents having the possibility to

submit a response several times to willingly distort the result. Implementing controls to prevent this also comes with its issues. If respondents get a personal password required to open the questionnaire, or as is possible with Google Forms, are required to sign in with their google account to answer, there is risk that they will worry that they aren't anonymous (Oates, Griffiths & Mclean, 2022). In the settings of the questionnaire, the option to limit to one response requires sign in. After long consideration, the decision was made to not require any sign in or other form of authentication. The reasoning behind this was that there should be no form of doubt from the participants about the anonymity, which comes at the expense of the data's reliability. It can however be argued that since we to a high degree utilise convenience sampling, the risk of participants intentionally distorting the results should be lower, since we have some kind of connection to a majority of the participants.

3.7 Ethical Considerations

As a participant in surveys, you have rights that need to be respected just like in society in general (Oates, Griffiths & Mclean, 2022). These rights have been taken into consideration, and measures have been taken to ensure that they are followed.

Firstly, the respondents have the right to not participate (Oates, Griffiths & Mclean, 2022). The researchers are in no position of power over the respondents, and the questionnaire is sent out via email once to possible respondents. After that no further messages are sent and no further pressure is applied to answer. Participation of the survey is very voluntary, and possible respondents can simply ignore the email with no negative consequences. No incentives are offered for completing the questionnaire. Even if you start to answer the questionnaire, it is possible to back out and cancel at any time given, simply by closing the questionnaire tab down in the used browser.

When starting the questionnaire, respondents are met with important information that enables them to give informed consent, which means the respondents' consent to participate is given after being made aware of facts about the study (Oates, Griffiths & Mclean, 2022). They are informed that their responses will be treated confidentially and stored securely. Further it is stated that no information that can identify an individual will be collected or presented in the study's results, as well as that the collected data will only be used for research purposes within the scope of this study and will be analyzed anonymously. It is informed that the study is a part of a bachelor's thesis at Lunds University, that it is estimated to take a maximum of 5 minutes to complete the questionnaire and that it is voluntary to participate.

The questionnaire is accessed through a public link with no requirement of providing personal information. The setting "collect email addresses" is turned off in Google Forms, so that there is no way for the researchers to decipher who any of the answers belong to. The respondents' ages are collected from a question in the beginning of the questionnaire. This is not to be viewed as unnecessary intrusion (Oates, Griffiths & Mclean, 2022), as parts of prior research has found age to be a significant factor of phishing susceptibility (2.2), and thus age is a factor of interest to this study. The exact age is not asked about, but rather to select an age range you belong to. The same explanation goes for collecting data about gender and education. All other data collected consists of non-identifiable metrics.

As mentioned in 3.3, the title and description of the topic of the questionnaire is "*How students manage everyday digital communication*". This is not completely false, but it is a

rather vague description of the real topic which is phishing susceptibility. It is not faulty to claim that phishing is tightly connected to how one manages every digital communication. It is also later down in the questionnaire made clear that phishing susceptibility is a topic of the questionnaire. It can be argued that it is unethical to not be completely transparent with the topic and intention of the survey in the beginning. Fact is however that respondents would be much more alert if it is stated clearly in the beginning that they will decide which e-mails are phishing and which are not. In order to get accurate responses and results, it was necessary to not be completely honest in the description, while still not deceiving the respondents too much. It was also concluded that the respondents would take no type of harm as a consequence of this, which is of utmost importance.

Since fabricated E-mails with real brands and companies are used in the questionnaire to replicate real life phishing attempts, it is clearly stated in the beginning that any logos, names, or trademarks that appear belong to their respective organizations and are used for illustrative purposes only, and does not represent actual communication from these organizations nor imply any form of collaboration. It is also stated that the fabricated E-mails are for research purposes only.

4 Empirical Results

4.1 Demographic Questions (Section 1)

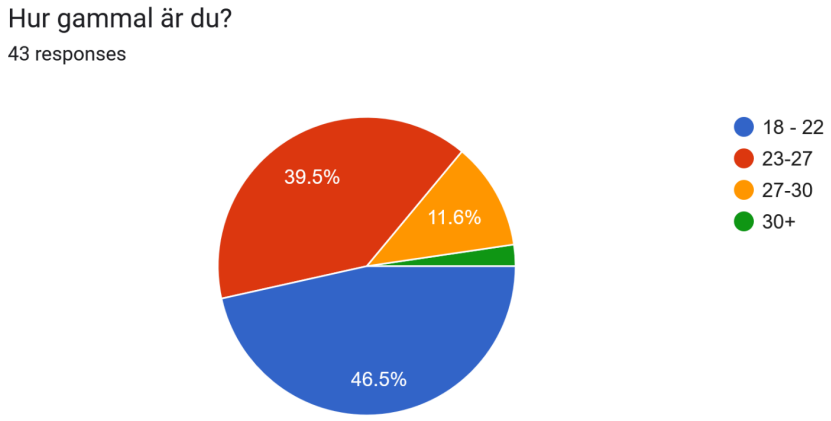


Figure 2.1: How old the participants are.

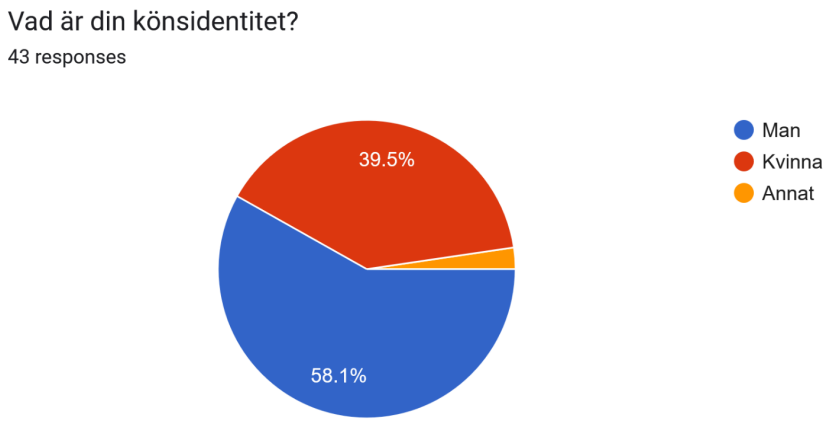


Figure 2.2: The gender identity of participants, Male (blue), Woman (red), Other (orange).

Due to these previous questions being, overall not related to the goals of the survey there is not much to analyze. But it is a good way to see the demographics of the participants. Overall for age most were around 18-27 years old, which are among the more common ages for university students. As for gender, the reason for there being more men answering is most likely a mix of us all being men, and therefore most likely having more male friends, and in general more men being within IT-education.

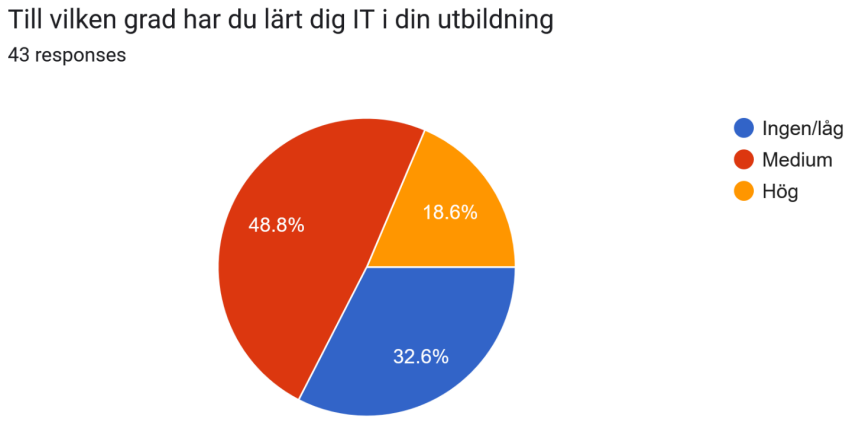


Figure 2.3: Level of perceived level of IT-education from participants, ranging between none/low(ingen/låg), medium and high (hög)

Table 1: A selection of the more common lines of education for each perceived level of IT-education

Perceived level of IT-education	Line of education
Hög(High)	Systemvetenskap
Hög(High)	Datateknik

Medium	Systemvetenskap
Medium	Civilingenjör
Låg(Low)	Juristprogrammet
Låg(Low)	Statsvetenskap

While the general perceived level of IT-education among the participants is a bit lopsided, with “Medium” taking up nearly half of the total participants, it will still allow for a comparative analysis of the data between those with and without IT-education. As around a third of the participants consider themselves to have either low IT-education or none at all. With this we can count everyone who responded with having high or medium levels of education to be IT-students, and those who responded as low as non IT-students.

Something else of note is that the most common of the lines of education among participants, systemvetenskap/information systems, were split among if they had high or medium levels of IT-education. This most likely comes from how common of a response it was compared to other lines of education, leading to there being more chances for participants who study it to perceive their level of IT-education differently.

4.2 Phishing Susceptibility Testing (Section 2)

4.2.1 DHL e-mail

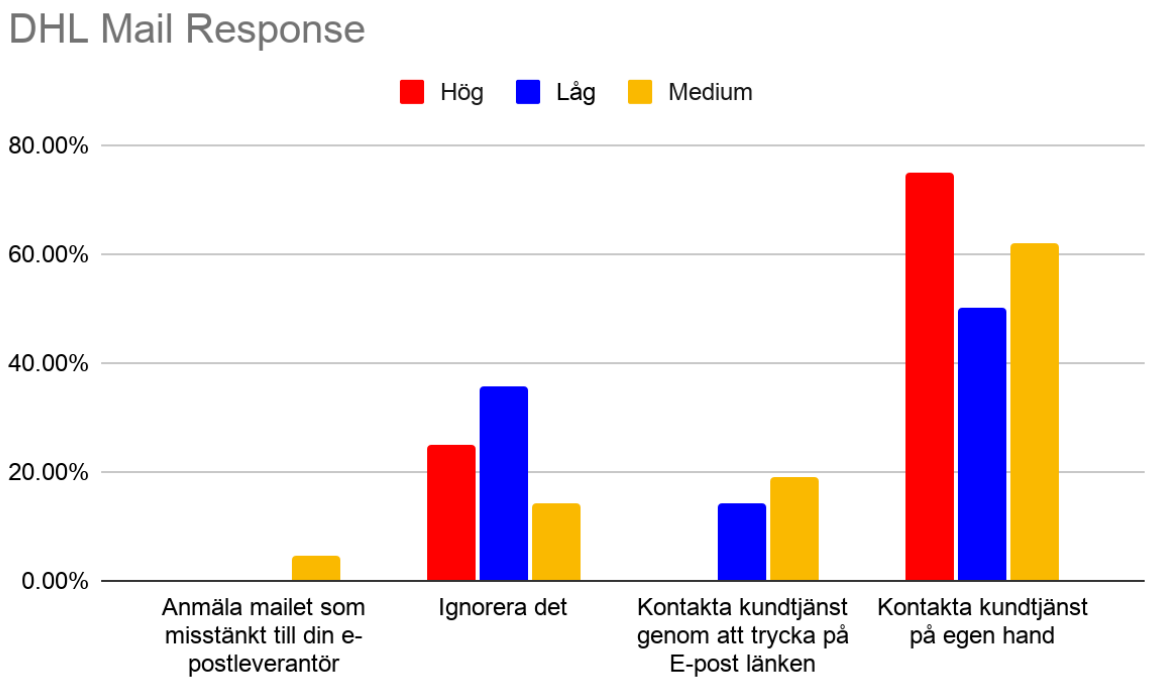


Figure 3.1: Responses from the first simulated mail, grouped by their perceived level of IT-education

Within the responses for the simulated DHL mail, which we intended to be legitimate, people with higher perceived levels of IT education were more likely to answer "Kontakta kundtjänst på egen hand" or "Contact customer support on your own" translated to English. With 75% of the respondents with a high level of perceived level of IT-education, 61.9% for medium and 50% for low.

Medium, being the largest demographic within the participants are the most likely to both report the mail as suspicious, and to use the link. But under 5% of them actually chose to press the link, while there is less than a 5% difference between low and medium for reporting the mail. As for ignoring the mail, low has the highest percentage at 35.7%, with high at 25% and medium at 14.3%.

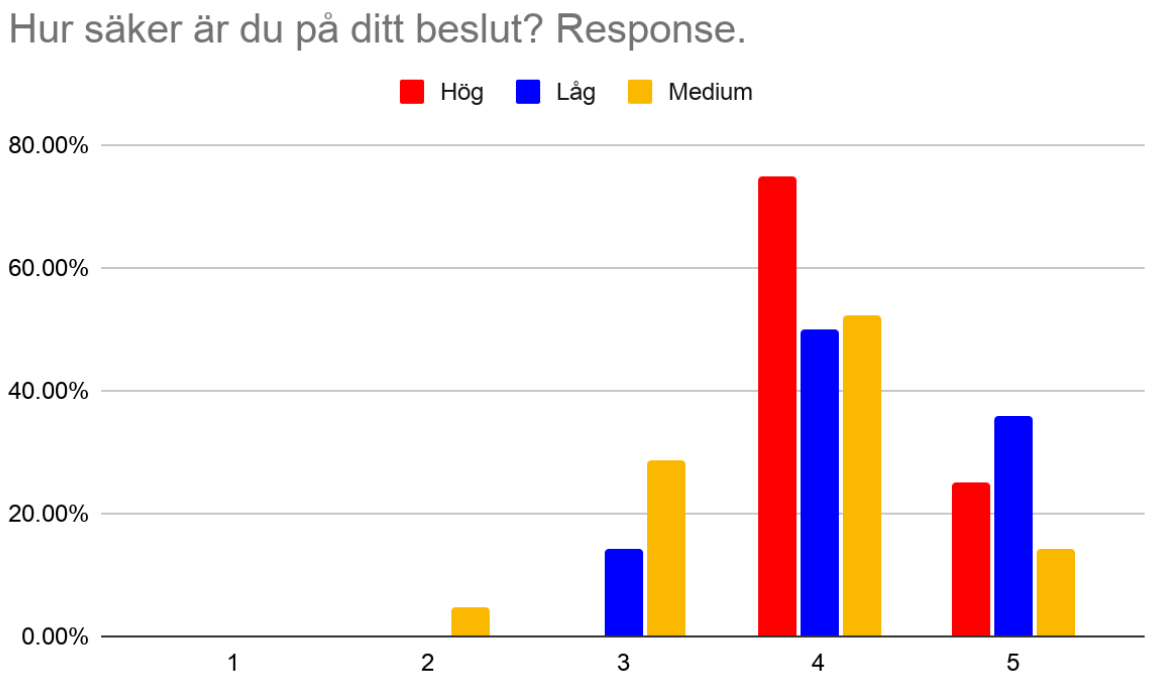


Figure 3.2: Responses for how sure of their answer they were on the first simulated phishing mail on a scale of 1 to 5, grouped by their perceived level of IT education.

Overall the participants were quite sure of their responses with overall the most sure of the 3 groups being those with a lower perceived level of IT-education. Though least sure were those who answered medium on their level of IT-education, with them being the only group where anyone answered with a 2.

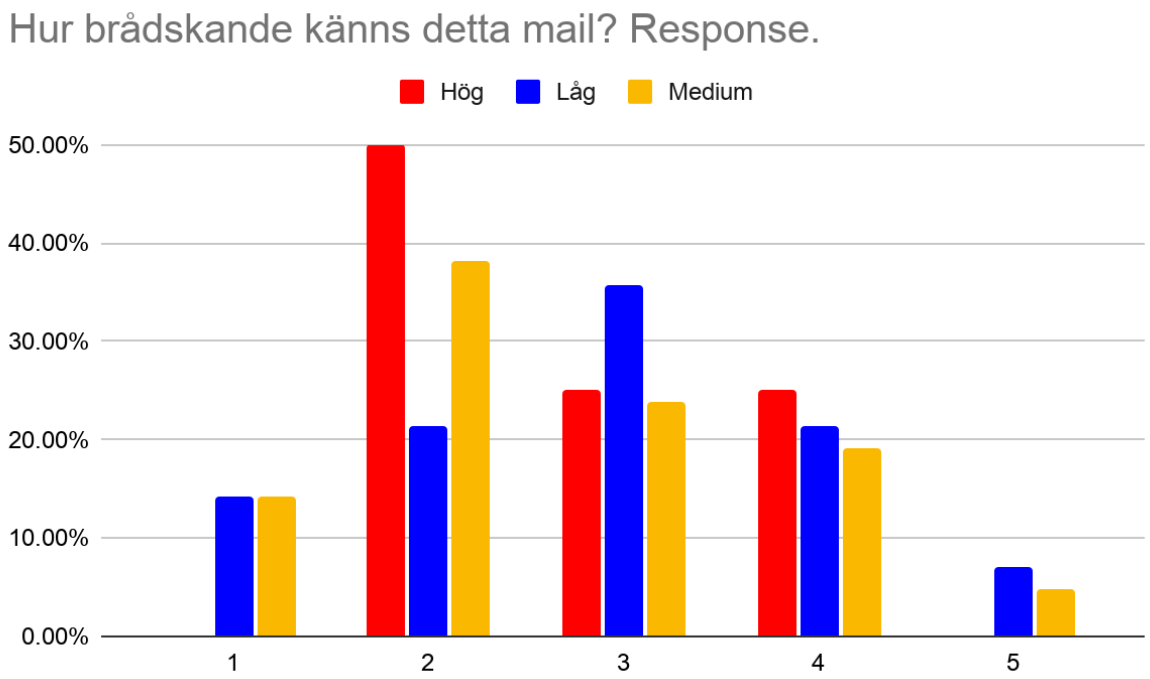


Figure 3.3: Responses for how urgent the first simulated phishing mail felt on a scale from 1 to 5, grouped by perceived level of IT education.

The participants did not find the DHL mail particularly urgent, with all groups mostly gravitating towards either a 2 or a 3. Naturally the 2 bigger demographics of low and medium were more spread out than the smaller group of people who answered high earlier.

Table 2: A selection of responses of the question “Varför anser du att det var bästa sättet att agera?”(Why do you believe this was the best way to act?) compared to how they answered the DHL mail, grouped by level of perceived level of IT-education

IT-education	Mail Response	Answer
Hög	Kontakta kundtjänst på egen hand	Inte klicka på länkar direkt. Detta förutsätter ju också att avsändaradressen ser 100% korrekt ut
Hög	Ignorera det	Jag hade antagligen kontrollerat mejladressen direkt. Ofta är det något som inte stämmer, särskilt när de efterfrågar personliga uppgifter. Sedan hade jag nog ignorerat det, men det bästa vore egentligen att rapportera det, men de är lätt att glömma. Möjligtvis hade jag också kontrollerat min trackerlänk eller gått in på hemsidan på egen hand för att vara helt säker.

Medium	Kontakta kundtjänst på egen hand	Det är lätt att låtsas var officiell via e-postmeddelanden. Genom att kontakta kundhjälp via deras officiella sida får jag klart reda på om det faktiskt finns ett problem
Medium	Kontakta kundtjänst genom att trycka på E-post länken	Det känns autentiskt och Icke brådskande
Låg	Kontakta kundtjänst på egen hand	Känns som ett konstigt problem att behöva ge ytterligare adressuppgifter när jag gjort en fullständig beställning redan. Men anser samtidigt inte att det ser ut att vara något fuffens därför väljer jag kontakta DHL på egen hand för att säkerställa trovärdighet samt åtgärda möjligt problem.
Låg	Ignorera det	För att undvika eventuella scams.

For the free form question of why they believed their course of action was the best for the DHL e-mail, it generally followed a tendency of those with higher levels of education giving a more concrete answer. But of course there are outliers among both of the bigger groups of low and medium. But overall these responses point towards those with higher education being more aware of why they are doing what they are doing, rather than those of lower levels of IT-education.

4.2.2 Netflix e-mail

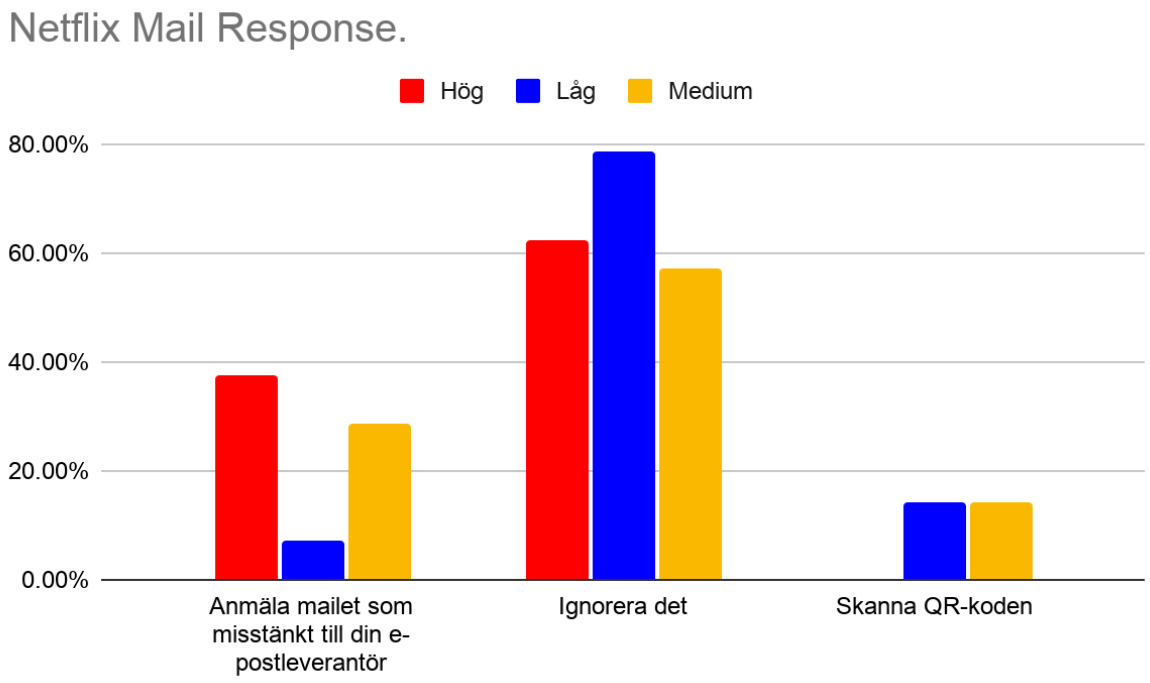


Figure 4.1: Responses from the second simulated phishing mail, grouped by their perceived level of IT-education.

For the Netflix mail, which was the first of our "phishing attempts", the participants clearly favoured ignoring the mail, with more than half of all the answers being that. But even still people who responded with a high or medium level of IT-education had a far higher tendency to report the mail for suspicious behaviour, while medium and low were about equal for the tendency to scan the code. This points towards that people with a higher perceived IT-education are in general better, but of course you cannot say with just one question.

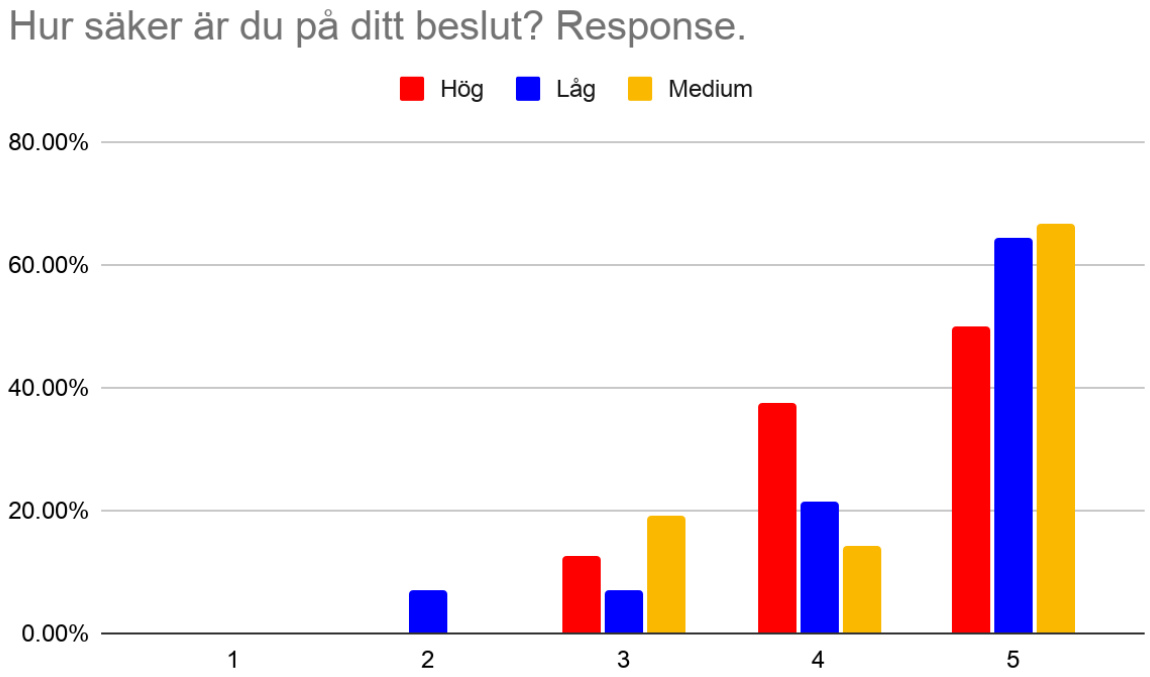


Figure 4.2: Responses for how sure of their answer they were on the second simulated phishing mail on a scale of 1 to 5, grouped by their perceived level of IT education.

As with the DHL mail, the participants are quite sure of their decisions for this one as well. The group who answered a 5 in their certainty the most on this question were those with a medium level of IT-education. But they were also the group who had the highest percentage of uncertainty, with them having nearly 20% of their responses at a 3. But overall there is no major difference on the certainty of the three different groups for this question.

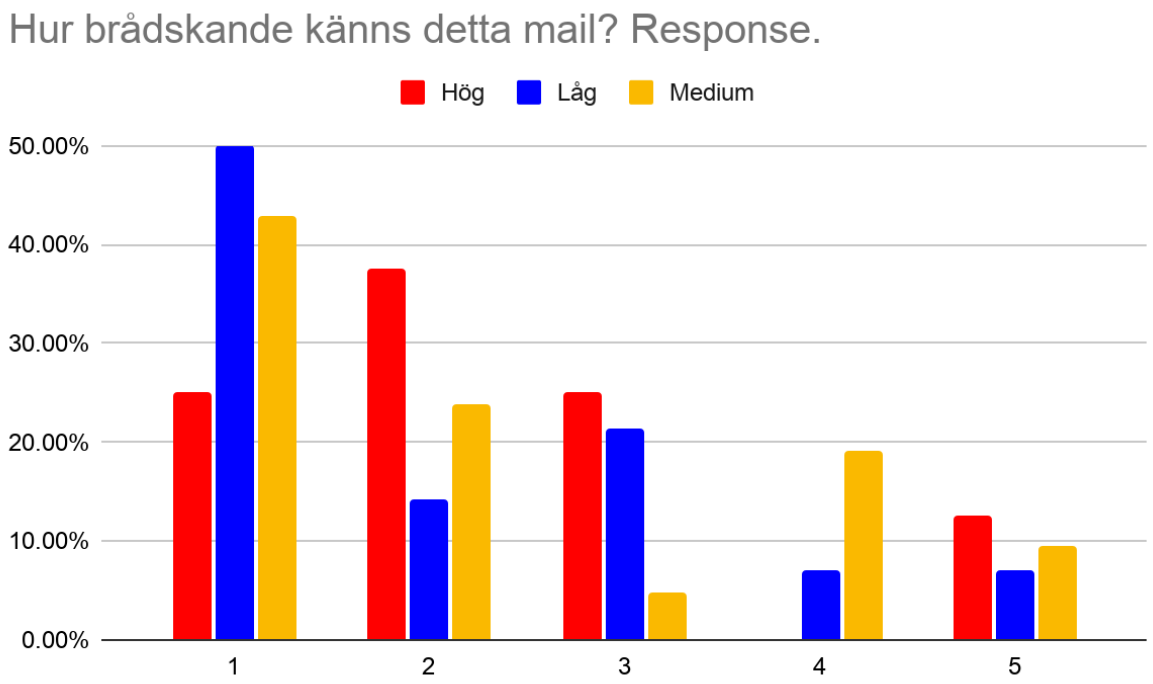


Figure 4.3: Responses for how urgent the second simulated phishing mail felt on a scale from 1 to 5, grouped by perceived level of IT education.

Once more the participants did not find this mail to be particularly urgent. This might be part of why the overall response was to ignore, rather than report it for suspicious behavior. As it is common among phishing emails to give a sense of urgency to whomever receives it. But out of the different levels of IT-education, medium was the one who found it the most urgent, while low found it the least urgent.

4.2.3 Swedbank e-mail

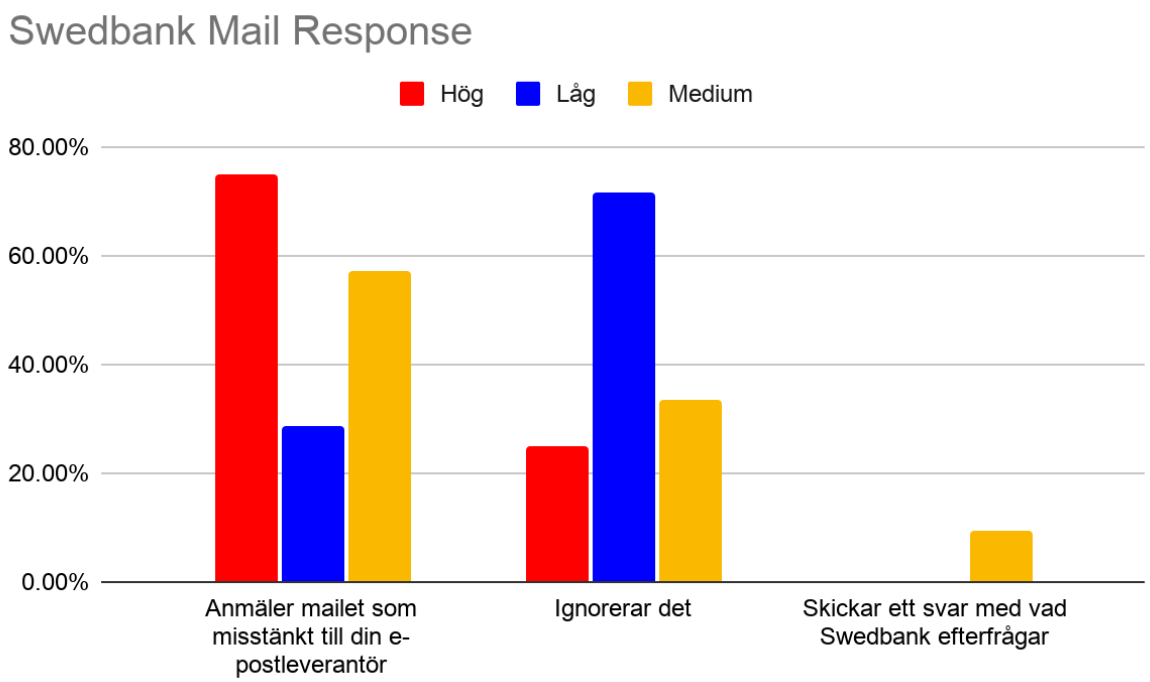


Figure 5.1: Responses from the third simulated phishing mail, grouped by their perceived level of IT-education.

The Swedbank mail is another of the "phishing mails" within the survey. In this one there is a much larger tendency among all participants to report the mail, rather than ignoring it. With participants of the medium and high groups having a clear majority among them who responded that way, with 57.1% and 75% respectively choosing to report it . Meanwhile the low group is more inclined to ignore it, due to 71.4% choosing to do that. This may indicate that those with higher levels of IT-education are better at properly identifying phishing emails, or that those with lower levels are less likely to report them if found.

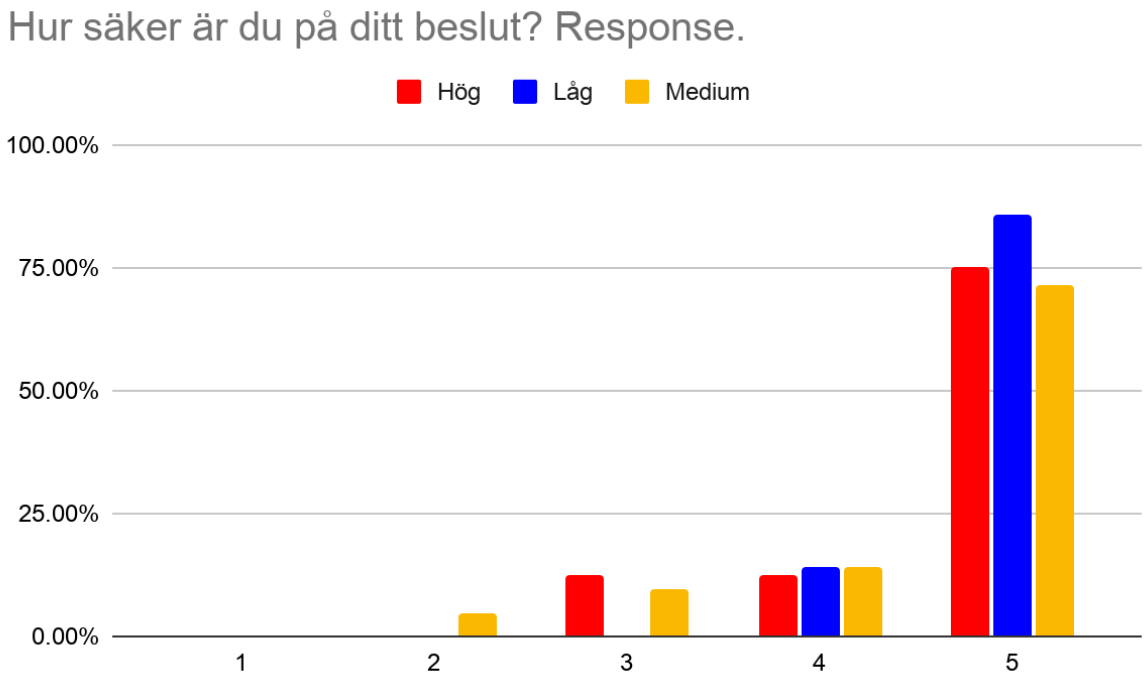


Figure 5.2: Responses for how sure of their answer they were on the third simulated phishing mail on a scale of 1 to 5, grouped by their perceived level of IT education.

Following the trend set by the previous questions all groups are certain about their answers, with just a few of them not choosing that they are absolutely certain of their decision. This may be a case of overconfidence, since as of yet the participants have been completely sure in their responses.

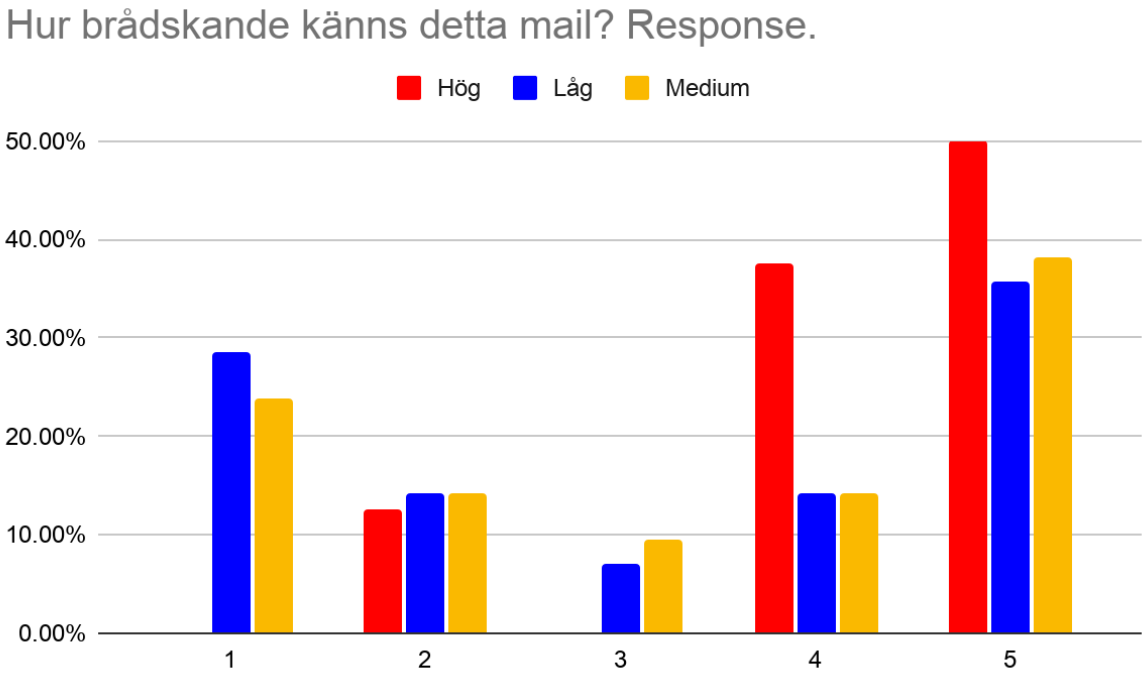


Figure 5.3: Responses for how urgent the third simulated phishing mail felt on a scale from 1 to 5, grouped by perceived level of IT education

There is a clear split between how urgent the respondents believe the Swedbank e-mail was. While it is clear that the most common response was that it felt extremely urgent within all levels of IT-education, the second place for both low and medium was that it didn't feel urgent at all. One reason for this might possibly be the lack of a specific deadline within the mail, while still being about something that the respondents find important. So while the ones that thought it was not urgent thought about the lack of a clear deadline, the ones who found it urgent thought about the potential locking of their bank account.

Table 3: A selection of responses of the question “Varför anser du att det var bästa sättet att agera?”(Why do you believe this was the best way to act?) compared to how they answered the Swedbank mail, grouped by level of perceived level of IT-education

IT-education	Mail Response	Answer
Hög	Anmäler mailet som misstänkt till din e-postleverantör	Bedrägeriet ber om extremt känslig info i ett mejl. Den skapar en artificiell konsekvens/deadline för att öka press & få individen att göra dåliga beslut. Extremt suspekt.
Hög	Ignorerar det	Hade ringt eller kollat mitt bankkonto istället, finns ingen riktig idé att svara på mailet om det skulle vara bedrägeri
Medium	Anmäler mailet som misstänkt till din e-postleverantör	Banken har bättre och mer säkra sätt att verifiera mina uppgifter, och jag kan enkelt ringa ifall jag misstänker fuffens. Jag skulle aldrig skriva in sådan känslig info bara pga ett Mail.
Medium	Skickar ett svar med vad Swedbank efterfrågar	För att det är Swedbank, det handlar om pengar
Låg	Ignorerar det	Hade sett det som skumt och hade kontaktat banken på egen hand för att kontrollera
Låg	Anmäler mailet som misstänkt till din e-postleverantör	e-post är inte krypterad. Riktigt lätt att fiska upp datapaket (Wiresharka det typ). Jag skulle inte tro att en bank får fråga om känsliga kontouppgifter via mejl. Dessutom känns det ovanligt brådskande vilket höjer misstankarna.

.

There was no big difference between the different responses as to why the participants chose what they did on the Swedbank e-mail. Those of all levels of IT-education gave both short answers, which often mentioned the fact that Swedbank was responsible for their money, and longer responses that stated as to why they believed it to be a phishing attempt. Though as stated before one common thing that is mentioned among most of the responses was in relation to money. While a lot of those that reported or ignored also mentioned that Swedbank would never ask for that kind of information in an e-mail.

4.2.4 Spotify e-mail

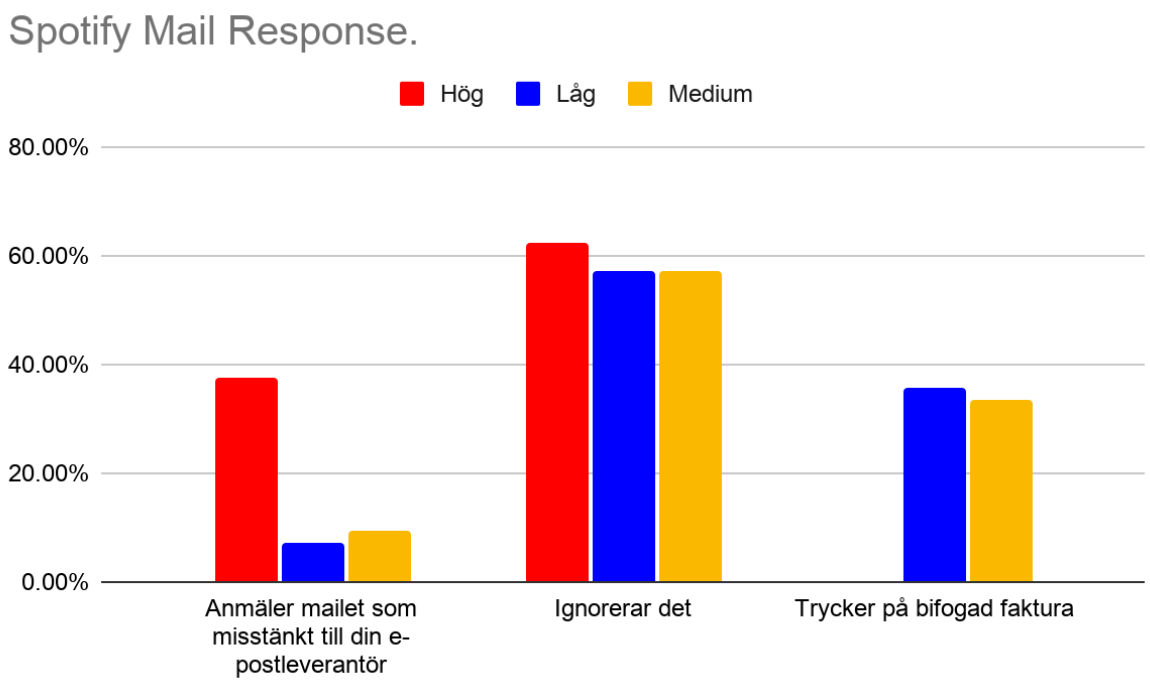


Figure 6.1: Responses from the fourth simulated phishing mail, grouped by their perceived level of IT-education

The Spotify mail was another of the phishing mails within the survey. Here the most common of the alternatives was to ignore the mail, rather than act upon it by either reporting it, or pressing the attached invoice. This was consistent among all three levels of IT-education, but the second most common alternative differed between groups. Among those of the high group, their second most common choice was reporting the mail as suspicious, with 37.5% choosing that and none of them choosing that they would click the invoice. Meanwhile those of the medium and low groups both had clicking the invoice as their second most common, with low being the most likely to choose that. Though the difference between low and medium is quite insignificant at only 35.7% and 33.3% respectively. This points towards those with higher levels being better at identifying the phishing mails.

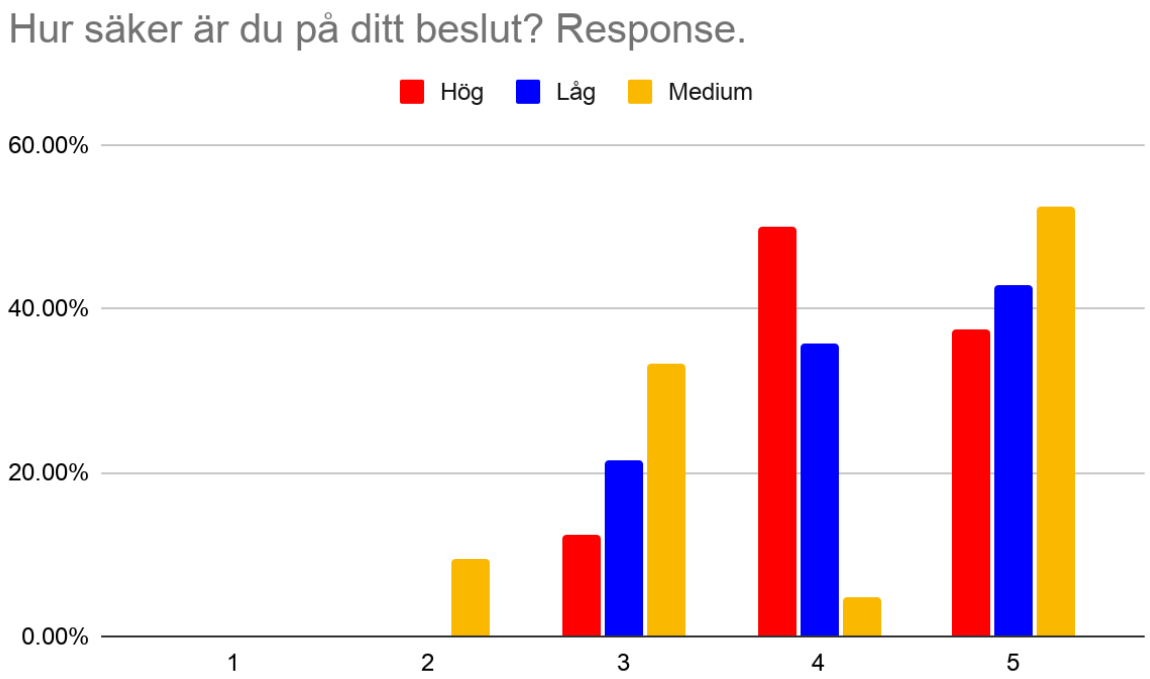


Figure 6.2: Responses for how sure of their answer they were on the fourth simulated phishing mail on a scale of 1 to 5, grouped by their perceived level of IT education.

The participants had a high level of certainty for their answers for this one, with most of them answering either 4 or 5 on the scale. It is worth noting that medium was the most unsure among this group, with nearly 43% of them choosing 3 or lower, and it being the only group where anyone picked a 2 for how certain they were of their answer.

4.2.5 Försäkringskassan e-mail

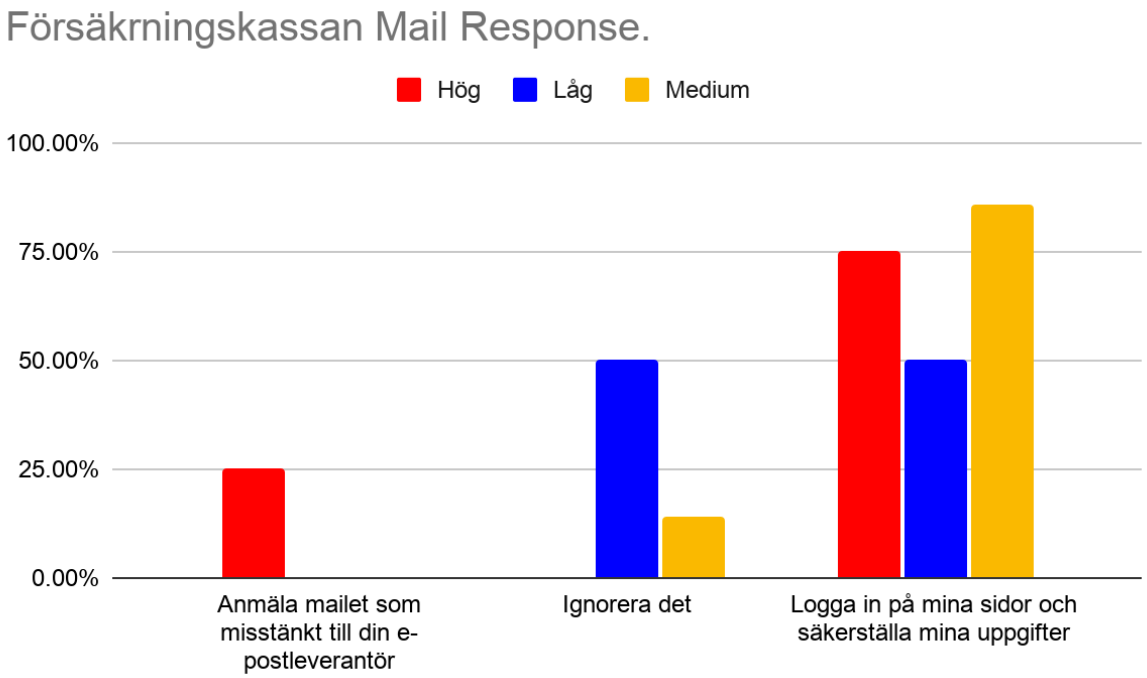


Figure 7.1: Responses from the fifth simulated phishing mail, grouped by their perceived level of IT-education.

The mail from Försäkringskassan was our second “legitimate” mail of the bunch, and most of the respondents could see that, as only 2 participants out of all of them chose to report the mail as suspicious. Both of the answers to report it were from those that said their level of IT-education was high. Though it is important to note that there was a spelling error within the mail, which might have made them a bit paranoid. But besides that those of the low group were generally more inclined to ignore it than to do as instructed, with 50% of them choosing to simply ignore it rather than log in on Försäkringskassan’s website. This also matches with the DHL mail, where despite the mail being “legitimate” those with lower IT-education were more likely to either ignore or believe it was a phishing email.

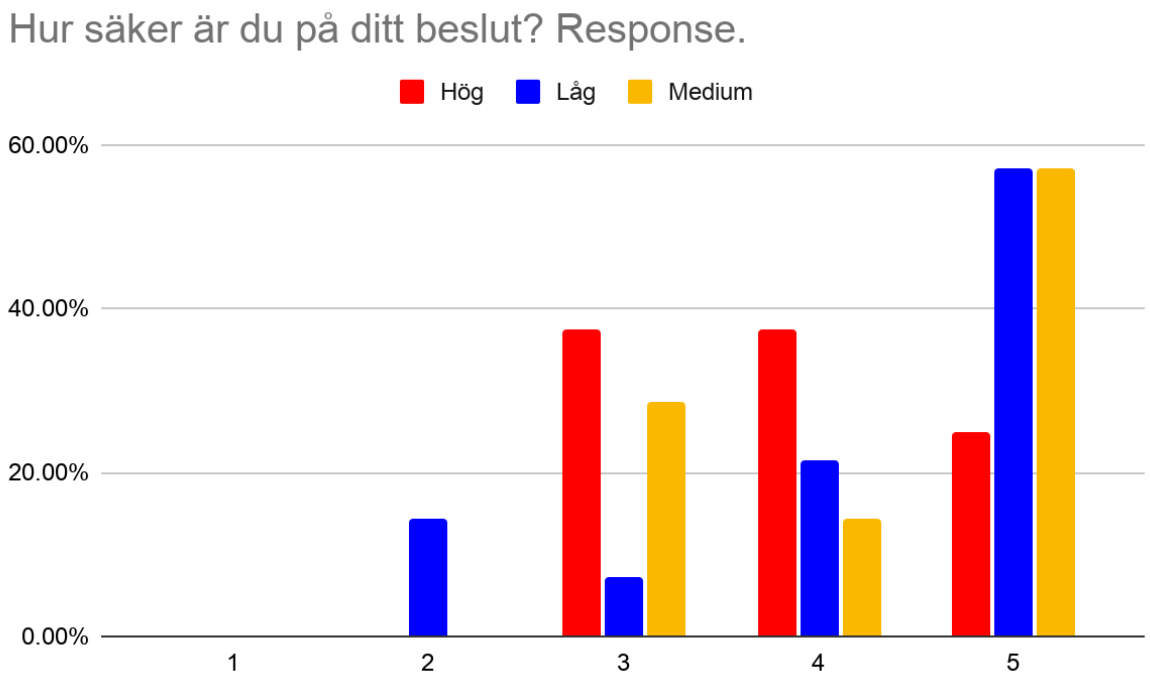


Figure 7.2: Responses for how sure of their answer they were on the fifth simulated phishing mail on a scale of 1 to 5, grouped by their perceived level of IT education.

As with all the previous mails, the respondents were quite sure of their choices. And as with those that came before high usually seems to avoid choosing a 5 for their level of certainty. It is also worth noting that overall the most sure of the groups in this case is those of the low group.

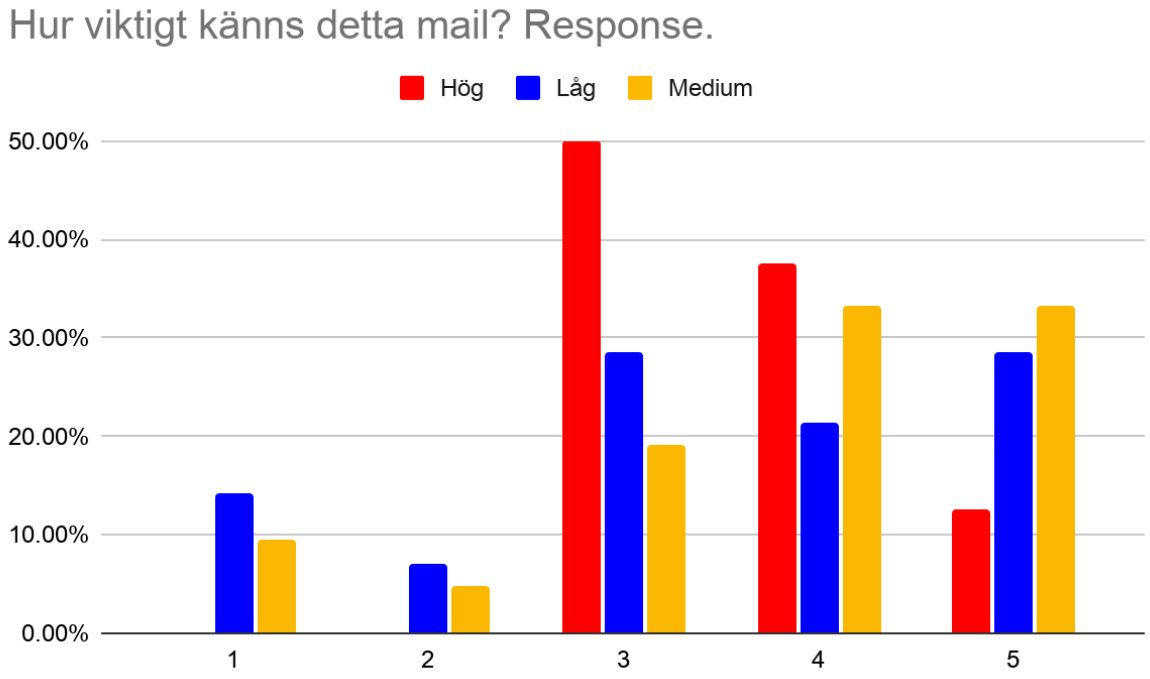


Figure 7.3: Responses for how important the fifth simulated phishing mail felt on a scale from 1 to 5, grouped by perceived level of IT education.

Here those of the medium group believed the mail to be important the most with 66.6% choosing either 4 or 5, while those of the high group saw it as least important among the groups, with 50% of them putting it at a 3. Low were quite split between 3 and 5, with both of those having equal numbers at 28.6% each, and a good amount also picking 4.

4.2.6 CSN e-mail

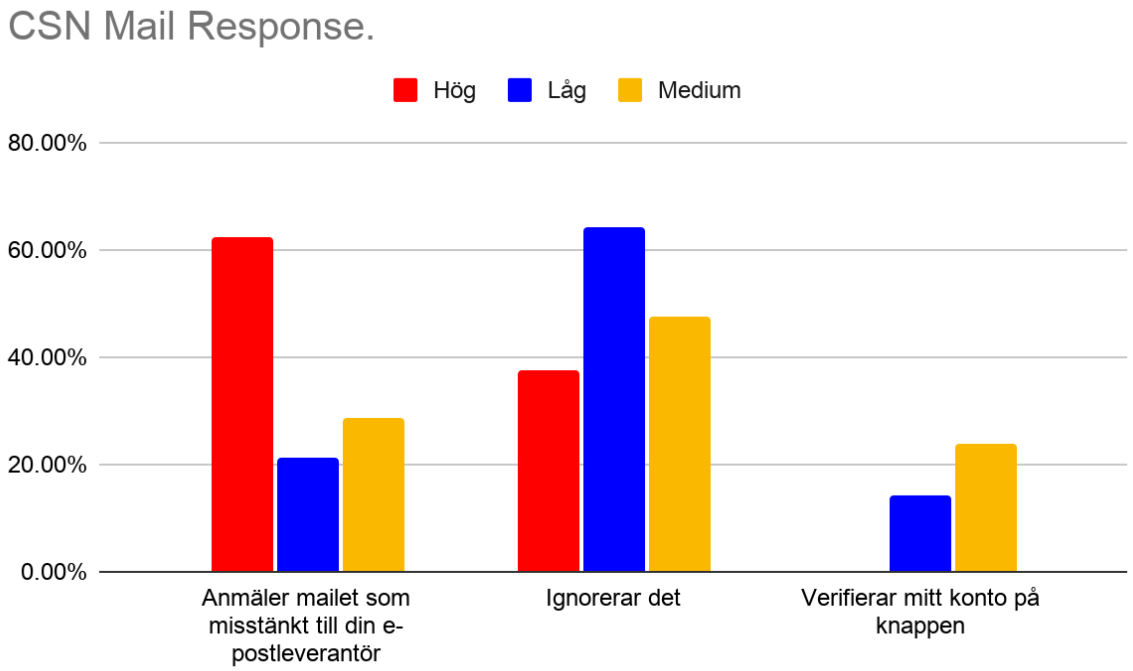


Figure 8.1: Responses from the sixth simulated phishing mail, grouped by their perceived level of IT-education.

The CSN mail was another of the phishing emails within the survey, and in this one most participants decided to ignore it, while the most uncommon answer was to press the button. Though most decided to ignore it, the answers are still quite split for all groups besides low. Medium is quite split among all the answers, with their lowest percentage of any option is 23.8% choosing to press the button. While high was only split between reporting the mail and ignoring it, having 62.5% and 32.75% respectively. This shows a higher tendency for those of the high group of reporting the mails rather than just ignoring it, while those with a low level of IT-education to ignore the mails. Meanwhile those of medium, who would be considered between high and low in education level are split.

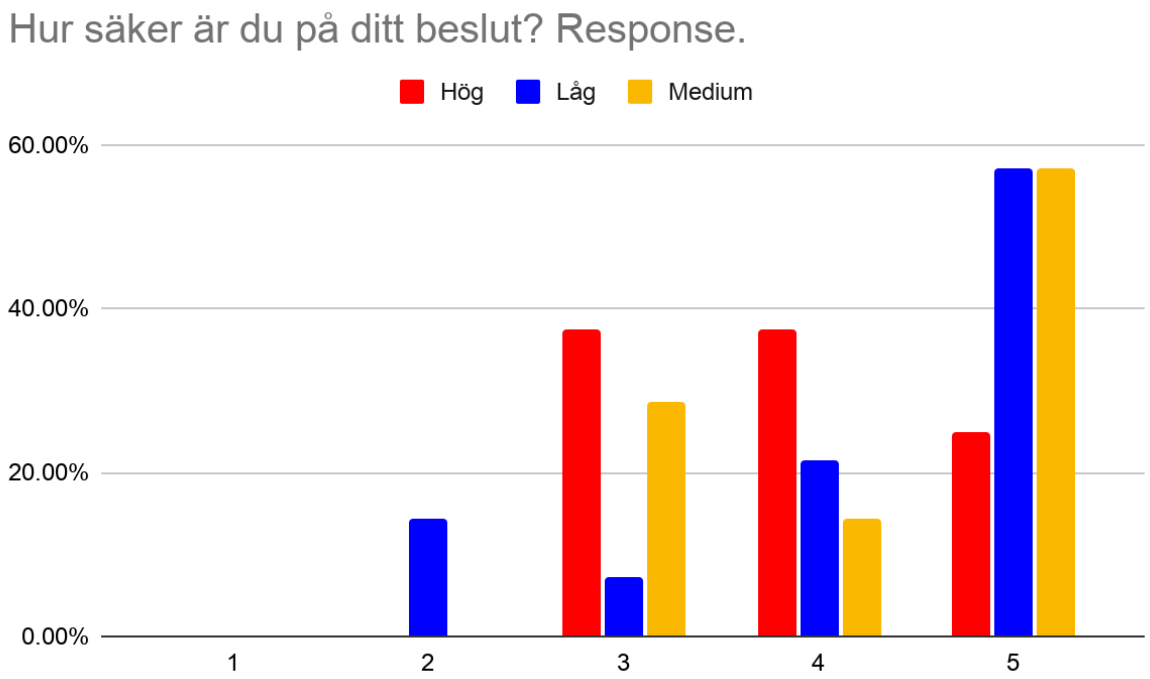


Figure 8.2: Responses for how sure of their answer they were on the sixth simulated phishing mail on a scale of 1 to 5, grouped by their perceived level of IT education.

For the CSN mail the medium and low groups seem to be mostly certain with their choices, both having 57.1% of them choosing 5 as their level of certainty. Meanwhile those of the high group were split among 3, 4 and 5. With 37.5% having chosen 3 and 4, while 25% chose 5. There was also a substantial amount of the medium group that chose 3 at 28.6%. So in general those with a low level of IT-education were overall more certain for this question, than those with higher levels.

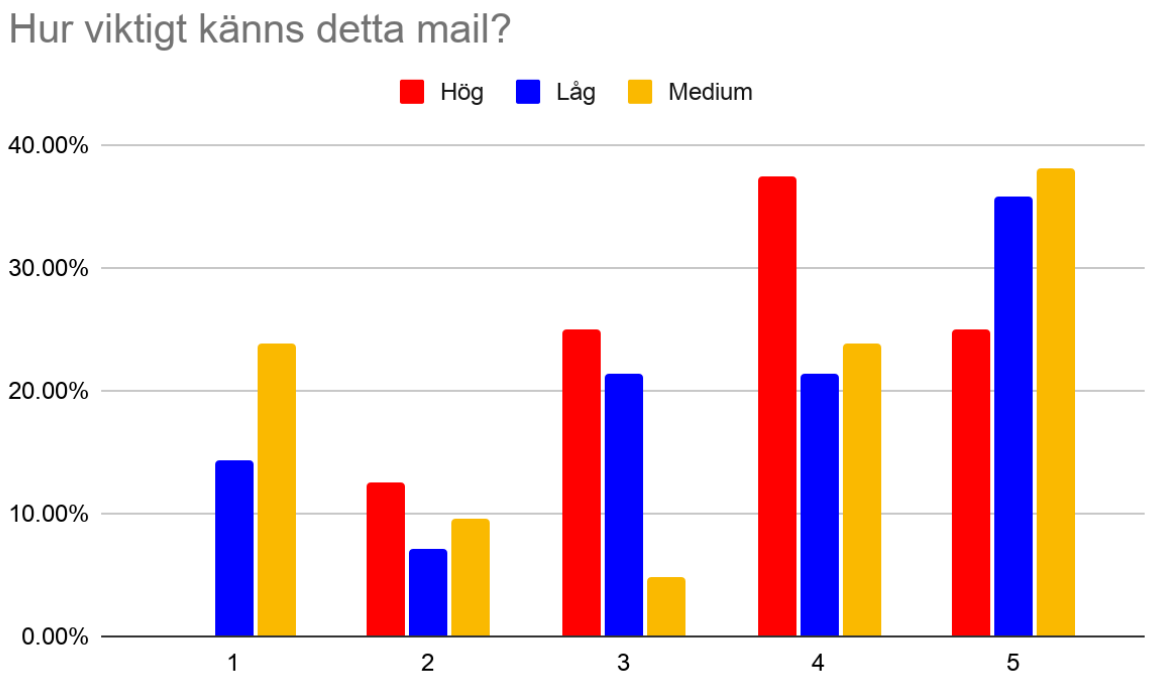


Figure 8.3: Responses for how important the sixth simulated phishing mail felt on a scale from 1 to 5, grouped by perceived level of IT education.

People of all groups found this mail quite important, with those of the medium group both being the most likely to find it crucial at 5 and to find it completely unimportant 1, at 38.1% and 23.8% respectively. High is the only group where the most common choice was 5, with 37.5% of them choosing 4 with 3 and 5 sharing a second place at 25% each. But it is to be expected that a mail from CSN would be considered important here, as the participants are students and CSN is a major source of income for them.

Table 4: A selection of responses of the question “Varför anser du att det var bästa sättet att agera?”(Why do you believe this was the best way to act?) compared to how they answered the CSN mail, grouped by level of perceived level of IT-education

IT-education	Mail Response	Answer
Hög	Anmäler mailet som misstänkt till din e-postleverantör	Mailet såg mer legit ut så hade kanske råkat trycka om jag inte var på alerten
Hög	Ignorerar det	Eftersom jag kan logga in på appen och se om det stämmer, alltså det går att lösa på ett annat sätt som är mindre riskabelt
Medium	Verifierar mitt konto på knappen	Jag tror att jag känner mig mer säker om länken kommer i form av en knapp

Medium	Ignorerar det	Loggar hellre in på CSN än att trycka på länk i mejl eftersom jag aldrig haft liknande problem med CSN
Låg	Ignorerar det	Jag hade loggat in på mina sidor. Mailet såg ut som ett hot.
Låg	Verifierar mitt konto på knappen	Eftersom hela min inkomst hänger på att känns det angeläget att se till att det blir fixat snabbt.

Out of all 3 questions about why they would respond the way they did on the different e-mails this one had by far the shortest answers among all groups. But among those that decided to do as the mail asked, there was a common trend of them being worried about their income, as CSN is the primary source of income for many students. Otherwise the trend among those that ignored or reported it was that it is generally safer to go to their website by yourself, rather than clicking on a link. There was also those that selected that they would either ignore or report, but that they might fall for it. But there was no general trends that matched the responses for any specific groups here.

4.2.7 PostNord e-mail

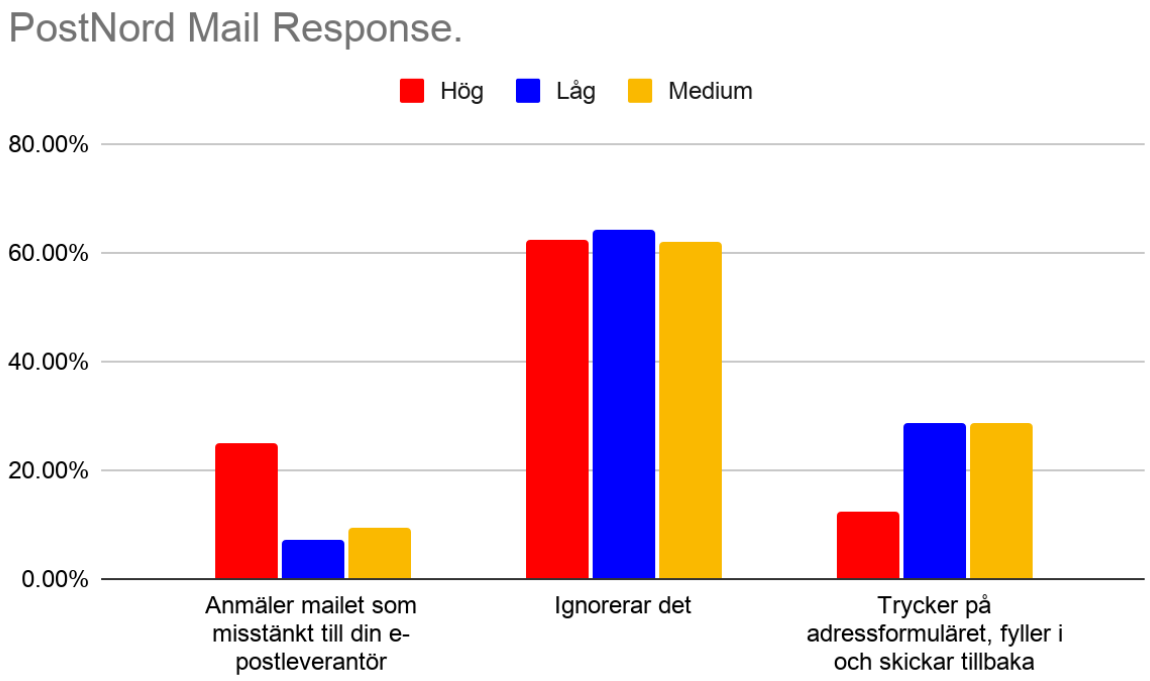


Figure 9.1: Responses from the seventh simulated phishing mail, grouped by their perceived level of IT-education.

PostNord was the final mail question and among the phishing e-mails. Here the vast majority chose to ignore it, with a little over 60% of all groups choosing to that option, with low being the most likely to do so at 64.3% and medium being the least likely at 61.9%. High was the

group most likely to report it for being suspicious at 25% while low were unlikely to do so at 7.14%. Medium and low were also equally likely to fill in the form at 28.57% each. Which shows that for this question those with higher levels of IT-education were more likely to identify that the mail was phishing, and also more likely to report it.

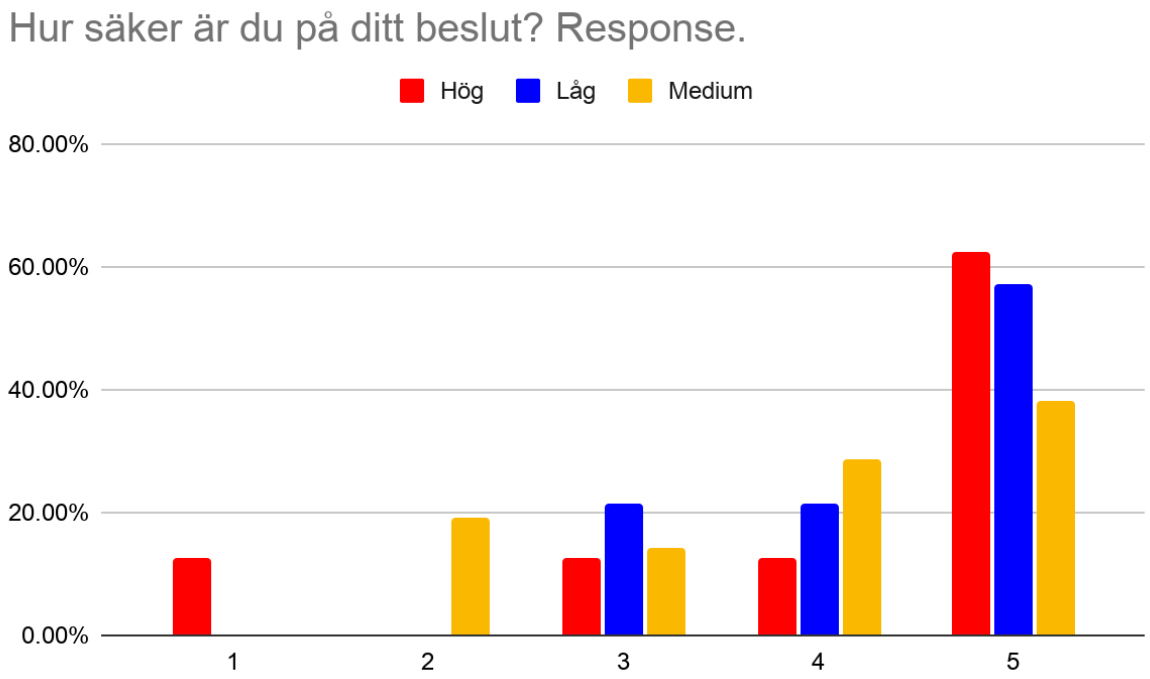


Figure 9.2: Responses for how sure of their answer they were on the seventh simulated phishing mail on a scale of 1 to 5, grouped by their perceived level of IT education.

How certain the different groups were of their decision for the PostNord mail was quite spread out, especially among the medium group that had substantial amounts saying they were anywhere between a 2 and 5 in certainty. Low and high were quite a bit more certain, with 57.1% and 62.25% choosing that they were absolutely certain at a 5. So for this question how certain the person was seemed to first go down with their education level, but start going up again after a certain point.

4.3 General Phishing Questions (Section 3)

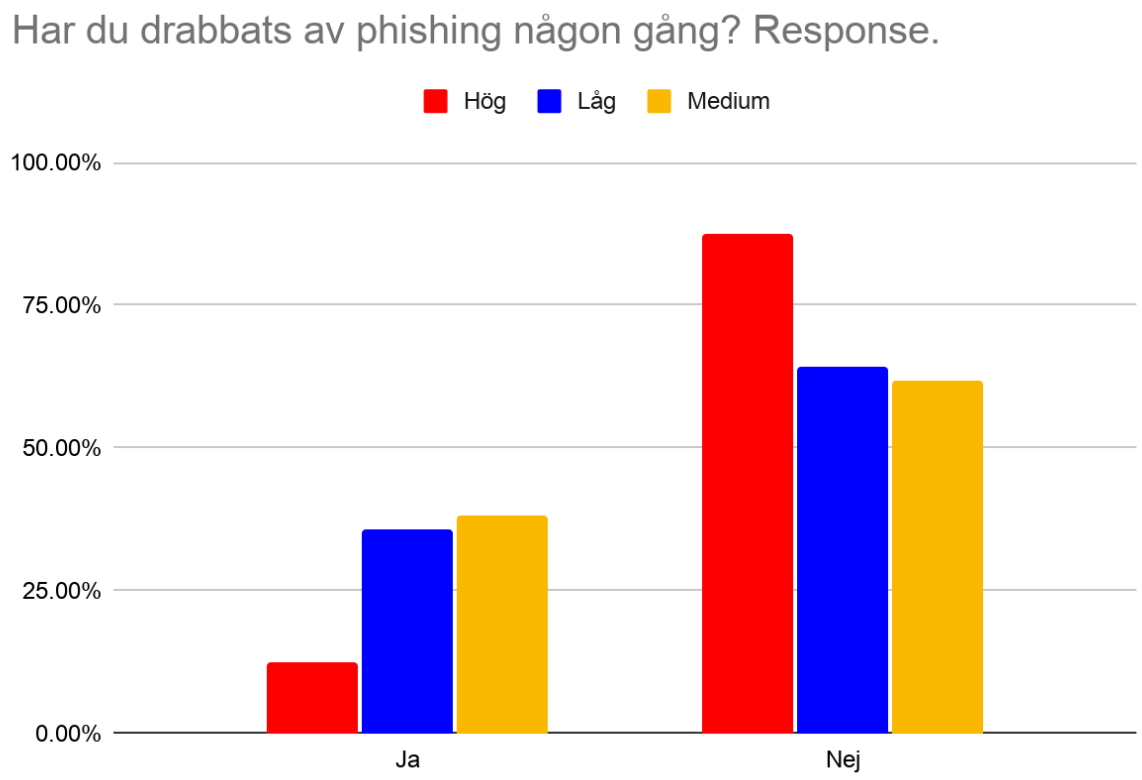


Figure 10.1: Response for if they have ever been affected by phishing, grouped by their perceived level of IT education. Ja = Yes, Nej = No.

Most participants seemed to believe that they had not been affected by phishing, with high being those who responded with the most at 87.5% and medium at the lowest at 61.9%. This might of course just be circumstantial, especially since high is the smallest group out of the respondents.

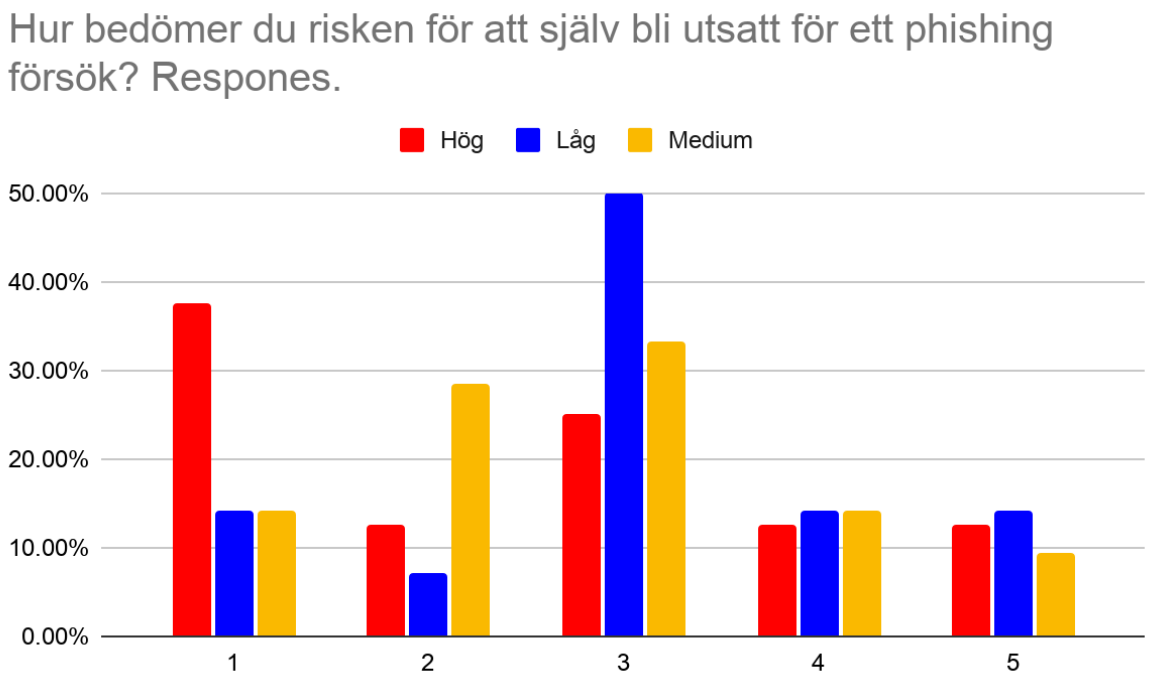


Figure 10.2: Response for how big of a risk they see of themselves being the victim of a phishing attempt on a scale from 1 to 5, grouped by their perceived level of IT education.

All of the groups seem to believe that they are at quite the low risk of being the victim of a phishing attempt. How likely they felt the risk also seems to decrease with higher levels of IT-education, as the high group had 50% respond either 1 or 2, while 50% of those within the low group responded with a 3.

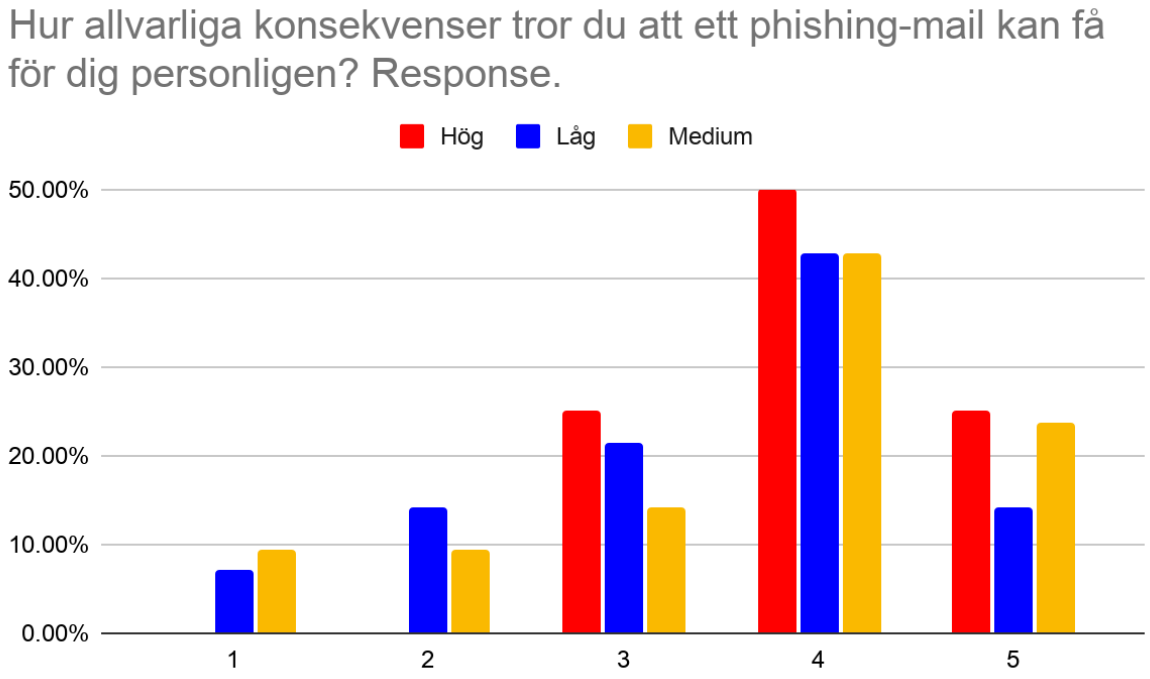


Figure 10.3: Response for how serious the consequences a phishing mail could have on them on a scale from 1 to 5, grouped by their perceived level of IT education.

Inversely to the risk of being the victim, how serious they believed the consequences seems to increase with their level of IT-education, while 4 is the most common among all groups, among those who picked that they have a low level of IT-education, 42.9% of them chose a 3 or lower, while high and medium only had 25% and 33.3% pick below a 3 respectively. Which points towards those with an IT-education generally knowing about the potential risks better than those without one.

Table 5.1: A selection of responses from the free form question “Har du någon strategi eller tumregel för att inte bli drabbad av phishing? “, grouped by perceived level of IT-education

IT-education	Answer
Hög	Att inte rusha igenom mejl och liknande. Kolla noggrant, ladda inte ner något, klicka inte på någon länk. Om all relevant info finns i mejlet, och/eller mejlet ber dig att självmant logga in/gå genom legitima kanaler är det förmodligen okej.
Hög	Klicka inte på okända länkar och ge alldigt ut personliga uppgifter om företag skickar mail om de.
Medium	Nej, men överlag godkänner jag ingenting som jag inte har sökt upp. T.ex. ringer en telefonförsäljare till mig så tar jag aldrig erbjudandet.
Medium	Inte klicka på några länkar och ignorera det mesta
Låg	Klicka inte på länkar jag inte litar på, om jag behöver verifiera något så ringer jag till deras nummer från hemsidan eller en pålitlig sida och frågar om meddelandet eller mailet jag har fått stämmer.
Låg	Vara vaksam och inte fatta förhastade beslut.

For this question about what strategies they used most of the answers mentioned being calm and avoiding links within their e-mails. With this trend following for all three of the groups. Interestingly enough though it was medium and high that had more people responding about lacking an actual strategy to avoid them, rather than low.

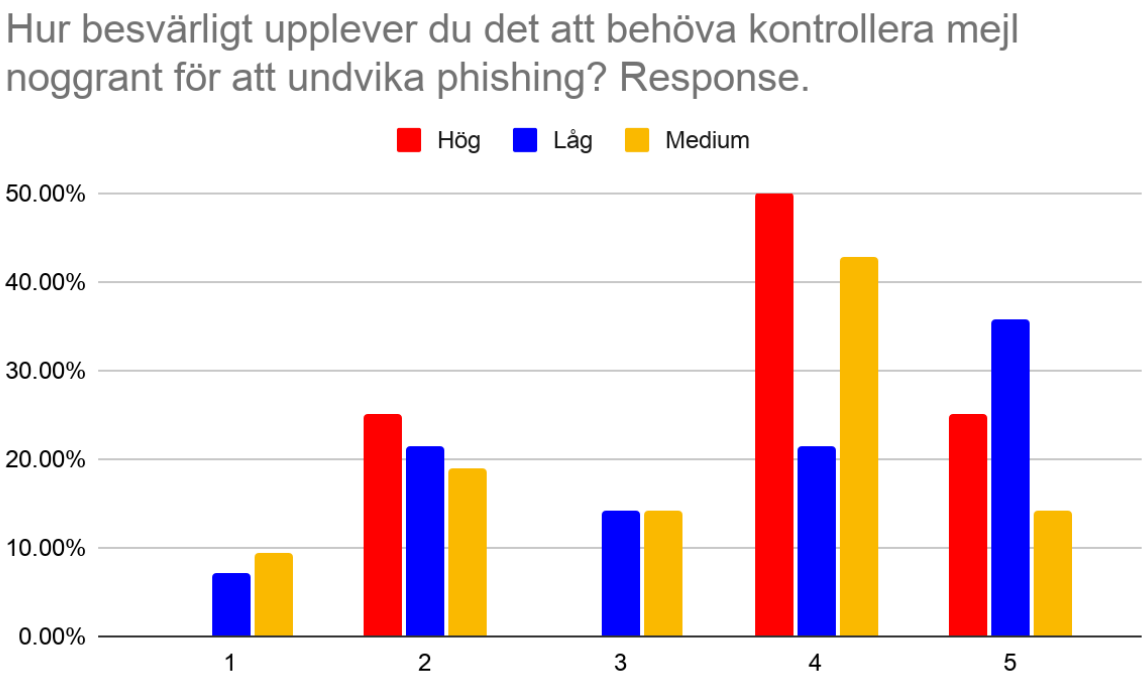


Figure 10.4: Response for how troublesome they find it to carefully check mails to avoid phishing on a scale from 1 to 5, grouped by their perceived level of IT education.

In general those with a low level of IT-education found it to be more troublesome to check their mails to avoid phishing. With 35.7% of them choosing a 5 on the scale. Though it is important to note that all three groups found it quite troublesome, just that both those of the medium and high groups had a larger tendency to pick 4 on the scale. The group who found it the least troublesome was overall medium, with 42.9% of them picking a 3 or lower. But overall there is no big difference between the groups.

Table 5.2: A selection of response from the question “Hur anser du att din utbildning har påverkat dina val? “, compared to the person’s perceived level of IT-education

IT-education	Answer
Hög	Den här väl gjort mig försiktigare. Mer uppmärksam. Man lär sig och hör om alla sätt folk kommer runt cybersäkerhet, och får en bättre uppfattning av hur skadliga dessa saker kan vara: exempelvis XSS som bara har ett helt farligt skript i sin phishing-länk. Man kan nog se det bara genom att ha musen ovan en suspekt URL och se hur långt dess innehåll är. Saker rör sig så snabbt, och det är inte överraskande att så många blir av med pengarna när någon kan pilla av QR-kod menyerna i McDonalds och phisha 3 dussin kunder.
Hög	Jag tror att mycket av min riskhanteringsstrategi kommer från mig som person och inte riktigt min utbildning. Däremot så har min kunskap om hur phising och andra cybersäkerhetsattacker fungerar samt deras omfattning blivit tydligt förbättrad av min IT kurs
Medium	Jag tror att min utbildning inom programmering har gjort att jag känner mig säkrare i att vara nära sketchinga sidor då jag vet ungefär vad jag kan och inte kan göra för att få virus eller ge iväg viktig information
Medium	Inte särskilt mycket, min utbildning tar inte upp någonting sånt här. Men en livslång karriär som internetsurfare samt några tidiga, i internets barndom, näsbrännor i form av virus har lärt en ett och annat
Låg	Inte alls, alla svar jag gett hade varit så gott som opåverkade utan min utbildning på högskola och universitet.
Låg	Inte alls. Kunskap som sprids i samhället och att jag har sett liknande mejl innan, påverkade mina svar mer.

The biggest common trend among the answers for the question of how they believe their education has affected their choices during the survey was that those with a higher perceived level of IT-education had a much larger tendency to believe their choices were affected by that education. But it is quite important to note that nearly no one believed it was the main factor of those choices, but rather a complement to personal experiences and time they had spent online.

5 Discussion

5.1 General Behaviour and Awareness

The results of this study indicate that students generally demonstrate a cautious approach when interacting with emails, as a large proportion of responses involved either ignoring or reporting suspicious messages rather than actively engaging with them. This pattern is evident across several of the phishing scenarios, where “ignore” was the most common response (see Figures 4.1, 5.1, 6.1, 8.1, 9.1). This suggests that students possess a basic awareness of phishing risks and are familiar with common warning signs associated with malicious emails.

However, despite this overall cautious behaviour, the results also show that unsafe decisions still occur across multiple scenarios (Figure 6.1 & 8.1), including those that were designed as phishing attempts. In several cases, participants chose to interact with emails by clicking links or engaging with content, indicating that awareness does not consistently translate into secure behaviour in practice. This finding highlights a gap between knowledge and action, which has been identified as a key challenge in cybersecurity research (Rohan et al., 2021; Mwangala et al., 2023).

A notable pattern in the results is that many participants expressed relatively high confidence in their decisions, including in some cases where their chosen action could be considered unsafe (see Figures 3.2 & 5.2). This suggests the presence of overconfidence in certain situations, although confidence levels do appear to vary depending on the scenario and correctness of the response. Such discrepancies between perceived and actual ability have been highlighted in previous research, which suggests that confidence is not always a reliable indicator of competence in cybersecurity contexts (Corradini, 2020).

Furthermore, the results indicate that contextual factors such as perceived urgency and importance can influence participants decision-making. Emails that were perceived as more urgent or personally relevant appear to trigger more active responses in some cases (see Figures 4.3 and 5.3), which aligns with common phishing strategies that rely on creating a sense of urgency to prompt immediate action (Workman, 2007; NCSC, 2018). This suggests that even when users are aware of potential risks, situational factors may override cautious behaviour and lead to less secure decisions.

5.2 Comparison Between IT and Non-IT Students

An important finding of this study is the relatively small difference observed between IT and non-IT students in their ability to identify phishing emails. While students with a higher level of IT education showed a tendency towards more secure behaviour, the overall difference between the groups was limited. Both groups demonstrated a mix of correct and incorrect decisions, indicating that neither group can be considered consistently effective in identifying phishing attempts.

It is worth noting that the group with high IT education made fewer unsafe choices overall in this sample. However, this group is relatively small, and the findings should therefore be interpreted with caution. The results nevertheless suggest that technical knowledge alone does not eliminate susceptibility to phishing attacks.

This finding is particularly noteworthy, as it challenges the expectation that individuals with a higher level of technical knowledge would perform significantly better in such tasks. Instead, the results suggest that phishing susceptibility is not solely determined by knowledge or education, but is also influenced by behavioural and psychological factors. This supports previous research highlighting the importance of the human factor in cybersecurity, where users actions often represent a key vulnerability (Rohan et al., 2021; Mwangala et al., 2023).

One possible explanation for this limited difference is that both IT and non-IT students rely on similar decision-making processes when evaluating emails. Even if IT students possess greater technical knowledge, they may still be influenced by factors such as perceived urgency, familiarity, or confidence in their own judgement. As a result, their behaviour may not differ substantially from that of non IT students in practice.

Furthermore, this finding suggests that improving cybersecurity behaviour cannot rely solely on increasing technical knowledge. While education may enhance awareness, it does not necessarily ensure correct decision-making in real world situations. Instead, it may be necessary to address how individuals interpret and respond to potential threats, including their confidence levels and susceptibility to cognitive biases.

5.3 Interpretation Through Technology Threat Avoidance Theory (TTAT) and Protection Motivation Theory (PMT)

From a theoretical perspective, the findings can be interpreted using Technology Threat Avoidance Theory (TTAT) and Protection Motivation Theory (PMT). In this study, participants often demonstrated awareness of potential threats, suggesting that threat appraisal was present. However, this did not always result in secure or protective behaviour, as some participants still chose to interact with phishing emails. This may indicate that coping appraisal plays a critical role, where individuals either overestimate their ability to handle the situation or underestimate the effectiveness of precautionary actions.

Participants' confidence levels suggest that perceived self-efficacy may influence decision making. When individuals believe they are capable of identifying threats, they may be more likely to engage with emails rather than avoid them, even in uncertain situations (Figures 9.1 & 9.2). This aligns with TTAT, where high perceived coping ability does not necessarily lead to safer behaviour, but may instead increase risk if it results in reduced caution (Chen & Liang, 2019).

The fact that some participants still chose to interact with phishing emails may be explained by the influence of perceived rewards or habits, where engaging with the email is perceived as more convenient or necessary than avoiding it. Furthermore, PMT highlights that individuals may engage in maladaptive coping strategies when faced with threats. In this study, such behaviour may be reflected in participants who ignored warning signs or rationalized their decisions despite potential risks. This aligns with previous findings suggesting that individuals do not always act in accordance with their knowledge when evaluating cybersecurity threats (Jamil et al., 2024).

5.4 Interpretation Through Signal Detection Theory (SDT)

The findings can also be interpreted through the lens of Signal Detection Theory (SDT), which distinguishes between correct and incorrect decisions under uncertainty, such as hits, misses, false alarms, and correct rejections (Martin, Dubé & Coovert, 2018). The variation in the respondents' answers (Figures 3.1, 4.1, 5.1) suggests that respondents differ in their decision thresholds, where some adopt a more cautious strategy and avoid interaction altogether, while others are more willing to engage, increasing the risk of falling for phishing attempts. The results therefore highlight that phishing detection is not only about knowledge but also about how individuals balance risk and uncertainty when making decisions, which is a central concept in SDT (Martin, Dubé & Coovert, 2018).

5.5 Confidence and Decision-Making

A central finding of this study concerns the relationship between participants' perceived confidence and their actual ability to identify phishing emails. The results indicate that confidence levels are often relatively high, including in some cases where participants made unsafe decisions (see Figures 3.2 and 5.2).

This discrepancy between perceived and actual ability suggests that overconfidence may be present in certain situations. However, confidence levels appear to vary depending on both the context of the email and the correctness of the response, indicating that the relationship between confidence and performance is not straightforward.

While high confidence may increase the likelihood of engaging with emails, particularly when individuals believe they can accurately assess risk, lower confidence may instead lead to more cautious behaviour. Participants who are uncertain about their ability may be more inclined to avoid interaction altogether, for example by ignoring emails rather than engaging with them.

At the same time, the presence of some high-confidence errors suggests that confidence can reinforce risky behaviour when individuals rely on their perceived competence rather than carefully evaluating each situation. These findings highlight the importance of not only increasing awareness, but also improving individuals ability to accurately assess their own competence.

5.6 False Alarms and Misses in Email Evaluation

An additional aspect of the findings concerns the different types of errors participants made when evaluating emails. While some participants failed to identify phishing emails and chose to interact with them, others treated legitimate emails as suspicious and chose to ignore or avoid them. This indicates that participants are not only prone to underestimating threats, but also to overestimating them in certain situations.

From the perspective of Signal Detection Theory (SDT), these behaviours can be interpreted as different types of decision errors, such as misses and false alarms (Martin, Dubé & Coovert, 2018). A miss occurs when a phishing email is not correctly identified as a threat, while a false alarm occurs when a legitimate email is treated as suspicious. The presence of

both types of errors in the results suggests that participants vary in how they balance risk when making decisions under uncertainty.

This highlights an important trade-off in phishing detection. A strategy that minimizes the risk of interacting with phishing emails may simultaneously increase the likelihood of ignoring legitimate communication. Conversely, a more open approach may improve responsiveness but increase exposure to potential threats. The findings therefore suggest that effective phishing detection is not solely about eliminating errors, but about managing the balance between different types of risk.

5.7 Over-Reliance on Avoidance Strategies

Closely related to this, the results indicate that many participants frequently chose to ignore emails as a default strategy. While this behaviour can be interpreted as cautious, it may also reflect an over-reliance on avoidance as a way of managing uncertainty.

Ignoring emails reduces the immediate risk of interacting with phishing attempts, and can therefore be seen as a protective behaviour. However, this strategy is not without limitations. In real-world contexts, users are often required to engage with emails in order to complete tasks, access services, or respond to important communication. A tendency to ignore emails indiscriminately may therefore lead to missed opportunities or important information being overlooked.

This suggests that while avoidance may be effective in reducing certain risks, it does not necessarily represent an optimal long-term strategy. Instead, effective email handling requires users to actively evaluate and differentiate between legitimate and malicious communication. The findings therefore highlight that secure behaviour is not only about minimizing interaction, but about making informed decisions regarding when and how to engage with digital content.

5.8 Limitations

Despite the contributions of this study, several limitations should be considered when interpreting the findings.

A key limitation relates to the structure of the questionnaire. Participants were able to navigate freely between the different sections, meaning that they could return to previous questions and modify their responses. As the survey gradually revealed its focus on phishing, it is possible that some participants became aware of the study's purpose during completion. This may have influenced their earlier responses, leading to more cautious or "correct" answers than would have been given under natural conditions. As a result, the findings may overestimate participants actual ability to identify phishing emails.

Furthermore, the study is based on hypothetical email scenarios rather than real-world behaviour. Although efforts were made to design realistic emails, participants were aware that they were part of a study, which may have influenced their decision making. In real life contexts, individuals are often subject to additional factors such as time pressure, multitasking and emotional stress, which are difficult to fully replicate in a survey setting. These factors

may affect how users respond to phishing attempts and could lead to different outcomes in practice.

Another limitation concerns the nature of the phishing scenarios used in the study. The emails included in the questionnaire were designed to reflect relatively common and recognizable phishing attempts. However, phishing techniques vary widely in sophistication, and more advanced attacks, such as highly personalized messages or more realistic AI-generated content, may be significantly more difficult to detect. As a result, the findings of this study may not fully capture users susceptibility to more complex or sophisticated phishing strategies.

Another limitation concerns the size of the sample. Although the study collected a sufficient number of responses to identify general patterns and tendencies, the total number of participants remains relatively limited. A larger sample size could potentially have provided more robust comparisons between groups and increased the reliability and generalizability of the findings. The relatively small sample size should therefore be taken into consideration when interpreting the results.

Another limitation concerns the sampling method. The study relies on non-probabilistic sampling, including elements of convenience and snowball sampling. As a result, the sample may not be fully representative of the broader student population. A large proportion of participants are likely drawn from similar educational and social contexts, which may influence the findings.

In addition, self-selection bias should be considered. Participation in the study was voluntary, meaning that individuals who chose to respond may differ systematically from those who did not. For example, participants may have a greater interest in digital communication or cybersecurity, which could lead to higher levels of awareness than in the general population.

Finally, while the study provides insights into participants behaviour and decision-making, it does not capture all aspects of phishing susceptibility. The results should therefore be interpreted as indicative rather than definitive, and understood within the context of the study’s design and limitations.

6 Conclusion

The purpose of this study was to investigate students awareness of phishing emails and examine whether perceived cybersecurity competence corresponds to the actual ability to identify phishing attempts. More specifically, the study aimed to compare the behaviour of students with different levels of IT education and explore how factors such as confidence, urgency and perceived importance influence decision making in phishing related situations.

The findings indicate that students generally demonstrate a cautious approach when handling suspicious emails. Across several phishing scenarios, ignoring the email was the most common response, suggesting that participants possess a basic awareness of phishing risks and common warning signs associated with malicious communication. At the same time,

unsafe behaviour remained present throughout the results, as participants in multiple scenarios still chose to interact with phishing emails. This suggests that awareness alone does not necessarily translate into secure behaviour in practice.

A central finding of the study concerns the relationship between confidence and actual performance. Many participants expressed relatively high confidence in their decisions, including in some situations where their chosen actions could be considered unsafe. This indicates that confidence is not always a reliable indicator of phishing detection ability and suggests that overconfidence may influence decision making in cybersecurity contexts. The results therefore support previous research suggesting that users may overestimate their ability to identify digital threats, even when their behaviour does not consistently reflect this competence.

The study also found that contextual factors appear to influence decision making. Emails perceived as urgent or personally relevant were more likely to trigger active responses in certain situations, indicating that phishing susceptibility is not solely determined by knowledge, but also by emotional and situational influences. This supports the idea that phishing attacks are effective not only because of technical deception, but because they exploit human behaviour and decision making processes.

When comparing IT and non-IT students, the findings revealed only limited differences between the groups. Although students with a higher level of IT education showed a tendency towards more secure behaviour, both groups displayed a mixture of correct and incorrect decisions. This suggests that technical knowledge alone is not sufficient to eliminate susceptibility to phishing attacks. Instead, the results indicate that behavioural and psychological factors play an important role regardless of educational background.

The theoretical frameworks used in this study further support this interpretation. Through TTAT and PMT, the findings suggest that individuals engage in cognitive evaluations of threats and coping strategies when interacting with emails. However, these evaluations do not always result in secure behaviour. The application of Signal Detection Theory additionally highlights how participants differ in their thresholds for evaluating uncertainty, with some adopting highly cautious strategies while others are more willing to engage with potentially risky emails.

Overall, the findings of this study suggest that phishing susceptibility should not be understood solely as a lack of technical knowledge. Rather, it appears to be shaped by a complex interaction between awareness, confidence, context and behavioural decision making. The results therefore highlight the importance of approaching cybersecurity awareness not only as a technical or educational issue, but also as a behavioural and psychological one.

Finally, the study contributes to a broader understanding of how students evaluate and respond to phishing attempts in a digital environment where cyber threats continue to evolve in sophistication. As phishing attacks become increasingly advanced and convincing, particularly through the use of AI-generated content and personalized communication, understanding the human factors underlying phishing susceptibility becomes increasingly important. Future research could therefore further investigate how users respond to more sophisticated phishing techniques and explore methods for improving not only awareness, but also decision-making and confidence calibration in cybersecurity contexts.

6.1 Further Research and Improvement Opportunities

Future studies could examine more advanced phishing techniques, including highly personalized phishing attacks and AI-generated phishing emails, as these are becoming increasingly common and sophisticated. In addition, longitudinal studies may provide insight into how phishing awareness and user behavior change over time, particularly following cybersecurity education or training.

Appendix 1: AI-bidragsredogörelse

Artificial intelligence tools were used to a limited extent during the completion of this bachelor's thesis. Specifically, ChatGPT was used as a supportive tool for language improvement, translation assistance and formulation of academic text throughout different sections of the thesis. The tool was also used to assist in generating examples of both phishing-related and legitimate emails that were included as part of the study material.

All AI-generated content was carefully reviewed, modified and adapted by the authors to ensure accuracy, relevance and consistency with the purpose and academic requirements of the study. ChatGPT was not used for data collection, statistical analysis or interpretation of the study results. The final responsibility for the content, analysis and conclusions of the thesis remains with the authors.

Appendix 2: Questionnaire questions

Vad är din könsidentitet? *

- ○ Man
- ○ Kvinna
- ○ Annat

Vad pluggar du? *

Short answer text

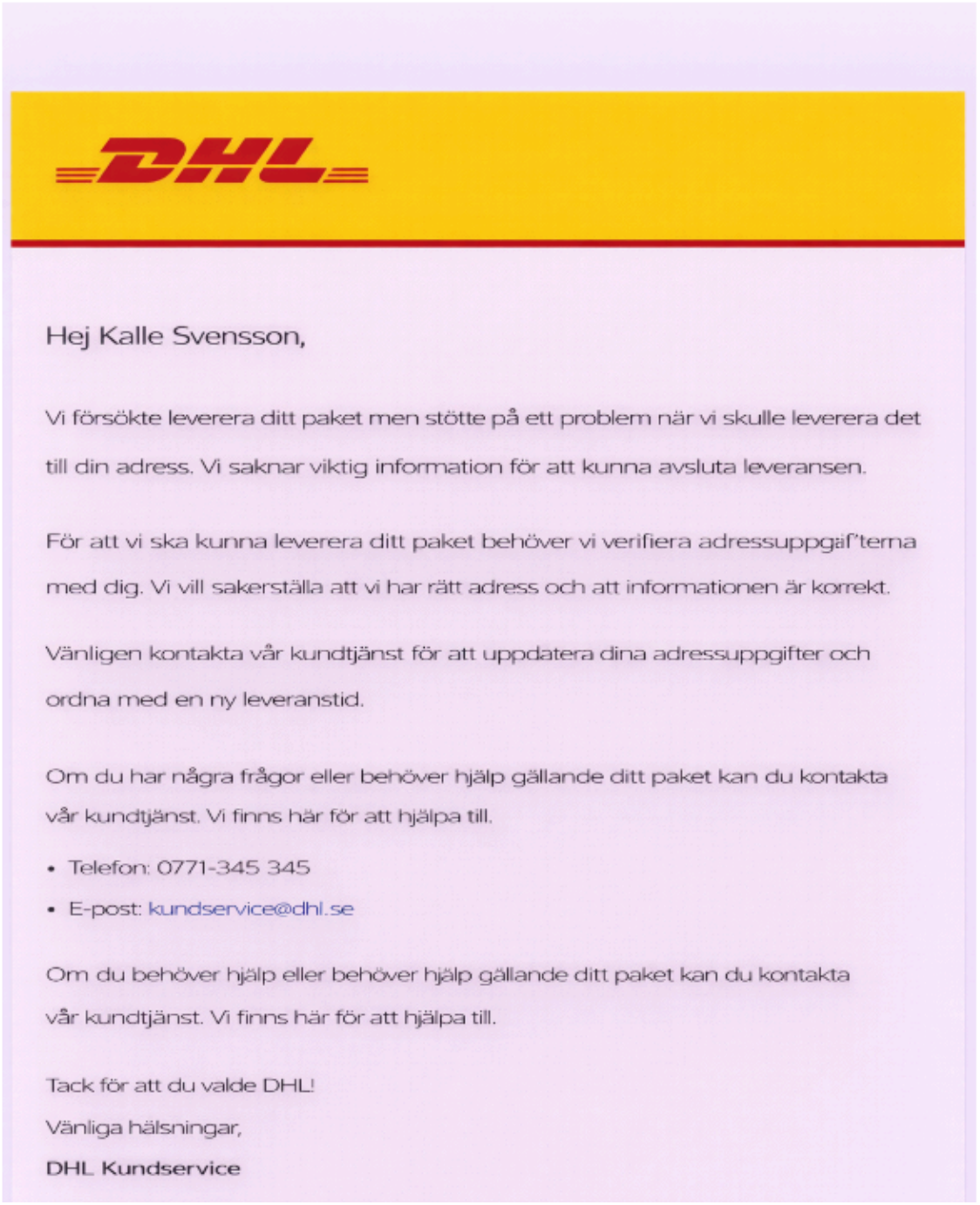
Till vilken grad har du lärt dig IT i din utbildning *

- ○ Ingen/låg
- ○ Medium
- ○ Hög

Föreställ dig att du snabbt kollar din e-post mellan föreläsningar. Hur skulle du hantera följande meddelanden?

Description (optional)

Vad skulle du göra med detta mail om du nyligen beställt från DHL? *



Hej Kalle Svensson,

Vi försökte leverera ditt paket men stötte på ett problem när vi skulle leverera det till din adress. Vi saknar viktig information för att kunna avsluta leveransen.

För att vi ska kunna leverera ditt paket behöver vi verifiera adressuppgäf'terna med dig. Vi vill sakerställa att vi har rätt adress och att informationen är korrekt.

Vänligen kontakta vår kundtjänst för att uppdatera dina adressuppgifter och ordna med en ny leveranstid.

Om du har några frågor eller behöver hjälp gällande ditt paket kan du kontakta vår kundtjänst. Vi finns här för att hjälpa till.

- Telefon: 0771-345 345
- E-post: kundservice@dhl.se

Om du behöver hjälp eller behöver hjälp gällande ditt paket kan du kontakta vår kundtjänst. Vi finns här för att hjälpa till.

Tack för att du valde DHL!
Vänliga hälsningar,
DHL Kundservice

- ○ Kontakta kundtjänst genom att trycka på E-post länken
- ○ Kontakta kundtjänst på egen hand
- ○ Ignorera det
- ○ Anmäla mailet som misstänkt till din e-postleverantör

Hur säker är du på ditt beslut *

	1	2	3	4	5	
Inte säker alls	○	○	○	○	○	Väldigt säker

Hur brådskande känns detta mail? *

	1	2	3	4	5	
Inte alls brådskande	○	○	○	○	○	Väldigt brådskande

Varför anser du att det var bästa sättet att agera? *

Long answer text

Vad skulle du göra med detta mail om du har en aktiv Netflixpreunmeration? *

NETFLIX

Hej Kalle Svensson,

Vi kunde inte debitera automatiskt från din betalningsmetod för den senaste betalningen. Om problemet kvarstår kommer ditt Netflix-konto att pausas.

För att undvika avbrott, vänligen skanna QR-koden nedan för att uppdatera dina betalningsuppgifter.

Skanna för att uppdatera betalningsinformation

Behöver du hjälp? Om du behöver support eller har några frågor, besök vårt hjälpcenter eller kontakta vår kundtjänst.

- ○ Skanna QR-koden
- ○ Ignorera det
- ○ Anmäla mailet som misstänkt till din e-postleverantör

Hur säker är du på ditt beslut? *

	1	2	3	4	5	
Inte alls säker	○	○	○	○	○	Väldigt säker

Hur brådskande känns detta mail? *

	1	2	3	4	5	
Inte alls	○	○	○	○	○	Väldigt

Vad gör du med detta mail om du har ett bankkonto på Swedbank? *

Swedbank

Hej Kalle Svensson,

Vi har upptäckt misstänkt aktivitet på ditt Swedbank-konto och misstänker att obehöriga kan ha försökt få tillgång till det.

För att skydda ditt konto måste vi verifiera din identitet omgående.

För att snabbt bekräfta att du är kontoinnehavaren, vänligen skicka ett svar till denna e-post och bekräfta följande uppgifter:

- Fullständigt personnummer
- Kontonummer eller kortnummer
- Din senaste transaktion

Observera: Om vi inte mottar ditt svar omgående kan ditt konto komma att låsas för säkerhetsändamål.

Med vänliga hälsningar,
Swedbank Säkerhetsavdelningen

- ◯ Skickar ett svar med vad Swedbank efterfrågar
- ◯ Ignorerar det
- ◯ Anmäler mailet som misstänkt till din e-postleverantör

Hur säker är du på ditt beslut? *

	1	2	3	4	5	
Inte alls säker	◯	◯	◯	◯	◯	Väldigt säker

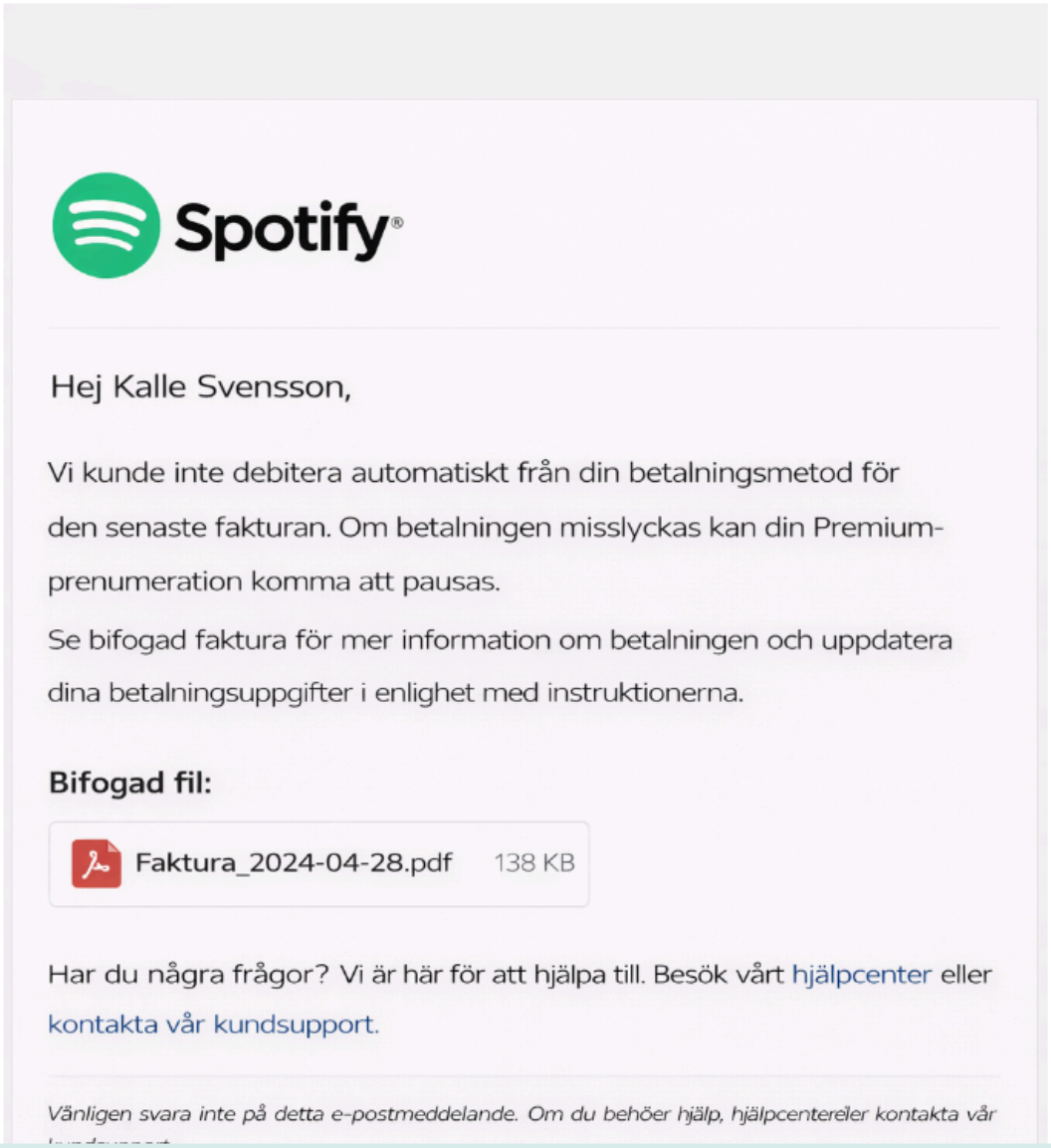
Hur brådskande känns detta mail? *

	1	2	3	4	5	
Inte alls	◯	◯	◯	◯	◯	Väldigt

Varför anser du att det var bästa sättet att agera? *

Long answer text

Vad gör du med detta mail om du har en aktiv prenumeration på Spotify? *



Spotify®

Hej Kalle Svensson,

Vi kunde inte debitera automatiskt från din betalningsmetod för den senaste fakturan. Om betalningen misslyckas kan din Premium-prenumeration komma att pausas.

Se bifogad faktura för mer information om betalningen och uppdatera dina betalningsuppgifter i enlighet med instruktionerna.

Bifogad fil:

Faktura_2024-04-28.pdf 138 KB

Har du några frågor? Vi är här för att hjälpa till. Besök vårt hjälpcenter eller kontakta vår kundsupport.

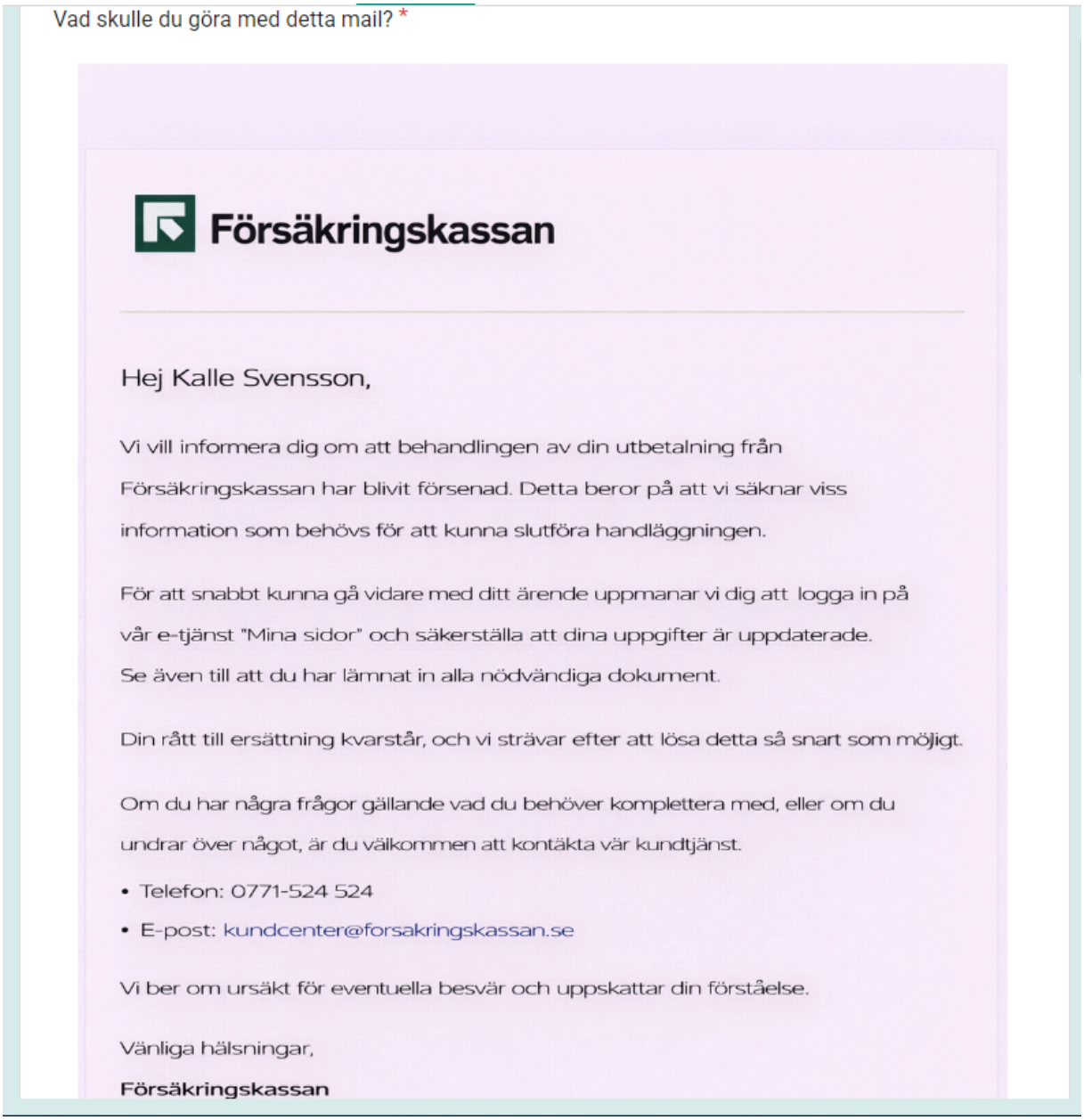
Vänligen svara inte på detta e-postmeddelande. Om du behöer hjälp, hjälpcentereler kontakta vår

- ○ Trycker på bifogad faktura
- ○ Ignorerar det
- ○ Anmäler mailet som misstänkt till din e-postleverantör

Hur säker är du på ditt beslut? *

	1	2	3	4	5	
Inte alls säker	○	○	○	○	○	Väldigt säker

Vad skulle du göra med detta mail? *



Försäkringskassan

Hej Kalle Svensson,

Vi vill informera dig om att behandlingen av din utbetalning från Försäkringskassan har blivit försenad. Detta beror på att vi saknar viss information som behövs för att kunna slutföra handläggningen.

För att snabbt kunna gå vidare med ditt ärende uppmanar vi dig att logga in på vår e-tjänst "Mina sidor" och säkerställa att dina uppgifter är uppdaterade. Se även till att du har lämnat in alla nödvändiga dokument.

Din rått till ersättning kvarstår, och vi strävar efter att lösa detta så snart som möjligt.

Om du har några frågor gällande vad du behöver komplettera med, eller om du undrar över något, är du välkommen att kontäkta vär kundtjänst.

- Telefon: 0771-524 524
- E-post: kundcenter@forsakringskassan.se

Vi ber om ursäkt för eventuella besvär och uppskattar din förståelse.

Vänliga hälsningar,

Försäkringskassan

- ◯ Logga in på mina sidor och säkerställa mina uppgifter
- ◯ Ignorera det
- ◯ Anmäla mailet som misstänkt till din e-postleverantör

Hur säker är du på ditt beslut? *

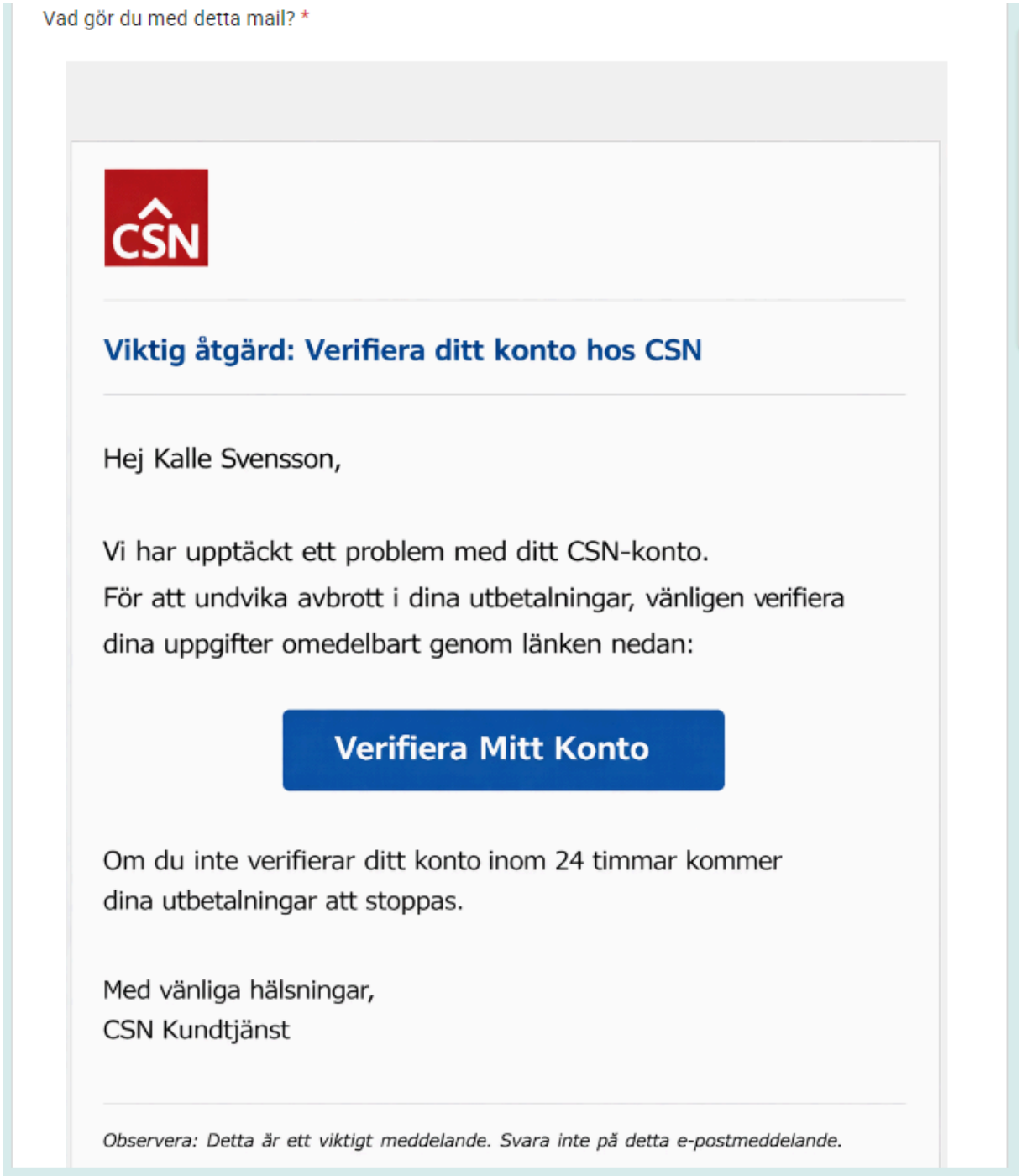
	1	2	3	4	5	
Inte alls säker	◯	◯	◯	◯	◯	Väldigt säker

*

Hur viktigt känns detta mail?

	1	2	3	4	5	
Inte viktigt alls	◯	◯	◯	◯	◯	Väldigt viktigt

Vad gör du med detta mail? *



- ○ Verifierar mitt konto på knappen
- ○ Ignorerar det
- ○ Anmäler mailet som misstänkt till din e-postleverantör

Hur säker är du på ditt beslut? *

	1	2	3	4	5	
Inte alls säker	○	○	○	○	○	Väldigt säker

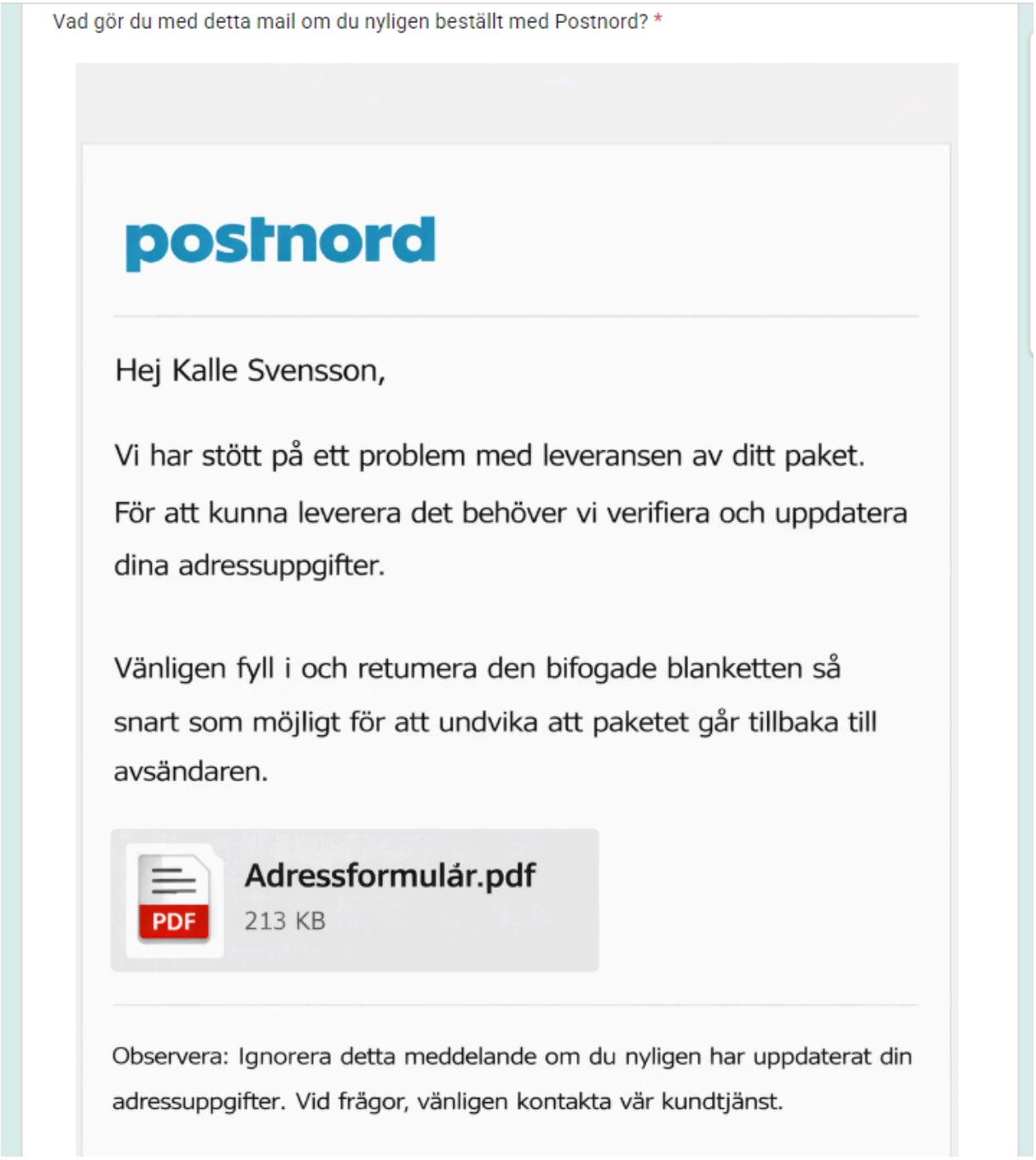
Hur viktigt känns detta mail? *

	1	2	3	4	5	
Inte alls viktigt	○	○	○	○	○	Väldigt viktigt

Varför anser du att det var bästa sättet att agera? *

Long answer text

Vad gör du med detta mail om du nyligen beställt med Postnord? *



- ○ Trycker på adressformuläret, fyller i och skickar tillbaka
- ○ Ignorerar det
- ○ Anmäler mailet som misstänkt till din e-postleverantör

Hur säker är du på ditt beslut? *

	1	2	3	4	5	
Inte alls säker	○	○	○	○	○	Väldigt säker

Section 3 of 3

Del 2

Nätfiske (phishing) är en form av bedrägeri på nätet där angripare utger sig för att vara en legitim aktör, ofta via e-post eller sms, med syfte att lura till sig känslig information som lösenord, kortuppgifter eller bank-id.

Har du drabbats av phishing någon gång? *

- ○ Ja
- ○ Nej

Hur bedömer du risken för att själv bli utsatt för ett phishing försök? *

	1	2	3	4	5	
Väldigt låg	○	○	○	○	○	Väldigt hög

Hur allvarliga konsekvenser tror du att ett phishing-mail kan få för dig personligen? *

	1	2	3	4	5	
Inte så allvarliga	○	○	○	○	○	Väldigt allvarliga

Har du någon strategi eller tumregel för att inte bli drabbad av phishing? *

Short answer text

Hur besvärligt upplever du det att behöva kontrollera mejl noggrant för att undvika phishing? *

	1	2	3	4	5	
Väldigt besvärligt	○	○	○	○	○	Inte besvärligt

Hur anser du att din utbildning har påverkat dina val? *

Long answer text

Referenser

Alotaibi, L., Seher, S. & Mohammad, N. (2024). Cyberattacks Using ChatGPT: Exploring Malicious Content Generation Through Prompt Engineering, *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*, Available Online: https://ieeexplore.ieee.org/

Barney, N. (2023). Definition: deepfake AI (deep fake), *TechTarget*, Available Online: https://www.techtarget.com/whatis/definition/deepfake

Butavicius, M., Parsons, K., Pattinson, M., McCormac, A., Calic, D. and Lillie, M., (2017). Understanding susceptibility to phishing emails: Assessing the impact of individual differences and culture. In: *Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017)*,

Chen, D. Q. & Liang, H. (2019). Wishful Thinking and IT Threat Avoidance: An Extension to the Technology Threat Avoidance Theory, *IEEE Transactions on Engineering Management*, vol. 66, no. 4, pp.552–567

Corradini, I. (2020).Building a Cybersecurity Culture in Organizations. Cham: Springer.

Cybersecurity Tech Accord (2021) *Cybersecurity Awareness in the Commonwealth of Nations*.

Das, S., Nippert-Eng, C. & Camp, L. J. (2022). Evaluating User Susceptibility to Phishing Attacks, *Information & Computer Security*, vol. 30, no. 1, pp.1–18

Diaz, A., Sherman, A.T. and Joshi, A., (2020). Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia*, 44(1), pp.53–67.

Jamil, H., Zia, T., Nayeem, T., Whitty, M. T. & D'Alessandro, S. (2024). Human-Centric Cyber Security: Applying Protection Motivation Theory to Analyse Micro Business Owners' Security Behaviours, *Information & computer security*, vol. 33, no. 1

Knaflic, C. N. (2015). Storytelling with Data: A Data Visualization Guide for Business Professionals, Hoboken, New Jersey: Wiley

Kolata, G., 2017. Many academics are eager to publish in worthless journals. *The New York Times*, 30 October. Available at: https://web.archive.org/web/20171108014011/https://www.nytimes.com/2017/10/30/science/predatory-journals-academics.html [Accessed 23 April 2026].

Martin, J., Dubé, C. & Coovert, M. D. (2018). Signal Detection Theory (SDT) Is Effective for Modeling User Behavior toward Phishing and Spear-Phishing Attacks, *Human*

Factors: The Journal of the Human Factors and Ergonomics Society, vol. 60, no. 8, pp.1179–1191

Mwangala, J., Bhunu Shava, F. and Chitauro, S. (2023). *Human Intelligence as an Enabler for Cyber Resilience: A Case for Namibian Public Institutions*. IST-Africa Conference. Available at: https://ieeexplore.ieee.org/document/10187836

National Cyber Security Centre (2018). *Phishing attacks: Defending your organisation*. Available at: NCSC phishing guidance

Oates, B. J., Griffiths, M. & Mclean, R. (2022). Researching Information Systems and Computing., Los Angeles: Sage

Ribeiro, L., Guedes, I. S. & Cardoso, C. S. (2023). Which Factors Predict Susceptibility to Phishing? An Empirical Study, *Computers & Security*, [e-journal] vol. 136, Available Online: https://www.sciencedirect.com/science/article/pii/S0167404823004686

Rohan, R., Funilkul, S., Pal, D. and Chutimaskul, W. (2021). *Understanding of Human Factors in Cybersecurity: A Systematic Literature Review*. Proceedings of the 2021 International Conference on Computational Performance Evaluation (ComPE). Available at: https://doi.org/10.1109/ComPE53109.2021.9752358

Shahbazi, Z., Jalali, R. & Molaeevand, M. (2025). AI-Based Phishing Detection and Student Cybersecurity Awareness in the Digital Age, *Big Data and Cognitive Computing*, [e-journal] vol. 9, no. 8, p.210, Available Online: https://www.mdpi.com/2504-2289/9/8/210

Tallapally, S. K., Mahesh, D., Rohith, B., Sandhya, K. S., Rajitha, K. & Sohail, M. (2025). Explainable Deep Learning Models for Phishing Email Detection, *2025 International Conference on Sustainable Communication Networks and Application (ICSCN)*, [e-journal] pp.2079–2085, Available Online: https://ieeexplore.ieee.org/abstract/document/11308654/ [Accessed 27 March 2026]

Thomson, S., Bewong, M., Mahboubi, A. & Zia, T. (2025). Social Engineering Attacks: A Systemisation of Knowledge on People against Humans, *ArXiv.org*, Available Online: https://arxiv.org/abs/2601.04215

Wang, J., Li, Y. & Rao, H. R. (2016). Overconfidence in Phishing Email Detection, *Journal of the Association for Information Systems*, [e-journal] vol. 17, no. 11, pp.759–783, Available Online: https://core.ac.uk/download/pdf/301380468.pdf

Workman, M. (2007). 'Gaining access with social engineering: an empirical study of the threat', *Information Systems Security*, 16(6), pp. 315–331. Available at: https://doi.org/10.1080/10658980701788165