Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Bjørn B Bilet

Security awareness training as a countermeasure to phishing attacks

Master's thesis in MIS4900
Supervisor: Einar Arthur Snekkenes
December 2020

NTNU
Norwegian University of
Science and Technology

Bjørn B Bilet

Security awareness training as a countermeasure to phishing attacks

Master's thesis in MIS4900
Supervisor: Einar Arthur Snekkenes
December 2020

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Abstract

This research project will investigate the effect of education and training to combat phishing attacks. The prevalence and sophistication of cyberattacks continue to increase, affecting private users, businesses, organizations, and government networks. One of the greatest cyberthreats and reason for security breaches comes from phishing; a cyberattack disguised as a harmless email.

The email asks the recipient to perform an action, such as clicking on a malicious link, typically to get a reward or to handle a problem. There are several techniques criminals use to deceive people. All of them, however, tends to fool the victim by exploiting human traits like *panic, excitement, curiosity, obligation, or empathy* so they perform the wanted act. The main goal is usually to steal data, either to get a competitional advantage, for espionage or for economic gain. The latter they do by tricking the victim to do a direct wire transaction, freezing the system as part of a ransom attack, or by using stolen personal, or corporate information at a later stage.

There are many technical measures a company may use to protect themselves from phishing attacks. This project, however, will focus on security awareness and training of individuals. At some point all of us will most likely receive a phishing email of some sort. In the end, it is the user clicking on the fraudulent links, giving away information or performing an unwanted action, that is the biggest security risk.

My research consists of unannounced phishing attacks against Gjøvik municipality's employees, mapping their resilience against such attacks. I tried to educate the users about phishing-emails with online information, hoping that would raise their awareness. When the training was completed, more phishing emails were sent out, at a monthly interval. As such, I could track how well the users retained knowledge gained from training over time, and hopefully get enough data to see at what intervals training is needed to maintain an acceptable security information awareness against these kinds of attacks.

This project also mapped users from different departments within the municipality, to see if any one group of workers are more susceptible to this kind of attack than others. This information may be valuable to the municipality to see who are the most vulnerable and where resources should be used, such as training and education.

Sammendrag

Denne oppgaven har til hensikt å undersøke effekten av opplæring som ett forsvar mot phishing-angrep via e-post. En av de vanligste formene for angrep i dag er phishing, og dette er ofte angriperens første steg inn i virksomhetens datanettverk. Ofte bes mottaker om å utføre en handling for å motta en belønning, eller for å hindre en negativ konsekvens. De kriminelle spiller ofte på menneskelige egenskaper som *frykt, opprømthet, nysgjerrighet, pliktoppfyllenhet* eller *empati* for å få mottaker til å utføre handlingene det bes om. Målet er som regel å få tak i informasjon, enten for å en fordel i markedet, for spionasje eller for økonomisk vinning. Det siste oppnås enten i form av at ansatte lures til å overføre penger direkte, eller ved å bruke personlig eller bedriftssensitiv informasjon som pressmiddel.

Det finnes i dag mange tekniske løsninger for å beskytte seg mot phishing-angrep, men denne oppgaven setter søkelys på opplæring og sikkerhetsbevissthet hos mennesker som forsvar. I en arbeidssituasjon vil alle kunne forvente å måtte motta og besvare e-post. Det vil være helt umulig for en teknisk løsning å luke ut alle phishing e-postene som kommer, uansett hvor sofistikerte de er. Det er brukeren som leser e-posten og som til syvende og sist er den største sikkerhetsrisikoen.

For å undersøke dette har jeg utført uannonserte phishing-angrep på alle ansatte i Gjøvik kommune, for å finne ut hvor sårbare de er for phishing. Deretter har jeg gitt alle ansatte en kort opplæring i hvordan behandle e-post og kjenne igjen phishing-angrep.

Til slutt har jeg fortsatt med jevnlige phishing-angrep på månedlig basis, for å se om effekten av opplæring forsvinner over tid, eller om de gjentatte angrepene gjør brukerne mer motstandsdyktige og på vakt. Målet med dette er å finne ut hvor ofte opplæring bør gis for å opprettholde ett akseptabelt nivå på sikkerhetsbevisstheten til de ansatte.
Et sekundært mål er å kartlegge om det er brukere fra en gitt sektor i kommunen som er mer mottagelige for phishing-angrep, slik at disse kan få målrettet opplæring.

Acknowledgments

I would like to express my appreciation for my supervisor, Einar Arthur Snekkenes. Even though the communication from my side has been sporadic at best, I have always gotten quick replies and valuable advice and guidance for my work on this thesis.

I also want to thank my wife for motivating and helping me get through this thesis. Her inputs to the form and language of the thesis has been invaluable.

I would also like to thank my younger brother for helpful discussions and assistance with the programming used for the phishing site, as well as valuable guidance in the more advanced workings of Microsoft excel. Also, my big brother for helpful feedback and proofreading of the thesis.

Lastly, friends supporting me by reading the paper and giving me valuable feedback.

Contents

List of Figures

List of Tables

Abbreviations

TLS	Transport Layer Security
STARTTLS	Command to start using TLS on an insecure connection
DKIM	DomainKeys Identified Mail
SPF	Sender Policy Framework
DMARC	Domain-based Message Authentication, Reporting and Conformance

Chapter 1 - Introduction

Topics covered by the project

In today’s business environment e-mail has become the de facto standard for communication. Depending on what kind of work or business you have, your employees potentially handle hundreds of e-mails every day. In a hectic work environment, not every e-mail is read and scrutinized before action is performed. This can often lead to users performing unwanted actions without being aware of it. These actions can in turn put their employer at risk, inflicting economical or reputational damage.

There are a lot of technical measures available to protect your network against phishing. Examples include STARTTLS, SPF, DKIM and DMARC to name a few (Nasjonal Sikkerhetsmyndighet u.d.). Nevertheless, no matter how well you configure your network, or how much money you invest on software and hardware, your employers need to receive emails to be able to their job. Some of the fraudulent e-mails will end up in the user’s mailbox. For this reason, educating and training in order to create higher awareness among users is key.

In conducting my research, I have used employees from Gjøvik municipality. Gjøvik municipality is situated in Norway and has about 3500 employees. These people work in different departments with different responsibilities, work hours, backgrounds, and education. This gave me a representative sample for my tests.

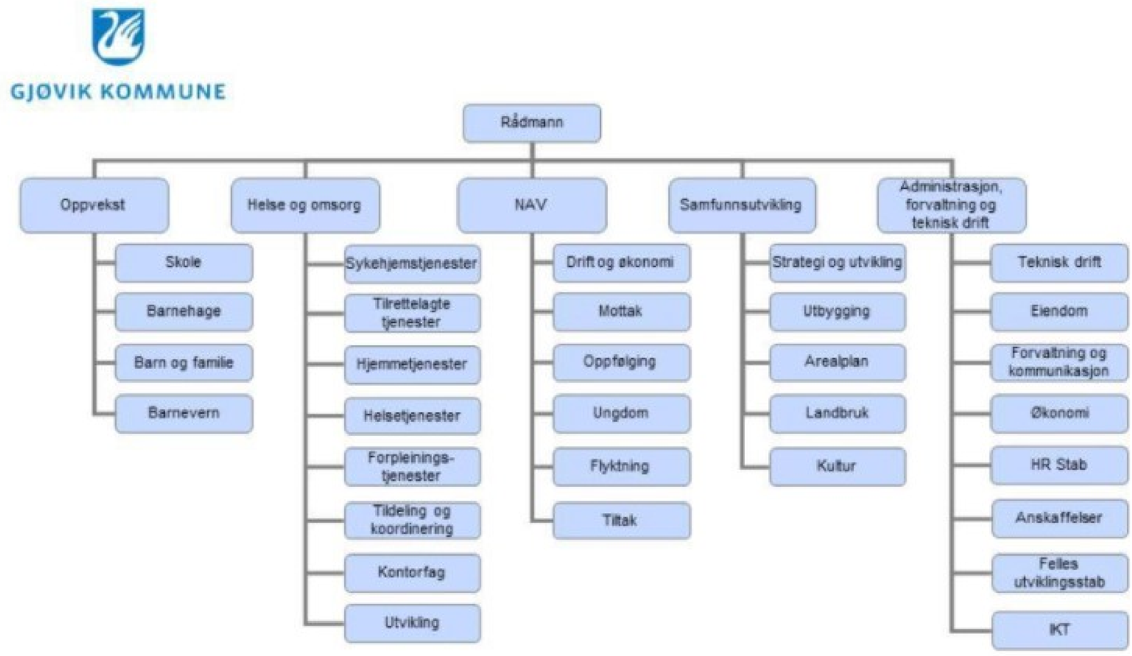


Figure 1 The structure of Gjøvik municipality

The first thing I did was an initial phishing test. The aim was to get the users to type their username after clicking on a fraudulent link in an e-mail. The results gave a base line indication of their security awareness. In addition, usernames were gathered and based on this, I could track in what part of the municipality they work. This information was used to analyze which groups were more susceptible to this kind of attack. This data is valuable for the municipality when they are deciding where to make an extra effort and invest on security awareness measures.

When constructing the various phishing emails, different approaches was used. Most emails contained information known to the recipients and expected to arrive in their mailbox. It was also linked to certain happenings in time, such as local wage negotiations, seasonal events, and holidays, to get the employees attention.

The emails were written in such a way that it could have been written by a real cybercriminal – an outsider with no access to internal information from the municipality. I did not rely on information from my contacts within the municipality to write with "spear phishing[1] accuracy", rather I wanted the employees to have a decent chance of figuring out that this could be a fraudulent email. The reason for this is that most phishing emails are built this way. The well-made spear phishing emails usually target people in higher positions, with access to funds, or with administrative privileges. These attacks are by far more advanced and harder to detect. This research project, however, focus on general spear phishing emails and the education required to recognize these. Once most users understand the basics of this, further training can be applied to the most vulnerable users.

After the initial test, each employee was given access to an online educational material, aimed to raise awareness regarding phishing attacks. Following this training, more phishing e-mails were sent out to monitor how the users performed, in order to see at what rate the effect of the training diminished.

The results will also show which departments are the most vulnerable to phishing emails. But why so, will not be answered. I have no background information about the employees' education, experience, or prowess when it comes to information security. Regardless, the results will give Gjøvik municipality a better idea as to where they should make

[1] Spear phishing is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons. This is achieved by acquiring personal details on the victim such as their friends, hometown, employer, locations they frequent, and what they have recently bought online

investments to strengthen their employees' knowledge regarding information security, including phishing emails.

The results will also indicate which employees repeatedly failed the tests, allowing the municipality to address them for further information security education. When we know that it takes only one person to fall for a phishing email for it to be a success, every employee counts.

Keywords

Phishing attacks, social engineering, malicious links, login credentials, e-mail, identity theft, spam, electronic mail, computer crime, computer hacking, social network, fake webpages, personal information, spoofing emails, crime, suspicious email, security, phishing.

Problem description

The main research question in this thesis is as follows: *what is the effect of education and training to raise user awareness as a counter measure to phishing attacks?* We know that with time, the effect of training and education diminishes. The interesting part is finding the threshold where training must be repeated to maintain an acceptable level of awareness. This in turn may help businesses, organizations and governments plan their training regime and make sure their investment is not wasted on too much, nor too little training.

On the other hand, this research could potentially reveal that there is little, or no measurable gains in providing training or working on employee education in information security and awareness. Such a result will also be considered a success.

No matter what the results will be, we can gain some understanding about the success rate of phishing attacks on different groups of individuals. There is a wide range of people within different departments that will be tested, and it will be interesting to see if any one group is more susceptible to phishing attacks than others.

I will also analyze the different subjects of the phishing emails and try to see if there is a particular trait that is easier to take advantage of, or if there is little to no correlation between how the email is written, its content, and how many people will click the link.

Justification, motivation, and benefits

A successful phishing attack may have severe impact on the businesses, organizations or governments affected. The repercussions may be economic losses, reputational damage, loss of classified government information and so on. The conclusions drawn from this research will not provide all the answers to avoid phishing attacks. However, it will highlight some important factors which can contribute to the fight against phishing.

Businesses and organizations invest a lot of money on counter measures, and potentially more so after recovering from a successful attack. An insight into the effects of training and the rate of decline in employee's awareness over time will help businesses make sound decisions about their training programs. This will in turn improve their security and save money. Previous research has discovered that well designed end-user security education can be effective (Le Compte 2015); (P. R. Kumaraguru 2007); (P. R. Kumaraguru 2007); (P. S. Kumaraguru 2010); (Sheng 2007)

Lastly, I hope my research was beneficial for the participants involved. I hope that they gained some knowledge and are now more cautious when handling emails at work and private.

Research questions

The research questions I aim to answer in this thesis are as follows:

- *After conducting information security awareness training, how long does it take for the effect to diminish, and to what degree does it diminish over time?*
- *How often do you have to run information training campaigns for it to have any measurable effect?*
- *In a multi group environment, is there a certain type of users that is more susceptible to phishing attacks then others (management, accounting, maintenance, nurses, teachers etc.)?*
- *How will the exploitation of different human traits affect the success-rate of a phishing attack?*

Planned contributions

Once the work is completed, businesses and others can use the results when making decisions on defensive measures against phishing attacks. Is it worth investing in training and educating employers, or is it better to invest in other countermeasures? The results will also help businesses and others make decisions regarding the frequency of training programs to get the desired effect. Lastly, the results will also show who are more vulnerable to phishing attacks, and help target the training towards the groups that need it the most.

The municipality used in this study (Gjøvik) will hopefully gain valuable information about their employees and their vulnerability towards phishing. This information can be used to tailor educational and awareness programs in a way that achieve increased security without necessarily increasing costs. However, if the results indicate training has in fact no large impact on combating phishing threats, they can use this knowledge to allocate their resources towards better technical solutions instead.

Related work

Existing studies on phishing attacks vary from phishing websites and phishing e-mails to phishing SMS'. Some of it focused on the use of programs, add-ons and devices for automated phishing protection or detection, whilst others are more targeted towards the mental state of the victim, and why they have fallen for the phishing email. Most of what I found however, was quite old, and some information was outdated.

Some of the relatively newer studies focused on the benefit of education for countering the problem of phishing. All of these were performed using relatively small sample sizes compared to what I have used in my research. Therefore, I hope that my work can contribute to the information security field with some new and updated information.

After conducting information security awareness training, how long does it take for the effect to diminish, and to what degree does it diminish over time?
How often do you have to run information training campaigns for it to have any measurable effects?

In "Phishing for user security awareness" (C. Dodge Jr. 2007) the results of recurring awareness programs show that the longer the programs run, the better the participants get at both avoiding to act on a phishing e-mail and reporting fraudulent e-mails. This article is the closest I have found to deal with these two research questions. This article, however, is almost 15 years old, so I expect to contribute with some updated results.

In a multi group environment, is there a certain type of user that is more susceptible to phishing attacks than others (management, accounting, maintenance, nurses, teachers etc)?

I have not found any literature that explores this research question, but there is literature on understanding phishing victims' profiles. "Towards understanding phishing victims' profile" (A. Darwish 2012) has summarized a lot of research in this area and have found that there is a connection between the victims age, gender, education, personality and the victims' internet usage behavior. This information can also be used by corporations and businesses to tailor their education so that the most susceptible users get the best education possible. On the other hand, this information can also be used by criminals to design their phishing attacks so that they target the vulnerable part of the population and tailor their e-mails so the receiver is more likely to fall for the phishing e-mail.

How will the exploitation of different human traits affect the success rate of a phishing attack?

In "Exploring susceptibility to phishing in the workplace" (Emma J. Williams 2018) they find that familiarity with the sender will increase the likelihood that the user will click on a link or otherwise do what the criminals want. The article also looks at the likelihood of clicking based on expectations, the work context, exposure to external emails and many more attributes.

Choice of methods

One of the projects main tasks is to collect enough data and information so that valid conclusions can be made. To analyze the data, a quantitative method was used. In my study 3432 participants received phishing emails 4 times (including the initial test) over a period of 4 months. After completing the 4 rounds of tests, the data was analyzed, and a conclusion was drawn.

The research questions were classified into three categories:

The first category addressed the success of the phishing tests before and after specific training was given. The users received a phishing email and then, after some weeks, they got a tailored educational package giving them information about the phishing test and specific guidance on how to avoid being deceived by phishing emails. Every month for 3 mounts a new phishing test was sent out to track the effect of the training (educational package) over time.

The second category addressed the demography of the users. I wanted to see if there was any difference in the results among the different areas within the municipality. I categorized what part of the organization the different participants worked, based on their username. All the data collected from this category was also analyzed quantitatively, using graphs and tables to visualize the outcome.

The third category took a closer look at how phishing e-mails are written, which human trait they seek to exploit, and if there is a connection between these, and the amount of people falling for the phishing e-mails.

Ethical and legal considerations

I have sent out phishing e-mails to participants with the aim to lure them into a specific action against their better judgement. It was crucial that the tests were unannounced so that the results would be as close to a real-world scenario as possible. As such, ethical and legal considerations was made before starting the phishing tests.

I had meetings with the IT department and the project manager at Gjøvik municipality about this. The response from them was that the tests were within the scope of what the municipality are allowed to do, without informing their users. The data I collected from the participants during these phishing tests, was stored on Gjøvik municipality's computer network, where I was given access. It was only the usernames that was stored. According to "Norsk senter for forskningsdata" (NSD) research where only the usernames are stored, does not warrant a notification. In the final report none of the data collected has been published. Further all the data used is aggregated and cannot be traced back to a single user.

The impact of covid-19

As I started my research in January 2020, covid-19 was an unknown variable. I had taken into consideration a lot of other disturbances, but a pandemic was not one of them.

The impact of the covid-19 virus' restrictions to my research has been quite severe. In March when the outbreak begun, my plan was to begin to send out the first phishing email. After speaking with the administration at the municipality we concluded that this was not a good time for them. Sending out fake phishing emails would generate more work and potential worry for people trying to cope with a new normal.

We decided to postpone till June to send the first email, 3 months after schedule. In addition, the education program was supposed to be sent out at this time, but due to the constant demands of covid-19 and the summer holiday, the municipality wanted to wait with this until after the summer holidays. The information package was therefore not sent out until mid-august. This left me with only 3 more months to send out phishing emails and gather data. The covid-19 situation then started to get worse again early winter and things slowed down again. In the end I had to send out two phishing emails during the last month to get enough data.

Chapter 2 - Background

This chapter aims to give some background into the field of email phishing.
The word phishing originated around 1996 and was used by hackers stealing America Online accounts and passwords. The word refers to the act of fishing, where you have a hook with bait that you throw out into the water, to try and catch fish. In computers, the fish are the victims, the bait is the e-mail, and the sea is the internet. As hackers often exchange the letter f with ph, the word phishing emerged.

Phishing is now a term covering different kinds of methods or attacks trying to achieve the same outcome, mainly luring the victim into disclosing sensitive information or performing an action putting them or their employer at a disadvantage. There are different techniques that are used to fool people with phishing, but all of them have one thing in common, they use human traits like panic, excitement, curiosity, obligation, or empathy to lure victims into performing the wanted action. A lot of effort has been dedicated to resolving the phishing threat with technical solutions, but little has been done in the area of educating users to protect themselves from phishing attacks. (Kirlappos 2012)
According to Europol (Europol 2019) "Social engineering, and in particular phishing, overwhelmingly represented the most significant cross-cutting cyber-threat faced by both European cybercrime investigators, and the most significant cyber-threat overall by Europol's private sector partners". This shows us the importance of taking the phishing threat seriously.

Different types of phishing

Below I will give a brief overview of the different methods used for phishing.

Website phishing

This method focuses on luring a victim to a fake or compromised website and making them either click on infected links, download infected files, or give up sensitive information like credit card numbers, social security numbers or other identification such as usernames and passwords. This method is often used together with phishing emails, where you get an email with a link to a known site or service. When you click on the link you are taken to the attacker's site, which is a duplicate of the original site. Everything you do from here on, the attacker will know about and record.

Previously, the common advice given to users was to look for the padlock sign in the address field. If this were present, the site was safe, and you could offer up your login credentials or personal information. This is not the case anymore. More and more phishing sites now use their own encryption, giving them the padlock symbol in the address field. This gives the victims a false sense of security because they think their information is safe and that no one can "listen in" on the data they enter. This is true to a certain degree since the information is in fact encrypted. But the criminals that devised the attack are the ones with the decryption key, so they can read everything in clear text.

Email phishing

Email phishing is what my master thesis focuses on. This is the act of sending someone an email with the purpose of luring them to do something that benefits you. There are different ways to do this, as explained below.

Generic email phishing

The easiest method is to compose a generic email and send it out to a large number of people. This way there is a big chance that at least some of the people follows the instructions, hence doing what the attacker wants them to do. We have seen emails like this for decades. Almost everyone is familiar with the email telling you to transfer a relatively small amount of money to a bank account, so that you can receive a much larger sum, so called Nigeria letters. Or the ones that supposedly comes from a friend who is stranded at an airport somewhere and need money to get home. There are endless variations of these emails.

Another, relatively new type of generic phishing email is the one disguised as coming from an established and trusted organization or institution (Greitzer 2014). This type of email is increasingly featuring logos and website links that appear legitimate (Workman 2008).

An effective way to compose these phishing emails is by using real world events in the narrative to make it seem more realistic (Freiermuth 2011) or exploiting social norms and obligations (Button 2014); (Cialdini 2006); (Karakasiliotis 2006); (Modic 2013); (Office of Fari Traiding 2009); (Raman 2008); (Stajano 2011).

Since there is always someone out there that is compromised by these phishing emails, there is always a market for perpetrators to continue committing these crimes. The costs and resources for the criminals are minimal, the chances of getting caught are small, and the payback can be large.

Spear phishing

Spear phishing is a more precise or targeted form of email phishing, targeting a specific individual, organization, or business. These phishing emails are the biggest threat to any organization. The attacker has placed a large amount of effort into making a spear phishing email, by gathering information on the target to tailor the email and give it the best chance of success. These emails are not generic and rarely have the typical grammatical errors or bad language usage we see in the generic ones. The sender is often also hidden behind an alias looking like a known or friendly source, or it could be from another compromised account that is trusted.

The aim of a spear phishing attack is much the same as for the generic attacks, except that they are more likely after a bigger economical gain or a foothold inside the targeted user's domain.

My method is a light form of spear phishing as I will pose as coming from inside the organization itself, either from HR, communications or from the IT department. However, as mentioned earlier I did not write the emails with "spear phishing accuracy", as I wanted the employees to have a decent chance of figuring out that this was a fraudulent email.

Countermeasures

There are two main ways of defense against an email phishing attack, a technical approach, and a human approach. I will briefly touch upon both and make a recommendation as to what may be the best way to defend against phishing attacks.

Technical approach

One way of defending your network against phishing attacks, is to use different kinds of software or hardware. There are many brands on the market for this kind of defense, but they mostly do the same thing. The system tries to block out links that go to known malicious sites, based on filters that are updated regularly. They scan incoming emails for signs of social engineering, rewriting all incoming links and scan the destination website in real-time when the links are clicked on, to block access to suspicious websites. They also prevent users from opening potentially harmful attachments or open them in a sandboxed environment to analyze their action. You can also configure your firewalls in different ways to help protect your users, by blocking for instance all incoming emails from the outside, that origins from internal addresses. These are just a few examples of technical countermeasures against phishing.

The problem with these solutions is that the filters can be outdated, the vulnerability could be unknown (zero-day), the analysis for detecting social engineering could be wrong, one could miss some emails, and so forth. Therefore, despite these countermeasures, several things can still occur that could lead fraudulent emails through the system and into the recipient's mailbox.

Human approach

Another way of combating the phishing problem, is to educate the users. The people responsible for opening the emails, clicking the links, or giving up sensitive information. The main strategy to do this is through education, as is the case study for this master thesis.

There are different ways of educating, from training sessions, online courses, or as part of the new employee program. For many organizations, this is a onetime information package, and the last thing the users hear about phishing.

Another approach is to combine the education with real life examples and tests. At periodic intervals you send out emails that are meant to fool the users, trying to get them to click on a potentially dangerous link, open or download a suspicious attachment or just log on to a fake site giving away login credentials. The next educational information about phishing will then comprise of the fake email as an example, and further educate the users in what they did wrong or how they should have handled the situation.
These training sessions must be made mandatory if they are to have any effect, and there should be a report sent to the managers showing the progress and attendance of the employees. Furthermore, there should be annual phishing tests and information campaigns, reminding the employees of the dangers with phishing emails. By the end of the year, they should make a decision to continue with this regime or not.

Recommendation

The best defense against phishing is a combination of these two methods, technical- and human approach. You need the right technical protection to weed out most of the phishing emails. Without this, the users would drown in all the spam and phishing emails that go around.

According to Europol 32% of the computer breaches involved phishing and 78% of cyber espionage incidents had phishing present (Europol 2019). Hence it is obvious that technical protection is not enough. Therefore, you also need the right amount of education to raise the resilience of your employees, so that they also can "filter out" unwanted email.

The cyber security landscape is constantly changing. Even more so today. It is increasingly difficult for companies and organizations to stay ahead of the hackers and cyber criminals. Unfortunately, the reality is that the attacker continues to be in the forefront finding new and ingenious ways to lure the defensive software. That is why finding a good balance between technical and human cyber defense measures is key to protect any organization against the threat of phishing in the best way possible.

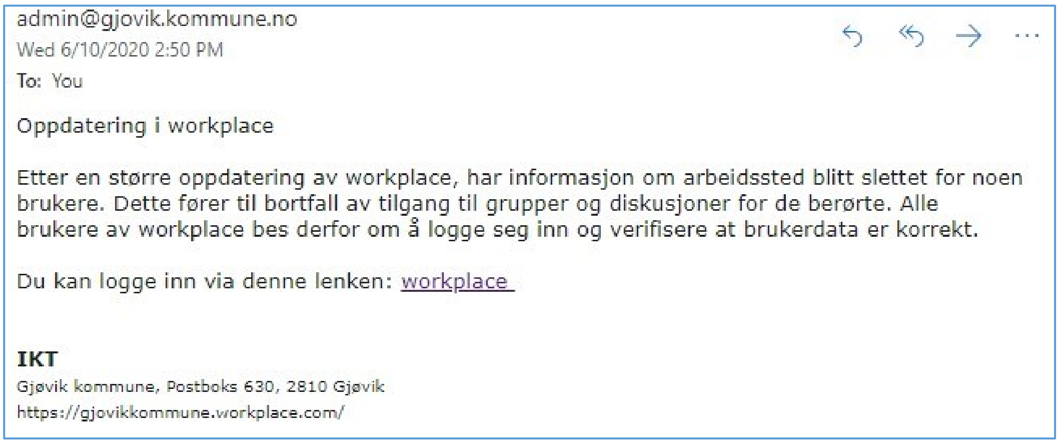
Chapter 3 - Process

This chapter describes the process behind the results. Each section represents the different stages of the process. The results will follow in chapter 4.

Phase 1 – Initial phishing test

The first thing I needed was a baseline of the user's susceptibility to phishing attacks. The best way to achieve this was to run an actual phishing test. Before doing so, I contacted The National Research Ethics Committee to make sure my research did not warrant a permit. In addition, I met with Gjøvik municipality to discuss the legal basis. They found it to be within their rights.

The email I created pretended to come from the municipalities' administration, informing the users that their Workplace[2] account has been updated, and that some information was lost. All users were asked to click on a link and log-in to check that their personal information was still correct.



admin@gjovik.kommune.no
Wed 6/10/2020 2:50 PM
To: You

Oppdatering i workplace

Etter en større oppdatering av workplace, har informasjon om arbeidssted blitt slettet for noen brukere. Dette fører til bortfall av tilgang til grupper og diskusjoner for de berørte. Alle brukere av workplace bes derfor om å logge seg inn og verifisere at brukerdata er korrekt.

Du kan logge inn via denne lenken: workplace

IKT
Gjøvik kommune, Postboks 630, 2810 Gjøvik
https://gjovikkommune.workplace.com/

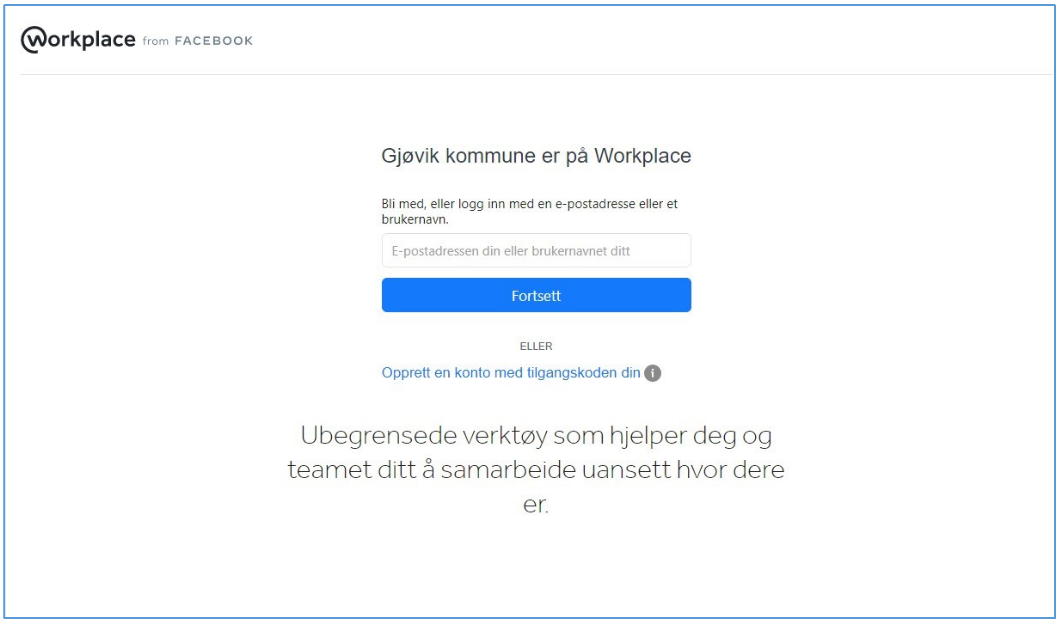
Figure 2 The first mail that was sent out.

As the email was fake and there was in fact no update, no action was required. The subject of this email was chosen for a couple of reasons. First, it required little time and effort, as no action was needed in terms of updating personal info. Secondly, I wanted to

[2] Workplace is a dedicated and secure working space for organizations to connect, communicate and collaborate.

test the recipient's susceptibility to the personality trait *obligation.* Hence, how many users felt obliged to click on the link.

To perform the test, a site mirroring their log in site for Workplace was created as shown in figure 3. From there I collected the usernames. The same site was used for all four phishing emails in my study.



Workplace from FACEBOOK

Gjøvik kommune er på Workplace

Bli med, eller logg inn med en e-postadresse eller et brukernavn.

E-postadressen din eller brukernavnet ditt

Fortsett

ELLER

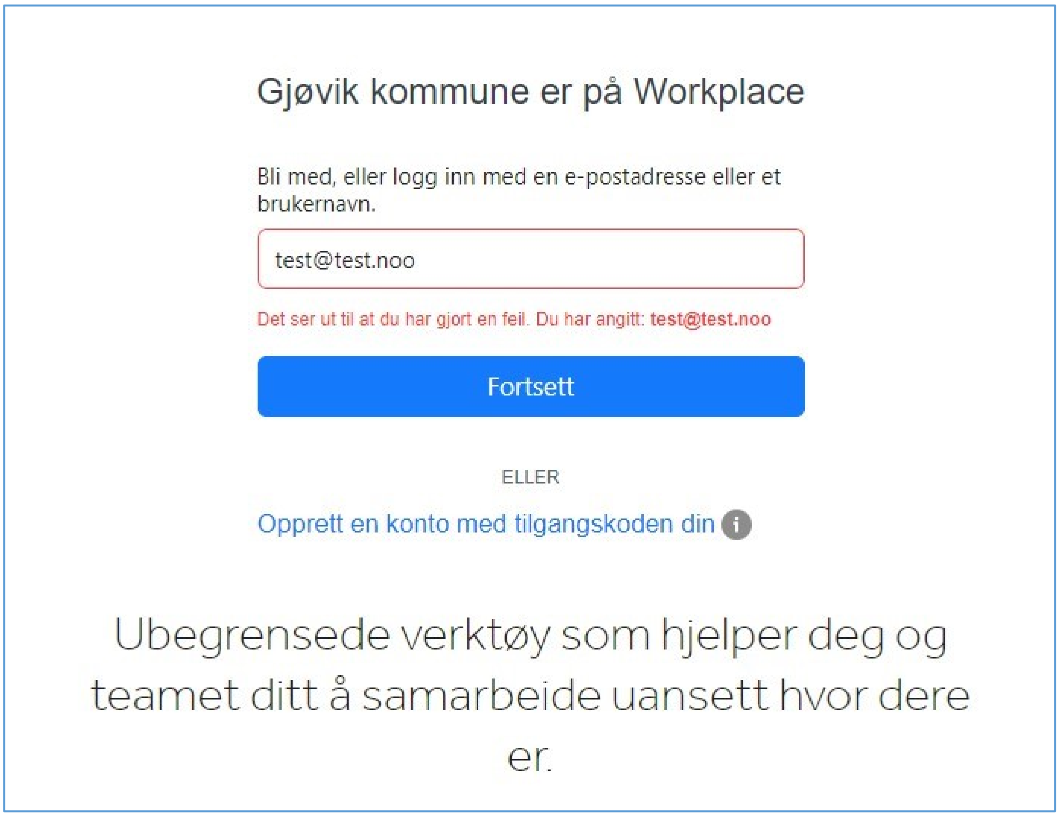
Opprett en konto med tilgangskoden din

Ubegrensede verktøy som hjelper deg og teamet ditt å samarbeide uansett hvor dere er.

Figure 3 This is a screenshot of the fake landing site.

When the users entered their username and hit continue, a script running in the background would store their username to a text file on the server. The users would then be redirected to the real company log-in site receiving an error message telling them they had entered the wrong username.

As shown in figure 4 I applied an extra letter "o" to the end of their username after they were redirected to the real company log-in site. As such, it seems that they typed the wrong username by mistake. Since most login names would be email addresses, which in Norway ends with an "o" (.no), this was a plausible error. When they tried again, they logged on to the real site, and would not suspect anything. As such, my tests did not require the participants giving up their password to me as I only stored their username in my text file.



Gjøvik kommune er på Workplace

Bli med, eller logg inn med en e-postadresse eller et brukernavn.

test@test.noo

Det ser ut til at du har gjort en feil. Du har angitt: **test@test.noo**

Ubegrensede verktøy som hjelper deg og teamet ditt å samarbeide uansett hvor dere er.

Figure 4 This is how the user sees the error message.

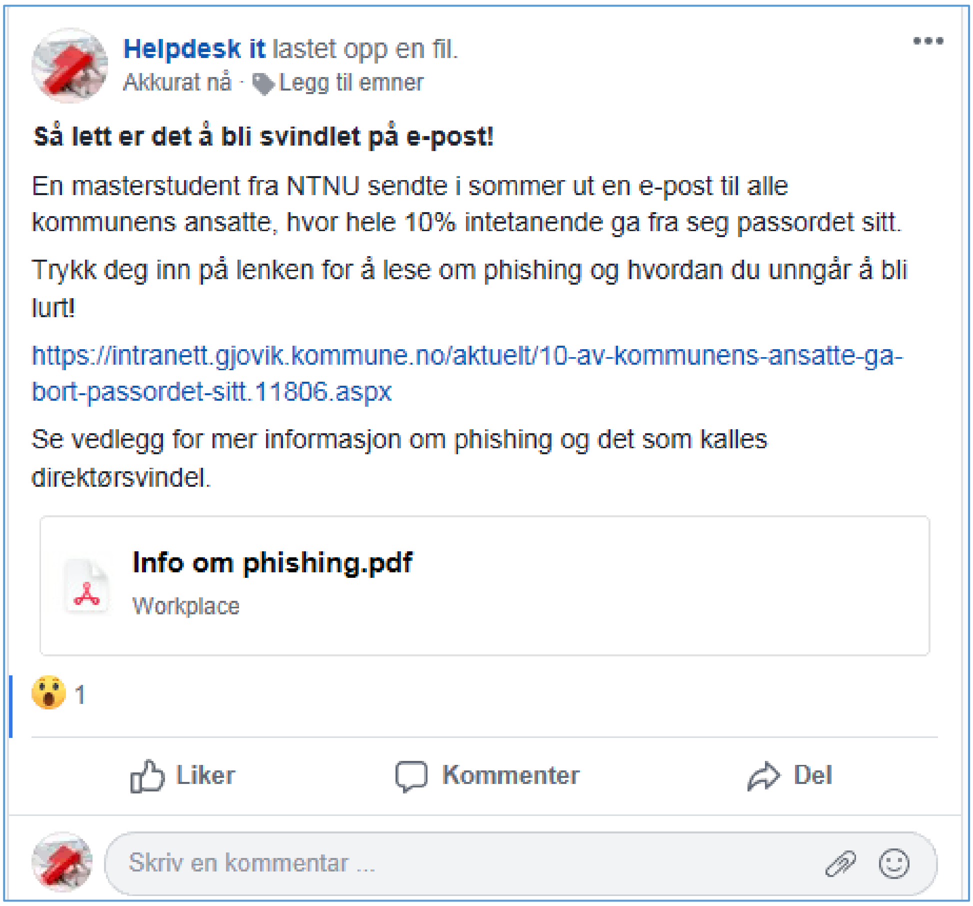
I used the municipality's own educational system to send out my emails. This means that I was already inside of their firewalls. As such, I circumvented the part of the attack that happens before the email enters the user's mailbox, as this was not part of my research. My research focuses on what the individuals do with the emails they receive; their actions is not dependent on me being inside or outside the network.

After two weeks, I collected the usernames and saved them in a excel workbook. This workbook was used for all the data I gathered, as well as the analysis I performed.

Phase 2 – Education

Following the initial phishing test, the next phase was training the employees. The education material was designed to teach users not to fall for phishing. In my experience most people are hesitant to make time to do courses on topics not relating to their specific line of work. That is why I decided on a short training program that focused only on a few critical signs of a phishing email. The training would take between 1 and 2 minutes to complete, finishing up with a short summary (see attachment 1).

As part of the training the Communications Department wrote a news article on Workplace, using my phishing email as click bait to get the users to read it (figure 5 and 6).



Helpdesk it lastet opp en fil.
Akkurat nå · Legg til emner

Så lett er det å bli svindlet på e-post!

En masterstudent fra NTNU sendte i sommer ut en e-post til alle kommunens ansatte, hvor hele 10% intetanende ga fra seg passordet sitt.

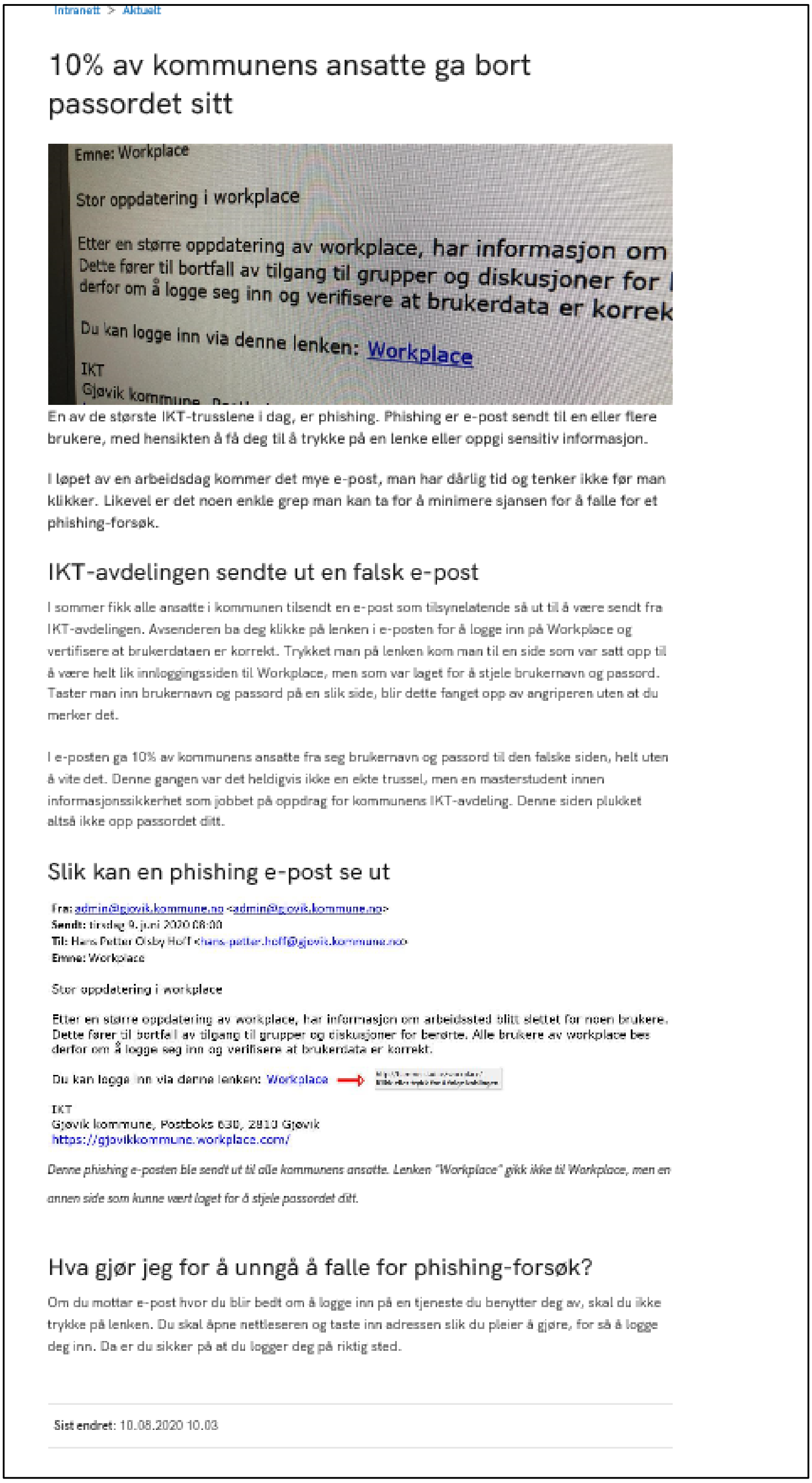
Trykk deg inn på lenken for å lese om phishing og hvordan du unngår å bli lurt!

https://intranett.gjovik.kommune.no/aktuelt/10-av-kommunens-ansatte-ga-bort-passordet-sitt.11806.aspx

Se vedlegg for mer informasjon om phishing og det som kalles direktørsvindel.

Info om phishing.pdf
Workplace

Figure 5 The article from the municipality's workplace.



Intranett > Aktuelt

10% av kommunens ansatte ga bort passordet sitt

Emne: Workplace

Stor oppdatering i workplace

Etter en større oppdatering av workplace, har informasjon om
Dette fører til bortfall av tilgang til grupper og diskusjoner for
derfor om å logge seg inn og verifisere at brukerdata er korrek

Du kan logge inn via denne lenken: Workplace

IKT
Gjøvik kommune

En av de største IKT-trusslene i dag, er phishing. Phishing er e-post sendt til en eller flere brukere, med hensikten å få deg til å trykke på en lenke eller oppgi sensitiv informasjon.

I løpet av en arbeidsdag kommer det mye e-post, man har dårlig tid og tenker ikke før man klikker. Likevel er det noen enkle grep man kan ta for å minimere sjansen for å falle for et phishing-forsøk.

IKT-avdelingen sendte ut en falsk e-post

I sommer fikk alle ansatte i kommunen tilsendt en e-post som tilsynelatende så ut til å være sendt fra IKT-avdelingen. Avsenderen ba deg klikke på lenken i e-posten for å logge inn på Workplace og vertifisere at brukerdataen er korrekt. Trykket man på lenken kom man til en side som var satt opp til å være helt lik innloggingssiden til Workplace, men som var laget for å stjele brukernavn og passord. Taster man inn brukernavn og passord på en slik side, blir dette fanget opp av angriperen uten at du merker det.

I e-posten ga 10% av kommunens ansatte fra seg brukernavn og passord til den falske siden, helt uten å vite det. Denne gangen var det heldigvis ikke en ekte trussel, men en masterstudent innen informasjonssikkerhet som jobbet på oppdrag for kommunens IKT-avdeling. Denne siden plukket altså ikke opp passordet ditt.

Slik kan en phishing e-post se ut

Fra: admin@gjovik.kommune.no <admin@gjovik.kommune.no>
Sendt: tirsdag 9. juni 2020 08:00
Til: Hans Petter Olsby Hoff <hans-petter.hoff@gjovik.kommune.no>
Emne: Workplace

Stor oppdatering i workplace

Etter en større oppdatering av workplace, har informasjon om arbeidssted blitt slettet for noen brukere. Dette fører til bortfall av tilgang til grupper og diskusjoner for berørte. Alle brukere av workplace bes derfor om å logge seg inn og verifisere at brukerdata er korrekt.

Du kan logge inn via denne lenken: Workplace →

IKT
Gjøvik kommune, Postboks 630, 2810 Gjøvik
https://gjovikkommune.workplace.com/

Denne phishing e-posten ble sendt ut til alle kommunens ansatte. Lenken "Workplace" gikk ikke til Workplace, men en annen side som kunne vært laget for å stjele passordet ditt.

Hva gjør jeg for å unngå å falle for phishing-forsøk?

Om du mottar e-post hvor du blir bedt om å logge inn på en tjeneste du benytter deg av, skal du ikke trykke på lenken. Du skal åpne nettleseren og taste inn adressen slik du pleier å gjøre, for så å logge deg inn. Da er du sikker på at du logger deg på riktig sted.

Sist endret: 10.08.2020 10.03

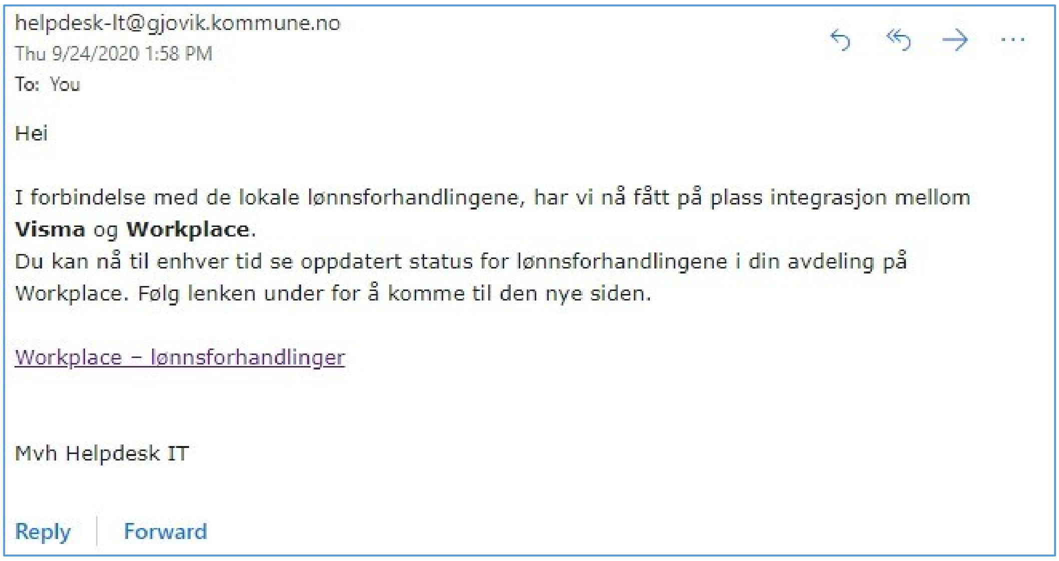
Figure 6 The information posted on the municipality's intranet.

Phase 3 – More phishing tests

After the educational material had been available for some time, new phishing emails were sent out. The first email was sent out one month after the training started, in September (figure 7). The second and third followed in November

As mentioned previously, all phishing tests used the same landing site for the users to log-in to. Every email was different, making use of real-time events and happenings to lure the recipients, such as local wage negotiations, and Christmas season (figure 7, 8 and 9). This can be one reason for the variation in the results and will be discussed more thoroughly later.

The last, and fourth phishing email was sent out just two weeks after the previous one, mixing up the frequency to catch the users off guard. I also wanted to take advantage of the fact that holiday season is approaching, and therefore target the human trait *excitement*. In addition, as the deadline for turning in my thesis was approaching, the last username data from test 4 had to be collected one week after sending out the email, and not two weeks as is the case for the other 3 tests.


helpdesk-It@gjovik.kommune.no
Thu 9/24/2020 1:58 PM
To: You

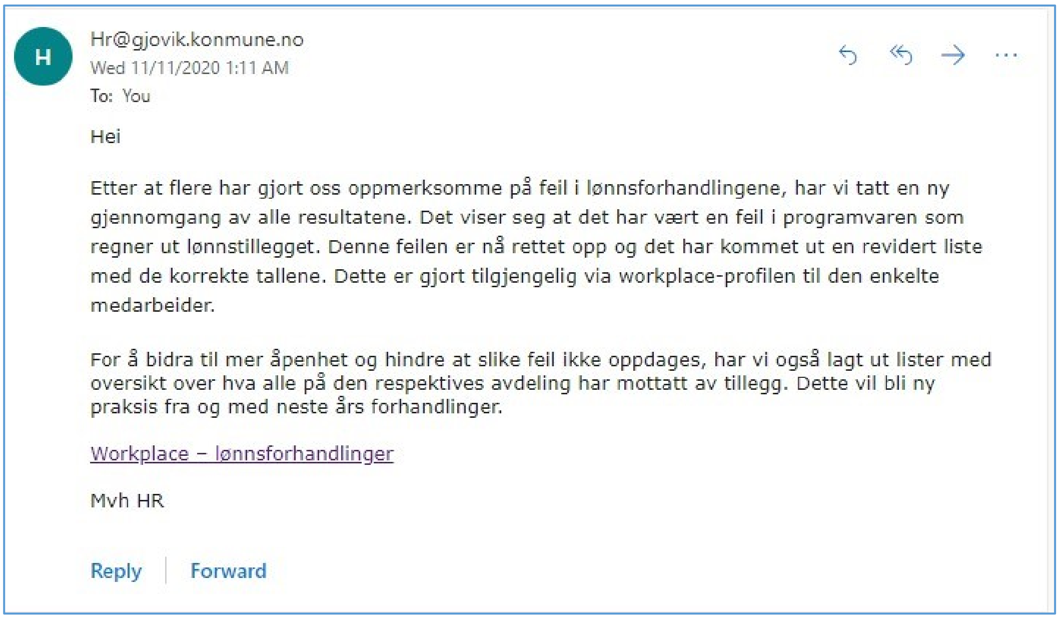
Hei

I forbindelse med de lokale lønnsforhandlingene, har vi nå fått på plass integrasjon mellom **Visma** og **Workplace**.
Du kan nå til enhver tid se oppdatert status for lønnsforhandlingene i din avdeling på Workplace. Følg lenken under for å komme til den nye siden.

Workplace – lønnsforhandlinger

Mvh Helpdesk IT

Figure 7 The second phishing test



Hr@gjovik.konmune.no
Wed 11/11/2020 1:11 AM
To: You

Hei

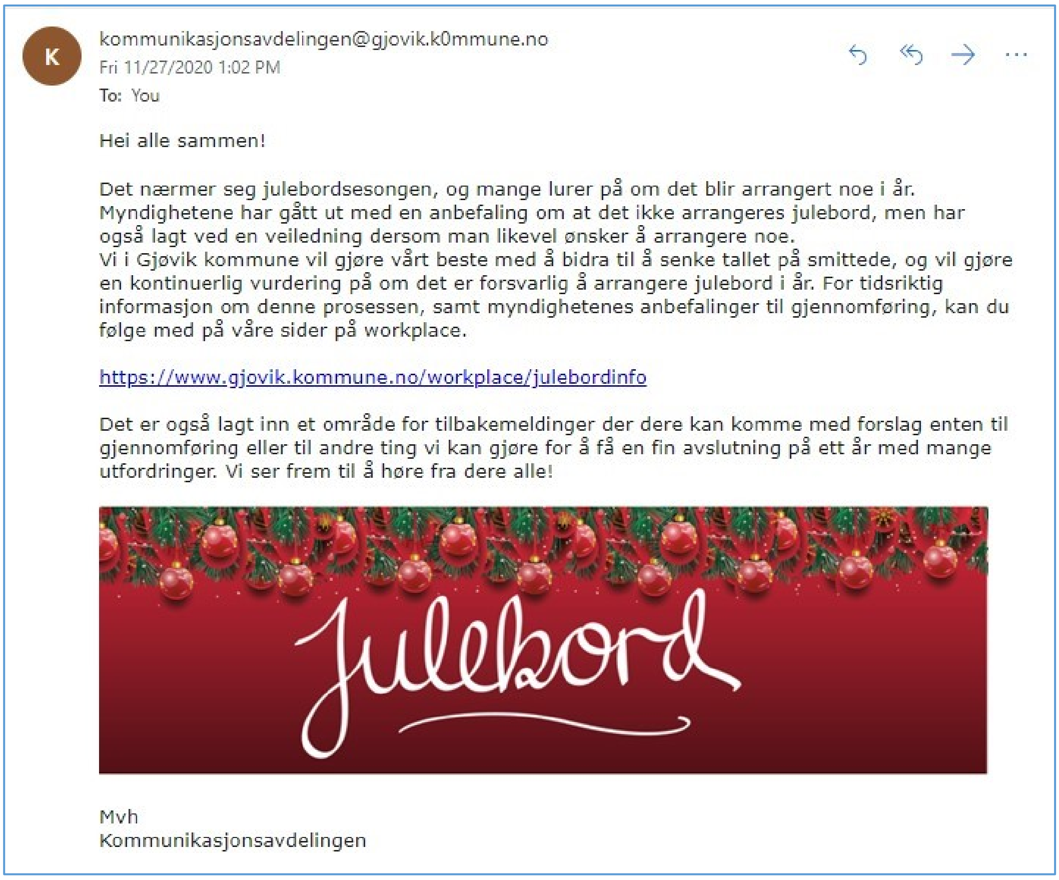
Etter at flere har gjort oss oppmerksomme på feil i lønnsforhandlingene, har vi tatt en ny gjennomgang av alle resultatene. Det viser seg at det har vært en feil i programvaren som regner ut lønnstillegget. Denne feilen er nå rettet opp og det har kommet ut en revidert liste med de korrekte tallene. Dette er gjort tilgjengelig via workplace-profilen til den enkelte medarbeider.

For å bidra til mer åpenhet og hindre at slike feil ikke oppdages, har vi også lagt ut lister med oversikt over hva alle på den respektives avdeling har mottatt av tillegg. Dette vil bli ny praksis fra og med neste års forhandlinger.

Workplace – lønnsforhandlinger

Mvh HR

Figure 8 The third phishing test



kommunikasjonsavdelingen@gjovik.k0mmune.no
Fri 11/27/2020 1:02 PM
To: You

Hei alle sammen!

Det nærmer seg julebordsesongen, og mange lurer på om det blir arrangert noe i år.
Myndighetene har gått ut med en anbefaling om at det ikke arrangeres julebord, men har også lagt ved en veiledning dersom man likevel ønsker å arrangere noe.
Vi i Gjøvik kommune vil gjøre vårt beste med å bidra til å senke tallet på smittede, og vil gjøre en kontinuerlig vurdering på om det er forsvarlig å arrangere julebord i år. For tidsriktig informasjon om denne prosessen, samt myndighetenes anbefalinger til gjennomføring, kan du følge med på våre sider på workplace.

https://www.gjovik.kommune.no/workplace/julebordinfo

Det er også lagt inn et område for tilbakemeldinger der dere kan komme med forslag enten til gjennomføring eller til andre ting vi kan gjøre for å få en fin avslutning på ett år med mange utfordringer. Vi ser frem til å høre fra dere alle!

Mvh
Kommunikasjonsavdelingen

Figure 9 The fourth phishing test

Phase 4 – Analysis

The last phase consists of analyzing the data gathered to see if I had enough information to answer my research questions. Most of this work was done using excel spread sheets. As there was not enough time for all the phishing tests I had planned, there is a greater risk of error in the final results, which is something I have accounted for.

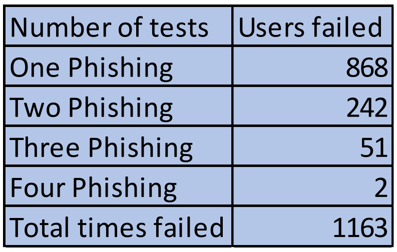
The main task of the analysis is to determine if the information security awareness training has had any effect on the users. This can be observed in the results by looking at the (potential) decrease in number of people falling for the phishing emails with each subsequent test. The assumption is that with training, people will be better at detecting a phishing email. Therefore, the results should show a decrease in usernames gathered after each test. There is of course other factors and uncertainties that can impact the results. These will be discussed in the next chapter.

The second part is analyzing the results by grouping the users into their respective departments. This way I can see if there is any specific area where there are more users falling for the phishing emails. I also checked for repeated victims, people falling for more than one phishing email.

The last part will discuss the wording and theme of the phishing emails. Different triggers and content may have different effects on the users. As such, the results will vary. Some topics and events may be more interesting than others, for example wage negotiations. Looking at the number of users falling for each different type of email will give an indication as to which subjects or events are the most interesting for the users, and what personality trait may be the most vulnerable, hence the best one to use for an attacker.

Chapter 4 - Results

As shown in table 1, there was a total of 868 persons that failed at least one test. The total number of recipients were 3424. This means that at least 25.3% were lured into clicking on one or more links.



Number of tests	Users failed
One Phishing	868
Two Phishing	242
Three Phishing	51
Four Phishing	2
Total times failed	1163

Table 1 Users who failed at least one, two, three or all four of the phishing tests

Further, many employees got lured not only once, but several times. There is 242 persons who failed two tests or more, and 51 persons that have failed three tests or more. There is even 2 people that failed all four tests.

As the distribution list has been static since it was created, the real percentage could be a bit higher, as people may have quit the organization, or been removed for some reason.

Figure 10 is a graphical representation of the numbers from table 1. A total number of 1163 unique hits have been registered on the fake landing site. For a hit to be registered, a user must type in his or her username and push the log-in button. Users that just clicked the link in the email, but did not go further, were not registered. The results are from the total of 13,696 emails sent out, hence all four tests. This equals an average of 8.5% of the users clicking the fraudulent link, per testing phase. For a cybercriminal this is fairly good odds of success.

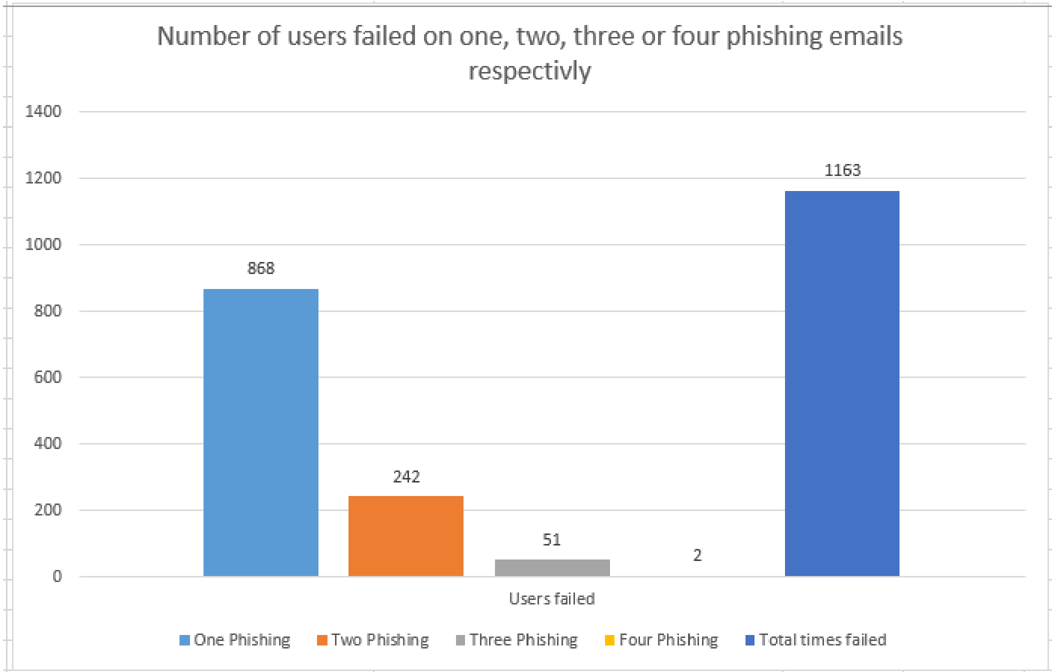
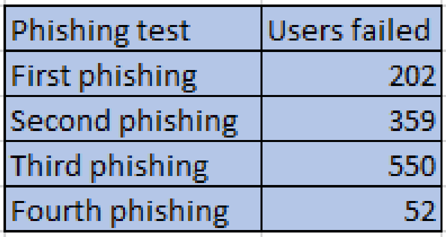


Figure 10 Graphical presentation of users who failed one or more tests

Table 2 and figure 11 below shows how many people failed the different phishing tests. The assumption is that with time and training, users become better at recognizing phishing emails, which in turn should decrease the number of usernames gathered. This does not seem to be the case for my tests, rather there is a steady increase for each new phishing email, except for the last one. As will be discussed in chapter 5, there are valid reasons for this.



Phishing test	Users failed
First phishing	202
Second phishing	359
Third phishing	550
Fourth phishing	52

Table 2 Users who failed each phishing test

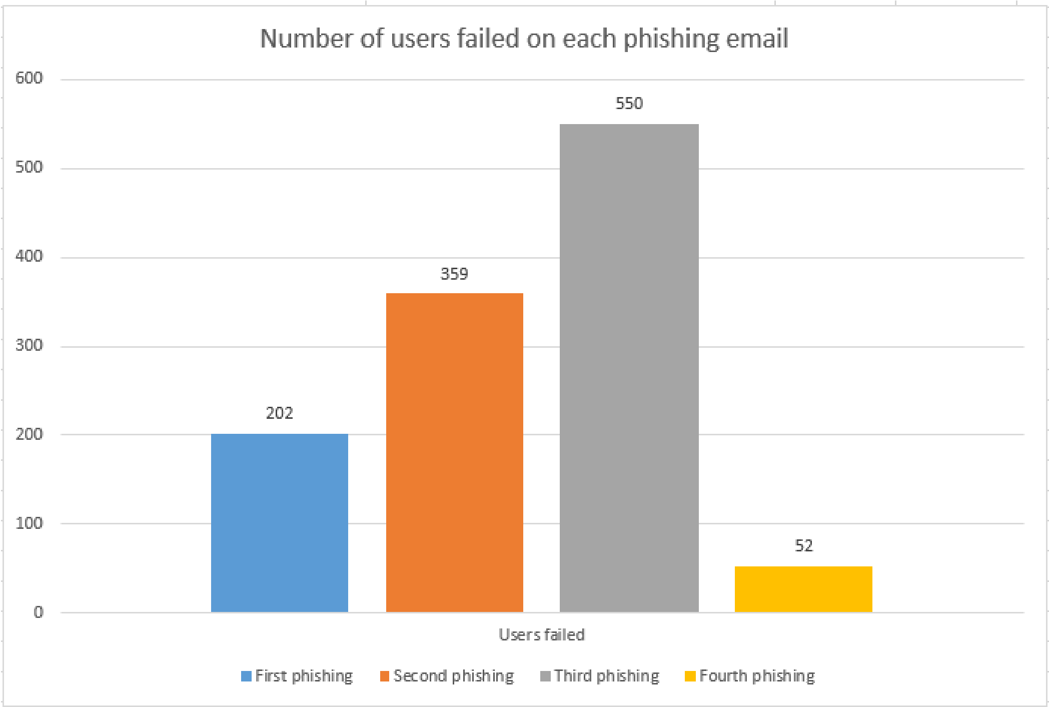


Figure 11 Graphical presentation of users who failed each phishing mail

Different departments within the municipality have also been analyzed to see who might be the most vulnerable to phishing attacks. Figure 12 shows the departments where five or more employees failed the tests.

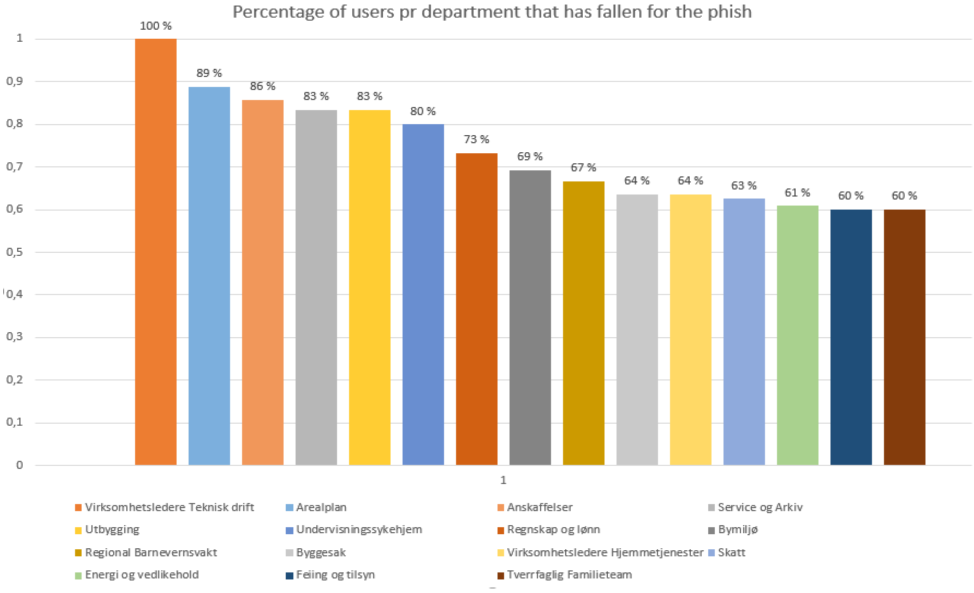


Figure 12 Shows which departments have the most users fail the tests

Since there are so many departments, only the ones where more than 60% of the users failed at least ones are shown. The total amount of persons that make up this graph is 182, representing 15 departments. As shown on the graph, there is one department where every single person failed at least one phishing test.

Chapter 5 - Discussions

Critical reflection

When deciding upon the research questions for this thesis, I predicted it would be fairly easy to reach a conclusion that supported my initial assumption. I did not see many obstacles with gaining enough data to draw a conclusion that would be scientifically sound. However, with time, more and more variables continued to present themselves, making it hard to reach a definite and solid conclusion.

In my professional career working with information security, I have used phishing tests to assess the organizations vulnerability to this specific threat. Based on my experience, my assumption was that there would be little or no difference in the results when training was offered only once.

Under, I will account for the uncertainties I encountered which had an impact on the results and their validity.

Inaccuracies and discussions

Firstly, the distribution list of employees who received the phishing tests was static. This may result in loss of some recipients as people change jobs, move etc. No new additions (potential new employees) were added. The reason however, for using a static list of employees, is that the study required that the exact same people was part of the initial benchmark and educational training, as well as the actual phishing tests. Nevertheless, since the sample size was relatively large, I believe the (little) variation in users receiving the email would not have a large impact.

Secondly, the frequency of the phishing emails themselves. I initially intended for the educational information to be distributed in April and phishing emails to be sent out every month thereafter. This would give me seven sets of results to work with. I ended up with only three additional phishing tests, and hence, less data to work with. Since I did not have the chance to send out as many phishing emails as planned, I only focused on spear phishing emails, pretending to be someone on the inside, targeting them with realistic information I knew they might be interested in.

My prediction as to why the number of participants who failed the tests kept rising after each test, is the way the emails were written, and their content. The first email that was used as a benchmark for the user's susceptibility, had instructions from the municipality to check their user profile in workplace. This is a somewhat boring task you do because you must and targets the user’s sense of obligation. The response, however, was not great, only 5.9% clicked and hence, failed the test.

The next phishing test seemed to be slightly more interesting, targeting their curiosity. They were told of a new functionality in conjunction to the local wage negotiations, allowing them to follow the process via their workplace platform. A lot of users were interested in how the wage negotiations went, and I think this is the reason for the rise in respondents. Almost twice as many people, 10.5% clicked the link, and gave away their username.

The third phishing email came after the wage negotiations ended. Also, this email targeted peoples’ sense of *curiosity,* as people want to know if they can expect an increase in salary. The recipients were told that there had been errors made in the negotiations, and that a new salary list was published. The new functionality also allowed them to see what everyone else would be earning. This email was exceedingly popular, and a total of 16.1% clicked the link and gave away their username.

For the fourth phishing email, I took another approach, targeting the famous Norwegian Christmas party; julebord. This is a seasonal event most companies arrange for their employees, and something the employees look forward to. Due to the short amount of time from when the email was sent out and my deadline, the test only ran for a couple of days before I had to collect the data.

Only 1.8% of the recipients were lured to click the link in this last phishing email. The reasons for the outcome to be as low can be attributed to one or more of these four factors. First, this phishing email was sent out not long after the previous one. Therefore, I think the users still remember the last one quite well, and hence skeptical. Second, the subject of this phishing email might not have been as interesting as the last two emails. In addition, some might even find it suspicious that the municipality would arrange a Christmas party in these COVID-19-times. Third, we could see an impact of the frequent phishing tests, making the users more aware and conscious when working with email. Finally, the test could only run for a couple of days, while the other tests ran for 2 weeks, hence loosing potential data.

Another uncertainty I could not account for is the effect of the information security training. I wanted the education material to be sent to every individual, but instead it was posted on the intranet of the municipality. It was published together with a news article about municipality employees giving away their usernames (and passwords). Despite an interesting headline, the material would probably receive more attention if delivered to everyone's email account.

A total of 961 people saw the news article on workplace, but only 182 visited the information page on the municipality's intranet. Therefore, it is hard to know how effective the training was. This again makes it hard to trust the end results when it comes to the decline in awareness and phishing resistance. If I were to do this again, I would make sure that I could make the training mandatory and track the attendance. In addition, reporting attendance to the management could help motivate the users to participate.

Another factor I was not able to track, was how many users read or opened the phishing emails I sent out. It could be that a lot of users does not work on a PC with email access on a daily or weekly basis. Since I let the tests run for two weeks, this could potentially exclude people working on some sort of rotation who might click on the link after the results had been gathered. Either that, or their click would be counted in the next phishing test, as their results would be registered for that attempt.

For users working in an office environment, there is also a possibility that some employees falling for a phishing email alert their coworkers, resulting in the numbers failing the test being lower than what they could be. This is not a problem as such, rather something to be expected to occur with a real phishing attack. This is also something that should be encouraged.

When we are trying to decide how often an information campaign or training should take place to maximize its effect, there are a few factors to consider, excluding however factors like costs. How often can people get education material before they get tired or irritated to the point that they start ignoring it. Hence, one should not overload people with education material.

Based on my personal experience, the right kind of frequency is two to four times a year, depending on how comprehensive the information is. However, in order to get accurate answers to this question, more tests and benchmarks is needed.

When looking at the overview of the different departments in the municipality, the results show that people working in nursing homes and schools do very well. The percentage falling for the phishing tests were below 30%. At the other end of the scale, the results show people in leadership positions, administrative support, and construction. Regarding leadership positions that was across all areas, Technical maintenance, Home service, Nursing homes, Kindergarten, Schools and Property. One reason for this could be that the people at the top of the list do their work at a computer, and will open emails faster and in greater quantity, making them easier targets. Given potential higher gains, cyber criminals tend to target leaders and the team around them specifically. As such, raising their security information awareness is key.

Chapter 6 - Conclusion

When you decide on how to protect your system and its users against a threat like phishing, you need to focus on two main areas. You must use the right hardware and software, making the system as technically sound as possible, and you need to target the end users, giving them training and education so that they are protecting your system as well.

The data gathered from my tests, show that there is little to gain in just educating the users, when it is done on a voluntarily basis as a one-time event. We did not see a decline in users who fell for the phishing tests until the last test, even though training and information was published informing the employees of the risk posed by unfriendly emails.

A lot of participants in my study who failed the tests, contacted the helpdesk or the administration, voicing their concern when they realized the link they had just clicked, was either not working or that it redirected them to a false site. These people were then informed that this was a phishing email. As such, one should presume that they would be even more conscious and prepared for the next email. Nevertheless, as seen in table 2, this is not the case at all.

These results do not coincide with what earlier research has found, that users tested improved in subsequent years. Both their ability to be cautious and not click on false links, and their rate of reporting improved (Ronald C. 2007). One would have to do more research on the correlation between education and testing over a longer period of time than what I did to be able to verify this. The fact that so few people read the education material that was published, made it impossible to say if the training had any effect or not.

It is impossible to say with certainty the cause for the high (and rising) number of victims in the two subsequent phishing tests. It could be that the knowledge retained from training diminished over time or it could be the differences in the subject and wording of the emails. This is something to take into consideration when doing research like this. It is hard to get reliable results, as you will not get the right effect if you send the exact same email more than once. If you change the subject of the email, you have altered the test and therefore it is hard to compare the results to each other.

Further, due to my research, the users are getting more phishing emails than normal, and as such it would be anticipated that this in itself would have a decreasing effect on the number of victims. In this case, it does not seem to have any impact at all. Especially when many of the users repeatedly fall victim to the phishing emails. It is not until the last email, which was sent a couple of weeks after the previous one, a decreasing trend is seen. This is an indication as to how long the users retain their awareness.

Regarding the second research question, *how often do you have to run information training campaigns for it to have any measurable effect,* it is also challenging to draw conclusions with the data collected. Since the last two phishing tests were so close in time, this may help as a reminder to be cautious. This might indicate that some training in the form of repeated tests, does in fact help, and that knowledge is at least retained for 2-3 weeks. However, also here the way the email was written, and the theme of the email might have an impact as well.

When looking at who are more susceptible to phishing attacks, my results point to people in leadership- and administrative positions to be the most vulnerable. The reason for this is not clear, but they do spend considerably more time in front of a computer than teachers or nurses, and hence need to handle a lot more emails.

From this research, and my professional experience, it seems likely that the subject and theme of the phishing email is a critical factor for the phishing to be a success. The more interesting the subject is, and the more people it targets, the more people will potentially click on the link. Unfortunately, I only got to test three of the five human traits: *curiosity, obligation, and excitement.* My results show that the two emails using the *curiosity* trait as bait had by far more success than *obligation* and *excitement.*

Cybercrime is here to stay. Phishing attacks is one of the best tools to lure victims, usually for economic gain. It is relatively easy and low-risk and may entail potential high return. Everyone should learn the basics about phishing, to be prepared and thereby protect themselves and ensure cyber- and email security throughout a business, government, or organization. I believe that by implementing obligatory training and information, making sure the users are knowledgeable and aware, we can achieve a higher level of protection.

Future work

There is a lot of potential for future work in this field. I would begin with a new baseline test for the same user mass, but with an updated distribution list to account for new employees and take out the ones that are no longer valid. Then I would follow up with another training session for half of the users, leaving half without training to compare the results better. Furthermore, training should be made mandatory, and it should be possible to check if the persons falling for the phishing attack, completed the training or not. In addition, I would use software to track how many users opened the phishing emails, to get more accurate results when analyzing the data.

For more comprehensive results I would also include more phishing emails after the training was done and add in some generic phishing tests that are not tailored for the municipality. These would pretend to be from Facebook, LinkedIn, and other commercial sites. Ideally this whole campaign would run for almost a year, gathering data on the success of the phishing tests.

After a year or longer of doing these tests, hopefully the users would then understand not to give away their login credentials, and then it is time to diversify the testing. We would move from trying to get the users to click on a specific link, to attaching a document with macros and checking if the users would run it.

It could also be an idea to do this work annually and see how the results vary over the years with new people entering the organization and old ones leaving. I believe it would be necessary to keep this going for two to three years to get any valuable results and make a sound conclusion as to whether the training does in fact have any measurable effect.

Finding out why people fell for the different phishing emails could also be interesting, and especially the people falling for more than one. To complement my quantitative analysis, I would like to do some qualitative analysis, interviewing the persons repeatedly failing the tests. It would be interesting to see if they went through the training, and their thoughts on the education material. It would also be valuable to hear why they keep clicking on links in these emails.

With much more time and resources, I could also investigate the difference in time spent on the computer and number of phishing test fails. Is there a correlation between how much time you spend on the computer, and how susceptible you are to phishing? What about the age and gender of the people falling for the phishing emails?

Bibliography

A. Darwish, A. El Zarka, F. Aloul. 2012. "Towards understanding phishing victims profile." *Computer systems and industrial informatics (ICCSII).* IEEE.

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. 2014. "Online frauds: Learning from victims why they fall for these scams." *Australian & New Zealand Journal of Criminology, 47(3)*, 391-408.

C. Dodge Jr., Curtis Carver, Aaron J. Ferguson. 2007. "Phishing for user security awareness." *Computers & security*, 73-80.

Cialdini, R. 2006. *Influence: The psychology of persuasion.* HarperCollins.

Emma J. Williams, Joanne Hinds and Adam N. Joinson. 2018. "Exploring susceptibility to phishing in the workplace." *International journal of human-computer studies*, December: 1-13.

Europol. 2019. *Internet Organised Crime Threat Assessment.* Europol.

Freiermuth, M. R. 2011. "Text, lies and electronic bait: An analysis of email fraud and the decisions of the unsuspecting." *Discourse & Communication, 5(2)*, 123-145.

Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. 2014. "Analysis of unintentional insider threats deriving from social engineering exploits." *IEEE Security and Privacy Workshops*, 236-250.

Karakasiliotis, A., Furnell, S. M., & Papadaki, M. 2006. "Assessing end-user awareness of social engineering and phishing." *Proceedings of 7th Australian Information Warfare & Security Conference.*

Kirlappos, I., & Sasse, M. A. 2012. "Security Education against Phishing: A modest Proposal for a Major Rethink." *IEEE Security & Privacy*, December 20: 24-32.

Kumaraguru, P, Sheng, S., Acquisti. A., Cranor, L. F., & Hong, J. 2010. *Teaching Johnny not to fall for phish.* Pittsburgh: CyLab Carnegie Mellon University, 7:1 - - 7:31.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. 2007. "Protecting people from phishing: the design and evaluation of an embedded tranining email system." *Conference on Human Factors in Computing Systems.* San Jose: Carnegie Mellon University.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., et al. 2007. "Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer." *APWG eCrime Researchers Summit.* Pittsburgh: ACM.

Le Compte, Elizondo, & Watson. 2015. "A renewed approach to serious games for cyber security." *International Conference on Cyber Conflict: Architectures in Cyberspace.* Tallinn: IEEE. 203-216.

Modic, D., & Lea, S. E. G. 2013. "Scam compliance and the psychology of persuasion." Paper.

n.d. *Nasjonal Sikkerhetsmyndighet.* https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/sikring-av-e-post.

Office of Fari Traiding. 2009. *The psychology of scams: Provoking and committing errors of judgement.* Report, Office of Fair Trading.

Raman, K. 2008. *Ask and you will receive.* Macafee Security Journal, Mcafee.

Ronald C., Dodge Jr., Curtis Carver, Aaron J. Ferguson. 2007. "Phishing for user security awareness." *Computers & Security 26*, 73-80.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., et al. 2007. "Anti-Phishing Phil: The design and evaluation of a gam that teaches people not to fall for phish." *SOUPS 07: Proceedings of the 3rd symposium on Usable privacy and security.* Pittsburgh: Association for Computing Machinery. 88-99.

Stajano, F., & Wilson, P. 2011. "Understanding scam victims: Seven principles for systems security." *Communications of the ACM, 54(3)*, 70-75.

Workman, M. 2008. "A theory-grounded investigation of phishing and pretext social engineering threats to information security." *Journal of the American Society for Information Science and Technology*, 662-674.

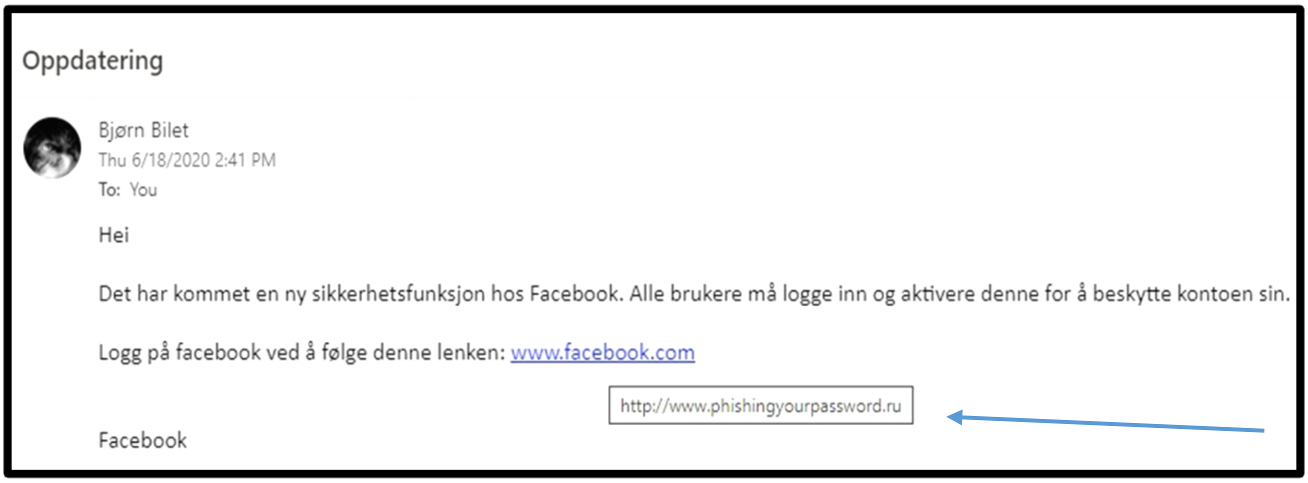
Attachement 1 – Informational package

Phishing

En av de største ikt-trusslene i dag, er phishing. Phishing er e-post sendt til en eller flere brukere, med hensikten å få disse til å trykke på en lenke eller oppgi sensitiv informasjon.

I løpet av en arbeidsdag kommer det mye e-post, man har dårlig tid og tenker ikke før man klikker. Likevel er det noen enkle grep mann kan ta for å minimere sjansen for å falle for ett phishing-forsøk.

Her ser vi et eksempel på hvordan en phishing e-post kan se ut. Avsender ønsker å få deg til å trykke på en lenke, i dette tilfellet for å logge på Facebook. Ved å holde musepekeren over lenken, kan vi se hvilken adresse som ligger bak. Dersom man trykker på lenken, vil man komme til angriperens hjemmeside, som er satt opp til å være helt lik innloggingssiden til Facebook. Dersom bruker taster inn brukernavn og passord, blir dette fanget opp av angriperen.



Oppdatering

Bjørn Bilet
Thu 6/18/2020 2:41 PM
To: You

Hei

Det har kommet en ny sikkerhetsfunksjon hos Facebook. Alle brukere må logge inn og aktivere denne for å beskytte kontoen sin.

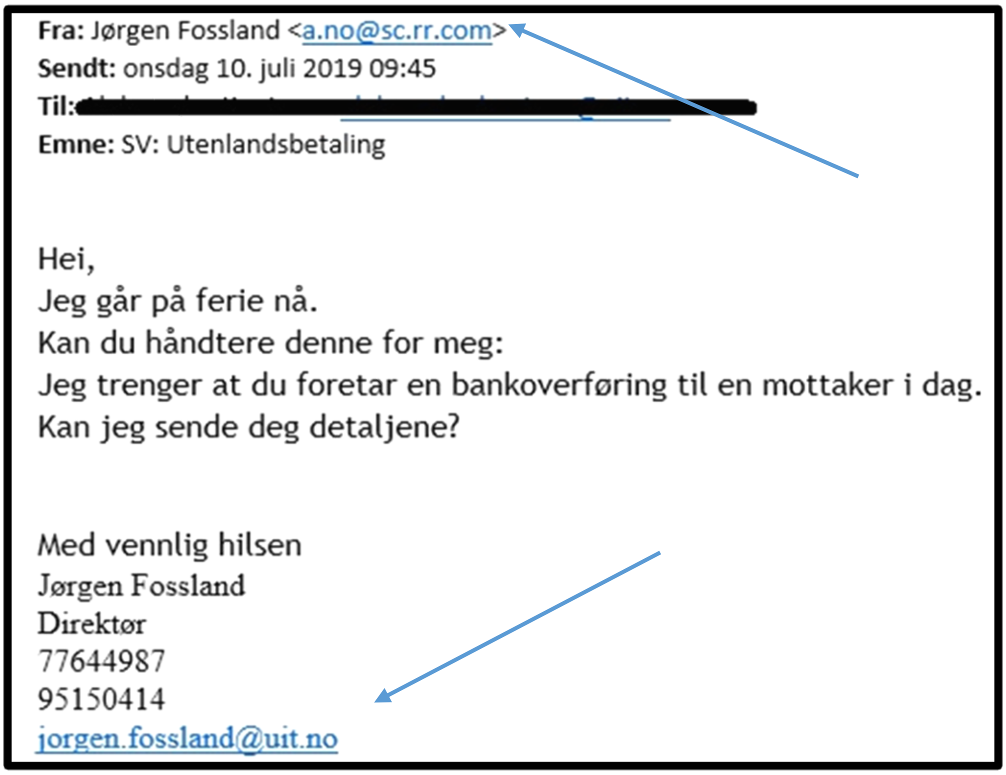
Logg på facebook ved å følge denne lenken: www.facebook.com

http://www.phishingyourpassword.ru

Facebook

Dersom du mottar e-post hvor du blir bedt om å logge inn på en tjeneste du benytter deg av, skal du ikke trykke på lenken. Du skal åpne nettleseren og taste inn adressen slik du pleier å gjøre, for så å logge deg inn. Da er du sikker på at du logger deg på riktig sted.

Andre phishing e-post kan være ute etter å få mottaker til å utføre en transaksjon eller overføring. Disse metodene kalles direktørsvindel og har de siste årene blitt mer og mer vanlig. Her vil angriper sende en e-post til noen som jobber i administrasjonen med tilgang til å utføre utbetalinger. Angriperens avsenderadresse er endret til å være den samme som adressen til en i ledelsen, og teksten i e-posten forklarer at det haster med å utføre en utbetaling til en gitt konto.
Her ser vi ett eksempel fra UiT:



Fra: Jørgen Fossland <a.no@sc.rr.com>
Sendt: onsdag 10. juli 2019 09:45
Til: [redacted]
Emne: SV: Utenlandsbetaling

Hei,
Jeg går på ferie nå.
Kan du håndtere denne for meg:
Jeg trenger at du foretar en bankoverføring til en mottaker i dag.
Kan jeg sende deg detaljene?

Med vennlig hilsen
Jørgen Fossland
Direktør
77644987
95150414
jorgen.fossland@uit.no

For å beskytte seg mot denne typen eller lignende angrep, er det noen ting man kan se etter:
Først og fremst avsenderadressen. Navnet kan forfalskes, men man kan her se at selve adressen ikke stemmer med direktørens adresse, som du ser nederst i e-posten.
For det andre må man spørre seg om dette er vanlig prosedyre i bedriften. Dersom det ikke er det, eller man er i tvil, kan en telefon til direktøren avsløre om dette er reelt eller ikke. Det er også viktig at man ikke bruker telefonnummer eller annen kontaktinformasjon i e-posten, da dette også kan være forfalsket.

Husk:
Vær kritisk til lenker i e-post, undersøk før du klikker.
Aldri oppgi sensitiv informasjon over e-post.
Tenk deg alltid om før du legger inn sensitiv eller personlig informasjon på internett dersom noen ber deg om dette.

NTNU

Norwegian University of
Science and Technology