Expertise
and insight
for the future

Timo Ukonmaanaho

Improving Security Awareness and Security Culture in a Company

Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Bachelor's Thesis

20 February 2019

Author Title Number of Pages Date	Timo Ukonmaanaho Improving Security Awareness and Security Culture in a Company 32 pages 20 February 2019
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Professional Major	Name of the professional major
Instructors	Kimmo Sauren, Principal Lecturer Lars Appelt, Project Manager

The purpose of this project was to improve security awareness in a company. Due to increasing amounts of security attacks and the company's outdated user awareness program, it was an important project for the company.

A program for security awareness was designed to be an interactive online program. Due to time limitations, Construct 3 was chosen as the development tool. Construct 3 enabled a quick development cycle because of the easy implementation tools and graphical user interface.

The user awareness program was deployed to all company users in the Nordic countries with a one-month deadline. As the program was mandatory, the participation rate was nearly 100%.

Feedback for the program was positive and most users recognized it as a useful experience. The IT department received important information from the user behavior data. In addition to improving user awareness, the IT department can focus on problem areas based on the user data.

Keywords	Information Security, Phishing, Cybercrime, Awareness

Contents

List of Abbreviations

AJAX	A set of web development techniques. With Ajax, web applications can send and receive data from a server.
HTML5	A markup language used for presenting content on the World Wide Web.
PHP	Scripting language for server-side applications.
VPN	Virtual private network extends a private network over a public network.
DoS	Denial-of-service attack disrupts or overloads a service by repeatedly sending requests to it.

1 Introduction

Nowadays cybercrimes are a common threat to companies of all sizes. Protecting your data cannot only be solved by information security software, but it also needs user awareness. Often, the reason for a security breach is because of human carelessness than an issue with information security systems. Therefore, companies are investing more and more resources to train their employees to recognize security threats. By doing so, users should be able to avoid social engineering and phishing attempts. In addition, it is important to know about data integrity and protection. Company's security culture is an important factor, as it should encourage users to report security incidents.

GEODIS Freight Forwarding is a supply chain operator, which helps other companies to solve their logistical challenges. The goal of this thesis is to develop a user awareness program for GEODIS Freight Forwarding, which gives the users basic knowledge and skills to work in a pro-active IT security environment. The program is an interactive course to learn about IT policies, cybercrime and how users are targeted by cybercriminals. GEODIS Freight Forwarding will use the program as part of their employee induction plan.

Information security and other security breaches are a growing cost and risk for companies. Thus, the thesis strives to improve users' security awareness with a quick but compact online program.

This thesis is divided into six sections. After the introduction section, the following section is about information security threats and their relation to user awareness. It also includes theory about course design and data concepts. The third section describes the meetings, planning and testing of the project. The topic of the fourth section is the project's focus, i.e. implementation and deployment. It goes into detail regarding how the program is designed and how it is implemented in the company. The fifth section covers the results and analysis. The analysis focuses on the user data in order to plan improvements for the program and to provide extra training if necessary. In addition, this section includes a vision for the future development of the program. One development aspect is, for example, how the program can be implemented to other GEODIS offices in other countries.

Further, the program can be used as a template for new programs for other topics and applications. The last and sixth section provides the conclusion of the project.

2 User Awareness in Relation to Information Security

This section explains the theory behind user awareness programs and the related IT security. Further, it covers best practices of creating an online course.

2.1 Information Security Threats Directed at Users

Users are targeted by many different types of security threats. Usually the attacks are social engineering and phishing e-mail attacks, but on-site security threats can also happen.

2.1.1 Social Engineering Attacks

Social engineering attacks are designed to deceive people by influencing and persuading them to believe that the attacker is someone else. With this deception, the attacker has the possibility to gather intelligence even without using any technology [1]. Despite having the best possible security training, hardware and software, a company is still vulnerable to social engineering attacks due to the human factor [1, 3].

Social engineering is an especially challenging area as humans have a built-in desire to be helpful. In an example from Hadnagy, he points out that even a major antivirus support technician can be tricked by appealing to the built-in need to be helpful. In his example, an ethical hacker pretended to be a customer of the antivirus company and convinced the support technician to visit a third party website. As this was an ethical hacking situation, the website itself was safe, but in a real world situation, it would have contained malicious software, which could have compromised the technician's computer. Hadnagy states that being aware of the value of information is an important element when dealing with social engineering attacks. [2, 344]

Even a small innocent piece of information can be useful to a social engineer. Usually social engineering attacks follow a framework, which is shown in figure 1. The attacker gathers information about the target company and builds an information database [2, 26]. There are multiple sources, which the attacker can use to gather information, and

often this information is available to anyone. For example, physical locations, job openings, contact numbers, e-mail naming conventions etc. can be found by searching from the internet or making a couple of phone calls. [2, 34]

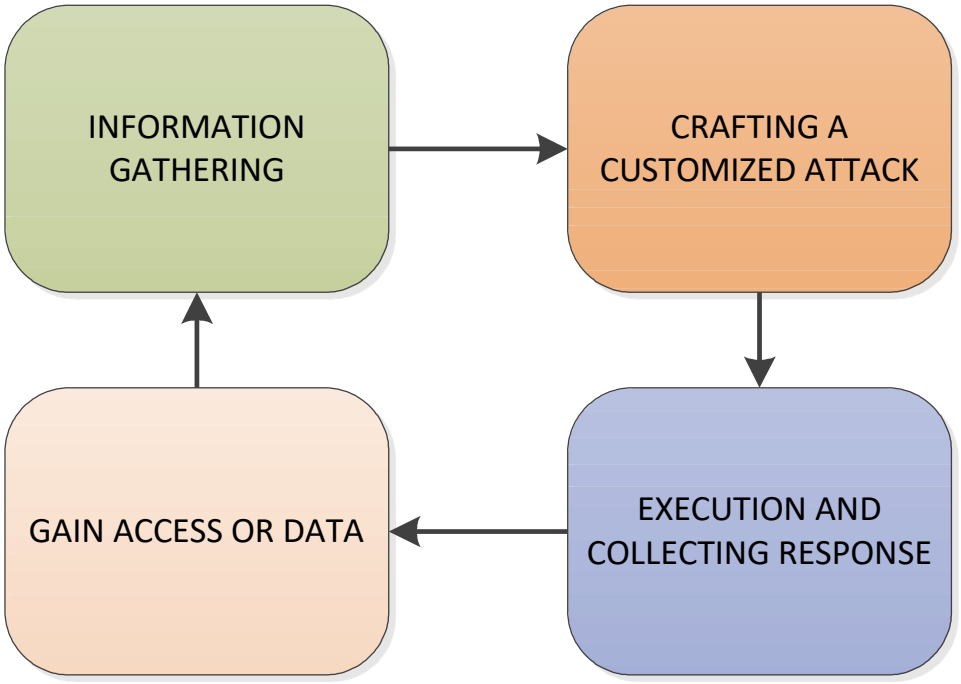

Figure 1. Social engineering framework

Once the attacker has obtained enough information, he will devise a plan how to use the information to manipulate users at the target company to reveal valuable data or to gain access to the company's systems. [2, 42]

2.1.2 Phishing Attacks

Phishing attack is attempted by an e-mail, which is designed to seem like it is from a trustworthy source. In reality, the e-mail's purpose is to manipulate users or obtain personal information. Phishing is not usually pure social engineering as it mixes both social engineering and hacking techniques. Usually the e-mail contains a malicious attachment or a link to a website, which tricks users to download malicious software or give up their personal information. Phishing attacks are usually sent in large quantities and the attacker hopes to deceive as many users as possible. [3, 2]

A more advanced technique of phishing is called spear phishing. In spear phishing, the attacker focuses their efforts on a certain target. First, they collect information on the target and then they design e-mails, which are suitable and personal. As the phishing e-mail is more detailed and focused, it can be difficult to identify and protect against it. [3, 2]

Whaling is a form of phishing where an attack is directed towards high-level executives and managers. It is similar to spear phishing, but the attack requires a specific design to appeal to the target's interest. Main difference between spear phishing and whaling is the target. Whaling attack tries to seize the interest of executives with seriousness and urgency. The fake e-mail or website may be masked as a critical invoice or an urgent claim. Alternatively, it may seem like a sensitive file that the executive would need a special program to open. The special program would contain a virus, trojan or malicious software. [4]

2.1.3 Other Types of Information Security Threats

The attackers use various other methods to obtain information or valuable assets. Many methods are purely technical and can be prevented only by technical solutions such as firewalls, anti-virus systems etc. From a user awareness perspective, it is possible to mitigate methods, which include social and physical factors.

An attacker may want physical access to information or hardware. Therefore, they have to actually show up and obtain access to a target's premises. One common method for accessing buildings is tailgating, where an attacker will follow an employee or a group of employees in order to enter the premises with them. Shoulder surfing is another common method, where an attacker tries to spy on the user’s password or access code while they are typing it. [5, 241]

Users should also be aware of the information they are throwing out to the trash bin. All sensitive information should be discarded securely as the attacker can go "dumpster diving". This literally means that the attacker will go through a target's trash in order to find valuable information or something that will help them get access to the information. [5, 240]

2.2 Security Awareness Culture and Threat Mitigation

2.2.1 Creating a Training and Awareness Program

An information security policy does not mitigate security threats if users are not properly trained. The training program should compel the users to change their way of thinking and activate them to contribute to the company's security awareness. It is important to explain the reasoning behind the policies, so the users understand why security policies are in place and why it is not allowed to break the rules due to convenience.

Motivating users to protect the company's data is essential for a good security program. One way is to personalize the task for the users. For example, companies have a large amount of employee data, so it is also beneficial for them to protect the data as it could be their information that could be stolen. [1, 249]

Security awareness is a program that needs continuous development and support. The training has to be applied to each person in the company who has access to sensitive data or company assets. On the manager level, a commitment to security policies is important as it relays a message of importance to the employees. [1, 250]

2.2.2 Data Confidentiality, Integrity and Availability

The confidentiality, integrity and availability triad (CIA) is a concept for organizations to protect data against exploits or attacks. It is a model designed to ease users to realize the important parts of information security. As seen illustrated in figure 2, the CIA triad forms a connected triangle between confidentiality, integrity and availability. [6]

Figure 2. Confidentiality, integrity, availability triad [7]

Confidentiality focuses on the access of information, data or assets. Access should only be assigned to those who need it. This requires that the information is organized to appropriate access levels and that the access levels are maintained. In IT systems, confidentiality is managed usually with file permissions, encryption and access control lists. [6][8]

Data integrity is a principle that is designed to protect the data from tampering, deletion and alteration by unauthorized persons. Integrity also includes an aspect of backups as if the data has been falsely modified, it can be restored. Data's integrity means that data is accurate and complete. [6][8]

The final component of the triad is availability of the data. Without data availability, users cannot work properly as various information systems would not function correctly. Availability can be boosted by preparing for possible failures and issues. For example, networks could have a second redundancy network in case the main network has a failure. For a power outage, a company might have their own power generator, which enables them to work during the outage. In network security, the system could be designed to handle potential attacks from outside such as denial of service attacks (DoS). [6]

2.3 Mitigating Security Threats

Mitigating security threats and attacks starts by identifying the threat. Anti-virus, firewall and other technical security systems will protect computer systems to some extent, but mitigating attacks, which use the human factor, is more challenging. An average everyday user does not have the technical skills to recognize finer details in security attacks. Usually companies do not have a full-time IT security person to help the everyday users. Therefore, user awareness programs are an extremely important part of the overall information security plan.

2.3.1 Critical Thinking

Critical thinking can prevent many attacks with very little effort. When a user receives a message or phone call, they should stop for a moment and think about what is happening. Hadnagy [3, 76] lists the following questions that the users can ask themselves to help evaluate the situation:

- Does the e-mail come from someone I know?
- Was I expecting this e-mail?
- Are the requests being asked of me reasonable?
- Does this e-mail employ the emotional content of fear, greed or curiosity, or most important, does it try to get me to take an action?

With these questions, a user can identify phishing mails more reliably than before. An attacker wants users to react, not think. Therefore, spending a small amount of extra time with this method will increase the change to prevent certain types of social engineering attacks. [3, 77]

2.3.2 Emotion and Perception

Phishing e-mails and fake websites rely on the target's carelessness. The attacker aims to invoke an emotional reaction to nullify the target's logical thinking. For example, an e-mail that says you have won a prize is meant to invoke surprise and joy. The attack could

also be about danger and urgency, but the main goal is to get a target to act based on emotion and not logic. [3, 41]

To avoid reacting with emotion as shown in figure 3, the target should take a moment to think about what is happening and use critical thinking. After relaxing, the user is again in control of his emotions and can make a logical decision. [3, 48]

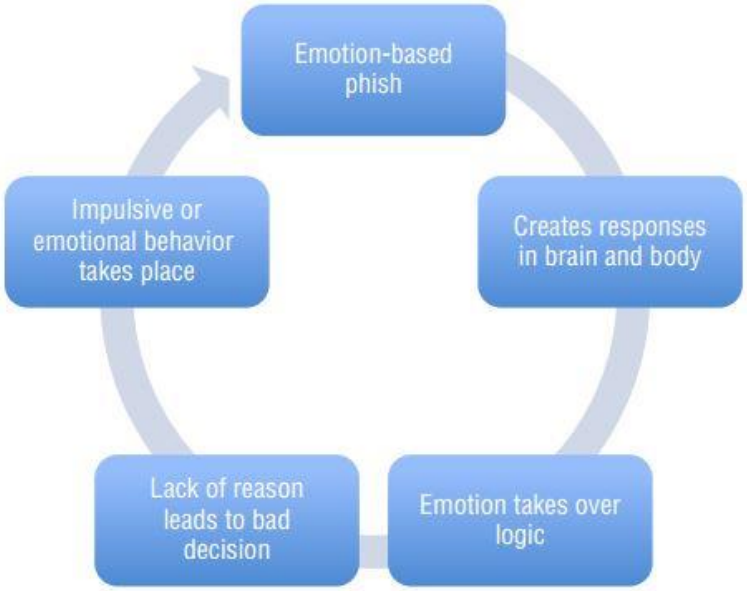

Figure 3. Emotion cycle in a phishing attack [3, 43]

Being perceptive helps identifying phishing e-mails and fake websites. There are many ways to spot a fake mail, but usually it only needs a bit of perception. For example, many phishing e-mails look like they are sent from a certain company or individual. However, by looking closely at the sender details, it is clear that the e-mail is coming from a different address. Attackers use various methods to mask the actual sending address. One common method is to use a domain that resembles the actual legitimate domain. For example, instead of @microsoft.com they could use @microsoftware.com. If a user is in a hurry, they might mistake the phishing e-mail for a real e-mail and click the harmful link or attachment. [9]

Figure 4. Example of a fake e-mail sender information

Hovering, as shown in figure 5, is a basic method that can be used to examine links on the mail. When the mouse cursor is hovering over the link, the actual address of the link is shown. With this method, fake addresses can be identified effortlessly. [3, 77]

Figure 5. Example of hovering

If an e-mail contains spelling mistakes, it can be a sign of a fake e-mail. Usually companies have precise rules about communication and they encourage users to send presentable messages. Therefore, valid emails have less spelling errors and the format of the message is clean. [9]

Checking basic aspects of an e-mail or a website helps identifying if it is valid or not. These methods are quick to use once the user makes it a habit.

2.3.3 Professional Methods

More advanced methods are for situations where it is difficult to identify the trustworthiness of the e-mail.

By analyzing e-mail headers, it is possible to check how the e-mail was sent to the recipient's address. E-mail headers include detailed information about the sender, which

gives an accurate insight where the e-mail came from. Analyzing e-mail headers require technical knowledge, so this method is not that useful for a basic user. [3, 85]

For professional users, it is possible to create a sandbox where they can test a suspicious file or code. Sandbox is essentially an environment, which is isolated from the main system. This means that whatever is running inside the sandbox, cannot affect the rest of the system. [3, 90]

2.3.4 Reporting Culture

Promoting a security culture in companies encourages users to report poor security practices and incidents. It is important for companies to recognize the value of incident reporting and it should not affect the users in a negative way. If users must worry about punitive measures, they may not report the security incident at all. In addition, if the process for reporting is cumbersome and requires extra work, it can also lead to silence.

By showing the positive impact of reporting, users will see that their actions have an effect to the company's security and they feel that they have something to contribute. Even if many of the reports might be false positives, it will still improve the overall awareness at the workplace. Creating a security incident report should be easy for users. As most users will not report incidents often, it must be encouraged by an excellent user experience. If a company’s reporting culture is not working, it is difficult to know and estimate how many security threats users are experiencing. [10]

2.4 Security Training Course Design

2.4.1 Best Practices of Security Training

Companies have their own style and design for their security awareness programs, but there are some best practices that should be considered. One key element is to make a program for the whole organization. If some employees are excluded from the program, it can affect the mind-set of the employees who are participating in the program. Security should be everyone's concern and not just certain employees. [11]

Establishing a baseline for security knowledge levels and security incidents helps to measure the effectiveness of the security awareness program. Before implementing a new program, creating a report of incidents, phishing attacks etc. can give valuable information and a way to compare the results of the awareness program. [11]

A security awareness program needs to be updated constantly and employees should also reinforce their knowledge by revisiting the program. For example, a yearly or bi-yearly schedule would be sufficient for re-training. In addition, occasional phishing tests are a way to keep employees alert and to test their security awareness levels. However, following up on the phishing test is equally important to inform employees and give them a chance to improve their security awareness. [11][12]

Applying gamification to the security awareness program can motivate employees to use their security knowledge. For example, scoreboards, positive reinforcement and rewards can elevate the effectiveness of the security awareness program. [11][12]

2.4.2 Online Course Design Theory

For an online security awareness program, there are best practices that should be applied. Even though, the training program includes interactive elements, it should follow the basics of instructional design. According to Debbie Morrison's course design, it should include a plan for instructional plan, learning materials, activities and assessment. In addition, Morrison presented a course design framework, which explains the basics of designing a course.

The instructional plan consists of content presentation details. How will the content be presented to students? The learning materials include all the content and material, which is provided for the students. Activities would include various interactive ways to learn and apply the content in to practice. Finally, a way of assessment should be presented to the student, so the learning experience can be evaluated.

In the basic course design framework, Morrison divides the design into four parts: analyze, develop, implement and evaluate/redesign. The first step is to analyze the problem or the need for training. The next step is to analyze the target audience: What is their

motivation, background and skill level? Knowing the limitations, strengths and properties of the delivery platform makes it easier to develop a course.

The develop phase focuses on the learning strategy and how to optimize it. Selecting, creating and using content efficiently is a key part when designing a course. Students should be guided with activities to apply the content and build knowledge. In addition, course evaluation and assessment methods should be considered.

On the implementation stage, it is time to evaluate the course format and test with a pilot group. After implementation comes evaluation and redesign if necessary. It is important to collect and analyze feedback and revise the course based on that. [13]

3 Meetings, Planning and Testing

This chapter describes how the project was planned, tested and what kind of meetings were held during the planning phase.

Due to the increasing amount of phishing mails received by the employees of the case company, it was obvious that employees need more training on security awareness. The old security awareness information was a bloated PowerPoint presentation, which did not catch employees' attention efficiently enough. It was decided that a new lighter and interactive version of the security awareness program could be more effective.

3.1 Meetings

In order to figure out if the project would be valuable for GEODIS, an initial meeting with the GEODIS Nordic's security manager was held in the beginning of 2018. It was concluded that the current user awareness program was not effective enough and required too much resources from the IT department. A solution would be to create a new improved program, which fixes the issues from the old program. It was decided that the new program should fulfill the below requirements:

- Clear and quick content
- Stand-alone program
- Maximum length of 15 minutes
- Available for all GEODIS Nordic employees

The content should be based on the old user awareness program, but a great deal of it would be cut out to make the new program more accessible. Stand-alone program means that the IT staff should not spend time with the user while they are completing the program. A maximum length of 15 minutes was decided so it would not take too much time from the employees and to ensure high completion rate for the program. The program should be available to all employees as a mandatory course. This was an extremely important requirement as the user awareness program should be a part every employee's basic training.

In the second meeting, content was discussed in more detail. Basic structure for the course was decided and gamification possibilities were considered. However, because of the tight schedule, it was decided to settle for simpler interactive slides. The program was to be developed during the summer of 2018, when the IT department has more resources available due to users' summer vacations. The program was scheduled to be deployed after the summer vacation period in September.

3.2 Planning

After the initial meetings, detailed project planning started. The first stage of planning was to find out the development method for the new program. As programming time and skills were limited, it was suggested that a 3rd party tool might be better suited for the project. After some initial testing with a development tool called Construct, it was chosen for the main tool for the project.

During the planning stage, a basic flowchart, as shown in figure 6, of the program was suggested. The program would be hosted on a web server, which users would have access through their web browsers. The user input would be saved as data to the server and eventually the IT department staff would handle the data.

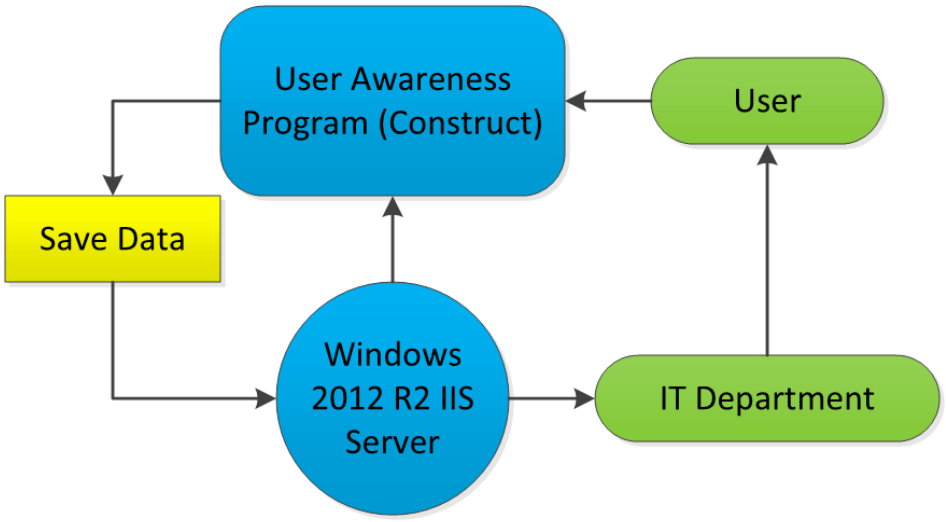

Figure 6. Initial flowchart for the program

Content planning followed the structure from the old user awareness program, however a large amount of the old content was cut out. The remaining content was re-written to match the compact vision of the new program and designed to fit the layout plan. Content was organized into balanced order so it would be a mix between reading and interactivity. The program would follow a slide structure for presenting the content.

In order to receive user data, it was decided to include a quiz about the program content. Quiz questions were created based on the content and subjects which the IT department wanted to emphasize. The questions were not to be too complex or difficult as the user base varies from basic users to experienced users. The amount of questions were to be kept below ten, as the quiz should fit on one slide.

The overall look for the program were to follow the GEODIS branding. The marketing department provided various GEODIS brand logos and icons for the program. In addition, the color scheme was to match with the GEODIS brand.

3.3 Testing

Testing was done within the IT department. First, each layout was tested separately once it had been created. Once the project reached alpha version where all layouts were available, the IT department staff tested the program and searched for issues. Initial testing revealed issues with data collection as in some cases the quiz scores would reset. Other bugs were found on slide transitions as in some cases the user could not continue to the next slide.

After the initial issues were fixed, the focus shifted on improving the user experience. The login function was limited to geodis.com addresses to simplify the login process. Text size and the overall look were improved based on test feedback. The data collection format was finalized so reports were easier to create.

4 Development, Implementation and Program Focus

This chapter explains the development phase of the program. It goes in detail to how the program was designed and what is included in the program. Program implementation, target group, program focus, current security threats and program deployment are also explained here.

4.1 Programming Engine – Construct 3

The security awareness program was created with an HTML5-based game/multimedia engine called Construct [14], which is developed by Scirra Limited. Construct 3 was released on March 28 in 2017 and it is the latest edition of the software. Construct 3 was chosen for this project due to its quick development cycle and HTML5 compatibility. Construct is written in C++ and JavaScript, but using it does not require traditional programming. Instead, Construct 3 uses a visual editor in a drag-and-drop fashion including a behavior-based logic system.

The main programming method in Construct 3 uses “event sheets”, which are comparable to source files used in more traditional programming languages. The event sheet contains triggers and statements with programmable conditions. When a trigger or a condition is matched, the function will perform its task. In addition, sub-events and groups can be used to create more complex systems when necessary.

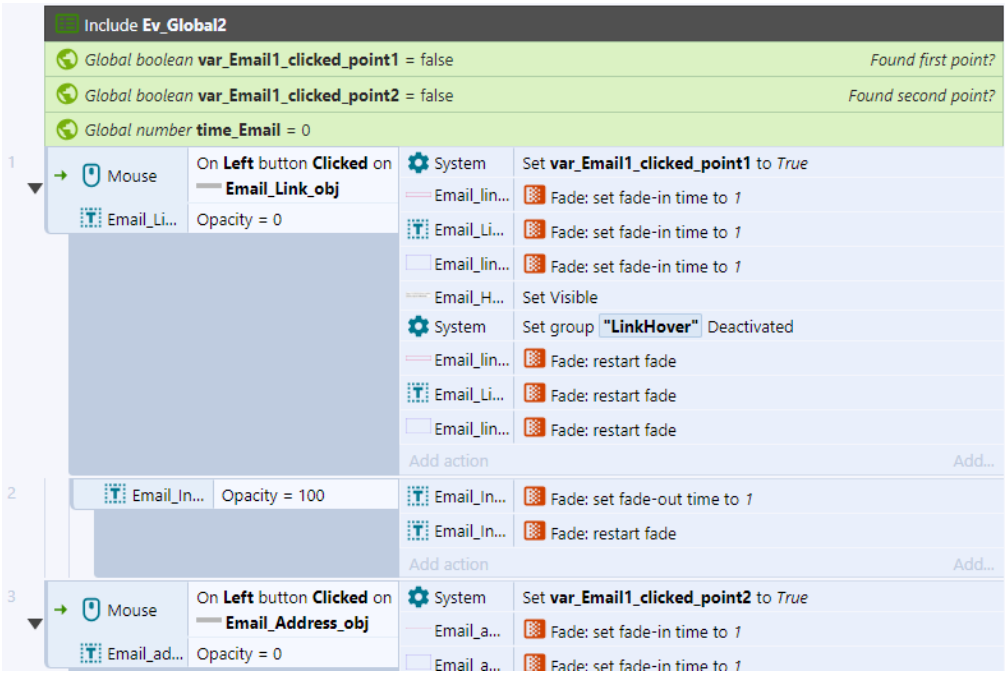

Figure 7. Example of an event sheet in Construct3

Construct 3 supports multiple platforms and storefronts. For example, it is possible to export to several different online platforms such as Facebook, the Chrome Web Store and the Amazon Appstore. In addition, it is possible to create native apps for Windows, Linux and OS X. [14]

4.2 Program Design

The program is divided to 17 different layouts, which are essentially like a slide or a page in the program. As the user goes through each slide, the program will save data about the user's progress. Data includes quiz scores, total time spent, clicks on info boxes and program feedback. After the program is finished, the data is saved to a server by Construct's AJAX plugin and a PHP script. The data is saved to a variable, which is pushed to the PHP script by request URL method. The flow of the program is described below in figure 8.

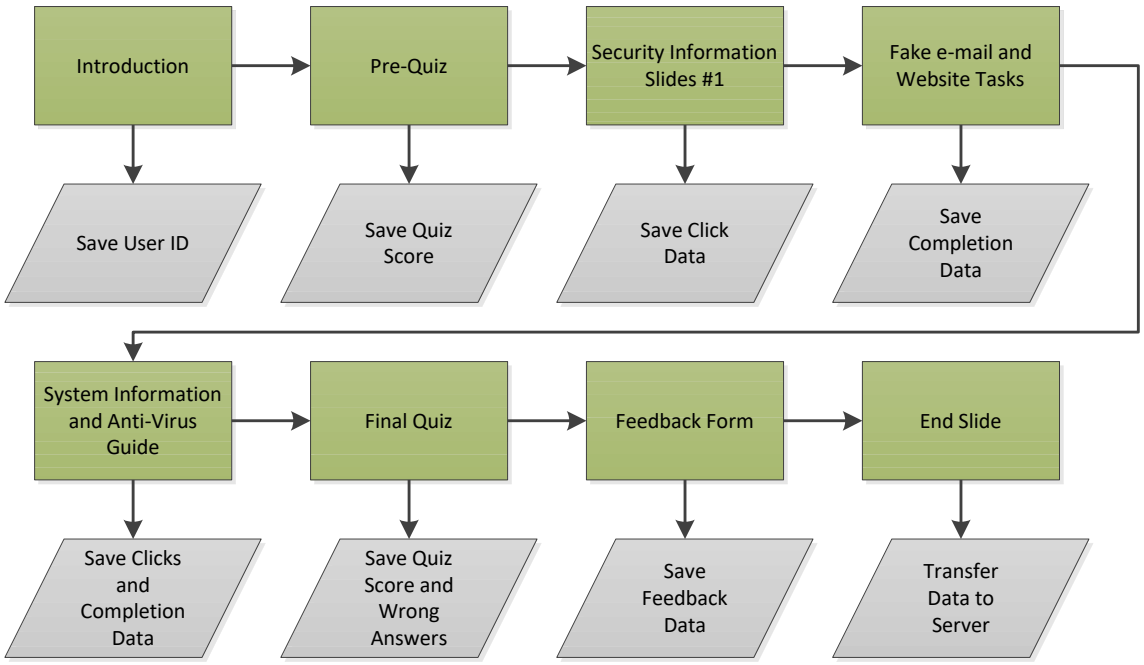

Figure 8. Basic flowchart of the program

The program is running from a Windows Server 2012 R2, which has Microsoft Internet Information Services version 8 (IIS) enabled. In addition, PHP module has been installed to support the data export scripts for the program. The web server is only for internal GEODIS access as the program is meant only for internal use.

4.2.1 Layouts and Event Sheets

The 17 layouts of the program are the visual structure of the security awareness program. The layout structure begins from the starting page of the program and continues with an introduction and login page. This introduction page gives the user a list of contents and asks them to login to the program. The login function is only a simple “save a variable” function, as it is not necessary to have an authentication system for this program. The only requirement is that users write their work e-mail address to the login field, which is why there is a built-in check for the e-mail address variable. The address has to be in the form “@geodis.com” in order for the login to work.

After logging in, the actual program content starts with a quiz to map the user's starting knowledge. The quiz is constructed from eight multiple-choice questions and each question is worth one point. At this stage, detailed answer data is not saved. Quiz points are saved to a variable, which will be used to compare to the results of the final quiz at the end of the program. The final quiz is otherwise identical, but it will save detailed data from the wrong answers.

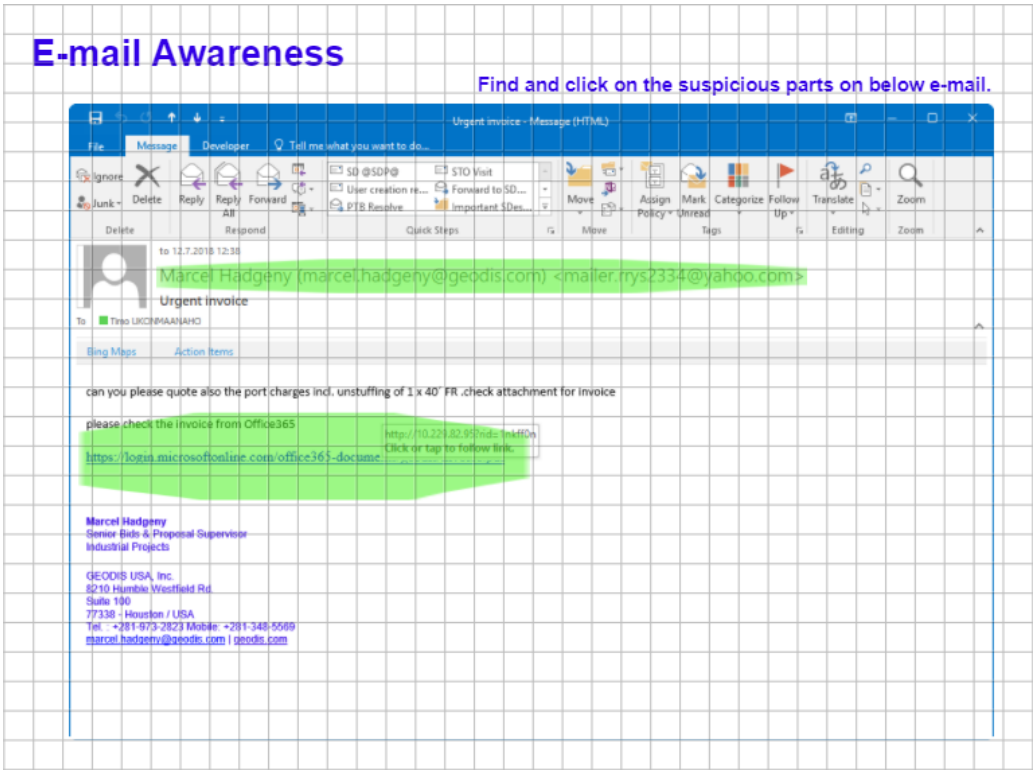

Figure 9. Example of a layout and clickable triggers with green color

The following four layouts are informative pages with some minor interaction. The user can click on objects and receive more detailed information about the content of each page. The information content fades in and out according to the user's actions. User interactions are saved to a variable to follow user behavior on these pages. In addition, throughout the program, data on time spent is recorded for each page.

The next slides about phishing mails and a fake website are more interactive and contain clickable objects for user to find. The goal is that the user would see the examples and pick out any suspicious signs. After clicking the hidden objects, detailed information

about the content will appear. In case the user tries to skip the task, the content is revealed and the user is urged to read it through.

The rest of the slides before the final quiz contain information about password policy, explanation of VPN connections and two guides on internal systems. The information content is similar to previous pages, which contain clickable objects. As for the guides, the second guide for anti-virus is an interactive animation, which shows the user how to perform a virus scan on their client machine. The slide contains an animation with clickable triggers. As the user follows the instructions, the animation proceeds identically to the real application. The guides have a variable, which records if the user skipped them or completed them.

After the final quiz, there are only two slides left: feedback form and ending page. On the start of the feedback page, the final time is calculated and saved to a variable. At the end of the layout, the feedback will be composed to a single variable. Once the user reached the ending page, the final user data variable is constructed and sent to the server via PHP script. PHP script saves the data to a new line on a txt-file. To make the data easier to handle, the user data, feedback data and wrong answer data is saved to different txt-files.

4.2.2 Data Files

The user data is saved to semicolon delimited text files, which are designed to be imported to Excel. The data is divided to three different files: behavior, feedback and wrong answer data. The first two are linked to the user's login information, but the wrong answer data only shows the amount of each wrong answer. The user behavior data contains the following information:

- Date of completion
- User login information
- Quiz scores
- Amount of time spent on each slide and total time spent on the program
- Clicked objects on the slides

- Completed guides

For the feedback data, in addition to open feedback, the users are asked to answer the below questions:

- Do you feel that you are more familiar with IT security than before?
- Do you think that the content of this course is useful?
- Was it easy to understand the course content?
- What grade would you give the course?

The main purpose for the feedback is to measure user satisfaction for the program. The questions were designed to get the user's impression of how their security knowledge improved after completing the course. Also for future development, it was important to receive feedback from the content. Therefore, users were asked to give their opinion on the content's usefulness and comprehensibleness. Finally, users were asked to grade the course from one point (worst) to five points (best).

4.3 Program Focus

The goal of the program is to teach users about security awareness, therefore the focus is on the current popular frauds and phishing attempts. In addition, the program includes general information about security awareness, local IT policies and local security related tools. Some interactivity was dded to the contents to encourage user participation. For example, in the beginning and end there are a startup and a final quiz for the user. The intention is to get the user to notice their improvement and to get data of their progress.

Another goal is to extract useful data about possible problem areas in security for the IT department. This data will be used to improve security by focusing directly on the possible problem areas. In addition, there are two phishing mail examples, which require users to find suspicious elements from the mails. Phishing mails are one of the main elements of the program as they are the most common threat affecting GEODIS now.

Gamification elements were originally planned for the project, but due to time restrictions, it was decided to use more straightforward interactive elements. For future releases, the gamification elements are still being considered.

4.3.1 Target Group

The program was designed to teach security awareness to every employee in the company. This includes for example warehouse workers, operational staff, sales people, local managers and country managers. It is mandatory for all employees to know basic elements of IT security and be aware of possible threats. Although the security awareness program was designed for the Nordics division of GEODIS, with minor changes it can be implemented in other countries also.

Nearly all of GEODIS employees in Nordic countries have a personal e-mail account and use e-mail daily for their work. In addition to employees' e-mail access, logistics and shipping companies are often targeted by phishing attacks. This is why it is very important that all employees of GEODIS are trained against social engineering and phishing attacks. Employees handle a large amount of invoices and shipping notifications on a daily basis, therefore it can be quite easy to open a fake attachment from a phishing mail.

4.3.2 Security Threats

In 2017 and 2018, GEODIS has seen an increase in e-mail based attacks. Crypto-ransomware [15] attacks caused issues before proper protection was placed on clients and servers. Different variations of cryptovirus are still a threat, which is one reason for users to be aware of e-mail based attacks. Ransomware attacks typically come through an attachment in an e-mail. After the user has tried to open the attachment, a trojan is installed on the client machine. The trojan will then start contacting control servers to generate an RSA key pair for encrypting the client machine's files. In worst cases, the trojan will also start encrypting files on fileservers if the user has access to them. Usually it is possible to restore the encrypted files from backups, but there has been incidents where user's local data has been lost due to ransomware.

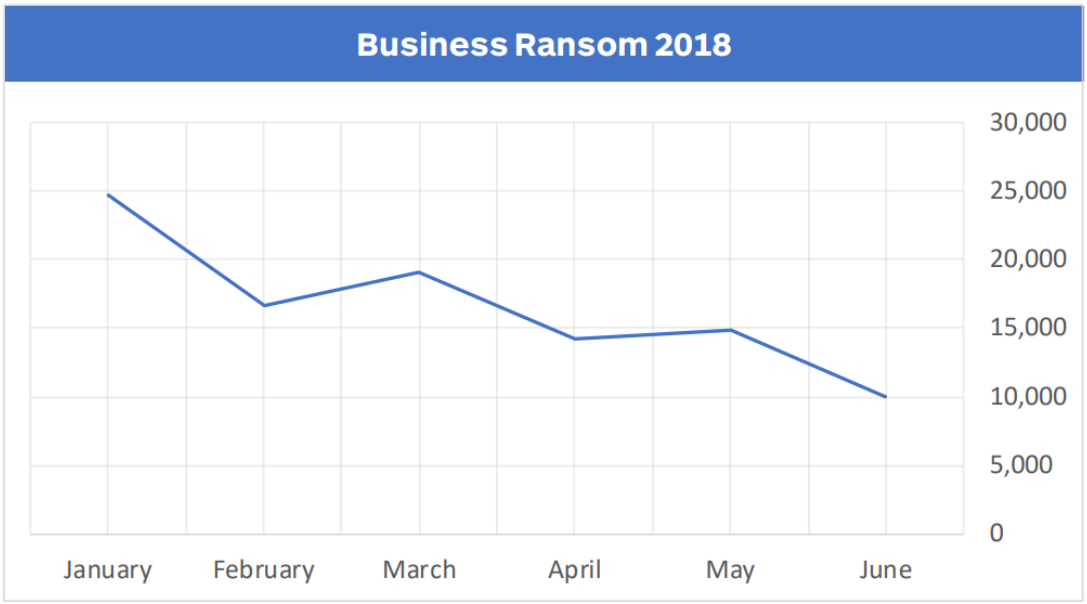

Figure 10. Business ransomware detections, from January to June 2018 [15]

Since 2017 crypto-ransomware attacks have been declining, as shown in figure 10, but phishing mail attacks have increased.

In 2018, Office 365 related phishing mails have increased to a weekly problem, which makes security awareness extremely important. An example of an Office 365 phishing mail can be seen in figure 11. As phishing mails target users instead of clients, security software cannot block every attempt. The current trend of phishing mails is designed to capture user's Office 365 credentials and then use those credentials to send more phishing mails inside the organization. In addition, the attacker will create mailbox rules so that any replies to the phishing e-mails will be automatically deleted. These rules makes it more difficult for the user to notice that something is wrong. This method has been quite dangerous as users are often less careful with mails within their organization. One of the goals in the security awareness program is to teach users to recognize fake e-mails and Office 365 login pages.

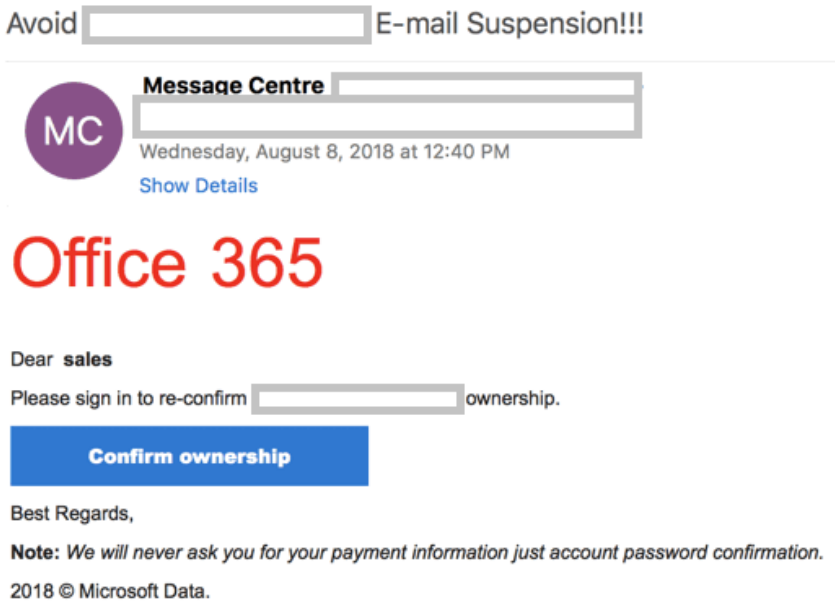

Figure 11. Example of Office 365 phishing e-mail

More traditional phishing mails focus on malicious attachments. Often the attackers mimic a well-known company, for example DHL, and try to trick users to open the malicious attachment. In the logistics and shipping industry, these phishing mails might be especially effective as the users deal with these companies in their daily work.

4.4 Implementation

The security awareness program consists of 14 pages. The purpose of the program is to familiarize the users with the company's security policy, improve security awareness, encourage security incident reporting and provide information about security threats. In the beginning of the program, there is a short quiz to measure the user's starting level. At the end of the program, the same quiz is presented to measure the user's progress.

The focus of the program is e-mail awareness, phishing mails and fake websites. The program includes two interactive examples of phishing mails and one interactive website to spot fake login pages. The e-mail examples teach users about fake sender information, which is also called e-mail spoofing. Users will learn to recognize the fake address from the sender field. Links are the second focus of the e-mail examples. Once

users click on the suspicious link in the example, they receive an explanation how attackers try to make the links look authentic. The example goes on to inform users how to use hovering to check the actual link. On the fake website example, users are reminded to always check the URL of the page. The example also explains the difference between HTTP and HTTPS. On the login part, users are shown how the real Office 365 login window looks like with the official GEODIS branding. In addition, users learn about data handling (CIA) and basic IT security. After completing the program, users have a possibility to leave feedback about the program.

The program also has two guides for applications used in the company. One guide is for a self-service portal called iForgot. The guide opens the iForgot portal webpage and helps the user to enroll to the service. Another guide is for antivirus software McAfee Endpoint Security. The user has to follow detailed instructions on how to use the scan function in McAfee.

The program saves data based on user activity. Beginning and final quiz scores are saved to have a comparison between starting level and after completing the program. To monitor user activity, time stamps are saved to measure time spent on each slide. Total time is saved at the end of the program. This data is used to evaluate if the users have gone the content through or merely skipped to the end. Click data for the information boxes, completion rate for the guides, fake e-mails and website are saved as well. This data is used similarly to the time data to see if users have actually clicked on anything on the pages.

On the final quiz, the program saves data about wrong answers. This data is not personalized, but it gives an idea what can be improved and what kind of information can be emphasized in the future versions of the program. In addition, users were sent an info package based on the wrong answers. This was done to emphasize the common mistakes and spread correct information to the users.

4.5 Deployment

The program is mandatory for all users in the company. Users were sent a link to the program via e-mail and the participation was followed based on the completion data received from the program. Users were given one month to complete the program. Reminders were sent in the middle of the month to ensure high completion rate. After the deadline was up, a final reminder were sent to users. In total, 570 users completed the program.

Deployment started with two smaller Nordic countries, Finland and Norway. A day later, program was deployed to Danish users. Then again, a day later the program was deployed to the largest user base, Sweden. The gradual deployment made it possible to fix minor bugs and apply the needed improvements before most of the user base were completing the program. The early feedback included issues about font size and minor graphical bugs. In addition, the data collection for wrong answers was optimized on the backend.

User participation was monitored and updates to IT management were sent almost every workday. This ensured that the participation rate was on track to achieve 100% completion rate.

5 Result Analysis and Future Development

The user awareness program provided different kind of user data, which can be analyzed to improve the security training and culture at the company. User behavior and feedback data will be useful for the future improvements on the program. Quiz answer data is useful to determine problem areas in the current user database.

5.1 User Behavior

User behavior data includes data about click counts on the information boxes, time spent and guide completions. In total, 570 users completed the program during its one-month run. On average, users spent 805 seconds on the program, which shows that most users have completed the program properly. It was estimated that it would take roughly 5 to 10 minutes to go through the program thoroughly. Eight % of the users spent less than 250 seconds on the program, which is not enough time to go through the content.

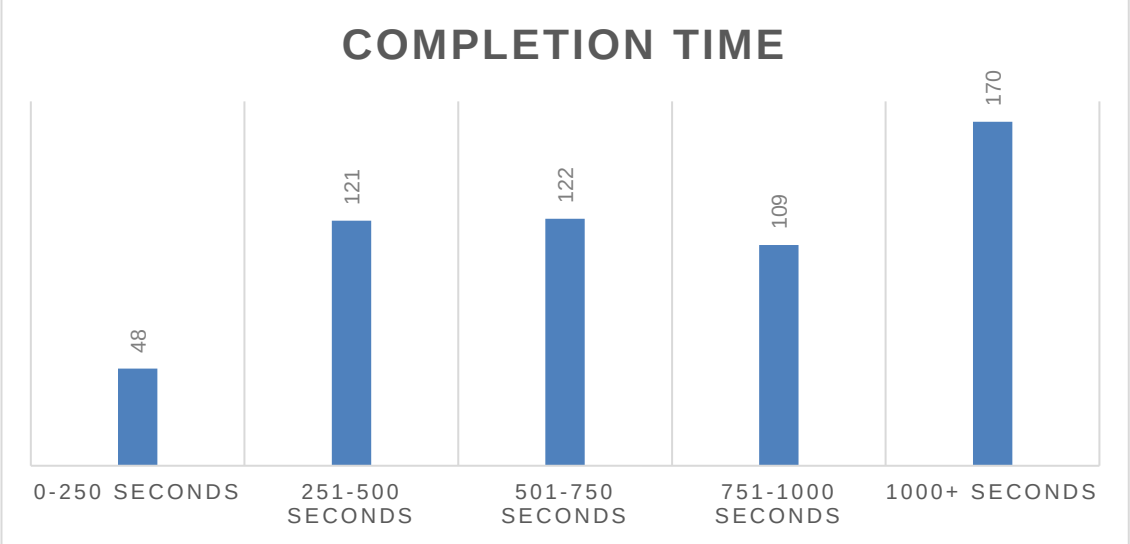

Figure 12. Amount of users in different completion time categories

In figure 12, users are divided to five columns by their completion time. 60% of the users completed the program between 251 and 1000 seconds. 170 users spent over 1000 seconds to complete the program. However, since many users are taking the program during work hours in an uncontrolled environment, they may have interruptions during

the program. This increases the completion time. Therefore, these results are not objective, but give only an approximate estimation. For the 48 users who completed the program in less than 250 seconds, it is clear that the program content was skipped through. It is possible that these users will have to participate in extra training due to the IT security requirements of the company.

5.2 Feedback Data

As expected, 87% of the users thought that they feel more familiar with IT security after completing the program while 13% of the users felt that the program made no difference at all. The majority of the users said that the content of the program was useful. However, a small amount of users felt that the program was not useful and one user reported it to be a waste of time. As for understanding the program content, most users felt it was easy to understand the content. Only a small percentage felt that the content was somewhat difficult to understand.

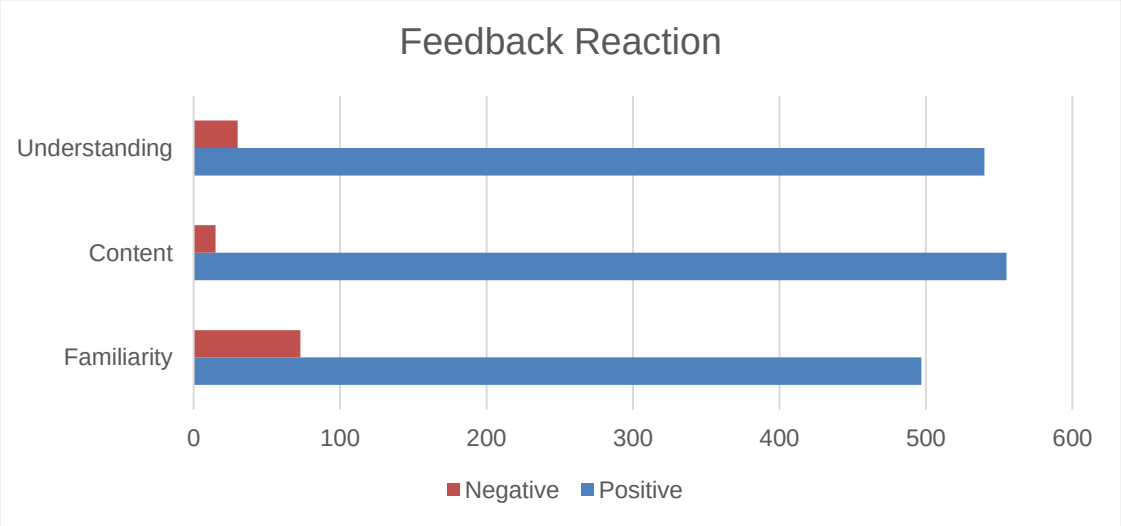

Figure 13. Negative and positive feedback

Overall, the users were satisfied with the program as the average score was 4.44 out of 5 points. Optional feedback from the users included mostly positive comments and reports on issues such as small text size. Users appreciated the fact that the program had a good balance between length and content.

5.3 Quiz Data

The program included two quizzes: a start level quiz and a final quiz. Both quizzes are exactly the same and the goal was to measure the user's improvement after completing the program. In addition, it was designed to give users a feeling of success as they can see their result improved after the program.

The start level was quite good as the average score was 5.7 points. The final quiz average score was 6.6 points, which is a small improvement compared to the starting level.

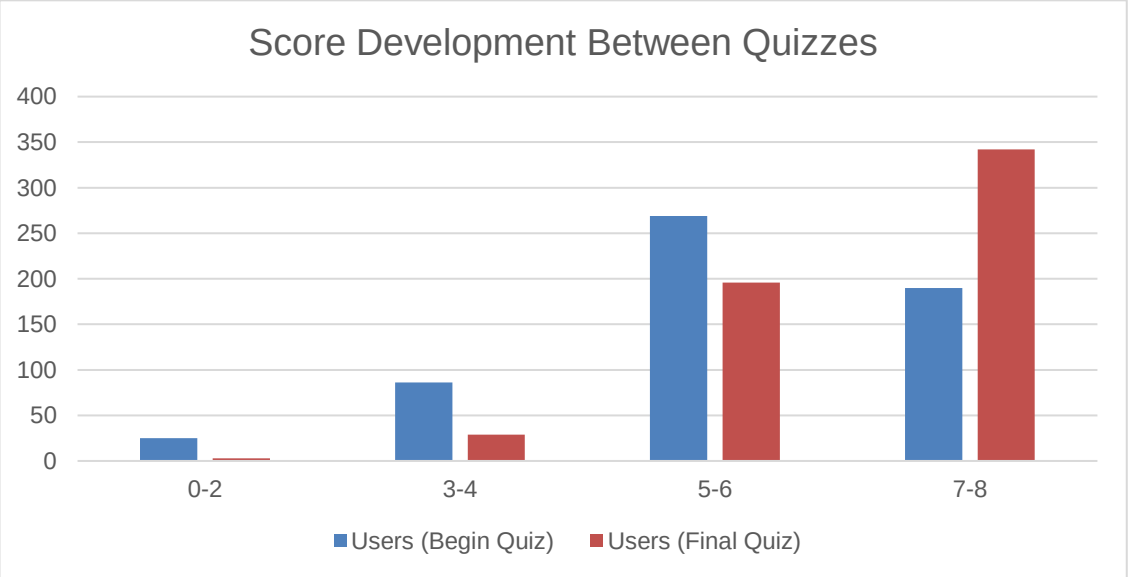

Figure 14. Comparison between beginning and final quiz scores

In figure 14, it can be seen that most users were performing well already in the beginning quiz. 459 out of 570 users achieved a score between five and eight. When comparing to the final quiz scores, the majority of the users (342) scored in the higher category of seven to eight. Compared to the beginning quiz, where most users (269) scored between five and six, it is a clear improvement. The lower score categories between zero and four shrank from 114 user to 32 users, which shows that the course content helped many users to improve their scores significantly.

As the quiz was not extensive and some questions were more about the company's IT policy than IT security, it is difficult to determine definite analysis from the quiz data. The

answer data shows that users need more information about password security, company's IT policy and phishing mails. 201 participants out of 570 had problems with a question about password complexity. Data backups were also another problem as 41% participants did not know where their files would be backed up.

This data was used to compile an information package to the users. In the package some of the results were presented and the problem areas were explained more thoroughly.

5.4 Future Development

The program is planned to be deployed every year to refresh the users' IT security skills. Therefore, the program needs yearly updates and improvements, which means that the content and backend programming will be updated according to the ever-changing security climate. The first priority is to improve the quiz questions to make them more relevant and to measure the users' knowledge more precisely. To make sure users go through the content properly, new minigames and miniquizzes could be implemented to the e-mail awareness section.

Internal phishing e-mail testing is being considered as an additional element for the program. These phishing e-mail tests could give valuable data about the program's actual effect on the users. One possibility is to have an internal phishing e-mail test a month before the next security training deployment. Then about two months after the deployment is done, there would be another test to see if there has been any improvement on the internal phishing e-mail test.

Language selection is one big improvement that could be implemented in the future. This requires extensive changes on the program, but it would be easier to update in the future. The feedback form will be extended and the feedback choices will be blank on default. In the middle of the implementation, it occurred that having the best choices as default in the feedback form might skew the feedback results. Many participants might click forward on the feedback form without caring what kind of feedback they are giving.

The program will also have a manager version, which focuses on more in-depth to content for department managers. Managers need to be more aware of IT security as they

are popular targets for phishing attempts. In addition, managers usually have more access rights than a general employee, which makes it even more important to have knowledge of possible security threats.

During the implementation, a couple of bugs were discovered related to Internet Explorer 11. As these were limited only for a few users, the issues were not fixed. Instead, the issues will be fixed in the upcoming version next year.

6 Conclusion

The goal of the project was to create an interactive way for users to learn about IT security and to replace a static PowerPoint presentation. This main goal was reached successfully as the program was completed and implemented among the users. This program was a step forward in creating a new security oriented culture in GEODIS.

Overall, GEODIS' Nordic IT management was very satisfied with the program and would like to keep building on it. Based on the user feedback, the program was successful and other IT departments within GEODIS countries were interested to adapt the program to their organization. Phishing mails are an increasing issue for companies and a serious security risk each time a user falls for it. This project presented a quick and easy way to deliver important content to the users. As the program can be used as a template, the following projects will be easier to develop and they can be deployed within weeks. Compared to a more traditional static online program structure, it might take months to deploy a new program. By then, the security threat might have already be fading out or evolved to different kind of threat thus negating some of the content for the traditional online course.

As a learning experience, this project was a great experience because of the easy to adapt game/multimedia engine Construct. Programming with Construct has its own challenges, but after getting familiar with it, building applications is quite fast and easy. As the project was more or less a one-man operation, the experience was diverse due to the many aspects of the project. Among other things, the project contains animation, graphic design, pedagogical design, programming and theory of information security.

References

1 Mitnick KD, Simon WL. The Art of Deception: Controlling the Human Element of Security. Indianapolis: Wiley Publishing; 2002

2 Hadnagy C. Social Engineering: The Art of Human Hacking. Indianapolis: Wiley Publishing; 2011

3 Hadnagy C, Fincher M. Phishing Dark Waters. Indianapolis: Wiley Publishing; 2015

4 Gil P. What is "Whaling"? [Internet]. Lifewire. 2018 [cited 21 March 2018]. Available from: https://www.lifewire.com/what-is-whaling-2483605

5 Allsopp W. Unauthorised Access. Hoboken: John Wiley & Sons, Ltd.; 2009

6 Perrin C. The CIA Triad [Internet]. TechRepublic. 2018 [cited 21 March 2018]. Available from: https://www.techrepublic.com/blog/it-security/the-cia-triad/

7 Purcell A. 3 key ideas to help drive compliance in the cloud [Internet]. IBM. 2018 [cited 21 March 2018]. Available from: https://www.ibm.com/blogs/cloud-computing/2018/01/drive-compliance-cloud/

8 CIA Triad [Internet]. InfoSec Resources. 2018 [cited 21 March 2018]. Available from: https://resources.infosecinstitute.com/cia-triad/

9 Harris L. 10 Tips on How to Identify a Phishing or Spoofing Email [Internet]. Return Path. 2015 [cited 22 March 2018]. Available from: https://blog.returnpath.com/10-tips-on-how-to-identify-a-phishing-or-spoofing-email-v2/

10 Gjære E. Four Steps to Have Employees Report Security Incidents (And Save the Day) [Internet]. Security & People. 2017 [cited 16 May 2018]. Available from: https://securityandpeople.com/2017/08/four-steps-to-have-employees-report-security-incidents/

11 Egan G. Security Awareness Training: Best Practices to Consider [Internet]. Wombatsecurity.com. 2018 [cited 16 May 2018]. Available from: https://www.wombatsecurity.com/blog/security-awareness-training-best-practices-to-consider

12 10 Steps: User Education and Awareness [Internet]. National Cyber Security Centre UK. 2015 [cited 8 June 2018]. Available from: https://www.ncsc.gov.uk/guidance/10-steps-user-education-and-awareness

13 Morrison D. How to Design an Excellent Online Course [Internet]. Slideshare.net. 2013 [cited 7 April 2018]. Available from: https://www.slideshare.net/debbiemorrison505/how-to-design-an-excellent-online-course

14 About Construct [Internet]. Construct.net. 2018 [cited 19 June 2018]. Available from: https://www.construct.net/en/about

15 Kujawa A, Zamora W, Umawing J, Segura J, Tsing W, McNeil A et al. Cybercrime tactics and techniques: Q2 2018 [Internet]. Malwarebytes Labs; 2018 [cited 7 October 2018]. Available from: https://resources.malwarebytes.com/files/2018/07/Malwarebytes_Cybercrime-Tactics-and-Techniques-Q2-2018.pdf