TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

TTU IT College

Carlos Rodríguez Flórez 201841IVSB

Cyber Security Awareness Program for a Materials Research Start-up

Bachelor's thesis

Supervisor: Kaido Kikkas

Tallinn 2023

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

IT Kolledž

Carlos Rodríguez Flórez 201841IVSB

Küberturbeteadlikkuse programm materjaliuuringute iduettevõttele

Bakalaureusetöö

Juhendaja: Kaido Kikkas

Tallinn 2023

Author’s declaration of originality

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

Author: Carlos Rodríguez Flórez

08.05.2023

Abstract

The aim of this thesis is to cope with the lack of cybersecurity awareness in a materials research start up by performing a cyber security awareness program.

The program will be tailored to the company in question. The content of the training will be given by the main processes and the recommended training content included in CIS Critical Security Controls guide for a company of similar characteristics.

The content will try to be interactive and as much visual as possible, so it is light and easy to digest, especially for the basic concepts. It will include more extensive readings to widen the knowledge.

The training will try to call further the attention of the staff by performing some ethical hacking in elements such as phishing or brute forcing email accounts and by showing real breaches in enterprises and its fatal consequences.

For the solution to the problem statement, free open-source tools will be preferably used so it is not creating any economic burden to the company.

The progress is evaluated through a set of multiple-choice questions, and the results are presented.

This thesis is written in English and is 78 pages long, including 6 chapters, 13 figures and 2 tables.

Annotatsioon

Käesoleva lõputöö eesmärk on lahendada materjalide uurimisega tegeleva alustava ettevõtte küberturvalisuse teadlikkuse puudumise probleem, rakendades küberturvalisuse teadlikkuse programmi.

Programm kohandatakse vastavalt käsitletava ettevõtte vajadustele. Koolituse sisu põhineb CIS Critical Security Controls juhendis toodud peamistel protsessidel ja soovitatud koolitusmaterjalidel sarnaste omadustega ettevõtetele.

Koolituse sisu on võimalikult interaktiivne ja visuaalne, et see oleks kergesti arusaadav, eriti põhiliste kontseptsioonide puhul. See sisaldab ka laiemat lugemismaterjali, et suurendada teadmisi.

Koolitusel püütakse töötajate tähelepanu veelgi juhtida, sooritades eetilist häkkimist sellistes elementides nagu andmepüük ja toore jõu rünnakud e-posti kontodele ning näidates tegelikke turvanõuete rikkumisi ettevõtetes ja nende saatuslikke tagajärgi.

Probleemi lahendamiseks kasutatakse eelistatavalt tasuta avatud lähtekoodiga tööriistu, et see ei tekitaks ettevõttele majanduslikku koormust.

Edukuse hindamiseks kasutatakse valikvastustega küsimuste komplekti ja vastavad tulemused esitatakse.

Käesolev lõputöö on kirjutatud inglise keeles ja koosneb 78 leheküljest, sealhulgas 6 peatükist, 13 joonisest ja 2 tabelist.

List of abbreviations and terms

2FA	2 Factor Authentication
AI	Artificial Intelligence
CIS	Center for Internet Security
Confidential data	Set of rules to limit access to certain types of information
DNS	Domain Name System
End point	End-user device
ENISA	European Union Agency for Cybersecurity
IdP	Identity Provider
IGS	Controls Implementation Groups
IM	Instant Messaging
Infosec	Information Security
ISA	Information Security Awareness
MFA	Multi Factor Authentication
MITM	Man in the middle
OTP	One Time Password
PM	Password Manager
Pentest	Penetration test
Public data	Information available to everybody
Restricted Data	Default classification for any information not specifically designated. This information will be disclosed to third parties only if reviewed by the appropriate body
SFA	Single Factor Authentication

Table of contents

List of figures

List of Tables

1 Introduction

The task of completion of the thesis for the Cybersecurity Bachelor program has been a great opportunity to think about possible cybersecurity related topics that could be applied to the start-up which is object of study. A lack of cybersecurity awareness has been spotted over time. This thesis has been built with the goal of improving that, having a real impact.

The nature of the company is important in the sense that has some peculiarities. One of them is the fact that, some of the major assets that need to be protected are prepared patents ready to be published. The company's final goal is to move forward and become manufacturer and for that reason, the intellectual property and know-how processes need to be protected and encrypted. This is another motivation that justifies this program and the necessity of it.

It is also important to reflect the business logic or processes used, highlighting here the use of One Drive as a tool for sharing and saving information. Another common way of communication flow is the corporate email.

This awareness program is designed to be easily improved or modified over the time without extra cost and may be used for other companies as a guide.

1.1 Personal Contribution

The author is applying a cyber security awareness program in a company with particular features, which is in an early stage of growth. All the current business processes are taking into account and the program is tailored to the needs of it. It is fundamentally an awareness program but it also incorporates some elements of training or education in form of seminars or wiki entries in how to use a password manager, file encryption and back up mainly as it is shown in sections 4.1,4.2,4.3 respectively. These topics are adjusted to the company in question, so that, for instance the solution to encryption and backup is valid for a sharing cloud environment and scales well to a on premises storage solution.

The author is also taking advantage of the flexibility of being a small company and the possibility to enhance the awareness program with some ethical hacking to convince the staff of the unnecessary complexity of the attacks by using some of the free tools available as it is shown in section 4.4. Here the author's business account has been used to simulate an attack. On the script shown, the values have been changed by variables so the account and service provider are not left exposed.

The methodology used for the content and delivery can also be used as reference for other companies to help them understand which content should be included and how to induce it to the staff. For the content, CIS Controls guide will be used in order to avoid missing important topics and use it as a first contact to legal frameworks that could eventually be used if the company continues growing and certification becomes essential as it is shown in section 2. Then, several delivery methods are evaluated and its use is justified looking at its pros and cons in section 3.

From the results of the evaluation form (section 5), instead of the most common approach of repeating questions, once feedback is given, until the results are satisfactory enough, the author will try to use alternative delivery methods and alternative content. This way, the chances of success will increase.

1.2 Target Audience

The audience that is going to take part of the program is composed by 3 people. Two main personalities that are leading the company and they have a scientific research background. They are both doctors in Materials Engineering. Their main field of expertise is therefore materials science, in particular experimentation, analysis, communication, presentation in a greater or lesser extent. There is another person who has been intermittently helping out as Product Owner in order to create a final product. Their cybersecurity background is limited, even though the Product Owner is now involved in a web development project for another company. In any case, in order to be able to measure their current knowledge level and improvement, it has been decided to use a quiz form.

1.3 Background and Relevance

Many small companies, like the one which is object of study, are starting to operate on specific sectors such as material science and are lacking enough expertise in cyber security. Moreover, it is commonly happening that the staff working, lack the sufficient awareness and often underestimate the risks [1], which may lead to compromise the main assets of the company.

Attackers very often take advantage of this insufficient knowledge and use human behaviours as exploits to break into information systems.

By 2025, it is anticipated that damages from cybercrime worldwide might reach $10.5 trillion annually [2]. And according to Verizon, human factors play a role in 82% of security breaches and incidents[3].

One of the rising and more disrupted attacks is the Ransomware. The ransomware attacks consist in encrypting organisation's information and as an extra can send victim's data offsite, so attacker can blackmail the victim and threat with making data publicly available[4]. It is common to spot on the media, successful attacks against hospitals, educational centers or manufacture organisations, putting in hold business process and dramatically damaging its reputation. Some examples the author happened to come across recently (March 2023) are the one at Hospital Clinic de Barcelona and other affecting an educational institution in Colombia that was not made public. More examples of companies affected by Ransomware in 2022 are[5]:

- Ferrari. Data from Ferrari's website was leaked on a dark web leak site run by the ransomware group RansomExx. The hackers claim to have obtained private information totalling nearly 7 GB.

- IKEA stores in Morocco and Kuwait. Vice Society allegedly posted data taken from IKEA stores in Morocco and Kuwait, with snippets from the gang's leak site indicating that they were able to steal confidential business data and even sensitive employee information.

- Lincoln College. Following the devastating financial impact of the COVID-19 outbreak and a recent ransomware attack, the small private college located in USA

has announced that it will close its doors in May 2022. The December incident was the tipping point, and the decision to close the facility on May 13, 2022, was unavoidable. After payment, a decryption key was delivered, but not enough data was recovered.

Some measures to mitigate this threat are to train to recognize and report phishing attempts or enable and enforce multifactor authentication[6], for that reason is utterly important to provide an awareness program in order for them to understand the risks and how to properly handle the assets of the company. This program has to be considered as one of necessary steps for the company to keep growing and reach its goals, becoming a manufacturer company with a clear footprint in technology and research.

1.4 Methodology and Planning

From Cybsafe report[7], it is important to distinguish between awareness, education and training. The understanding of these terms will help to elaborate a good awareness or training program. With awareness, people realize how important cyber security is to them helping to identify IT security issues and take appropriate action. Through education, people can acquire information to better understand how they can defend themselves once they are eager to learn more about cyber security. Also support through training will make the learning process more pleasant.

The importance of tailoring and participation is of great importance for the learning process. A trainee needs to feel that the information is credible and relatable. When producing security training content, it is needed take your audience into account and personalize it correctly. Each training and communication should take into account the fact that certain groups will have some background knowledge while others won't [8].

It is important to balance security and productivity since security shouldn’t be felt as an impediment to perform effectively the normal tasks [9].

To limit and tailor the awareness program, the main assets, that need to be protected, will be named.

Then, it is necessary to determine the main processes that happen with that information. How this information is created, shared and saved.

In order to cover the most important cybersecurity topics for the company of study and avoiding skipping important ones, the author will be following CIS Critical Security Controls [10], using it as a guide where most common cyber-attacks are referenced by different legal and policy frameworks. These CIS Controls are ordered in sequence by categories. Then, it incorporates the CIS Controls (IGs) option, that address a subset of the CIS Controls for every category in enterprises with similar characteristics. For the case of study, IG1 "essential cyber hygiene" will be applied. This group will typically include small companies where the sensitivity of the data to protect is low and the safeguards aim to protect against general attacks. This thesis will cover the training and awareness topics, referred in this guide, for this group.

For the practical part, a questionnaire will be presented to the users to know which areas are needed to be reinforced. Then, from the results of the quiz and some topics the author considers important to mention regardless, some content will be presented in different ways, mainly notes/wiki pages but also using some already built-in online courses in areas such as how to spot phishing emails (many offer trials that are covering the topic).

Finally, similar questions will be shared and users will be evaluated and final results presented and compared with the initial ones.

1.5 Assets and Business Process

The company funding comes mainly from different consortium projects, in which the company is part of them. Sometimes some service is provided to a costumer in form of a report.

The main assets are related to scientific output from theoretical and experimental research works. Often, this output is either kept inside the company for further investigation and analysis, or delivered to the costumer or partner in question.

This information may be saved locally in a computer and in the cloud as well as transmitted to partners through email. The files transmitted back and forth by e-mail, are mainly word, pdf files and power point presentations.

Sometimes the company has also to buy some products, equipment or services to external entities. Accounting services are also externalized. The type of files shared between parties will also be word, excel and pdf.

The software used by the company to produce the investigation results are:

1 Office Package

2 Microsoft Teams

3 Mail Service ZoneWebmail

4 Hot Disk TPS 7 software

5 Solidworks

6 Preform Formlabs

7 Origin Lab Pro 2022

8 TOPAS-Academic V7

9 Comsol Multiphonics software

All members of the company are authorized to create, access and modified any files.

The company counts with 4 computers, one for every person involved, some experimental devices which are not possible to control remotely, so they don't impose any cybersecurity risk. The company rents one laboratory in Mektory, whose management board provides physical security and network management, but the work may be done at any location.

2 Analysis and Scope of Topics

Here below the list of recommended CIS controls that are part of control 14, “Security Awareness and Skills Training” and that apply to IG1 [[11], p 43].

Table 1. Recommended safeguards for control 14, Security Awareness and Skills Training.

Security Awareness and Skills Training	1. Security awareness program
	2. Phishing and pretexting attacks
	3. Authentication best practices
	4. Data handling best practices
	5. Reasons for unintentional data exposure
	6. How to spot and report security incidents
	7. Risks associated with connecting to and sending business data over unreliable networks

2.1 Security Awareness Program

The learning process is a “continuum”[[11], p18], that should start with awareness followed by training and ending with education. In this thesis the main goal will be to provide awareness over cyber training. The following figure depicts this strategy, where there is not enough training to get to the next level.

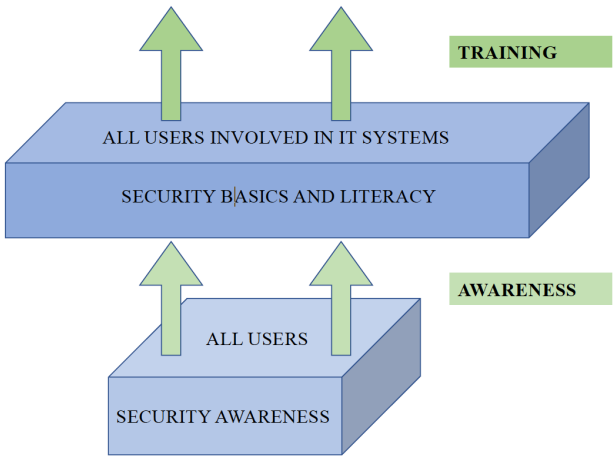


Figure 1. The IT Continuum. Adapted from source [[11], p18]

The necessary steps to produce an Awareness and Training program are the following [[11], p 31]:

- Needs analysis
- A strategy to make the program effective and attractive
- An awareness and training program plan for implementing that strategy
- Results and Conclusions of the program

Needs analysis. The staff field of expertise is not IT related but materials engineering, and even though, the company is not a big target due to size and economic impact, it is still very important for the sake of the company's growing and stability, that the staff increase their awareness in cyber risks.

About the **strategy**, the awareness program will try to cover the main cybersecurity concepts developed on the subsequent subchapters. It will try to induce some of these concepts in an interactive way through experience. Examples may be: checking password strength on a website testing tool or, proving the lack of complexity of many attacks through ethical hacking by performing some attacks in testing environments. It will be accompanied by some written content available in wiki pages.

The **implementation** will be scheduled and measured. A set of multiple-choice questions will be presented at the beginning to the staff involved. The results will be evaluated but correct answers won't be provided.

The tools and software used for the implementation part will be mentioned in the practical part of this work.

After the topics have been completed, the same or similar set of questions will be once more presented and the new **results** will be evaluated and compared with the initial ones. The author will be able to draw some conclusions and propose further work.

2.2 Phishing and Pretexting Attacks

Particularly in pretexting and phishing. A pretext is a made-up scenario created by threat actors with the intention of stealing the personal or business information of a victim. For instance, a scammer tells customer that someone has tried to access his bank account from another country and they need to update the information.

Phishing is a social engineering attack where the attacker sends emails pretending to be some legit entity and trying to deceive people into revealing sensitive information or installing malicious programs.

When pretexting and phishing are working together, they are more dangerous. For instance, the attacker creates an invented scenario where he informs the victim of a password leakage in mail server, so then, he tells the client to check his inbox and click on the link in order to reset its credentials. Of course, the link redirects to a website controlled by the attacker and where the credentials will be logged in.

Some common characteristics, that social engineering attacks have, are:

- Message arrives and you didn't expect it.
- Sender makes an unusual request. Even when the sender is known, this may be a victim himself of a scam and the attacker is using the stolen account as a tool to reach other victims.
- Requested action may include execute some program or insert passwords.
- Unexpected attached files or links on the message.
- Attacker Includes a Sense of Urgency.

The webmail solution, the company is using, lacks spam and phishing filtering in high degree, so it makes it even more important to be aware and informed about the risks.

Special attention will also be put on the files attached and how harmful they can be. Since the company is receiving many office files, the risk derived from macros will also be considered for the training.

2.3 Authentication Best Practices

There are many authentication options out there. From a simple SFA, where the user inserts his/her credentials to authenticate into the service. The most common instance of this type of authentication is the password-based authentication. In this case the use of a strong and unique password is essential since this is the only layer of protection.

Then, there is 2FA, where an additional layer is added, adding complexity at the process of taking control of the account. The factors follow this philosophy:

- Something you know, like a password
- Something you have, like a smartphone
- Something you are, like your fingerprint

This 2FA, may also be called MFA, especially when more than 2 different authenticators are used.

Sometimes the Authentication is done by an IdP, which is an authentication service by itself and have many benefits such as a variety of authentication solutions, simplification of the user's insertion of credentials with the single sign-on (SSO) or removing the burden of maintaining and protecting user's identities.

The authentication heavily relies on the authentication options the service provider gives. The mail service of the company in question, only provides the option of password authentication. Other services, daily used, such as windows log in also rely totally on this (unless there is biometrics hardware available).

Password strength and avoidance of repetition is another important topic to be covered. There are two fundamental things to take into account when dealing with this matter. First, the password must be un-guessable, therefore we will avoid the risks derived of dictionary attacks. There are wordlists as large as 562000 entries like "rockyou" that contains the filtered most common and repeated passwords used by users from a database leak over a sample of 32.6 million passwords[12].

The other important thing, is that, it must have a big enough entropy, which means that it will take years for any brute force attack against it to break it. The longer the bit size, the more difficult will be to try all different combinations. Depending the different "symbols" that are used to create the password, a different entropy will be obtained. For instance, when only numbers are used (0-9), 10 symbols in total, the entropy per digit will be 3.3 bits.

$$2^n = 10^1; n = \log_2 10\,; n = 3.3\ bits$$

A computer that is able to make 30 million operations per second, will be able to brute force a password of 6 lower characters in less than 10 seconds. To have an idea of what is considered good and bad in terms of entropy, the author has considered appropriate to present the following graph[13].

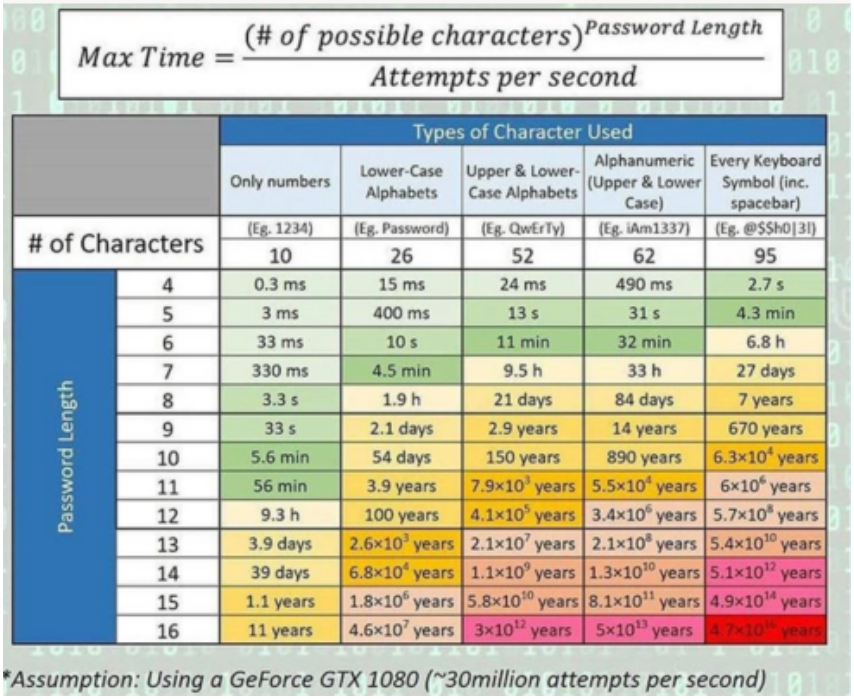


Figure 2. Password strength (entropy feature)

For meeting these fundamental properties, combining long passwords of unguessable words such as a combination of misspelled ones seem to be the perfect solution. The issue is that user needs to remember that. For that reason, a password manager will be of great help. Another important common rules to follow are:

- Don't share them with others

- Lock your computer if you are not working with it and check if others are looking at you, especially when inserting password
- Don't save passwords on browser
- Don't use http websites specially when it comes to insert login details
- It is advised that users check their selected passwords against a "black list" of inappropriate passwords[14]

2.4 Data Handling Best Practices

Data handling will englobe encryption, back up, naming and file organization.

Name files must fulfil certain criteria since sometimes it is a good idea to use some automation scripts for data transformation and visualization, by modifying output data from experimental devices. Special characters are not recommended to be used. Camel case or underscore character is recommended, being enough descriptive.

It is also important inform that the information that individuals send by mail or to the cloud may be saved in plaintext or encrypted. It is always better when it is encrypted but the encryption is implemented by the host and it has always the option to decrypt it whenever it wants, so for that reason the information that is meant to be confidential must be encrypted in origin. One may think in a situation where law enforcement or any other organisation push the service provider to give up some data. Therefore, before uploading or placing files in sync folder, confidential files must be encrypted. A solution suitable for a share folder in cloud service will be used.

Backup is a very important topic to cover, since having copies of your information will be immensely valuable when you lose your data, because of a hardware-software failure or you are just a victim of a ransomware attack and all your data is encrypted and a ransom is asked.

A common policy 3-2-1 will be followed. 3 copies in 2 different media and 1 off site. That will be achieve with the common folder synced in 3 different computers and additional copy in external physical hard drive and full backups every week, since losing

a week of newly created information may be acceptable. The staff will be lectured in different techniques to backup information. The aforementioned rule and types of backups:

- Full backup.
- Incremental backup. Backing up the files that have changed since the last backup happened.
- Differential backup. The difference with the previous type is that, it backs up all the altered files since the last full backup.

The author will try to lecture on these topics and encourage the use of these techniques. It will also be covered the use of different software solutions that will include some features that are considered essential by the author such as encryption, automation and backup restoration to origin, altogether with an easy-to-use graphical user interface, so it can also be used by the staff for other professional or personal projects.

2.5 Reasons for Unintentional Data Exposure

It will be shown the risks of using unattended external hard disks. Next to that, it will also be shown some common social engineering scams. On the following figure, a good schema of possible social engineering attacks, included the already seen phishing and pretexting can help to understand them and have a better global picture[15].

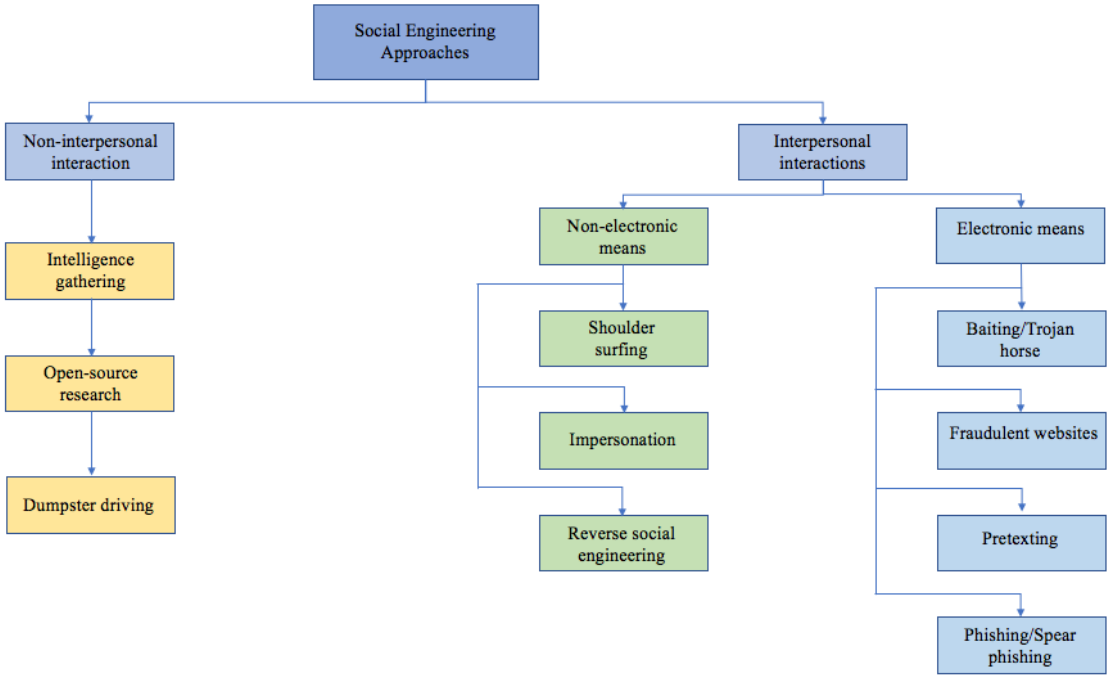


Figure 3.Social engineering attack taxonomy. Adapted from [[15], section 2.3.2]

Some recurrent attacks are the, so called CEO FRAUD, where an employee receives often a call and he is pushed to make a monetary transfer. For instance, this could happen with a partner and the opportunity to get a business together.

Another one, it may be trying to scam you by saying that you have been caught nude with your computer camera and asking for some money to have it destroyed.

A very common attack that is commonly used is the so-called Microsoft call, when a supposedly Microsoft employee, tricks you to install some malware in your computer and then, asking for money to fix those errors.

Other more advance and recent techniques may be the use of AI for voice modulation. With this technique the scammer may convince the victim to be a person the victim relies and trusts.

At the end, reverse engineering techniques can be used to detect this type of scams such as verifying by mail and phone that you are talking to the person that you just talked over the phone. Asking for proves that he/she is a Microsoft employee and just be cautious and consult with other people within the company when the petition may derive in a dangerous outcome.

Another important topic is to control what information is shared in social media. For instance, a spear-phishing attack can be performed by using the given information in the LinkedIn profile.

2.6 How to Spot and Report Security Incidents

Some indicators of a security incident in a computer may be high CPU usage, changes in configuration, having new start-up programs installed or scheduled tasks added. Some unexpected hidden files or suspicious registry entries. The person with more experience in IT topics will be informed and asked for advice.

2.7 Spot Missing Security Updates and Report them

The staff will be informed of the importance of keeping the system and software up to date. In every update, some bugs, including security risk related will be patched, therefore, making it more difficult to attackers to exploit the more or less known vulnerabilities. Normally the apps and system prompt to accept and install these updates. There are also software solutions used to explore vulnerabilities (outdated software) and it can be briefly explained and discussed.

2.8 Risks Associated with Sending Business Data Over Unreliable Networks

It is insecure to surf in public networks because you don’t know who has access to the network infrastructure. Even though, the communications over the web are normally done via https, which is encrypted, there are still other ways to obtain information and use it against you. MITM is a type of attack that can forge your requests to a server and modify them. Other attack can be obtaining your DNS queries, which are unencrypted and a step further will be to spoof your DNS request, readdressing your request to a malicious site which the attacker is controlling.

By knowing this, users should only surf to https sites and avoid entering any credentials or sending confidential information over the network.

3 Solutions for Delivering Awareness Programs

The author has reviewed some literature concerning training methodologies[16]. Aspects like span of attention and training methods are important to help the trainees understand and remember the most out of the training. A variety of learning methods has been proving to be effective.

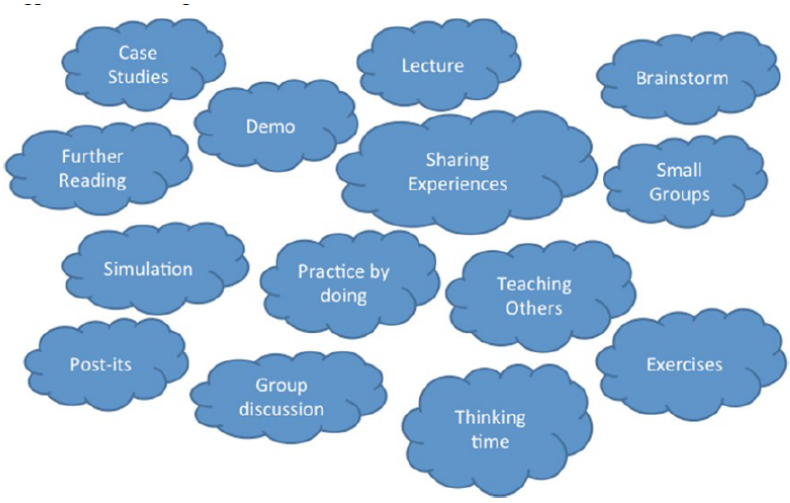


Figure 4. Training methods

With this variety of methods, the training will permit the trainees learning by watching, listening, reading and doing with the goal of reaching the base of the “learning pyramid” at certain point in time.

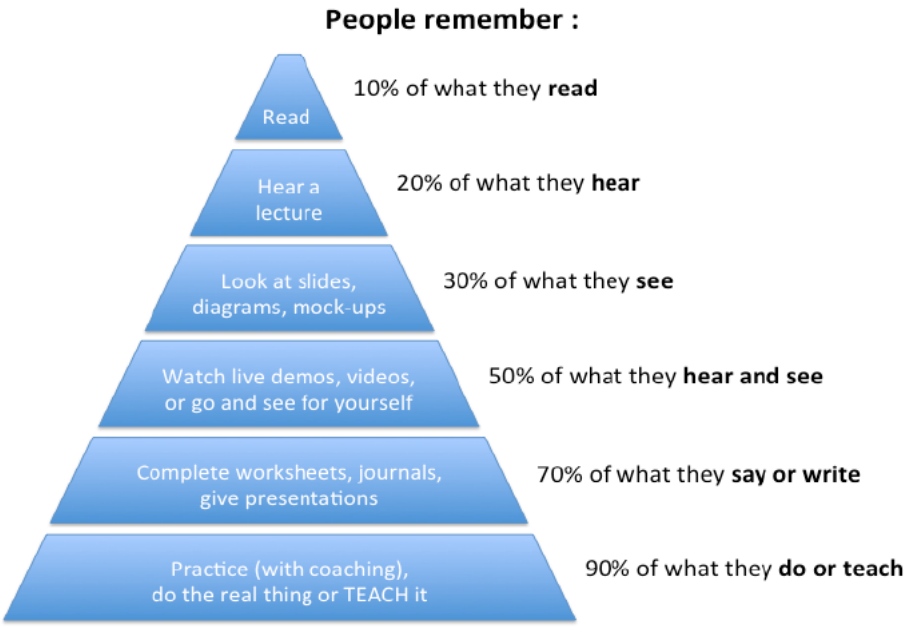


Figure 5. Learning pyramid

There are several ways to induce awareness to the recipients. A list of these methods is the following[11]:

Table 2. Delivering awareness methods

Delivering Awareness Methods	1. Electronic or paper-based products
	2. Seminars led by instructor
	3. Online platforms for content hosting and shared information
	4. Video training
	5. Game delivery method
	6. Simulation tests

The author will evaluate all these methods, looking at the advantages and disadvantages and decide which ones will fit better for the possibilities of the company and its personnel.

3.1 Electronic or Paper-Based Products

These methods can refer to the chance of using paper-based products, such as posters or notes, and electronic ones like emails or screensavers to remind everyone to for example

don’t leave their computers unattended and unlocked or to check twice the content and sender of an email before downloading and opening an attachment.

Products like posters can be seen as banal, but in reality, many sources remark its importance as an awareness element and a good way to reinforce awareness concepts[11][17]. It is still worth to say that it doesn’t create awareness by its own and it has to be complemented with other methodologies.

Figure 6. Awareness phishing poster[18]

The author will be using electronic products for hosting the content, a form to set initial ground and evaluate progress. For communication in general (mail, IM, etc).

3.2 Seminars Led by Instructor

The main advantages of this method are that the instructor may perceive the level of awareness of every different person by interacting with them. Also, distractions will be minimised since all the attendants will have to schedule some time to attend and focus on the seminar. It also allows live interaction between the staff and the instructor, enhancing the learning process by learning from each other and obtaining instant clarification to the questions that may appear on the process.

The disadvantages need also to be taken into consideration and they are related to the lack of flexibility.

Since the staff have different schedule and live at different locations, it is difficult to organise these seminars, however follow ups and business meetings are taking place almost every week, so they can be incorporated at these times.

3.3 Online Platforms for Content Hosting and Shared Information

One of the advantages is the flexibility to connect individuals working from different locations and the ability to consult, follow and participate at their own schedule.

The author has considered the use of wiki pages concept as a resource to share and distribute the information among the staff involved. The information is supposed to be valid for a long period of time and it can be further developed as the company continues growing. In addition to this, wiki pages are also very useful for planning, explaining and sharing procedures and as a source of knowledge that is relatively easy to browse, navigate and search.

Different solutions for the wiki pages have been studied. Firstly, it has been considered to use a free tool called Tiddlywiki[19]. It is regarded to be very powerful and written in Javascript, with several advantages such as the fact that can be run locally and offline in a browser or node.js instance or the simplicity of its architecture by not requiring the use of a database to store data. This is possible because the software uses the native data structures of Javascript to store the basic element called “Tiddlers”. It has some disadvantages like the high learning curve due to the complexity of the language, the lack of existing solutions for sharing and saving content online. After this one, other options have been reviewed like Nuclino, which carries on with the missing features of Tiddlywiki, since it is cloud-based and offers collaboration and information sharing in real time. Another tool that has been reviewed is One Note. The amount of tools that One drive offers is significant. For instance, Microsoft Forms, Office package in general, online drive storage, Microsoft One Note and others. For that reason and due to the nature of the company, it has decided to use Microsoft One Note.

3.4 Video Training

This is the most common way of delivering awareness training for any organisation. It is a very flexible and cost-effective method since it can be used by any employee at any given time, and quite convenient in big organisations when there are always personnel joining and leaving the company. The video sessions are often coupled with reading exercises and quizzes to enhance the experience and evaluate the progress. As it was mentioned at the beginning of the chapter, combine video and audio will help participants to remember about 50 % of it[16].

The content is often delivered at once at the beginning of the job experience and it is logical to be like that, since a new employee has to be "aware" of the risks and comply with the security policy.

Vendors use different approaches and solutions to get the attention of the trainees with the final goal of engaging the audience and increasing their cybersecurity awareness to the greatest possible extension. Some of latest trends are to provide short videos, lifelong learning methodologies. Companies like Defendify or KnowBe4 are offering continuously refresh knowledge. Other options are to engage the staff with stories, plots and real attacks like Ninjio. Synthesia company is offering creating your own videos so it is possible to adapt the training to the particular necessities of the company with AI video and audio.

For all the afore mentioned, it is clear that some of the wanted features for videos are short duration to cope with the **span of attention**, continuous refreshing and **lifelong learning**, create more impact and engage participants by introducing **real attacks**, **tailoring** the awareness program to the company in question.

3.5 Game delivery method

Video games are frequently computer-based, and they blend teaching ideas with graphics to produce engaging learning environments. Gamification helps to make learners figure the consequences of their acts when they lose in the game. It closes the gap between theory and practice. As it has been shown at the beginning of the chapter, with this

delivery method, users are reaching the base of the pyramid and the staff will likely **remember** quite a lot information from this delivery method.

This delivery method is very often used in companies since it can change behaviour of the staff, the effort is not perceived as such, and it is quite **practical** and **interactive.**

The disadvantage of this method is that it doesn't often cover an extensive list of topics or possibilities but a reduced list of topics and deeply analysed.

3.6 Simulation tests

This exercise is highly interactive and it is used for example to test phishing recognition capabilities by simulated phishing emails and checking if user falls victim of it, so it will certainly make a difference for both the trainee and trainer that other methods can't.

This delivery method goes one step further and show managers a valuable insight of the behaviour of the staff. For the employees, it also shows the consequences of taking bad decisions. Next time, they will pay more attention and probably change behaviour.

Here it also can be shown that the technical abilities to perform these attacks are not outstanding. In addition to this, participants can obtain another approach on how these scams are made.

4 Program Implementation

Already commented in the introduction of this thesis, the program will be implemented with some content that is included without prerequisites and other, that will be included based on the results obtained by the trainees in a quiz. The author considers 3 practical topics worth to cover regardless, because they have straight practical use. These concepts are the use of a password manager, encryption and backup. They involved some participation from the trainee, specially reading and trying the proposed software out.

To reinforce the awareness program and gain credibility, it will be shown the lack of complexity needed to perform many attacks, in this case brute forcing a mail account by using a dictionary attack in a video session. On the notes, it will also be included some harmful attacks suffered by recognized companies.

The notes are shared through One Drive, using One Note.

The initial quiz will be used to obtain more information and apply the right methodology. The program is meant to be running for a long time in a continuous learning way, being collaborative and interactive. More topics or a deeper analysis of these topics can be included at any time.

4.1 Password Hygiene

The author is proposing to the staff the use of a password manager. A wiki/note is created to inform about it. Many benefits come along using the PM tool. The fact that you just need to remember one very strong password is very beneficial. The note is created explaining or justifying the following points:

- Why using a password manager?
- Opportunity for the trainees to see the entropy strength of the password they are using. Also letter of caution not to fully rely on this because of dictionary attacks.
- The benefits of using a PM and quick guide to start using it.
- Encryption/Decryption working principle.

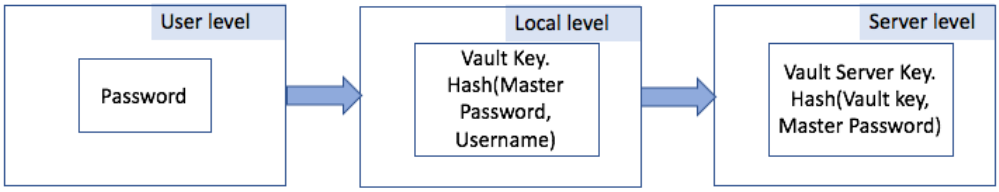


Figure 7. Encryption algorithm

- Other benefits or extra usage.

In the note/wiki, is also provided a quick guide to start using one of the possible commercial solutions, so the reader will get it done and start using it as fast as possible.

4.2 Encryption

Encrypting files is always a good practice and may become essential when you are working with sensitive data that, for different reasons, has been considered for non-disclosure and in cloud environments. An example of this, may be the results and conclusions of an experiment that can derive in a patent or when you work with personal data and for compliance. For all these reasons, it has been considered to prepare a guide to start using encryption and apply it straight away without the need of special technical requirements.

Several solutions have been studied to see which is best for the company in question. The one chosen is based on the properties of free open source, cross platform and its particular design that makes it adequate for cloud environments. The solution provided mounts a virtual driver every time you unlock the encrypting vault folder the user has created at the beginning. This vault/folder/portion of memory has been encrypted using AES 256 bit symmetric encryption algorithm, which uses a key or passphrase and is prompted to be filled in at the beginning, when creating the vault.

This virtual driver allows you to interact with the encrypted content of the drive, writing or reading more content there.

The note/wiki page includes the following chapters:

- Why do we need to encrypt our documents? Remarking the importance of it when saving information in mail or cloud servers in general.
- Solution proposed. An introduction with main features is presented.
- Installation. The link to the page to download and a video to follow.
- Letter of caution regarding the importance of not forgiving the key to unlock the vault.

4.3 Backup

Backup is one of the most important key topics for any information system. In terms of cybersecurity is important for many reasons too. For instance, the ability to keep and save the necessary logs that will enable the posterior study of any suspected attack, declared intrusion or failure. Other one, is to protect from the ransomware, which is a very disruptive and destructive attack, economically but also in reputation terms.

Several software solutions have been reviewed, looking to meet the following criteria:

- Free open-source solution preferred.
- Cross-platform.
- Scalability and extensibility. The author refers here to the fact that the software needs to be able to be applied to new users and new systems where backup may be saved in, either cloud, local drive or local server.
- Another important feature is that it should be automatically scheduled.
- The ability to produce encrypted backups.
- The capacity to be able to restore the data to origin.
- Incremental backups.
- Compression.

- Easiness for user.

The final solution adopted fulfils all the above points and adds other features such as the possibility to apply data retention policy, backs up metadata and makes available the logs of the operation. Maybe the easiness of use by the user may be questionable.

A wiki note is created explaining the basic concepts of back up and the tool used to complete the task. The note will cover the following points.

- Why doing backups?
- Why is a backup policy so important?
- Solution Proposed
- Installation

4.4 Mail Account Brute-force Attack

It has been decided to show the trainees how a password attack may be performed, in a video session, in order to obtain unauthorized access to one of the mail accounts, particularly the business account of the author of this thesis. The tools needed to perform this attack are free open source and they come together with Kali Linux-Debian distribution, which is used for penetration testing. Main tool needed is Hydra, which is a login cracker and supports a great variety of protocols such as SSH, HTTPs-FORM-GET, HTTPs-FORM-POST, etc[20]. For the attack, it has been considered that the username is known. The goal of this attack is to make trainees understand the lack of complexity of many attacks as well as showing them explicitly that if their passwords are contained in one of the multiple dictionary attacks available online, his/her account will be easily hacked.

Since the website uses https, then a https-post-form attack mode has to be used. For this particular case, there are 3 variables to considered for the payload POST/GET request. <Login Page>:<HTTP Request Body>:<Error Message>. To obtain these variables you have to find out the directory of the login page, the request body payload and then the error response header, since all the responses are considered successful by Hydra by

default. To get this information, it is just needed to go into developer tools and extract it from there or use a proxy feature to check request-response to server.

The session has been organised the following way:

1. Showing them the easiness to install Kali Linux, using a VM in Virtual Box.
2. Pointing out the fact that all the tools that may be needed are already installed in Kali Linux.
3. Showing them briefly how to get the information from browser to be used as a payload.
4. Different list of words or dictionaries used to perform this attack.
5. Running the script with the current used password which is not contained in the rockyou dictionary file; therefore, the attack is unsuccessful.
6. Changing the password of the mail to a password contained in the dictionary and running the script again. The script will stop once a successful response (not unsuccessful) has been obtained. Here below the skeleton of the script used. The exact values have been substituted with variables.

```
sudo hydra -t 8 -l <username> -P
/home/kali/Desktop/rockyou.txt <ip or url> -V https-form-
post '<directory of the login page>:<request
body>:<variable and value error response>' -f
```

4.5 Cybersecurity Awareness Questionnaire

The cybersecurity quiz has been created based on the already mentioned content, which has been described in chapter 2 and set to be shared with the staff. The questions have been created with the author's own experience and readings of similar tests like the ones presented by the Federal Trade Commission[21]. The questions have been tried to be adapted so they cannot be easily searched and found online, with limited time of 30 min for 33 questions and without showing the results when finished, so the same test or

something similar can be used to test the progress of the trainee and finally been able to give some feedback.

The author has tried to include the content main topics but could have missed some. Since the learning process and methodology used, fit perfectly in continuous learning, it is not a problem to include these or other needed topics for future learnings.

The quiz is divided in the following sections:

- Password Hygiene
- Phishing and Ransomware
- Encryption
- Backup
- Spot Security Incidents, Keep the System Up to Date and Surfing the Web
- Social Engineering

4.6 Additional Content

From the results obtained in the following section 5, the author has considered to enlarge some of the already listed content or create new one. The enlargements are detailed on the following points:

- Password Hygiene note. More content has been added referring to password strength. In particular entropy, unguessability, non-repetition and MFA techniques.
- Phishing – Ransomware. A new note has been created. It is remarked the dire consequences of this attack. The main characteristics that share the emails used to spread this malware, the special precautions to take in order to avoid running it. It is also advised to use a free online course that may help identifying these emails.

- Encryption and Backup. The importance of encryption, when it comes to protect against Ransomware, is included. About backup, a simple poster is added to remind about the importance of check the backups.

5 Results

The initial results of the questionnaire for cybersecurity awareness are presented. The idea is to capture the flaws in knowledge with the initial quiz and address these flaws with the different learning methods already explained. The analysis of the results will be done by sections. With the help of the excel file obtained from the Microsoft Form and making use of Tableau as visualization tool, the different results for every person can be spotted at a glance in charts. As explained in section 1.5, the target audience is composed by 2 Doctors and 1 Product Owner, defined in the different graph dashboards by DR1, DR2(Doctor 1 and 2) and PO (Product Owner). Eventually, the last subchapter will contain a summary with the results of the repeated quiz after the content has been shared with the trainees.

5.1 Password Hygiene

The results for this topic are all acceptable. For the question referring to password strength, the logic that all 3 followed, is correct but in some cases, they didn't pick up the right choice. For instance, DR1 and PO didn't recognize "Eh! My favorite movie is the Fast and Furious" as very strong and DR2 has incorrectly recognized passwords like "Robert87" and "Alex1978" as strong, so this topic has to be explained. It is also important to mention the rule of never sharing the password and clarify further MFA concept.

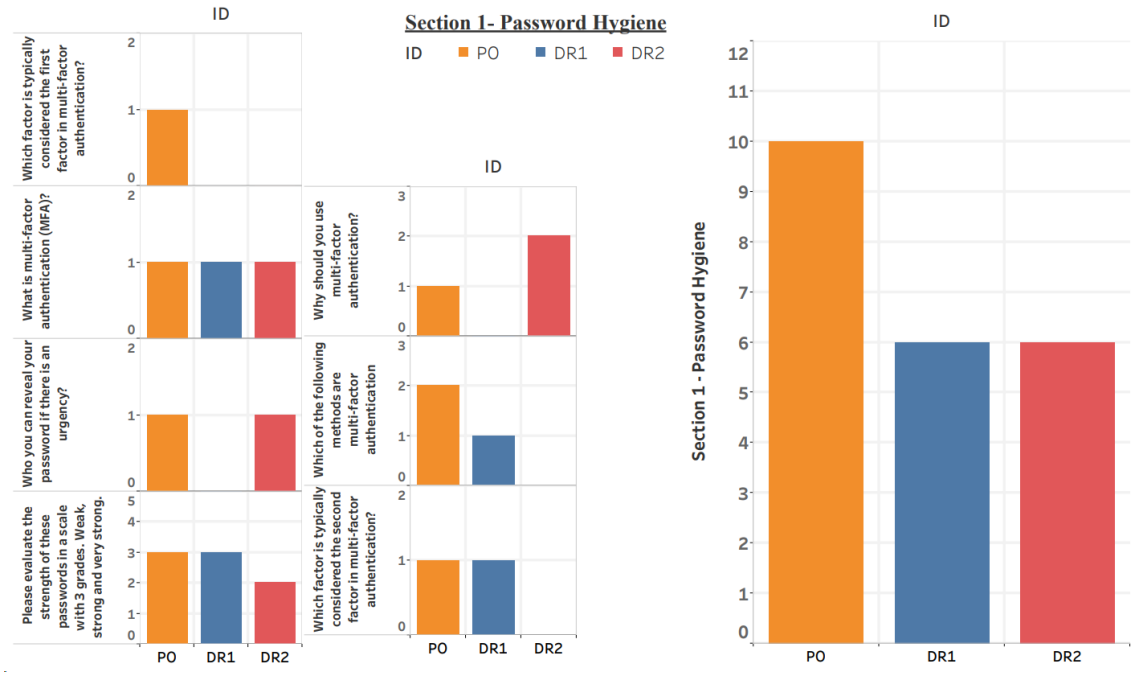


Figure 8. Password hygiene - graph results

5.2 Phishing and Ransomware

From the results obtained on this topic, it can be deducted that they all know the main characteristics of the attack and what is the best way to stop spreading it all over the internal network. However, it would be better to provide them with a bit more of practice in detecting phishing attacks.

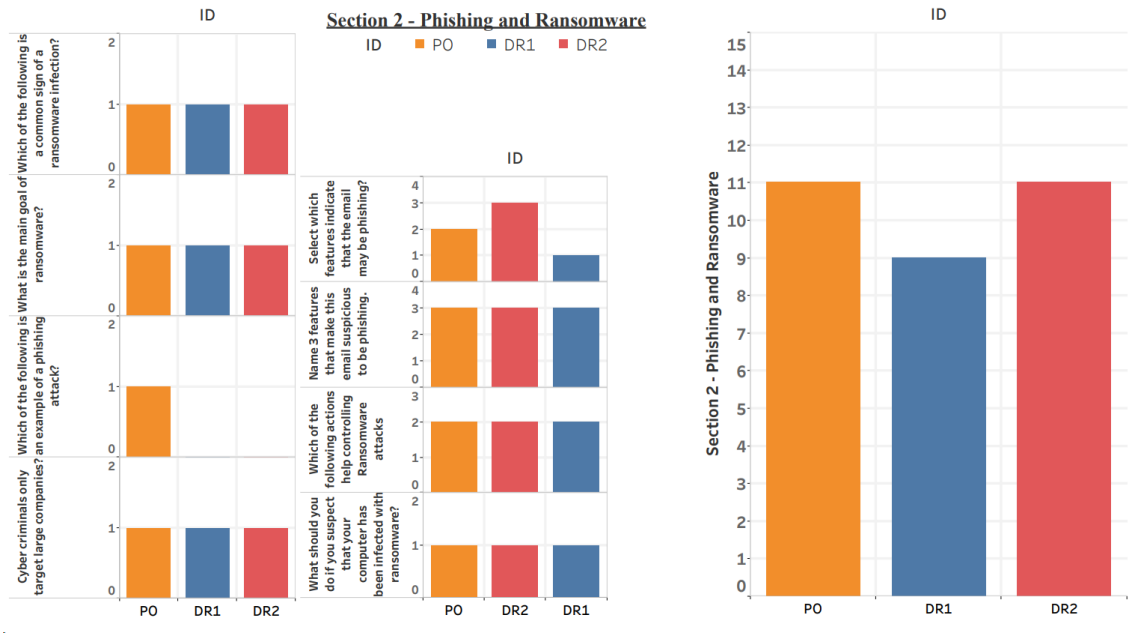


Figure 9. Phishing and Ransomware - graph results

5.3 Encryption and backup

In regards encryption and backup, the results are good. The author believes it is important and worth mention, the importance of encryption to protect against ransomware. As far as backup concerns, the only question they haven't all recognized is the importance to test your backups.

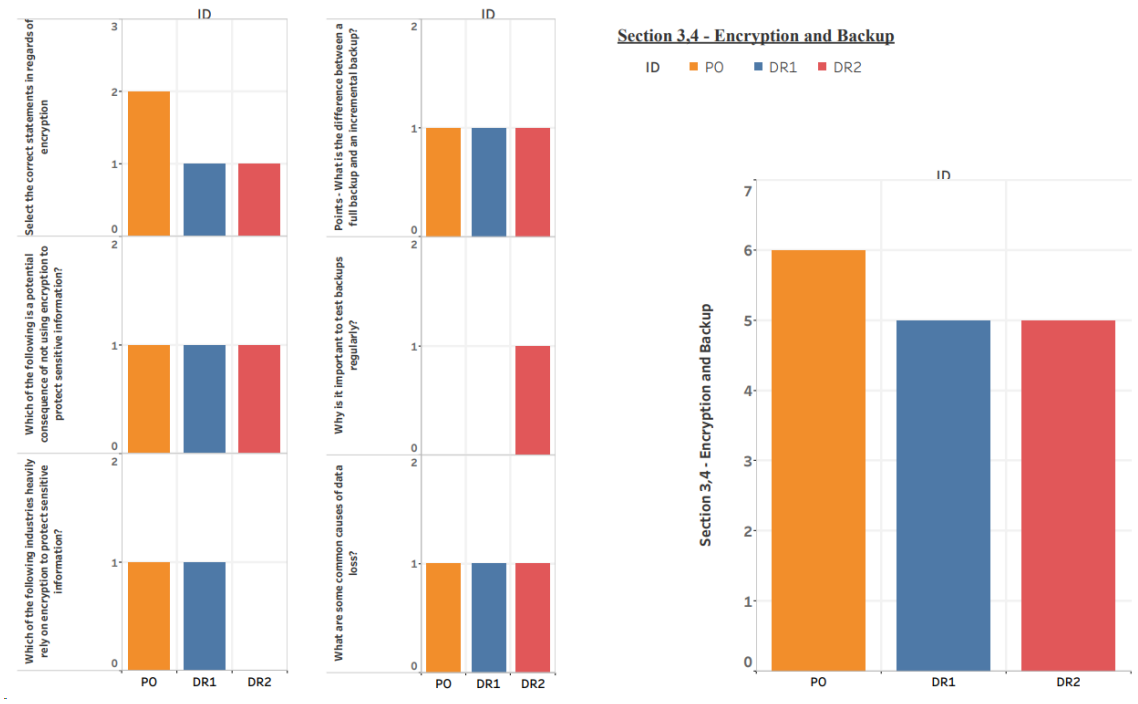


Figure 10. Encryption and backup - graph results

5.4 System and Surfing Best Practices

From the fundamental questions proposed, the results are almost perfect. About the question that hasn't been answered correctly, feedback is ready to be delivered for the follow up quiz, in case they fall in the same error. New topics have to be brough up to widen the knowledge in areas such as remote lock/erase or software possibilities to check the versioning of the software.

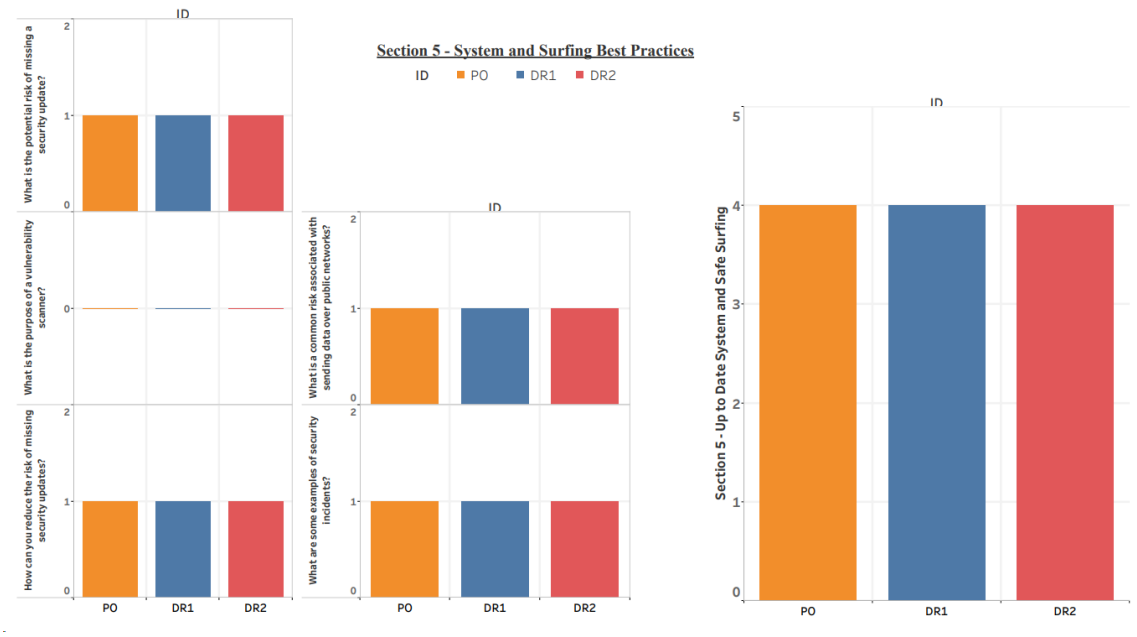


Figure 11. System and surfing best practices - graph results

5.5 Social Engineering

The results from this section are also considered acceptable. It could be studied the creation of a note touching different topics related to it. For the moment, it is just considered enough to provide feedback in the form for the follow up quiz.

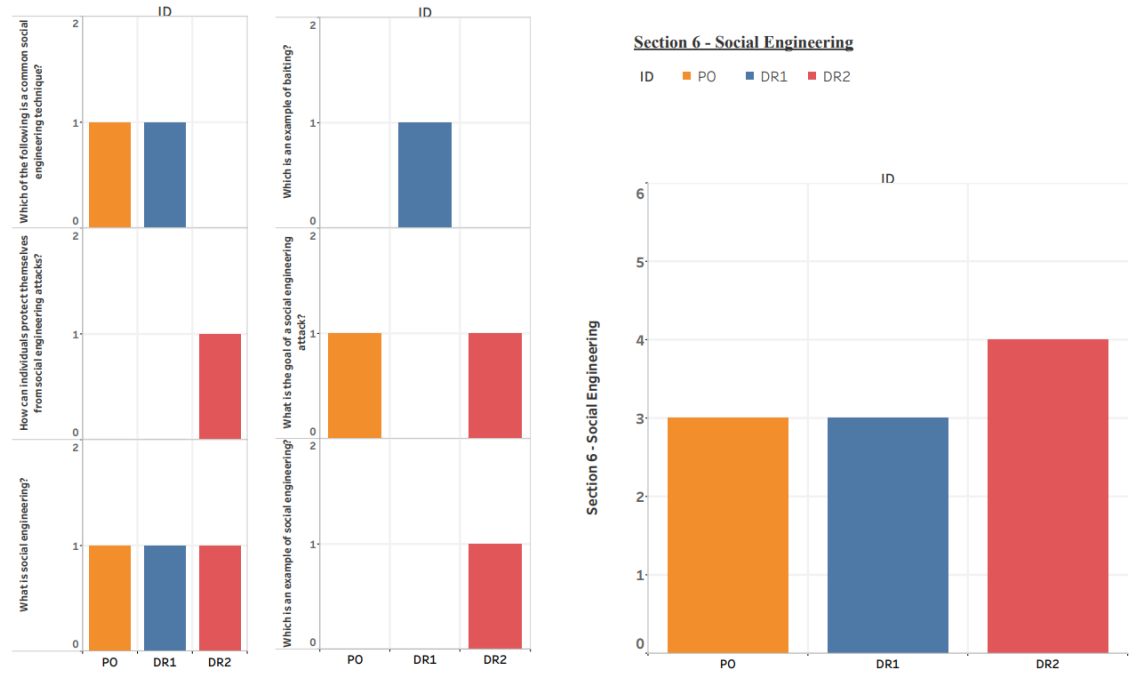


Figure 12. Social engineering - graph results

5.6 Final results

After the results and evaluation of the initial test, the content in form of notes has been shared with the trainees. They have had the opportunity to read and review the documentation and after around 2 weeks the same form has been presented to them. This time the form incorporates the right answers and feedback in case any question is wrong. For example, for the last question of the test which relates to an example of baiting, a further explanation is provided. This is also considered part of the training and it is commonly used in traditional awareness programs as well. The graph below shows the final results of this program.

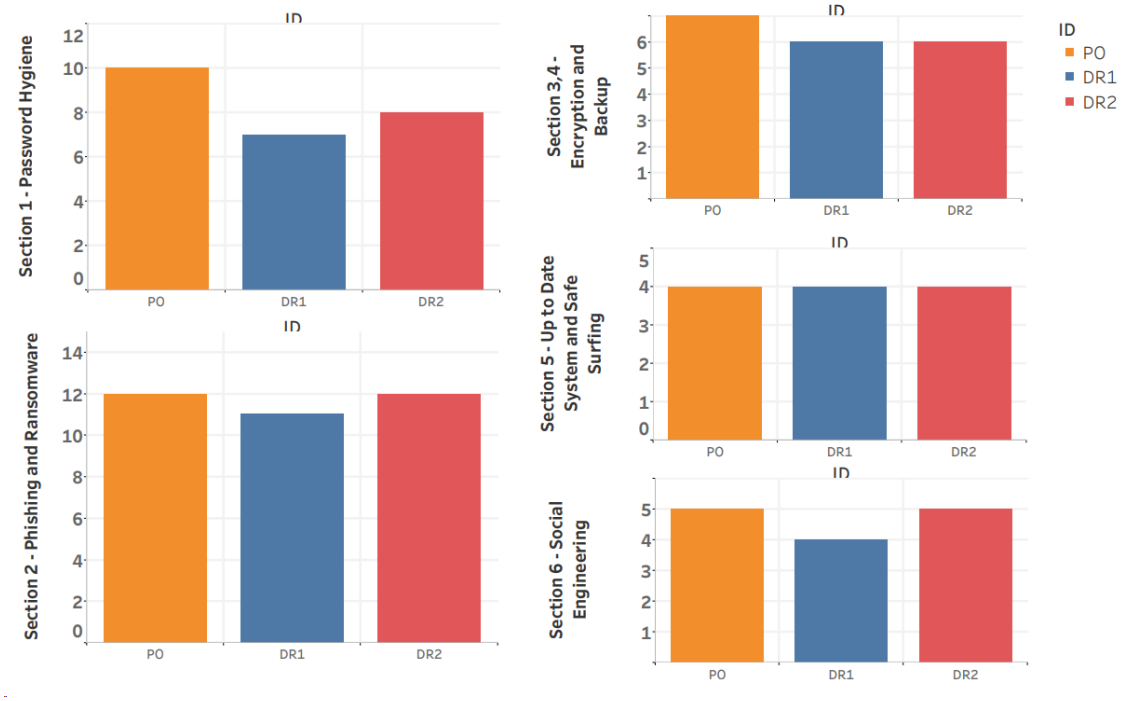


Figure 13. Final results program

6 Conclusions

The idea of carrying out this program was to give the company the necessary input in information technology in general and security in particular. It is necessary to move forward as a company, in particular to become a manufacturer, that the staff knows the importance of backup and encryption and is more aware of cybersecurity risks, having the right behaviour to minimize them. When the company starts saving personal or company data, is exposing some service to the world and has an infrastructure to run and maintain, this initial content will be highly useful and essential for more complex operations.

The learning methodology is ongoing basis and there are already some improvements from the initial form results to the second one. The intention is to continue with the learning process, updating the wiki pages or notes, reviewing more videos, games or even simulations to be certain of the progress.

This thesis offers an approach that may be considered an introduction to compliance with the use of CIS Controls and it offers an analysis of the different delivery methods suggested by NIST and its applicability to the program in question.

This work is also limiting its budget to almost zero, by using free open-source solutions or trial versions to cover the necessary topics. Thus, since Microsoft Forms doesn't offer an individual or groups chart visualization, then combining it with Tableau software, it is possible to achieve this without any extra cost or use of other technology.

Differing from other thesis, this thesis is offering to the trainees learning concepts such as the use of a password manager to apply password best practices as well as the use of backup and encryption solutions that adapt to the company's use of cloud shared environment.

This thesis is also showing the audience the lack of complexity of many attacks by proving and showing how a brute-force attack is performed against the author's business email account using free open-source software solutions and a list of words containing common passwords used by users.

All the proposed solutions have been tried by the author before being shared or explained to the audience.

This thesis is written without excessive jargon and complexity. It follows a line of reasoning, which can help to relate to other companies and scenarios since the analysis, methodologies, argumentation and implementation can be adaptable.

References

[1] Ryan West, “The psychology of security,” *Commun ACM*, vol. 51, no. 4, pp. 34–40, 2008, doi: https://doi.org/10.1145/1330311.1330320.

[2] Steve Morgan, “Special Report: Cyberwarfare In The C-Suite,” 2020.

[3] Verizon, “DBIR Data Breach Investigations Report,” 2022.

[4] Gabriella Antal, “2022 Ransomware Statistics & The Biggest Ransomware Attacks,” 2023. https://heimdalsecurity.com/blog/ransomware-statistics/

[5] Antonia Din, “Companies Affected by Ransomware ,” 2023. https://heimdalsecurity.com/blog/companies-affected-by-ransomware/

[6] CISA (Cybersecurity and Infrastructure Security Agency (USA)), “#StopRansomware: Royal Ransomware,” 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a

[7] CybSafe, *Cybsafe. Security Awareness Is Dead* . 2020. [Online]. Available: https://www.cybsafe.com/blog/security-awareness-is-dead-long-live-borderless-security-awareness/

[8] Lauren Zink, “How to Tailor Security Awareness Training to Employees’ Needs,” 2017.

[9] Emma W, “People: Strongest Link, UK National Cyber Security Centre,” 2017.

[10] Center for Internet Security, “CIS Critical Security Controls Version 8,” 2021.

[11] M. Wilson and J. Hash, “Building an Information Technology Security Awareness and Training Program, Special Publication (NIST SP),” *National Institute of Standards and Technology, Gaithersburg*, 2003.

[12] X. De Carné De Carnavalet and M. Mannan, “From Very Weak to Very Strong: Analyzing Password-Strength Meters,” 2013. [Online]. Available: http://dx.doi.org/

[13] University of South Wales, “Brute Force Password Hacking: How long will it take to Brute Force a password,” 2020. https://uwnthesis.wordpress.com/2020/07/01/brute-force-password-how-long-will-it-take-to-brute-force-a-password/,

[14] P. A. Grassi *et al.*, “Digital identity guidelines: authentication and lifecycle management,” Gaithersburg, MD, Jun. 2017. doi: 10.6028/NIST.SP.800-63b.

[15] D. Airehrour, N. V. Nair, and S. Madanian, “Social engineering attacks and countermeasures in the New Zealand Banking System: Advancing a user-reflective mitigation model,” *Information (Switzerland)*, vol. 9, no. 5, May 2018, doi: 10.3390/info9050110.

[16] Europäische Union Agentur für Netz- und Informationssicherheit, *Good practice guide on training methodologies how to become an effective and inspirational trainer*. 2014.

[17] S. Chaudhary, M. Kompara, S. Pape, and V. Gkioulos, “Properties for Cybersecurity Awareness Posters’ Design and Quality Assessment,” in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Aug. 2022. doi: 10.1145/3538969.3543794.

[18] InspiredeLearning, “Cybersecurity Posters,” *https://inspiredelearning.com/resource/cybersecurity-posters/*, 2020.

[19] Jeremy Ruston, “TiddlyWiki,” *https://tiddlywiki.com/*, 2004.

[20] G. D. Singh, *Learn Kali Linux 2019 : perform powerful penetration testing using Kali Linux, Metasploit, Nessus, Nmap, and Wireshark*. 2019.

[21] N. (National I. of S. and T. S. B. A. and H. S. Federal Trade Commission, “Cybersecurity Quizzes,” 2023. https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/quiz

Appendix 1 – List of questions used in the quiz to evaluate current cybersecurity awareness

Cybersecurity Questions

April 2023

The quiz will take approximately 20 -30 minutes to complete.
Let's evaluate our knowledge about cybersecurity best practices

Total: 45 Points

30 minutes

* Required

Instruction and personal information

1. Some of the questions admit **multiple answers**, so you will be **allowed** to mark several answers.
2. Vast majority are **single answer questions**, that **admit** only **one answer**.
3. Then 1 question where you need to write your answer and the first one about password strength where you select the right strength for every password.

1

Please enter your first name *

Password Hygiene

2

Please evaluate the strength of these passwords in a scale with 3 grades. Weak, strong and very strong. (4 Points)

	Weak	Strong	Very strong
Dictionary	◯	◯	◯
Robert87	◯	◯	◯
300x3=900	◯	◯	◯
roxette	◯	◯	◯
Eh! My favourite movie is the Fast and Furious	◯	◯	◯
That'samaz1n gandawes0m e	◯	◯	◯
Alex1978	◯	◯	◯
!Lovemycat	◯	◯	◯
SolySombra	◯	◯	◯

3

Who you can reveal your password if there is an urgency? * (1 Point)

- My colleagues
- My best friend
- The IT specialist
- No one

4

What is multi-factor authentication (MFA)? * (1 Point)

- A security measure that requires only one form of identification
- A security measure that requires two or more forms of identification
- A security measure that is not recommended for protecting sensitive information

5

Which factor is typically considered the first factor in multi-factor authentication? * (1 Point)

- Something you know
- Something you have
- Something you are

6

Which factor is typically considered the second factor in multi-factor authentication? * (1 Point)

- ◯ Something you know
- ◯ Something you have
- ◯ Something you are

7

Which of the following methods are multi-factor authentication * (2 Points)

- ☐ A confirmation you need to insert in a multi-factor app
- ☐ An SMS with a code to your mobile phone
- ☐ A password
- ☐ A one time password (OTP) valid for a minute and sent as a sms

8

Why should you use multi-factor authentication? * (2 Points)

- ☐ Because username and password can be captured in phishing attacks
- ☐ To protect against brute force attacks
- ☐ Because you don't need the a password anymore
- ☐ Because the additional effort that takes, compared to the security gain, is exponential

Phishing and Ransomware

9

Cyber criminals only target large companies? * (1 Point)

- ◯ Yes
- ◯ No

10

Which of the following is an example of a phishing attack? * (1 Point)

- ☐ An email that appears to be from a legitimate bank, asking the recipient to enter their account information
- ☐ An email that asks the recipient to click a link to download a file, which installs malware on their computer
- ☐ An email that asks the recipient to confirm their login credentials by entering a unique code sent to their mobile phone

11

What is the main goal of ransomware? * (1 Point)

- ◯ To steal personal information
- ◯ To install viruses on a computer
- ◯ To encrypt files and demand payment

12

Which of the following is a common sign of a ransomware infection? * (1 Point)

- ◯ Slow internet connection
- ◯ Computer slowness
- ◯ Inability to access files or programs

13

What should you do if you suspect that your computer has been infected with ransomware? * (1 Point)

- ◯ Pay the ransom to regain access to your files
- ◯ Disconnect your computer from the internet and seek professional help
- ◯ Ignore the issue and continue using your computer as usual

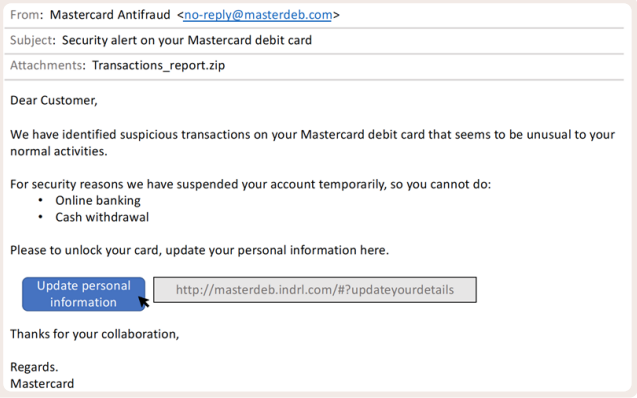
14

Which of the following actions help controlling Ransomware attacks * (3 Points)

- [ ] Save attachments and scan for viruses
- [ ] Activate macros
- [ ] Making backups in external drives not directly connected to the network
- [ ] Not opening attachments or not clicking on links from unknown senders
- [ ] Use strong and MFA to protect your accounts
- [ ] Making local backups in your local computer

15

Name 3 features that make this email suspicious to be phishing. (3 Points)


From: Mastercard Antifraud <no-reply@masterdeb.com>
Subject: Security alert on your Mastercard debit card
Attachments: Transactions_report.zip

Dear Customer,

We have identified suspicious transactions on your Mastercard debit card that seems to be unusual to your normal activities.

For security reasons we have suspended your account temporarily, so you cannot do:
- Online banking
- Cash withdrawal

Please to unlock your card, update your personal information here.

Update personal information http://masterdeb.indrl.com/#?updateyourdetails

Thanks for your collaboration,

Regards.
Mastercard

16

Select which features indicate that the email may be phishing? * (4 Points)

- [ ] The link in the body is https
- [ ] The link in the body is http
- [ ] The sender's email account is unknown
- [ ] The email prompts you to take action stiffly
- [ ] The email is impersonated
- [ ] You are in your google account and receive an email from the domain google.com to take action
- [ ] you receive an email from google but you notice sender domain is google.support
- [ ] You are prompted to allow permissions like view your mail messages and settings
- [ ] If the sender is known but he/she asks to take action immediately and is unexpected

Encryption

17

Which of the following industries heavily rely on encryption to protect sensitive information? * (1 Point)

- Healthcare
- Social media
- Entertainment
- All of the above

18

Which of the following is a potential consequence of not using encryption to protect sensitive information? * (1 Point)

- Increased privacy and security
- Reduced risk of data breaches and cyber attacks
- Loss of sensitive information to unauthorized users
- Improved user experience

19

Please select the statements you consider correct in regards of encryption * (2 Points)

- [ ] Encrypting information that is stored in the cloud or email service provider is redundant since they are already encrypted by the cloud/mail provider
- [ ] It prevents data breaches
- [ ] It is a necessary step to comply with certain regulations

Backup

20

What are some common causes of data loss? * (1 Point)

- Natural disasters, cyber attacks, and hardware failure
- Software updates, excessive use of storage space, and user error
- Device theft, employee turnover, and internet connectivity issues
- Marketing campaigns, software bugs, and social media

21

Why is it important to test backups regularly? * (1 Point)

- To ensure that the backups are working properly
- To free up storage space on devices
- To improve the speed of backups
- To reduce the risk of data loss

22

What is the difference between a full backup and an incremental backup? * (1 Point)

- A full backup includes all data, while an incremental backup only includes changes made since the last backup
- A full backup only includes changes made since the last backup, while an incremental backup includes all data
- A full backup is faster than an incremental backup
- A full backup is more reliable than an incremental backup

Spot security incidents, keep the system up to date and surfing the Web

23

How can you reduce the risk of missing security updates? * (1 Point)

- ◯ Disable automatic updates
- ◯ Use outdated software programs
- ◯ Check for updates manually on a regular basis
- ◯ Ignore update notifications

24

What is the purpose of a vulnerability scanner? * (1 Point)

- ◯ To fix security vulnerabilities in a software program
- ◯ To test the performance of a software program
- ◯ To identify missing security updates in a software program
- ◯ To add new features to a software program

25

What is the potential risk of missing a security update? * (1 Point)

- Reduced performance of the software program
- Increased risk of cyber attacks
- Improved security
- No apparent risk

26

What are some examples of security incidents? * (1 Point)

- Virus infections, phishing attacks, and data breaches
- Software updates, system backups, and hardware upgrades
- Network speed issues, disk space problems, and printer errors
- Employee turnover, staff training, and policy changes

27

What is a common risk associated with sending data over public networks? * (1 Point)

- Faster data transfer speeds
- Reduced risk of data interception
- Improved data encryption
- Increased risk of data interception and theft

Social Engineering

28

What is social engineering? * (1 Point)

- A type of malware that infects computer systems
- A technique used by hackers to break into computer networks
- The use of psychological manipulation to trick individuals into divulging sensitive information
- The practice of securing computer systems using encryption and other security measures

29

How can individuals protect themselves from social engineering attacks? * (1 Point)

- Being aware of the types of social engineering attacks
- Regularly updating software and security systems
- Using strong passwords and two-factor authentication
- All of the above

30

Which of the following is a common social engineering technique? * (1 Point)

- Shoulder surfing
- Intrusion detection
- Password cracking
- Firewall bypassing

31

Which of the following is an example of social engineering? * (1 Point)

- Installing a virus on a computer system
- Guessing a weak password to access a system
- Exploiting a software vulnerability to gain unauthorized access
- Sending a phishing email that looks like it's from a trusted source

32

What is the goal of a social engineering attack? * (1 Point)

- To steal sensitive information
- To install malware on a system
- To gain unauthorized access to a network
- All of the above

33

Which of the following is an example of baiting? * (1 Point)

- An attacker leaves a USB drive in a public place with a label indicating that it contains important documents
- An attacker uses social media to impersonate a friend or family member of the victim and gain access to their personal information
- An attacker uses a fake website to trick a victim into entering their login credentials
- An attacker sends a phishing email to a victim, asking them to click on a malicious link

Appendix 2 – Content used in notes and shared with trainees

Password Hygiene

Monday, 10 April 2023 20:59

Password Manager

Discussion and valuable information about a Password Manager tool, its advantages and synthesis of the way it is working.

Why using a password manager?

A good password, must be unguessable and long. These 2 features joined to the unwanted repeatability makes this tool very useful. Efficiency and security come together and gives you the ability to store as many different passwords as you want.

Check it out how unsecure are your passwords on the following link

[Is secure my password?]

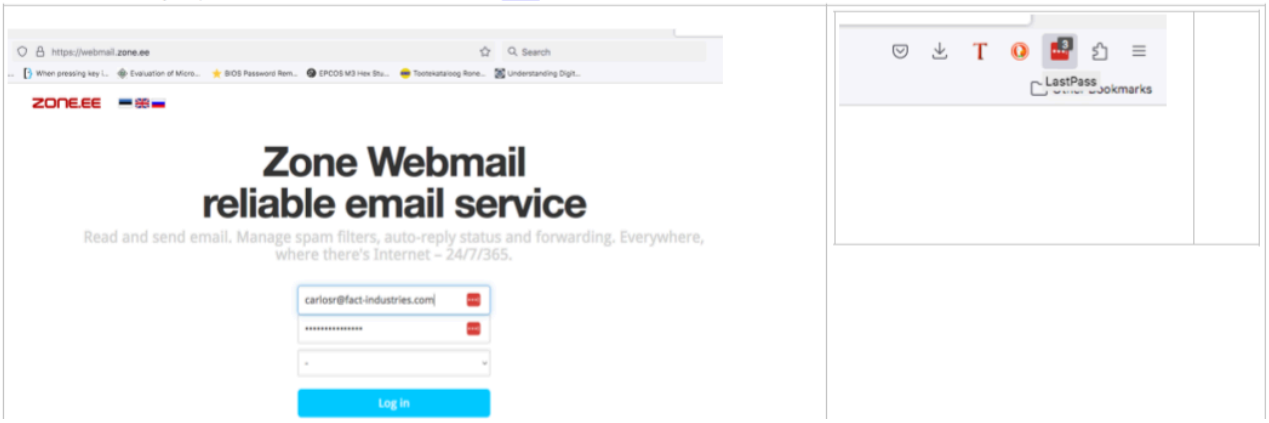
	Pay attention to the fact that a long password considered Secure enough like "siemprejuntos", it is contained in many dictionaries, meaning that it is not safe to use.

How convenient is just to know and remember a very strong password that will open the vault of all the others

There are 2 main solutions.

1. Save your passwords locally, which is not that convenient since you only have access to your passwords locally. The common software for this is keePass, which is free and open source. Commonly used in different companies as a password backup.
2. The other one is cloud based. Neither of them are totally free, which makes sense, since they have to maintain an infrastructure to host all users' secrets. You can use LastPass, https://www.lastpass.com/ which offers the option of trying it out in one type of device (desktop devices or mobile phones) for free. To be used in any device is less than 5 € and you can save other important notes.

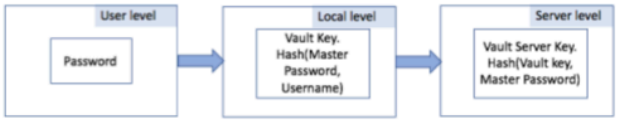
PM and in particular Last Pass come with browser extensions that automatically render web forms and allow you insert autogenerated passwords that will be saved altogether with the username in your password vault. Browsers' extensions link here.



How cloud based PM encryption-decryption works

Generally speaking, The "key" to enter all the data is encrypted on the client side and then send encrypted to server. This "key" is derived from the "Master Password" to get the "Vault key".

Last pass encryption is done through 2 steps. First a Vault Key is generated and, it is achieved hashing the username and password (H(username, password)), and iterating them multiple times. Then to authenticate in the server and get our vault, it is used once again, hashed, using your password so, (H(Vault key, password)) and we will call it Vault Server Key. So, with this, is proven that the service provider doesn't possess your master password and eventually, if there is a breach in the server and they can get your data, it is strongly encrypted through hash and iterations, so very difficult to guess.



Security is pretty much depending on your Master Password. You can enhance your MP with a 2 factor authentication login. Last pass offers the use of your fingerprint as a 2nd factor through a mobile app.

Other benefits of using a Password Manager

Other benefits that the passwords managers bring and in particular LastPass is the chance of storing notes, addresses or bank account information. All of them encrypted.

Password Strength

On this subsection we will talk about the main features that a password must have, so it can be considered "safe". Some of the features that help make stronger our passwords are the following:

1. Enough Entropy
2. Unguessable
3. Not repetition
4. Using MFA techniques

	A safer authentication method will be achieved by combining the best practices of all these techniques. For instance entropy alone sometimes may be totally insufficient. For instance password like "!carlitta4567", which seems to have enough bit length (

Enough Entropy

Password entropy means the bit size of the password itself. The greater this bit size is, the more difficult will be to brute-force it. Summarizing, the more diverse and longer password we use, the more difficult will be to brute force it. Check out the following link about it. Following table will show the entropy for different combination of characters. More info about entropy can be found Here.

Entropy per symbol for different symbol sets

Symbol set	Symbol count *N*	Entropy per symbol *H*
Arabic numerals (0–9) (e.g. PIN)	10	3.322 bits
Hexadecimal numerals (0–9, A–F) (e.g. WEP keys)	16	4.000 bits
Case insensitive Latin alphabet (a–z or A–Z)	26	4.700 bits
Case insensitive alphanumeric (a–z or A–Z, 0–9)	36	5.170 bits
Case sensitive Latin alphabet (a–z, A–Z)	52	5.700 bits
Case sensitive alphanumeric (a–z, A–Z, 0–9)	62	5.954 bits
All ASCII printable characters except space	94	6.555 bits
All Latin-1 Supplement characters	94	6.555 bits
All ASCII printable characters	95	6.570 bits
All extended ASCII printable characters	218	7.768 bits
Binary (0–255 or 8 bits or 1 byte)	256	8.000 bits
Diceware word list	7776	12.925 bits per word

A quick table that can be used to have an idea of the time needed to brute force a password with a home compute can be found below. So based on the set of characters that you are using and length, you will know in how much time the password can be broken.

$$Max\ Time = \frac{(\#\ of\ possible\ characters)^{Password\ Length}}{Attempts\ per\ second}$$

		Types of Character Used				
		Only numbers	Lower-Case Alphabets	Upper & Lower-Case Alphabets	Alphanumeric (Upper & Lower Case)	Every Keyboard Symbol (inc. spacebar)
		(Eg. 1234)	(Eg. Password)	(Eg. QwErTy)	(Eg. iAm1337)	(Eg. @5$h0(.)!)
# of Characters		10	26	52	62	95
Password Length	4	0.3 ms	15 ms	24 ms	490 ms	2.7 s
	5	3 ms	400 ms	13 s	31 s	4.3 min
	6	33 ms	10 s	11 min	32 min	6.8 h
	7	330 ms	4.5 min	9.5 h	33 h	27 days
	8	3.3 s	1.9 h	21 days	84 days	7 years
	9	33 s	2.1 days	2.9 years	14 years	670 years
	10	5.6 min	54 days	150 years	890 years	6.3×10^{4} years
	11	56 min	3.9 years	7.9×10^{3} years	5.5×10^{4} years	6×10^{6} years
	12	9.3 h	100 years	4.1×10^{5} years	3.4×10^{6} years	5.7×10^{8} years
	13	3.9 days	2.6×10^{3} years	2.1×10^{7} years	2.1×10^{8} years	5.4×10^{10} years
	14	39 days	6.8×10^{4} years	1.1×10^{9} years	1.3×10^{10} years	5.1×10^{12} years
	15	1.1 years	1.8×10^{6} years	5.8×10^{10} years	8.1×10^{11} years	4.9×10^{14} years
	16	11 years	4.6×10^{7} years	3×10^{12} years	5×10^{13} years	4.7×10^{16} years

**Assumption: Using a GeForce GTX 1080 (~30million attempts per second)*

Unguessable

Be aware that many passwords are meeting the criteria of having enough entropy, however are still easy to break. For example "lordoftherings" and any of its variants may have a good entropy but it can also be found in many dictionaries. One of them is "rockyou", here the link to download the list of passwords here(you can search if one of the ones you are using is there).

The way hackers used to break into your account, is often restricted to these dictionaries, since it is less resource and time consuming than brute force attacks. For that using unguessable passwords like "lord of the sun moon and 1 ring". This is very long pass, quite random and easy to remember and type. Using blank spaces may be also an advantage in many terms like helping typing it and adding randomness. One additional thing to improve previous version will be to add "0" instead of "o" on the 2nd "o" for instance. Therefore the new password will be "lord 0f the sun moon and 1 ring". Sometimes you are not allowed to use this kind of long strings, so it is better to incorporate symbols to add entropy and randomness.

Non Repetition

Just imagine, that for whatever reason your password gets exposed. We are all humans and we all make mistakes. To minimize the consequences, using different passwords for different services is the way to go. The password manager will be of great help in that sense.

MFA techniques.

When you are only using your password altogether with your username to log into a service, then you are using SFA(Single Factor Authentication). Normally, every security product follows the designing rule of adding layers of security to make it harder to be attacked.

Then, there is 2FA(Two Factor Authentication) or MFA(Multi Factor Authentication), where an additional layer is added, adding complexity to the process of taking control of the account. The factors follow this philosophy by order of implementation:

1. Something you know, like a password.
2. Something you have, like a smartphone.
3. Something you are, like your fingerprint.

That's all for now… Remember

Encryption

Tuesday, 11 April 2023 18:03

Why do we need to encrypt our documents?

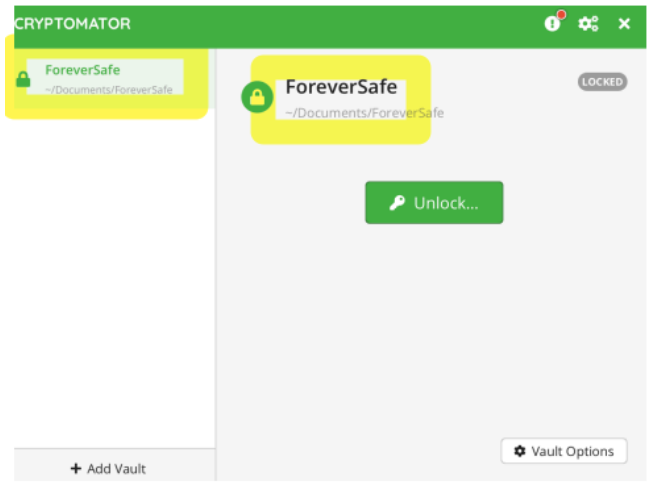
We are tending to save more and more content on the cloud or what if we want to share one document through mail? Share it unencrypted is not a problem as long as we are comfortable with that information being made public. If we consider the information has some intellectual value or privacy, then we don't want to do that probably. The information in mail or cloud servers in general is saved either unencrypted or encrypted with a ¨key¨ that Service Providers can use to decrypt by own interest, petition of law enforcement, "rogue employees" .

Encryption against Ransomware

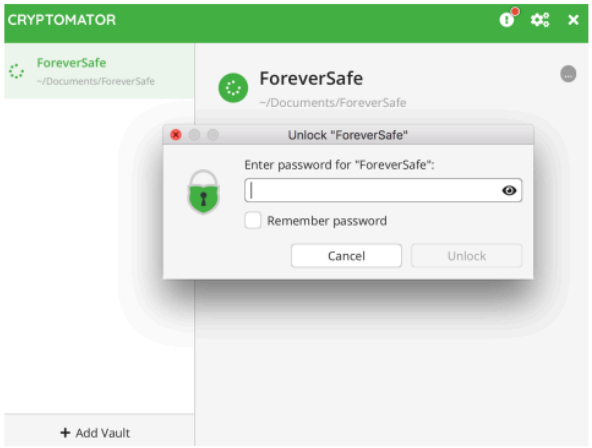
Ransomware attacks aim to affect 2 main functionalities. One of them is to lock the data by encrypting it, so it is not available. Another one is to use this data and blackmail the company affected by saying that they will sell or publish the personal data. This risk can be minimized by encrypting the content.

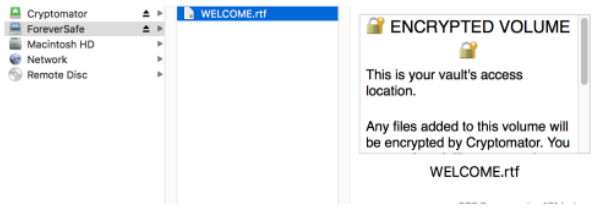
Solution proposed

The software **Cryptomator** allows the use of encryption in a simple and also safe way. It uses a **folder or Vault** that is created at the beginning where all the files encrypted. If you want to read them or add more, you just need to unlock the vault.



The **Vault** can be created in your local device or in the sync cloud drive folder (for instance Onedrive). In this way every time you create or add a file to the cloud that needs to be encrypted, you "unlock the vault" and the virtual drive is enabled and you will be able to add, read, delete,.. Files in the Vault folder.





Installation

The software is very simple to install, cryptomator.org/downloads/. For more information take a look on the website and you can also check this video for more details and step by step information to install.

Letter of Caution

If you cannot remember the key or passphrase you have inserted in, you won't be able to access the unencrypted files. Therefore the software comes with an additional feature, that is to mask a recovery password in a random file that is generated.
You either remember the password 100% or you need to use this option when creating the vault and safe this random file in a place you know and remember (Not in the cloud… for obvious reasons).

Back Up

Saturday, 15 April 2023 17:27

Why doing backups?

SSD (Solid State Drive) or HDD (Hard Disk Drive) can fail, in fact, they all have a limited lifetime like anything else, so in case this is happening, you are in risk of losing all your stored data. As long as you have a copy in some other device, you can rely upon that and continue you daily tasks with minimal disruption.

The hardware failure is not the only reason why you should do backups. There are many others among the which are:

1. Your laptop can be lost, stolen or have physical damage.
2. User involuntarily deleting files or making mistakes (you can rollback from those mistakes with the backup).
3. You are victim of a ransomware attack and your hard disk gets encrypted, therefore you cannot access the data anymore.
4. For compliance with certain regulations you are obliged to keep data for a certain period of time.

Why is a backup policy so important?

A backup policy will set the method/s used to backup the data and restore it. It will cover the following topics.

1. Backup Coverage. What needs to be back up.
   This topic has to be discussed and may be changed over time. In principle everything will be backed up
2. RPO (Recovery Point Objective)
   Max amount of data loss the company may accept. In the worst case scenario this can be accepted to be up to 7 days. Due to versioning and retention.
3. Versioning and Retention
   Versioning is referred to the different techniques used to backup. There are mainly 3 different techniques.
   3.1 Full backup. Full copy of the data we want to backup up.
   3.2 Incremental. We don't make full backups everyday. Instead we ¨increment the existing backup¨ with the information that is new.
   3.3 Differential. We make backup of all the new information since the last full backup.
   You can see the differences between incremental and differential below.

Image extracted from https://www.easeus.com/backup-utility/differential-backup-vs-incremental-backup.html

For retention, this is also subjected to change but for the time being that will be 2 years, only for billing.

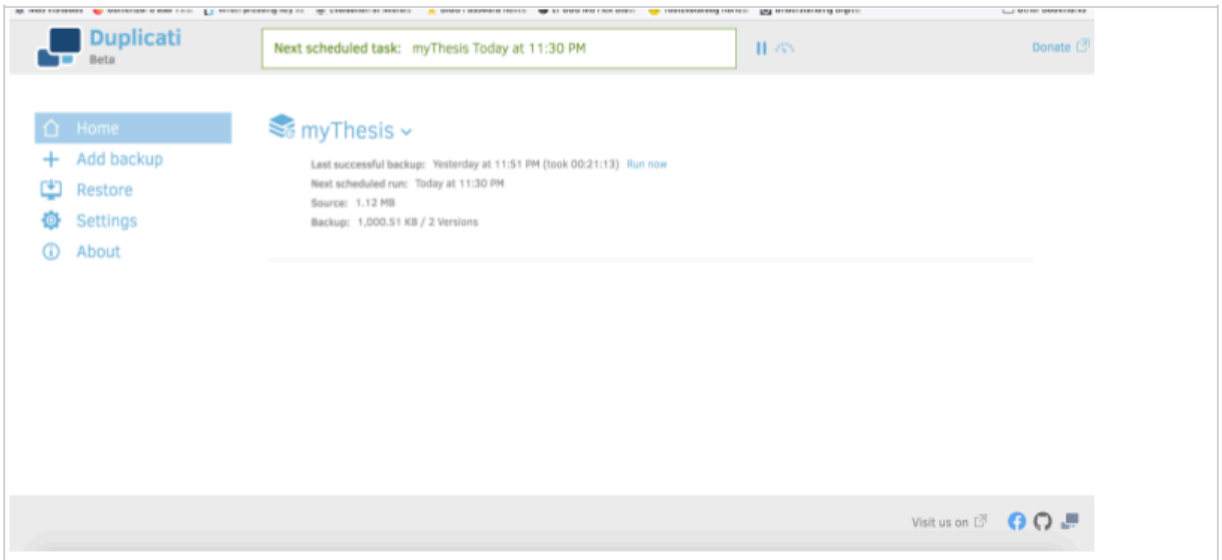
Solution Proposed

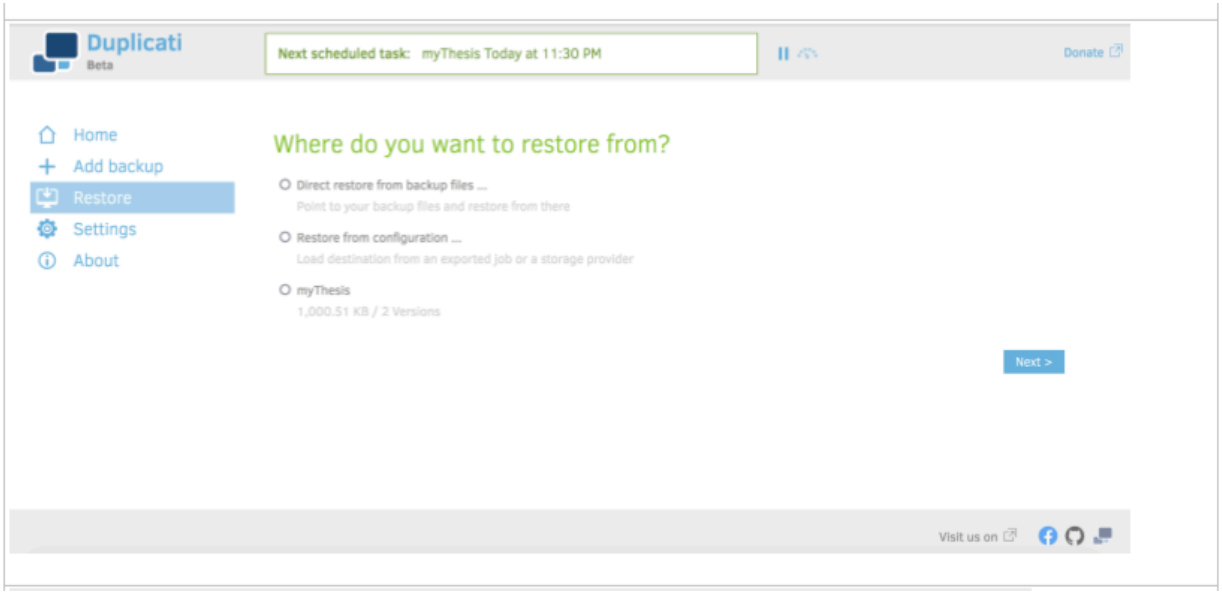
The solution proposed for the purpose of backup is **Duplicati**. It meets some very important requirements and can adjust to the companies' new challenges. It can be scheduled, offers encryption, incremental backup and compression. **Duplicati** can adapt to perform backups to local or remote servers or cloud as well as external physical drives.
It is very convenient to do set up once and not having to manually trigger it or care too much about it.

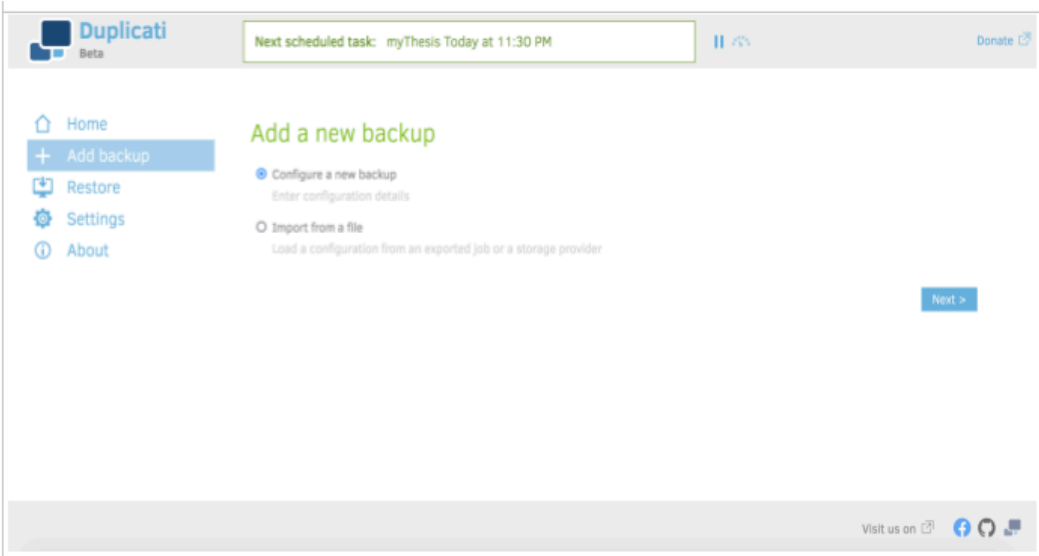
	It is very important to check that the operations are being running successfully from time to time. At least one every week and try to restore data at the beginning with several trials and then once every month.

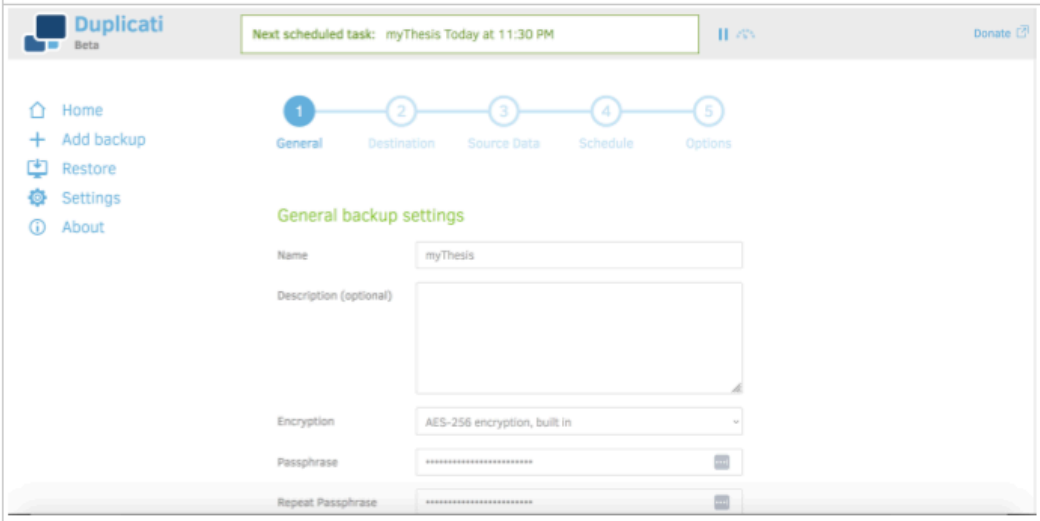
Installation

The installation link here. Below, some screenshots of a trial made. A web interface with the basic menus for create the set up , restore backup and some options of the setup like the encryption used.




Duplicati
Beta
Next scheduled task: myThesis Today at 11:30 PM
Donate
Home
Add backup
Restore
Settings
About
Where do you want to restore from?
Direct restore from backup files ...
Point to your backup files and restore from there
Restore from configuration ...
Load destination from an exported job or a storage provider
myThesis
1,000.51 KB / 2 Versions
Next >
Visit us on


Duplicati
Beta
Next scheduled task: myThesis Today at 11:30 PM
Donate
Home
Add backup
Restore
Settings
About
Add a new backup
Configure a new backup
Enter configuration details
Import from a file
Load a configuration from an exported job or a storage provider
Next >
Visit us on


Duplicati
Beta
Next scheduled task: myThesis Today at 11:30 PM
Donate
Home
Add backup
Restore
Settings
About
1
2
3
4
5
General
Destination
Source Data
Schedule
Options
General backup settings
Name
myThesis
Description (optional)
Encryption
AES-256 encryption, built in
Passphrase
Repeat Passphrase

For step by step easy guide you can follow this YouTube video tutorial in here

Phishing - Ransomware

Sunday, 16 April 2023 22:06

Phishing and Ransomware

Ransomware is one of the most common attacks with fatal economic and reputational consequences. They attack equally individuals and small or big companies. There are cases pulling out all the year long and this is just a bit portion of them, since many of them go unnoticed.

To demonstrate that they affect big, small organizations and individuals alike, let's name some examples:

WannaCry affected Microsoft **individual users**, with approximate losses of **$4 billion.**
Colonial Pipeline Attack affected Colonial Pipeline that is responsible for carrying gasoline in the US. It happened in 2021 and made the country declare Emergency State. Cause losses of **$4.4 million.**
(source: https://www.getastra.com/blog/security-audit/biggest-ransomware-attacks/#colonial)

The most common way of implementing ransomware is through phishing, so that is why they always come together.

How to spot phishing and avoid being a victim of ransomware

They frequently have the following characteristics:

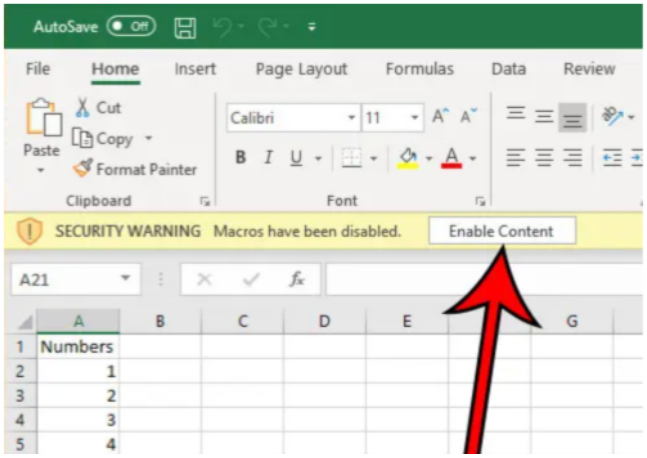
- Urgent action demands.
- Poor grammar and spelling errors.
- An unfamiliar greeting or salutation.
- Requests for login credentials, payment information or sensitive data.
- Offers that are too good to be true.
- Suspicious or unsolicited attachments.
- Inconsistencies in email addresses, links and domain names.

In order to practice more and see common scenarios in an interactive and quick manner, I invite you to enter https://cdse.usalearning.gov/local/pwt_privacy_policy/view.php, sign up and log in. Then, you just need to search for "Phishing and Social Engineering: Virtual Communication Awareness Training". You will be able to remind yourself about the typical features a phishing email may have.

The most important to avoid phishing and ransomware is to avoid opening or downloading attachments and also avoid clicking untrusted links and always "Double Check" when having to insert personal or important details such as passwords, personal information. A good technique is to hoover over it to see if it corresponds with what is written or going to developer options.

Never trust in unencrypted links (http). Sometimes hackers use Link manipulation techniques.

Another important feature to take into account is to disable macros. The company is always sharing and sending back and forth office documents. Often hackers use macros to inject malicious code so the malware can be run in case the macros are enabled. On recent versions of Microsoft office, macros are not disable, however is always worth double check that it is indeed like that.



Appendix 3 - Non-exclusive licence for reproduction and publication of a graduation thesis

I, Carlos Rodríguez Flórez,

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Cyber Security Awareness Program for a Materials Research Start-up”, supervised by Kaido Kikkas.

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

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

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

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

08.05.2023