New anti-phishing systems propositions for Eklamot

Coco Jumbo Heurystyka International

Hubert Perliński
Michał Krzyżański
Michał Małecki
Tomasz Michalczewski

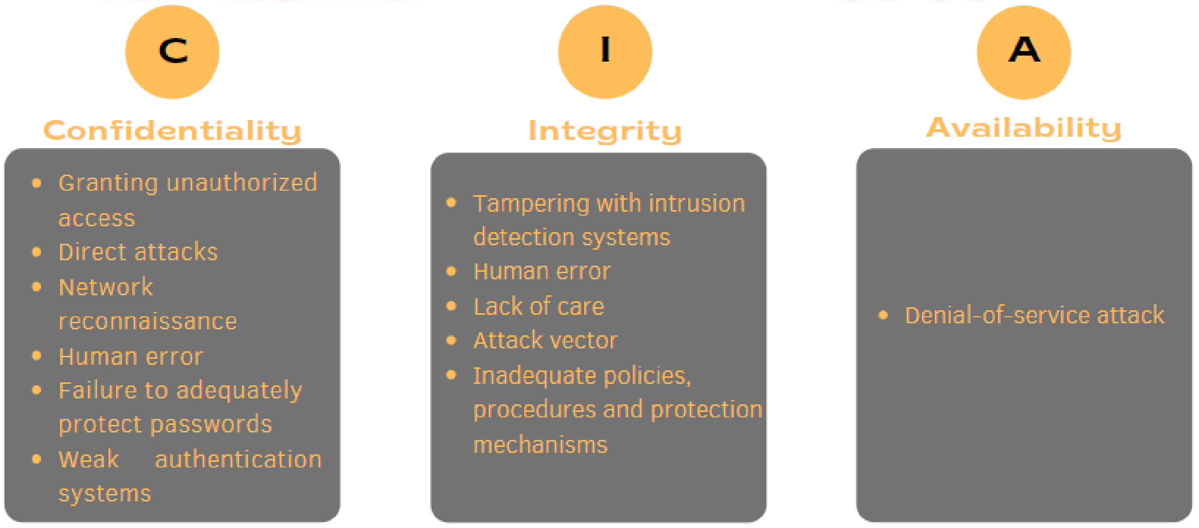
Introduction

This report refers to an inquiry about new anti-phishing methods, made by the Eklamot company in May 2022. The contents were prepared based on the data provided by Eklamot on the date of the request of action.

Threat level created by lack of phishing protection

Through the analysis of the material provided, we have determined that the current overall threat to Eklamot's operations coming from the risk of successful phishing attempts is **very high**. It is highly recommended to start implementing the proposed measures **as soon as possible.** The risks from phishing can be broken down into the following categories:

- Confidentiality - the company is exposed to a **high** confidentiality impact, as there exist multiple ways for the attacker to retrieve sensitive information.
- Integrity - the company is exposed to a **high** integrity impact, as many possible ways to access Eklamot's systems through phishing were identified.
- Availability - the company is exposed to **medium** availability impact, as an attacker could paralyze internal operations with the access gained through phishing.



C

Confidentiality

- Granting unauthorized access
- Direct attacks
- Network reconnaissance
- Human error
- Failure to adequately protect passwords
- Weak authentication systems

I

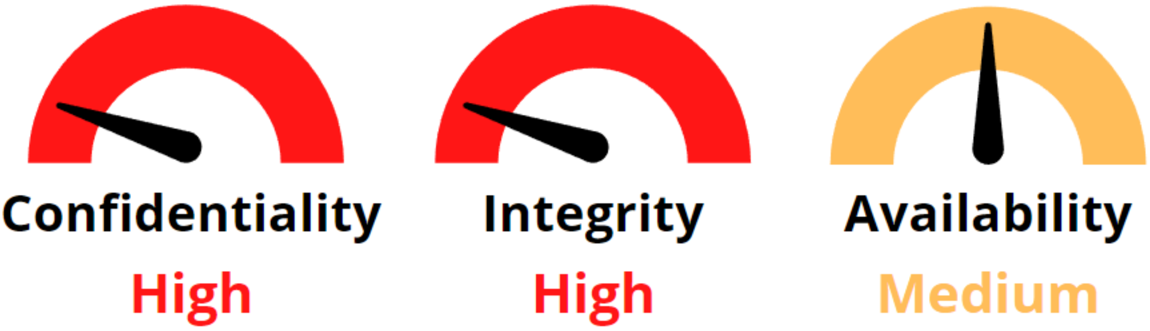
Integrity

- Tampering with intrusion detection systems
- Human error
- Lack of care
- Attack vector
- Inadequate policies, procedures and protection mechanisms

A

Availability

- Denial-of-service attack



What is phishing

Phishing can be described as a fraudulent practice of sending **misleading emails** in order to obtain sensitive business information, gain access to the company's system or manipulate an employee into helping the attacker.

The dangers of falling for phishing attempts range from trivial ones, like minor money transfers, to ones posing an existential threat to the operations of the company, like database encryption. This is the reason why it is essential to actively counteract this danger on a software level, as well as on the human level.

There are two major kinds of phishing Eklamot needs protection against:

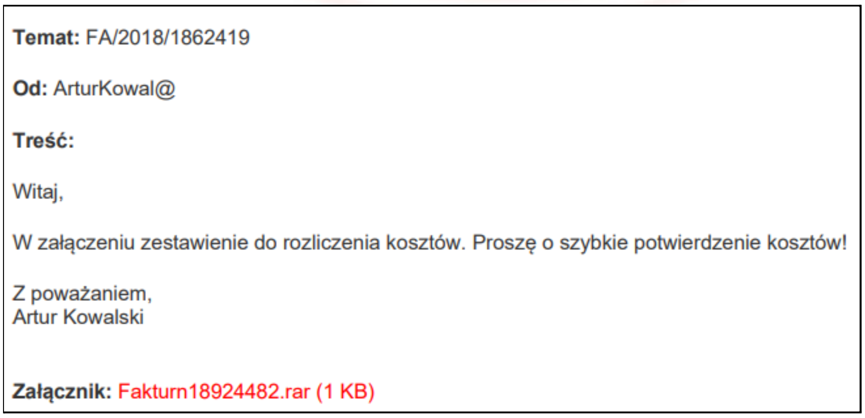
- "**Mass" phishing attempts**, which usually are:
    - Emails sent to often thousands of people.
    - Non-personal; asking for password changes or money transfers.
    - Simpler to detect, due to the use of words and emails associated with phishing.

- **"Spear" phishing attempts**, which usually are:
    - Targeting specific individuals within the organization.
    - Impersonating coworkers or using private information to gain the trust of the victim.
    - Harder to detect and protect against.

Examples of phishing attempts at Eklamot

The last security audit at the company revealed that spam and phishing attempts are prevalent **in all departments**. Reducing the number of malicious emails reaching the employees should be the **top priority** in the solution process. In the provided documentation containing the examples of emails identified as phishing attempts, some positions are especially concerning:

- This email impersonates a named employee and contains a hazardous file, which could potentially infect the system with tailor-made malware.



Temat: FA/2018/1862419

Od: ArturKowal@

Treść:

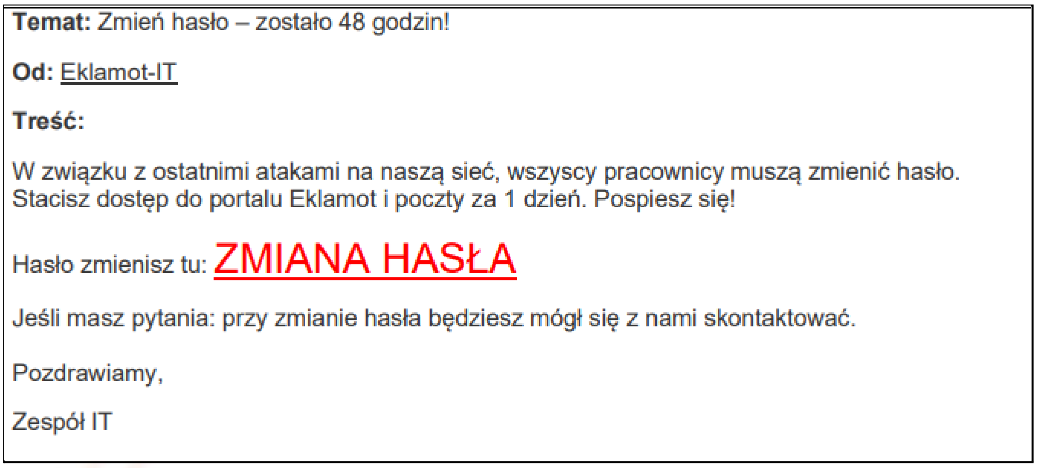
Witaj,

W załączeniu zestawienie do rozliczenia kosztów. Proszę o szybkie potwierdzenie kosztów!

Z poważaniem,
Artur Kowalski

Załącznik: Fakturn18924482.rar (1 KB)

- In this email, the attacker pretends to be the IT administrator and tries to gain access to the internal systems through an employee account.



Temat: Zmień hasło – zostało 48 godzin!

Od: Eklamot-IT

Treść:

W związku z ostatnimi atakami na naszą sieć, wszyscy pracownicy muszą zmienić hasło. Stacisz dostęp do portalu Eklamot i poczty za 1 dzień. Pospiesz się!

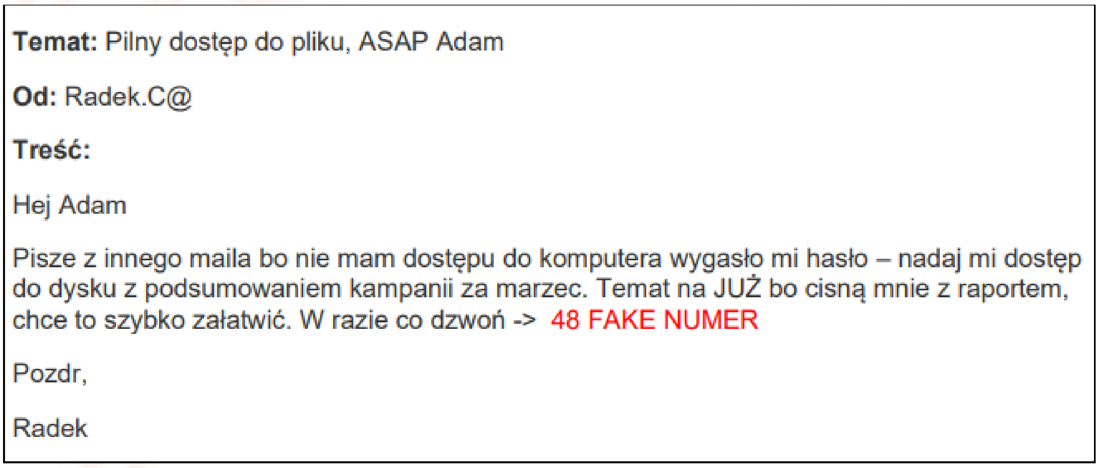
Hasło zmienisz tu: ZMIANA HASŁA

Jeśli masz pytania: przy zmianie hasła będziesz mógł się z nami skontaktować.

Pozdrawiamy,

Zespół IT

- This is the most dangerous kind of phishing, as it uses information about relations between employees to gain access to confidential files.



Temat: Pilny dostęp do pliku, ASAP Adam

Od: Radek.C@

Treść:

Hej Adam

Pisze z innego maila bo nie mam dostępu do komputera wygasło mi hasło – nadaj mi dostęp do dysku z podsumowaniem kampanii za marzec. Temat na JUŻ bo cisną mnie z raportem, chce to szybko załatwić. W razie co dzwoń -> 48 FAKE NUMER

Pozdr,

Radek

The presence of such **high-level threats** causes the need to implement **multiple** anti-phishing solutions to reach an **acceptable** level of security. Our propositions can be found below.

Solution propositions

The proposed solutions were divided into three major groups: short-, mid- and long-term. They require a different amount of time to implement and provide different levels of security. All relevant descriptions can be found in the respective sub-parts of the document.

Short-term solutions

We are able to start the implementation of those solutions immediately, at a relatively low cost. They are **vital** for general protection, however, are **not sufficient** for sustainable business practice. **Implementation of all of them is highly recommended**.

Basic defence system designed by CJHI

The current on-premise Microsoft Exchange Server, responsible for managing the Eklamot email domain, does not automatically filter out any messages. Implementation of a simple filtering system would be very simple and can be done with a programme designed by CJHI. The file with the basic logic of the programme can be found in the attachments.

Effectiveness: High
Most "Mass" phishing attempts can be filtered out and not reach the employees.

Cost estimate: $0
The system basics were developed already for the purpose of this report. Its implementation into the server is within the scope of the usual cooperation agreement between Eklamot and CJHI.

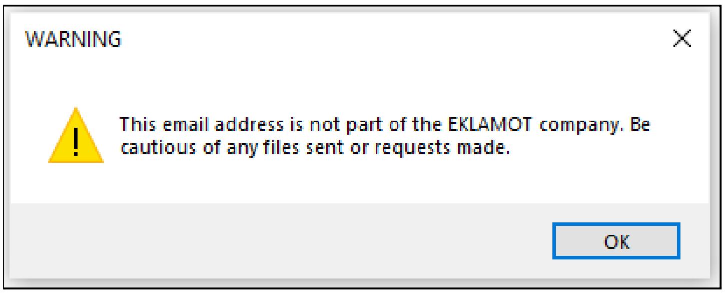
Timeframe: ~ 3 days
The solution can be implemented by the CJHI team within around 3 days from the decision of commitment.

Operation:
The proposed system would consist of three major parts:

- **Email blacklist** - Blocking blacklisted addresses from reaching the employees and informing the IT department of a phishing attempt. The blacklist contains emails from previous attacks, online sources and is always updating. Relevant code:

```
for x in email_blacklist:
   if content.__contains__(x):
       print("Message hidden and IT department informed")
       #SENDING INFORMATION TO THE IT DEPARTMENT
       #HIDING THE EMAIL FROM THE EMPLOYEE
   exit()
```

- **Email whitelist** - Checking if the email comes from within Eklamot and warning the user if not. Example warning:

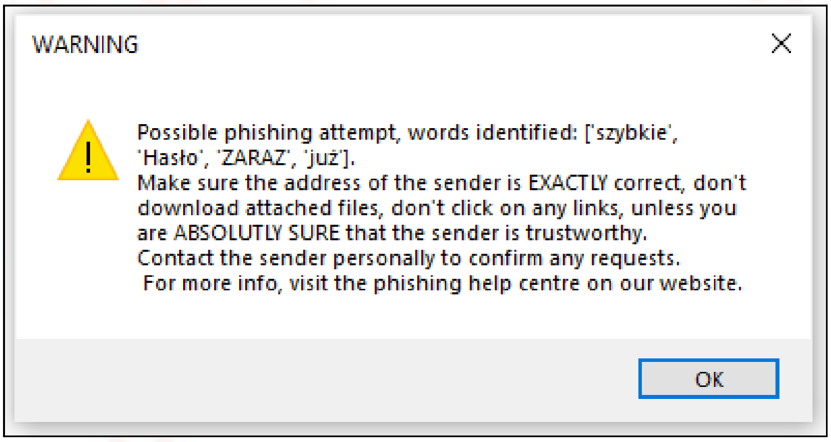


This email address is not part of the EKLAMOT company. Be cautious of any files sent or requests made.

Relevant code:

```
internalEmail = False
for x in email_whitelist:
   if content.__contains__(x):
       internalEmail = True
if internalEmail == False:
   ctypes.windll.user32.MessageBoxW(0, "The email adress: " + x + "is not part of the
EKLAMOT company. Be cautious of any files sent or requests made.", "WARNING",
MB_OK|ICON_EXLAIM)
```

- **Word filter -** Scanning the email for words typical for phishing attempts and spam, obtained from previous attempts and internet databases. If the email is suspicious the user is informed and if the email is highly suspicious the message is hidden and the IT administrator informed. Example warning:



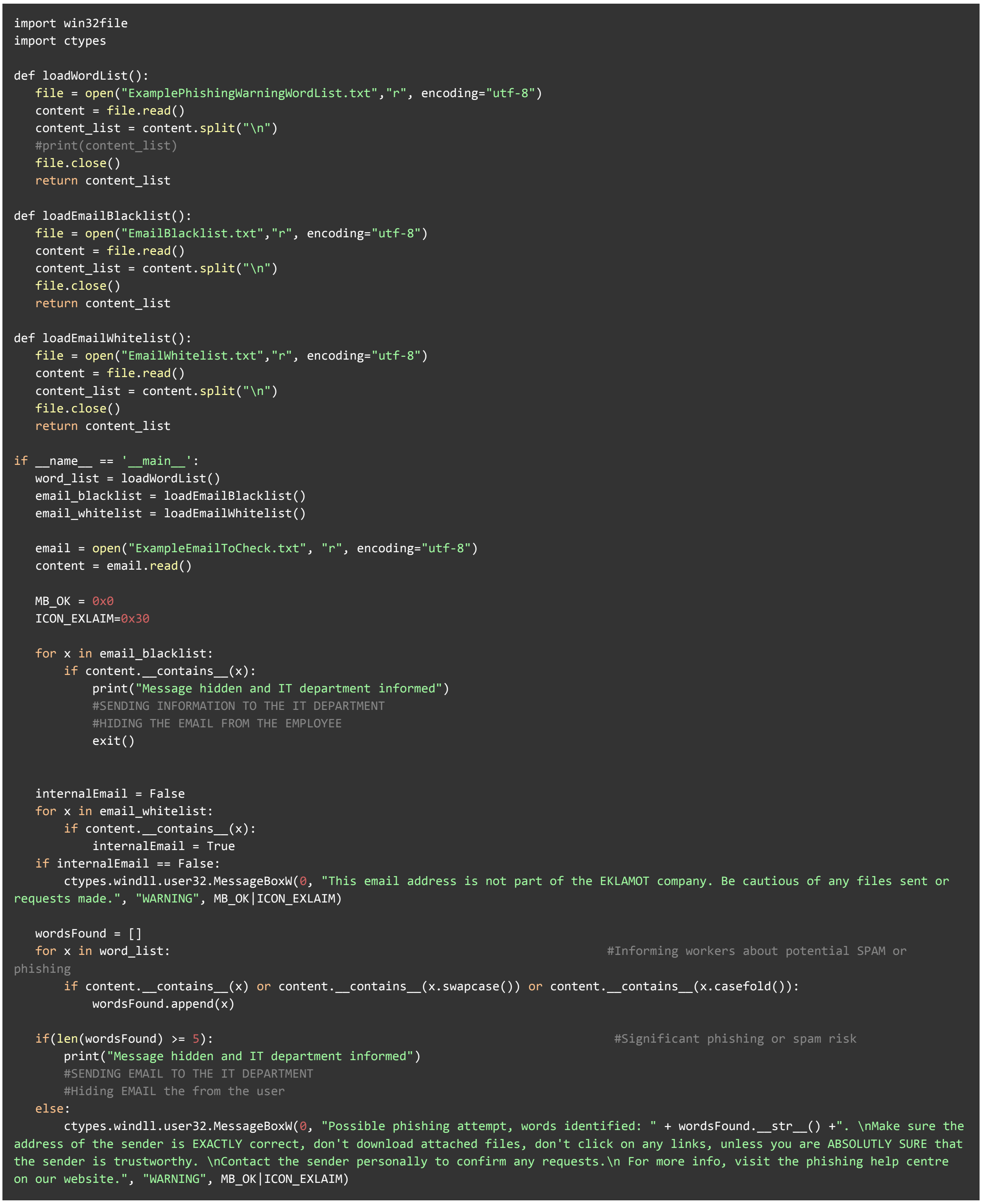
Possible phishing attempt, words identified: ['szybkie', 'Hasło', 'ZARAZ', 'już'].
Make sure the address of the sender is EXACTLY correct, don't download attached files, don't click on any links, unless you are ABSOLUTLY SURE that the sender is trustworthy.
Contact the sender personally to confirm any requests.
For more info, visit the phishing help centre on our website.

Relevant code:

```
wordsFound = []
for x in word_list:                                                    #Informing workers
about potential SPAM or phishing
   if content.__contains__(x) or content.__contains__(x.swapcase()) or
content.__contains__(x.casefold()):
       wordsFound.append(x)

if(len(wordsFound) >= 5):                                              #Significant
phishing or spam risk
   print("Message hidden and IT department informed")
   #SENDING EMAIL TO THE IT DEPARTMENT
   #Hiding EMAIL the from the user
else:
   ctypes.windll.user32.MessageBoxW(0, "Possible phishing attempt, words identified: " +
wordsFound.__str__() +". \nMake sure the address of the sender is EXACTLY correct, don't download
attached files, don't click on any links, unless you are ABSOLUTLY SURE that the sender is
trustworthy. \nContact the sender personally to confirm any requests.\n For more info, visit the
phishing help centre on our website.", "WARNING", MB_OK|ICON_EXLAIM)
```

The full basic solution code overview:



```
import win32file
import ctypes

def loadWordList():
   file = open("ExamplePhishingWarningWordList.txt","r", encoding="utf-8")
   content = file.read()
   content_list = content.split("\n")
   #print(content_list)
   file.close()
   return content_list

def loadEmailBlacklist():
   file = open("EmailBlacklist.txt","r", encoding="utf-8")
   content = file.read()
   content_list = content.split("\n")
   file.close()
   return content_list

def loadEmailWhitelist():
   file = open("EmailWhitelist.txt","r", encoding="utf-8")
   content = file.read()
   content_list = content.split("\n")
   file.close()
   return content_list

if __name__ == '__main__':
   word_list = loadWordList()
   email_blacklist = loadEmailBlacklist()
   email_whitelist = loadEmailWhitelist()

   email = open("ExampleEmailToCheck.txt", "r", encoding="utf-8")
   content = email.read()

   MB_OK = 0x0
   ICON_EXLAIM=0x30

   for x in email_blacklist:
       if content.__contains__(x):
           print("Message hidden and IT department informed")
           #SENDING INFORMATION TO THE IT DEPARTMENT
           #HIDING THE EMAIL FROM THE EMPLOYEE
           exit()


   internalEmail = False
   for x in email_whitelist:
       if content.__contains__(x):
           internalEmail = True
   if internalEmail == False:
       ctypes.windll.user32.MessageBoxW(0, "This email address is not part of the EKLAMOT company. Be cautious of any files sent or
requests made.", "WARNING", MB_OK|ICON_EXLAIM)

   wordsFound = []
   for x in word_list:                                                        #Informing workers about potential SPAM or
phishing
       if content.__contains__(x) or content.__contains__(x.swapcase()) or content.__contains__(x.casefold()):
           wordsFound.append(x)

   if(len(wordsFound) >= 5):                                                   #Significant phishing or spam risk
       print("Message hidden and IT department informed")
       #SENDING EMAIL TO THE IT DEPARTMENT
       #Hiding EMAIL the from the user
   else:
       ctypes.windll.user32.MessageBoxW(0, "Possible phishing attempt, words identified: " + wordsFound.__str__() +". \nMake sure the
address of the sender is EXACTLY correct, don't download attached files, don't click on any links, unless you are ABSOLUTLY SURE that
the sender is trustworthy. \nContact the sender personally to confirm any requests.\n For more info, visit the phishing help centre
on our website.", "WARNING", MB_OK|ICON_EXLAIM)
```

<u>The code above is meant to visualize a future implementation and not to be used in its current form.</u> A runnable example file can be also found in the attachments. Given the request, CJHI is able to quickly adjust the concept to Eklamot's infrastructure and put the basic defence online, providing basic filtering before more permanent solutions are implemented.

Employee training sessions

As the most important resource in the company, employees must be proficient in detecting and executing appropriate policies after recognizing phishing. It is crucial for e-commerce based companies to understand that phishing attempts are part of everyday business - not a one-off which can be ignored or left to the employee to decide. Implementation of any anti-phishing solutions is **useless** when the main target of an attack does not understand the specifics of a phishing attack. In our opinion, every employee should be a part of this course and successfully complete the test afterwards to ensure that we turn the human factor from the weakest link to our strongest asset in protecting against phishing and everyone understands basic rules, like the fact the IT department never sends direct links for password change.

Effectiveness: Medium - Very high

Effectiveness is highly dependable on the skill set and learning will of the team engaged. When properly conducted, will yield high returns and efficiently protect the company from even the most intricate forms of phishing

Cost estimate: Low

To institute employee training sessions, the company would have to contract a specialist for at least a few sessions; as this topic is in the scope of almost every company pricing is easily obtainable after terms & conditions of cooperation are set.

Timeframe: 1 week

If the CJHI team is chosen to deliver the training sessions, it would be able to start leading sessions immediately after the contract is signed. (More details on our website)

Company-wide phishing attempt tests

A recent phishing incident that impacted the accounting department and caused financial losses confirmed that the current state of anti-phishing knowledge among employees is insufficient to ensure the integrity of the company. While conducting Employee training sessions will provide employees with much-needed knowledge on the topic of phishing, we should not settle for only that. The process of preserving skills is an integral part of learning - conducting controlled phishing attempts will provide both parties with significant skills and feedback which will be used to further improve processes (both employee spotting & reporting and phishing-testing).

Effectiveness: High

Most phishing emails follow similar patterns - understanding them will help spot particular red flags, which ensures that suspicious emails will be omitted or escalated by employees.

Cost estimate: Low

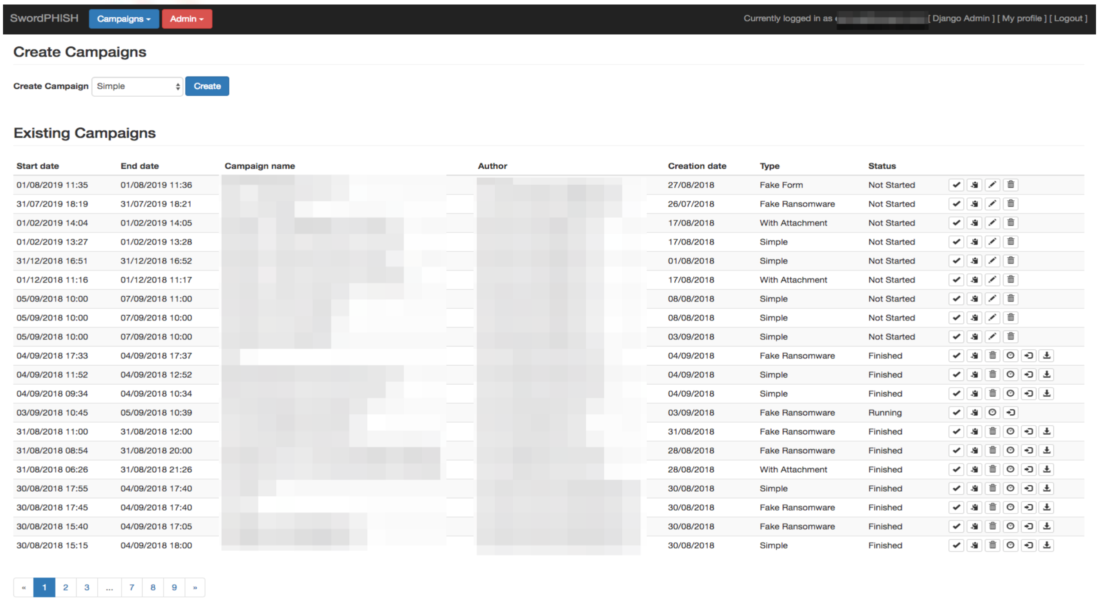
Implementing existing **open-source** phishing attempt test solutions such as Swordphish can be done almost instantly - the same is applicable for running phishing campaigns. Conducting an effective course on running phishing tests would require the engagement of an appropriate professional for 2-3 days.

Timeframe: <3 days

Our team estimates that the solution can be implemented within around 3 days or less from the decision of commitment.

Operations - Swordphish + IT team trained to conduct phishing tests

Swordphish enables running the aforementioned phishing tests and monitoring the abilities of employees to identify and escalate phishing attempts. It is recommended for tests to be managed by qualified staff to ensure the highest possible training value for employees



Currently logged in as [redacted] [Django Admin] [My profile] [Logout]

Create Campaigns

Create Campaign: Simple ⬍ Create

Existing Campaigns

Start date	End date	Campaign name	Author	Creation date	Type	Status	
01/08/2019 11:35	01/08/2019 11:36	[redacted]	[redacted]	27/08/2018	Fake Form	Not Started	✓ 👤 ✎ 🗑
31/07/2019 18:19	31/07/2019 18:21	[redacted]	[redacted]	26/07/2018	Fake Ransomware	Not Started	✓ 👤 ✎ 🗑
01/02/2019 14:04	01/02/2019 14:05	[redacted]	[redacted]	17/08/2018	With Attachment	Not Started	✓ 👤 ✎ 🗑
01/02/2019 13:27	01/02/2019 13:28	[redacted]	[redacted]	17/08/2018	Simple	Not Started	✓ 👤 ✎ 🗑
31/12/2018 16:51	31/12/2018 16:52	[redacted]	[redacted]	01/08/2018	Simple	Not Started	✓ 👤 ✎ 🗑
01/12/2018 11:16	01/12/2018 11:17	[redacted]	[redacted]	17/08/2018	With Attachment	Not Started	✓ 👤 ✎ 🗑
05/09/2018 10:00	07/09/2018 11:00	[redacted]	[redacted]	08/08/2018	Simple	Not Started	✓ 👤 ✎ 🗑
05/09/2018 10:00	07/09/2018 10:00	[redacted]	[redacted]	08/08/2018	Simple	Not Started	✓ 👤 ✎ 🗑
05/09/2018 10:00	07/09/2018 10:00	[redacted]	[redacted]	03/09/2018	Simple	Not Started	✓ 👤 ✎ 🗑
04/09/2018 17:33	04/09/2018 17:37	[redacted]	[redacted]	04/09/2018	Fake Ransomware	Finished	✓ 👤 🗑 ⏱ ↩ ⤓
04/09/2018 11:52	04/09/2018 12:52	[redacted]	[redacted]	04/09/2018	Simple	Finished	✓ 👤 🗑 ⏱ ↩ ⤓
04/09/2018 09:34	04/09/2018 10:34	[redacted]	[redacted]	04/09/2018	Simple	Finished	✓ 👤 🗑 ⏱ ↩ ⤓
03/09/2018 10:45	05/09/2018 10:39	[redacted]	[redacted]	03/09/2018	Fake Ransomware	Running	✓ 👤 ⏱ ↩
31/08/2018 11:00	31/08/2018 12:00	[redacted]	[redacted]	31/08/2018	Fake Ransomware	Finished	✓ 👤 🗑 ⏱ ↩ ⤓
31/08/2018 08:54	31/08/2018 20:00	[redacted]	[redacted]	28/08/2018	Fake Ransomware	Finished	✓ 👤 🗑 ⏱ ↩ ⤓
31/08/2018 06:26	31/08/2018 21:26	[redacted]	[redacted]	28/08/2018	With Attachment	Finished	✓ 👤 🗑 ⏱ ↩ ⤓
30/08/2018 17:55	04/09/2018 17:40	[redacted]	[redacted]	30/08/2018	Simple	Finished	✓ 👤 🗑 ⏱ ↩ ⤓
30/08/2018 17:45	04/09/2018 17:40	[redacted]	[redacted]	30/08/2018	Fake Ransomware	Finished	✓ 👤 🗑 ⏱ ↩ ⤓
30/08/2018 15:40	04/09/2018 17:05	[redacted]	[redacted]	30/08/2018	Fake Ransomware	Finished	✓ 👤 🗑 ⏱ ↩ ⤓
30/08/2018 15:15	04/09/2018 18:00	[redacted]	[redacted]	30/08/2018	Simple	Finished	✓ 👤 🗑 ⏱ ↩ ⤓

Mid-term solutions

The mid-term solution propositions take longer to implement than basic protection and may come with higher financial costs, however, they provide **significant improvements** to the company's security. Implementing all of them is recommended, however, there is more flexibility to them than in the case of short-term solutions. They make the business practice **more sustainable**, but **not necessarily future-proof**.

Moving Eklamot's Exchange server into the cloud

In the current network architecture, the Microsoft Exchange Server is located on-premise and as we describe in the network architecture part of the *IT infrastructure report*, it would be highly beneficial for the company to start using the Microsoft Exchange Online services instead. This would not only bring the main benefits described in the report but also allow for the use of Microsoft Exchange Online Protection services. The result is outsourcing a significant part of email filtering technology to Microsoft, which has a team of engineers working full time on providing up-to-date protection from phishing and spam - a trait that would never be cost-efficient for Eklamot. This service can also work in conjunction with the one developed in short-term solutions by CJHI.

Effectiveness: Very high

The software offered by Microsoft filters out 99% of basic "mass" phishing attempts and spam, with some effectiveness against "spear" phishing. Moreover, a 24/7 IT hotline is available.

Cost estimate: $5 - $13/user/month

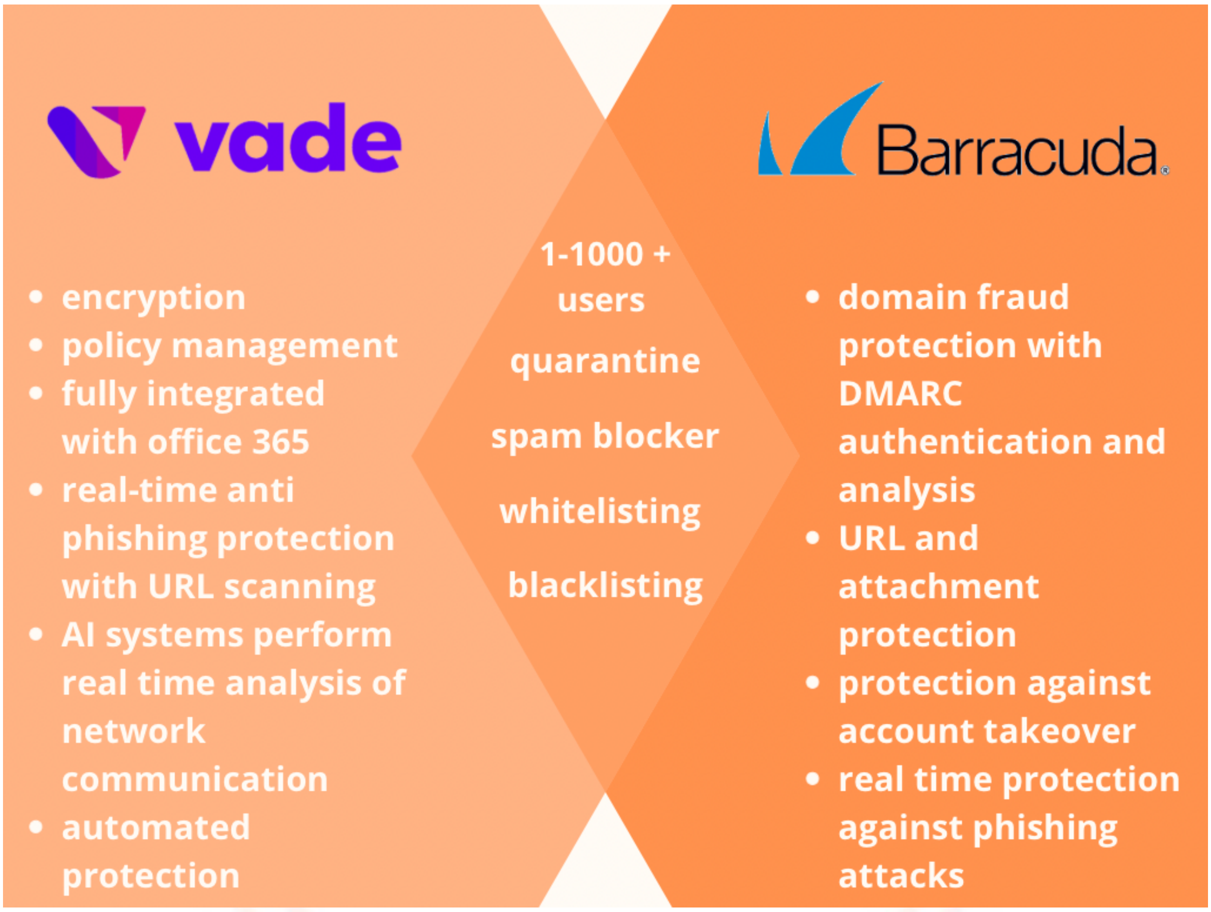
The estimate includes the costs of Microsoft Exchange Online servers. The Protection services alone are **$1/user/month** with an annual commitment.

Timeframe: 2-3 months

Implementation of this system is dependent on the migration to the Exchange Online services. After the migration is complete, turning the system online should take no more than 2 days.

Purchase of dedicated anti-phishing software

Although Microsoft Exchange Online Protection services are very convenient to implement (since Eklamot is already using a version of Microsoft Exchange), they can be used only after the cloud server is established. Moreover, there are services on the market, which could provide slightly better protection for a higher cost, namely Vade and Barracuda. It would be beneficial to the security of the company to buy and implement subscriptions to either one of those services for users with higher system access, to enhance the security for the time before other measures proposed are properly implemented. Below an infographic comparing the features of those systems can be found.



vade

- encryption
- policy management
- fully integrated with office 365
- real-time anti phishing protection with URL scanning
- AI systems perform real time analysis of network communication
- automated protection

1-1000 + users

quarantine

spam blocker

whitelisting

blacklisting

Barracuda

- domain fraud protection with DMARC authentication and analysis
- URL and attachment protection
- protection against account takeover
- real time protection against phishing attacks

Effectiveness: Very high

The software provides advanced functions, which would enhance the security of users with advanced access, while other solutions, including the Exchange Online Protection, are in their preparation phase.

Cost estimate: ~$3/user/month

Vade requires an annual commitment, while Barracuda doesn’t. Longer licences, however, come with a discounted price.

Timeframe: 1-2 weeks

The software can be implemented and can be used until other solutions are not ready.

Implementing 2-factor authentication in all of Eklamot’s systems

A strong password minimises the potential for brute-forcing unauthorised access, albeit it does not provide insight into the identity of the person accessing. We advise introducing **Google Authenticator** - a two-factor authentication which will minimise damage caused by password leaks. In order to unite in one solution our desired security target and keep the needed implementation time as low as possible ad hoc, we suggest a solution which provides API to us. Suggested long term solutions in 2FA scope (U2F) are discussed in the relevant chapter.

Effectiveness: Medium

The aforementioned 2FA solution provides an 80-bit secret key to each user - without knowledge of it an external agent is not able to gain access, moreover the length of the key makes brute-force access attempts futile. Unfortunately, - the human factor still plays an important role. In case of an employee becomes a victim of a more sophisticated phishing attack, the attacker might gain access to the system thanks to the employee providing the 2FA key mistakenly.

Cost estimate: Low

As the API is already in place, potential deployment costs significantly decrease, although implementation must be overseen to ensure that no weak spots are left. Man-hours needed to implement is the main constituent of cost, as Google Authenticator is an open-source solution.

Timeframe: 1 month

Although the whole implementation process can last only a few days, it is necessary to make sure that all mentioned short-term solutions are implemented and are stable. In case of outright deployment, 2FA will not become significant as there are existing critical infrastructure design flaws.

Long-term solutions

The long-term solutions are more elaborate project propositions, which will take the longest to become fully implemented but will provide **outstanding security**. They are more ambitious in their scope and have the potential to serve the company with **good results for years** to come.

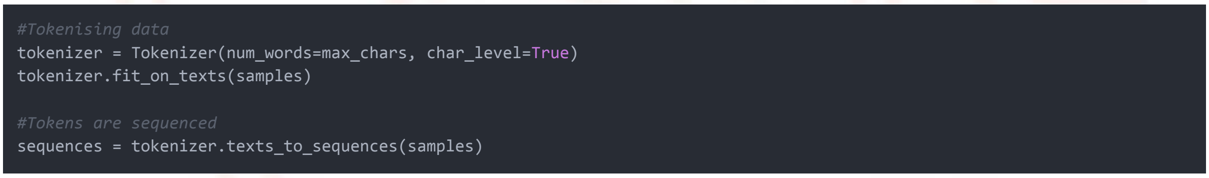
Introducing an advanced machine learning danger detection system developed by CJHI

The CJHI team has already trained 3 machine learning classificators that automatically detect malicious URL links, 2 of them with 85%-88% certainty. The algorithm can be viewed and tested in the “Machine Learning powered anti-phishing algorithm” folder. A combination of 2 best performing classificators yields 90-97% accuracy in most tests. This could be implemented to create an automated self-learning anti-phishing system. However, the system needs more training to start with to increase its base accuracy. A collection of URL links from phishing emails in Eklamot mailboxes would be a powerful training dataset if the company decides to implement this solution.

Moreover, CJHI could develop and integrate a machine learning algorithm that analyses the text of different mails and detects phishing. The combination of the two would create a very powerful security tool. This however requires more time and data from Eklamot.

Technical information

With the database of over 60 000 URLs, both malicious and safe, we tokenized them and then sequenced the tokens to be able to use them for fitting machine learning classificators.



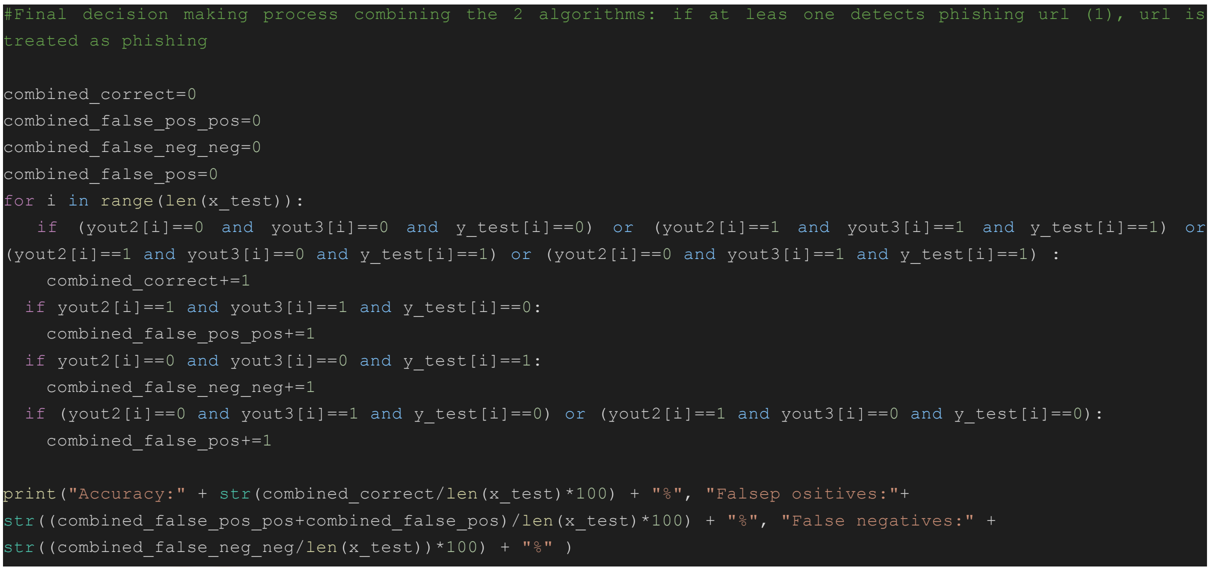
```
#Tokenising data
tokenizer = Tokenizer(num_words=max_chars, char_level=True)
tokenizer.fit_on_texts(samples)

#Tokens are sequenced
sequences = tokenizer.texts_to_sequences(samples)
```

The data was split (90% for training, 10% for validation) and shuffled. 3 different classificators were trained and tested:

1. Logistic regression ~66% accuracy
2. K-nearest neighbour ~88% accuracy
3. Decision trees ~86% accuracy

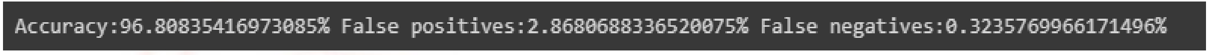
A combination of K-nearest neighbour and decision trees was used to develop a high accuracy algorithm.



```
#Final decision making process combining the 2 algorithms: if at leas one detects phishing url (1), url is
treated as phishing

combined_correct=0
combined_false_pos_pos=0
combined_false_neg_neg=0
combined_false_pos=0
for i in range(len(x_test)):
   if (yout2[i]==0 and yout3[i]==0 and y_test[i]==0) or (yout2[i]==1 and yout3[i]==1 and y_test[i]==1) or
(yout2[i]==1 and yout3[i]==0 and y_test[i]==1) or (yout2[i]==0 and yout3[i]==1 and y_test[i]==1) :
    combined_correct+=1
  if yout2[i]==1 and yout3[i]==1 and y_test[i]==0:
    combined_false_pos_pos+=1
  if yout2[i]==0 and yout3[i]==0 and y_test[i]==1:
    combined_false_neg_neg+=1
  if (yout2[i]==0 and yout3[i]==1 and y_test[i]==0) or (yout2[i]==1 and yout3[i]==0 and y_test[i]==0):
    combined_false_pos+=1

print("Accuracy:" + str(combined_correct/len(x_test)*100) + "%", "Falsep ositives:"+
str((combined_false_pos_pos+combined_false_pos)/len(x_test)*100) + "%", "False negatives:" +
str((combined_false_neg_neg/len(x_test))*100) + "%" )
```



```
Accuracy:96.80835416973085% False positives:2.8680688336520075% False negatives:0.3235769966171496%
```

Only ~0.32% of results are false negatives (phishing URLs that were considered safe) vs ~2.86% false positives (normal URLs that were considered phishing), meaning that the algorithm is conservative in its estimates which is in accordance with security principles.

Effectiveness: High to very high- consistency and universality

Because the algorithm focuses on URLs, it is universal regardless of the language of the mail. Moreover, it will be able to keep up with evolving creativity of the hackers, as more and more new phishing URLs could be added as training data.

Cost: TBD

The cost of this algorithm would be either a one-time payment, which would not require constant variable costs or a standard subscription agreement.

Timeframe: 1-5 months

Creating a full algorithm, training, implementing it into the system and creating automated learning based on received mails will take some time. Full efficiency will not be achieved immediately after implementation.

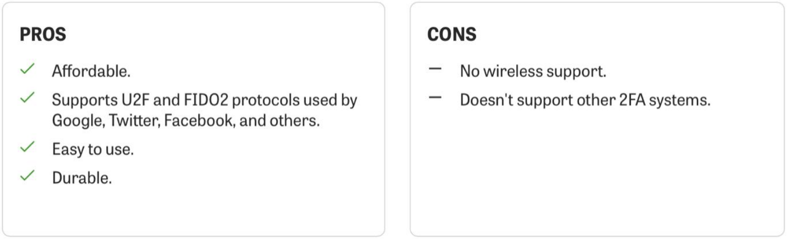
Implementing Universal 2nd Factor Authentication keys

Universal 2nd Factor (U2F) is an open standard that strengthens and simplifies two-factor authentication (2FA) using specialised USB or NFC devices based on similar security technology found in smart cards.

When an account requests 2FA verification, you will need to plug your security key into your phone or PC's USB port or (if supported) tap it to the back of your NFC-enabled phone. Then it is only a matter of pressing the button on the key to establish the connection.

A 2nd Factor key device recommended by our team is Yubico Security Key, which comes in two forms: the Yubico Security Key NFC (USB-A) and the Yubico Security Key C NFC (USB-C). These security keys are easy to use and work with most devices, including phones and laptops.

Yubico Security key
Price: 25 $



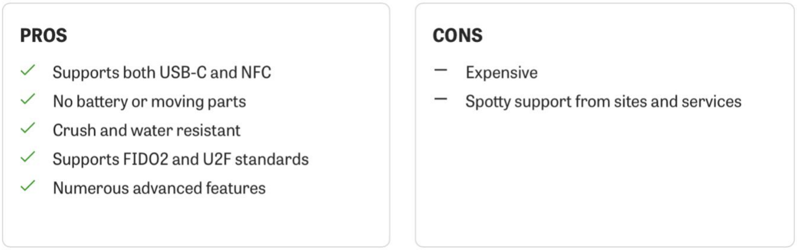
PROS

- ✓ Affordable.
- ✓ Supports U2F and FIDO2 protocols used by Google, Twitter, Facebook, and others.
- ✓ Easy to use.
- ✓ Durable.

CONS

- – No wireless support.
- – Doesn't support other 2FA systems.

Yubico YubiKey5 NFC
Price: 45-55 $



PROS

- ✓ Supports both USB-C and NFC
- ✓ No battery or moving parts
- ✓ Crush and water resistant
- ✓ Supports FIDO2 and U2F standards
- ✓ Numerous advanced features

CONS

- – Expensive
- – Spotty support from sites and services

Yubico YubiKey5 NFC has additional functions, but they are not necessary for a standard user. Yubico Security Key is a low-cost solution which can be easily replaced in the event of a key being lost by an employee. We would recommend getting the cheaper one as it is entirely sufficient. U2F solutions should be the company's long term target of ensuring only authorised access. Although they are pricier than standard software-based solutions (mainly the one we provided as our midterm target), potential losses caused by a successful attack could and most probably will be manyfold higher.

Moreover, Yubico keys can be used to sign e-mails. Its use by IT support would further decrease the chance of a phishing attack posing as a security message.

Effectiveness: High - simplicity and universality

Physical security keys (given no significant security issues are existing) are not interceptable by attackers and provide maximum safety. YubiKey 5 supports the most popular protocols, which assure a standardised level of safety. USB and optionally NFC based connection ensures compatibility with a wide spectrum of devices and a seamless work as these security keys do not require any special skills to use them.

Cost: Medium (25-55 $ per employee)

Cost depends on the version of the key device that we choose. It will vary depending on the needs and requirements of a company and their employees.

Timeframe: 4-5 months

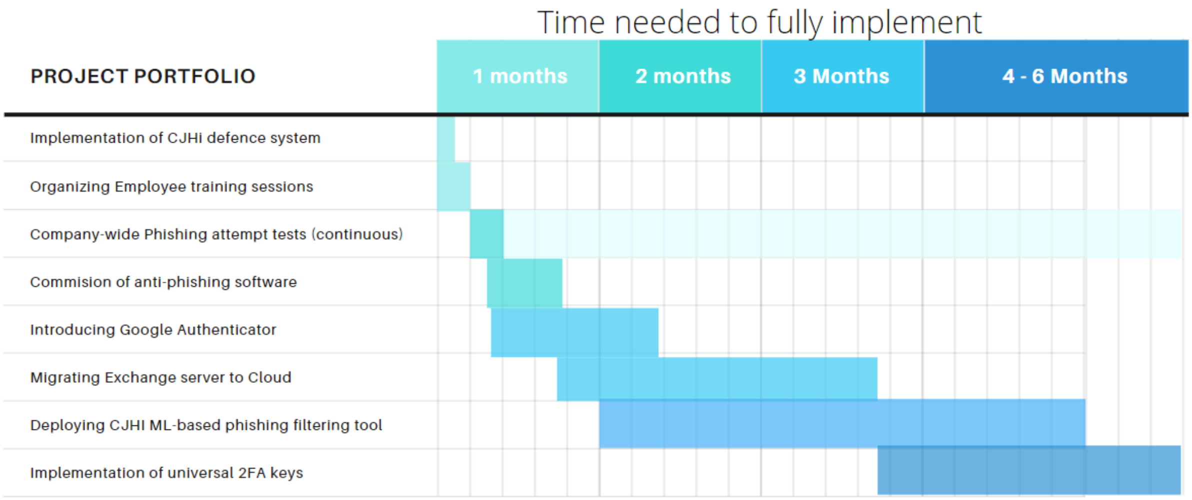
This solution cannot be implemented immediately. We recommend implementation after previous short-term and mid-term solutions have been integrated successfully, due to the minimum required level of IT infrastructure safety needed for physical 2FA tokens to yield more than software-based solutions.

Summary

Table with proposed solutions overview

Type	Measure	Effectiveness	Cost estimate	Time needed to implement
Short-term	CJHI defence system	High	$0	~3 days
Short-term	Employee training sessions	Medium - Very high	Low	~1-day
Short-term	Phishing attempt tests	High	Low	< 3 days
Mid-term	Purchasing anti-phishing software	Medium	3$ per user per month	1-2 weeks
Mid-term	Introducing Google Authenticator	High	Low	~1 month
Mid-term	Migrating Exchange server to Cloud	Very High	5 - 13$ per user per month	~2-3 months
Long-term	CJHI ML-based phishing filtering tool	Very high	TBD	~1-5 months
Long-term	Universal 2FA keys	High	$25-$55 per unit	~4-5 months

Systems implementation roadmap



It should be noticed that the timeline is just a rough estimate and the solution order is more important!

Final remarks

- Store security systems are not working properly, and Eklamot should strive to reduce the amount of potentially dangerous e-mails which are reaching our employees with the proposed solutions.

- Staff training can be crucial in increasing store security and preventing phishing attacks.

- Implementing a basic filtering programme designed by our team (CJHI) can significantly increase the level of security in the short term.

- Phishing attempt tests are essential and should be done on a regular basis.

- Moving Eklamot's exchange server to the cloud will have many benefits, such as the possibility of using Microsoft Exchange Online Protection services for filtering and detection of potential threats.

- Purchasing a dedicated anti-phishing software ensures protection against scams.

- Implementing 2nd Factor authenticator software such as Google Authenticator can be done immediately and can help with limiting access for unauthorised people.

- Our team (CJHI) can prepare advanced filtering software with confirmed effectiveness of 90-97% based on machine learning, that can be further trained to keep up with increasing scammers' creativity.

- In the long-term, it is recommended to upgrade from software authenticators to key device authenticators such as Yubico Security keys because they are less vulnerable to attacks.