CyberPhish

Project no: 2020-1-LT01-KA203-078070

IO1 A1: "RECOGNISING PHISHING AND SKILLS GAPS"

REPORT

2021

Partnership

Vilnius University, Lithuania

Website: http://www.vu.lt

University of Tartu

Website: https://www.ut.ee/et

MECB - Macdac Engineering Consultancy Bureau LTD , Malta

Website: http://www.mecb.com.mt/eu

Altacom SIA, Latvia

Website: https://www.altacom.eu/

DOREA Educational Institute, Cyprus

Website: https://dorea.org/

ECDL- Information Technologies Institute, Lithuania

Website: http://www.ecdl.lt/

Funded by the Erasmus+ Programme of the European Union

Contents

1. INTRODUCTION 6
   1.1. Cybersecurity in EU: realities and needs 6
   1.2. "Safeguarding Against Phishing in the Age of 4th Industrial Revolution" project 7
2. PHISHING 9
   2.1. What is Phishing? 9
   2.2. Social Engineering and Phishing 10
   2.3. Phishing during COVID-19 12
3. SURVEYS FOR STUDENTS, EMPLOYEES AND CEOS 13
   3.1. The methodology of data collection 13
   3.2. Compilation of the results 14
   3.3. Results and analysis of surveys 14
      3.3.1. Overview of the respondents 14
      3.3.2. General knowledge and behaviours 15
      3.3.3. Personal experience with phishing attacks 19
      3.3.4. Recognising phishing attacks 20
      3.3.5. Critical thinking skills 22
      3.3.6. Avoiding phishing attacks 23
4. SUMMARY AND MAIN FINDINGS 26
5. BIBLIOGRAPHY 30

ANNEX 1. Survey 31

List of Tables

Table 1. Number of respondents per country 14
Table 2. Respondents by genders 14
Table 3. The most and the least important criteria in recognising phishing attacks 21

List of Figures

Figure 1. Survey respondents' employment status 15
Figure 2. Survey respondents' education level 15
Figure 3. Survey respondents' awareness of phishing 16
Figure 4. Types of phishing respondents are most aware of 17
Figure 5. Types of phishing respondents are the least aware of 17

Funded by the Erasmus+ Programme of the European Union

Figure 6. Consequences most likely to occur after the successful phishing attack according to respondents 17
Figure 7. Types of emails respondents are most likely to click on the link or attachment in the email or message and/or provide sensitive information 18
Figure 8. Types of emails respondents are least likely to click on the link or attachment in the email or message and/or provide sensitive information 18
Figure 9. Ways survey respondents were phished in the past 19
Figure 10. Reasons why respondents think they were phished 19
Figure 11. Respondents' focus and attention to details when opening a message/email 22
Figure 12. Respondents being mindful when clicking on the link/attachment 23
Figure 13. Main reasons why phishing attacks are successful according to respondents 24
Figure 14. Actions to take to prevent phishing attacks according to respondents 24
Figure 15. Areas respondents feel most confident in 25

Funded by the Erasmus+ Programme of the European Union

List of abbreviations

BEC	Business Email Compromise
CEO	Chief executive officer
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUROPOL	The European Union Agency for Law Enforcement Cooperation

Funded by the Erasmus+ Programme of the European Union

1. INTRODUCTION

1.1. Cybersecurity in EU: realities and needs

The European Commission has prepared and conducted a special Eurobarometer survey[1] in 2019 aiming to understand EU citizens' awareness, experiences and perceptions of cybersecurity.

Unsurprisingly, the results showed that Internet use is continuing to grow in Europe, particularly via smartphones. The results[2] also showed that EU citizens are more aware of the potential dangers of going online, with 52% of respondents stating they are fairly well or very well informed about cybercrime, up from 46% in 2017. According to the survey's findings, concerns about online privacy and security have already led more than 9 in 10 Internet users to change their online behaviour – most often by not opening emails from unknown people, installing antivirus software, visiting only known and trusted websites and sign in only to their computers.

While these results are quite encouraging, many internet users still fall into online fraud and email phishing baits. According to Eurostat data, in 2019, approximately 1 in 3 EU citizens aged 16 to 74 reported security-related incidents when using the internet for private purposes in 2019 in the last 12 months.

During this period - phishing was the most frequent security incident reported in 2019[3]. 25% of respondents reported that they received fraudulent messages, known as phishing, while 12% of respondents reported being redirected to fake websites asking for personal information (pharming). The share of people who experienced security-related problems when using the internet for private purposes varied across the EU Member States. The highest rates were observed in Denmark (50%), followed by France (46%), Sweden (45%), Malta and the Netherlands (both 42%), Finland (41%) and Germany (40%). Contrary, the lowest shares were recorded in Lithuania (7%), Poland (9%), Latvia (10%), Bulgaria (13%) and Greece (13%). The share of people experiencing security-related problems in Estonia and Cyprus was 32% and 21%, respectively.

This can be explained by the differences between the level of cybercrime awareness among EU countries, the general decline in EU citizens confidence in being able to protect themselves against cyber-attacks, as well as more sophisticated cyber-attacks that are harder to detect and avoid, new techniques used and new platforms available to carry out such attacks.

When it comes to the business sector in Europe, they are also affected by cybersecurity issues. European countries and businesses are targeted with growing frequency. According to the 2017

[1] EU Commission (2020): Special Eurobarometer 499: Europeans' attitudes towards cyber security, URL https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG (accessed 11.02.2021)
[2] European Union Agency for Cybersecurity (2020): ENISA threat landscape 2019-2020
[3] EUROSTAT (2020): Is internet use safer today?, URL https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_pb/default/table?lang=en (accessed 11.02.2021)

Funded by the Erasmus+ Programme of the European Union

Global State of Information Security Survey, around 80% of companies in Europe have experienced at minimum one cybersecurity incident that year, and employees are responsible for 27% of all cybersecurity incidents.

Globally, based on recent data, in the first quarter of 2019, companies were targeted 120% more frequently than a year earlier, resulting in losses as high as €22,2 billion.

Over 99% of emails distributing malware required human intervention - following links, opening documents, accepting security warnings, and other behaviours - to be effective.[4]

Thus, people, whether at work or at home, who are aware of warning signs and have the knowledge of the right techniques, are the key elements to slow down or prevent cyber-attacks. Therefore, there is a need to update the existing cybersecurity programmes or create new ones to strengthen the skills, education and awareness of EU citizens on the latest emerging cybersecurity issues and threats.

There is also a need to offer such programmes to all the students, considering that according to ENISA, at universities, cyber-related subjects are underrepresented on non-technical programmes.

1.2. "Safeguarding Against Phishing in the Age of 4th Industrial Revolution" project

Cybersecurity becomes one of the biggest challenges in the digital age, because information becomes an expensive asset dealing with huge data volumes, improving communication with the digital environment. Digital devices and information systems increasingly become attractive for cyber-attacks.

Phishing is one of the highest problems because cybercriminals use faster and innovative technological tools to carry out phishing campaigns. Therefore human-driven phishing defence system that leverages human instinct for detection and technology to scale response should be developed and freely available for a broad audience. To create human-driven phishing defence, education is required for the user to identify and respond to phishing attacks in the correct manner.

The international project "Safeguarding against Phishing in the age of 4 Industrial Revolution" („CyberPhish") initiated by Vilnius University Kaunas Faculty and partners has started at the beginning of November 2020 and will last for two years.

The objective of the project is to educate students of higher education institutions, educators, university staff (members of the community), education centres, the business sector (employers and employees), and encourage critical thinking of the target group in the field of cybersecurity.

[4] Proofpoint (2019): Human Factor Report 2019, URL https://www.proofpoint.com/us/resources/threat-reports/human-factor (accessed 12.02.2021)

The project partners are going to design a curriculum, e-learning materials, a blended learning environment, knowledge and skills self-assessment and knowledge evaluation system simulations for students and other users in order to prevent phishing attacks, raise competencies, which will help to focus attention to threats and take appropriate prevention measures.

The project partnership is comprised of six organisations coming from five European countries:

1. Vilnius University, Lithuania (Coordinator)
2. Information Technologies Institute, Lithuania
3. DOREA Educational Institute, Cyprus
4. University of Tartu, Estonia
5. Altacom SIA, Latvia
6. Macdac Engineering Consultancy Bureau Ltd (MECB), Malta

For more information about the project and project activities, please visit the project's website: https://cyberphish.eu/

Funded by the Erasmus+ Programme of the European Union

2. PHISHING

2.1. What is Phishing?

Phishing is the fraudulent attempt to steal user data such as login credentials, credit card information, or even money using social engineering techniques. This type of attack is usually launched through email messages, appearing to be sent from a reputable source, with the intention of persuading the user to open a malicious attachment or follow a fraudulent URL.[5]

Phishing is also one of the oldest types of cyberattacks, dating back to the 1990s. Despite having been around for decades, it is still one of the most widespread and damaging cyberattacks.[6]

There are many different types of phishing, but the most common ones are:

1) *Spray and pray* – malicious emails that are sent to any email addresses in an attempt to steal sensitive information;
2) *Cat phishing* - luring someone in a relationship by adopting a fictional online persona;
3) *Advanced fee scam* - common fraud associated with nationals from Nigeria, e.g. asking for assistance in moving a large amount of money;
4) *Spear fishing* - malicious emails that are specially crafted and sent to a specific individual or organisation in an attempt to steal sensitive information;
5) *Whaling* - an attempt to steal sensitive information and is often targeted at senior management;
6) *Vishing* - refers to phishing scams that take place over the phone;
7) *Smishing* - refer to phishing by using SMS messages as opposed to emails to target individuals;
8) *Angler Phishing – a* relatively new type which refers to attacks that exist on social media using fake URLs, cloned websites, posts, and tweets as well as instant messaging;
9) *Clone Phishing* – a type of phishing where a legitimate and previously delivered email is used to create an identical email with malicious content;
10) *Malvertising* - this phishing type uses online advertisements or pop-ups to compel people to click a valid-looking link that then installs malware on their computer.

The growing sophistication of phishing has been noticed in the past couple of years, with phishing becoming more difficult to detect, many phishing emails and sites being almost identical to the real ones. At the same time, phishing campaigns have become faster and more automated, forcing

[5] European Union Agency for Cybersecurity (2020): Phishing - ENISA threat landscape 2019-2020
[6] Deloitte (2019): Understanding Phishing Techniques URL
https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-part10.pdf (accessed 112.02.2021)

respondents to act quicker than before, as in some cases, it takes one day from a credential leak to an attack.

Based on Europol research, cybercriminals are employing a more holistic strategy to phishing by showing a high level of competency concerning the use of tools, systems and vulnerabilities they exploit, assuming false identities and working in close cooperation with other cybercriminals.[7]

In the future, email is predicted to continue to be the number one mechanism for phishing, however not for long. Experts are seeing an increase in social media messaging, including WhatsApp and others, to carry out such attacks. According to ENISA, the most relevant change will be in the methods used to send the messages, which will become more sophisticated with the adoption of adversarial Artificial Intelligence (AI) to prepare and send the messages.

2.2.Social Engineering and Phishing

In the context of information security, social engineering is defined as the psychological manipulation of people into performing actions or divulging confidential information. Social engineering remains a top threat to facilitate other types of cybercrime, as 84% of cyber-attacks rely on social engineering (ENISA). The number of phishing victims continues to grow since it exploits the human dimension being the weakest link.

Targeting human weakness using social engineering have a high impact on society and enable the majority of cybercrimes, ranging from scams to the acquisition of sensitive information and advanced malware attacks. While cyber-criminals usually use social engineering to convince users to engage in fraudulent schemes unknowingly, they use phishing to obtain credentials and gain access to sensitive accounts/systems (EUROPOL).

Cyber-criminals have learned and became experts in social engineering, appealing to human nature to commit fraud. Their most common manipulation methods usually rely on fear, intimidation, sense of urgency, greed, curiosity, trusting nature and empathy. Cybercriminals know that carefully prepared and personalised email, voice message/call or text message can deceive people in providing sensitive information, transferring money or downloading the file that contains malware to the company's network.

To understand better the concept of social engineering, we could take a look at 6 principles of persuasion that Dr Robert B. Cialdini explained in his book "Influence: The Psychology of

[7] EUROPOL (2020): Internet Organised Crime Threat Assessment 2020

Funded by the Erasmus+ Programme of the European Union

Persuasion"[8]. While initially, these principles were used in marketing, they were easily adopted and used in social engineering and phishing as well[9]:

1) *Reciprocation* – "give and take". An email offering a discount or coupon on some purchases in exchange for sharing information or signing up for an account; an email promising to give access to confidential information if a specific attachment is downloaded, or a link are the classic examples.
2) *Scarcity* – it is in human nature to want what is difficult to get. Phishing emails that stress that a particular benefit is accessible only if action is taken within a short time. "The account will deactivate in 24 hours if you don't click on a link to get it resolved" is an example of this principle at play.
3) *Authority* – people tend to follow authority and credible experts in general. Therefore, many phishing emails seek to impersonate local leaders, CEOs, senior officers, human resource managers, etc. An email from the CEO (supposedly) asking the finance department to immediately wire some amount of money to an account unknown to the department is one example that has occurred many times.
4) *Consistency* – people are, in one way or another, creatures of habit. Phishing emails that look like official communications exploit this fact, hoping the recipient overlooks the unusual request that is included in such an email. An email with the Amazon logo saying a shipment is held up and asking the recipient to confirm their home address may not raise red flags even if no shipment is expected - that is the power of a widely recognised brand.
5) *Consensus* – people tend to follow other people, especially when they are not certain about something. A phishing email that mentions something like "544 of 800 employees have updated their software, click this link to download" is exploiting this tendency.
6) *Liking* – this is a quite simple principle – if people like you or conversely they want to be liked, they are most likely to say "yes". An email from the IT department (supposedly) asking a new employee for their personal details/ passwords to update the security system, is one example.
7) *Unity* – this principle was added later. The idea is that the more we identify ourselves with others, the more we are influenced by them. A phishing email supposedly sent by someone who shares the same interests as the recipient, information that can easily be sourced through social media, has a high chance of success. For example, if a person loves dogs, an email from another dog-lover (supposedly) with an attachment of cute dog pictures (supposedly) has a high chance of being opened.

[8] Dr Robert B. Cialdini is a Psychology and Marketing professor in the Arizona State University in USA
[9] NCC group (2020) :Psychology of the Phish: Leveraging the Seven Principles of Influence, URL: https://www.mynewsdesk.com/nccgroup/blog_posts/psychology-of-the-phish-leveraging-the-seven-principles-of-influence-95433 (accessed 12.02.2021)

Funded by the Erasmus+ Programme of the European Union

These techniques can lead to successful phishing attacks, using malicious links or malware as part of the attacks. Thus, it is crucial for people to recognise these principles and strategies to protect themselves, however, it is quite difficult as it is based on the essence of human beings – the way we think and behave.

2.3. Phishing during COVID-19

During the crisis and disasters, we tend to rely on computers, mobile devices, and the internet to work, connect with other people, find, share, and receive information, shop, etc.[10]

COVID-19 pandemic has highlighted our vulnerability and demonstrated the unfortunate impact potential of cybercrime on our daily lives across the globe. As physical lockdowns became the norm, and more people stayed and worked from home, cybercrime became more widespread than before.

Barracuda[11] researchers have observed an increase by 667% in phishing scams in only one month since the pandemic started back at the beginning of 2020.

There is evidence that cybercriminals are continuing to exploit the vulnerabilities to their advantage. Cybercriminals have adapted existing forms of cybercrime to fit the pandemic narrative, abused the uncertainty of the situation and the public's need for reliable information. Criminals have used the COVID-19 crisis to carry out social engineering attacks, namely phishing emails through spam campaigns and more targeted attempts such as business email compromise (BEC), for example[12]:

- Phishing campaigns and malware distribution through seemingly genuine websites or documents providing information or advice on COVID-19 are used to infect computers and extract user credentials.
- Offenders are obtaining access to the systems of companies or other organisations by targeting employees who are teleworking.

According to EUROPOL, the number of cyber-attacks is significant and expected to increase further. Cybercriminals will continue to innovate in deploying various malware and ransomware packages themed around the COVID-19 pandemic and vaccines in particular.

Cybercriminals are likely to seek to exploit an increasing number of attack techniques as many employers have and continue to adopt remote work and allow connections to their organisations' systems.[13]

[10] Council of Europe (2020): Cybercrime and COVID-19, URL https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19 (accessed 12.02.2021)
[11] Barracuda Networks is the worldwide leader in Security, Application Delivery and Data Protection Solutions
[12] Council of Europe (2020): Cybercrime and Covid, URL: https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19 (accessed 12.02.2021)
[13] EUROPOL (2020): Pandemic profiteering - how criminals exploit the COVID-19 crisis

3. SURVEYS FOR STUDENTS, EMPLOYEES AND CEOS

3.1. The methodology of data collection

As a part of the fieldwork, the CyberPhish project consortium partners[14] prepared and launched a survey addressed to students, business representatives and CEOs from Lithuania, Latvia, Estonia, Malta and Cyprus. Partners aimed to involve at least 70 participants (including 20 business representatives and 10 CEO's) in each partner country.

Based on the desk research and feedback from all the partners, an English version of the questionnaire was prepared, which was later localised and uploaded online in the English, Lithuanian and Latvian languages. The survey was launched in the mid December 2020 and finalised at the end of January 2021.

The main aims of the survey were:

- to identify people's awareness of phishing and different types of phishing;
- to determine how people recognise phishing attacks;
- to identify the skills gaps.

The questionnaire combined questions related to psychological and IT knowledge, critical thinking approach, as well as provided phishing examples for the respondents to evaluate their knowledge "in practice". Each phishing example was based on six principles of persuasion developed by Dr Robert B. Cialdini. Overall, the questionnaire was divided in several parts and gathered data relating to:

- Personal information - including gender, education level and employment status;
- General knowledge and behaviours in the area of phishing;
- Personal experience with phishing;
- Recognising phishing attacks – indicating main red flags;
- Practical phishing examples;
- Self-evaluation of critical thinking skills;
- Avoiding phishing attacks – why phishing attacks are successful, social engineering (human emotions exploited by attackers), actions to take;
- Self-evaluation of confidence in the use of skills needed to prevent phishing attacks.

The gathered data will be used to identify the skills gaps and prepare recommendations for a new curriculum to strengthen skills, education and awareness of internet users on the latest emerging cybersecurity issues and threats, in particular – phishing.

[14] CyberPhish project website: https://cyberphish.eu/

Funded by the Erasmus+ Programme of the European Union

Overall, based on the outcomes of this survey and a desktop study on the existing cybersecurity study curriculum, the partner consortium will develop training material, knowledge self-assessment and knowledge evaluations tests, and simulations scenarios for training.

3.2. Compilation of the results

The results of the questionnaire were transferred to the National Table of Findings (structured per country – Lithuania, Latvia, Estonia, Malta and Cyprus). In this table, partners included the most relevant results collected, delivering information about:

- characterisation of the target groups involved in the fieldwork;
- analysis of the results of the surveys, using graphics and text;
- main conclusions and suggestions made by the respondents;
- Findings and recommendations made by partners to support partners in the definition and development of other deliverables.

The tables provided an overview of respondents' knowledge and behaviour on the topic of cybersecurity, particularly phishing. These tables' results allowed the consortium to proceed with a comparison between countries, identifying the skills gaps and needs.

3.3. Results and analysis of surveys

3.3.1. Overview of the respondents

Despite the short period when the questionnaire was circulated, all the countries have reached the minimum number of 70 respondents. In total, 514 responses were collected from Cyprus, Estonia, Latvia, Lithuania, and Malta.

	Lithuania	Latvia	Estonia	Malta	Cyprus
Respondents per country	93	76	165	104	76

Table 1. Number of respondents per country

Out of 514 respondents – 259 were females, 248 were males, and 7 respondents preferred not to identify their gender. In all the partner countries, except Estonia, the number of female respondents was higher than male respondents.

	Lithuania	Latvia	Estonia	Malta	Cyprus
Female	63,4%	57,9 %	34,6%	54,8%	55,3%
Male	36,6%	40,8%	63%	45,2%	42,1%
Prefer not to say	-	1,3 %	2,4%	-	2,6%

Table 2. Respondents by genders

Funded by the Erasmus+ Programme of the European Union

The majority of respondents are students (59%), followed by employees (27%), business owners (10%), unemployed (2%) and self-employed (2%).

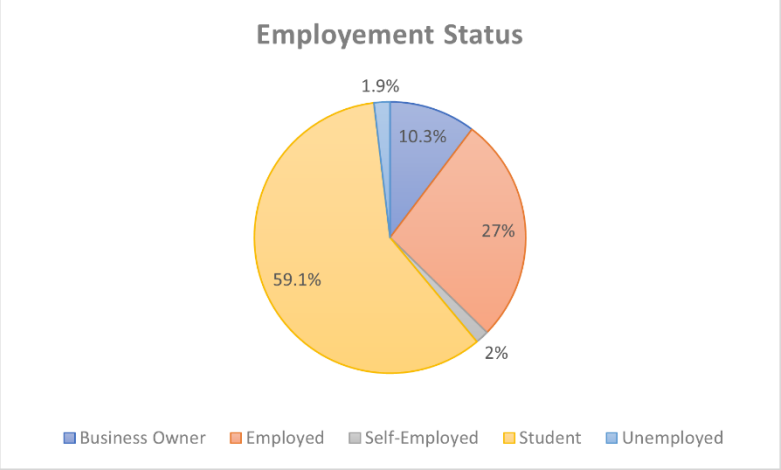


Figure 1. Survey respondents' employment status

The survey respondents are well educated – with the majority of respondents (38%) having a bachelor's degree, followed by a master's degree (23%) and PhD (6%).

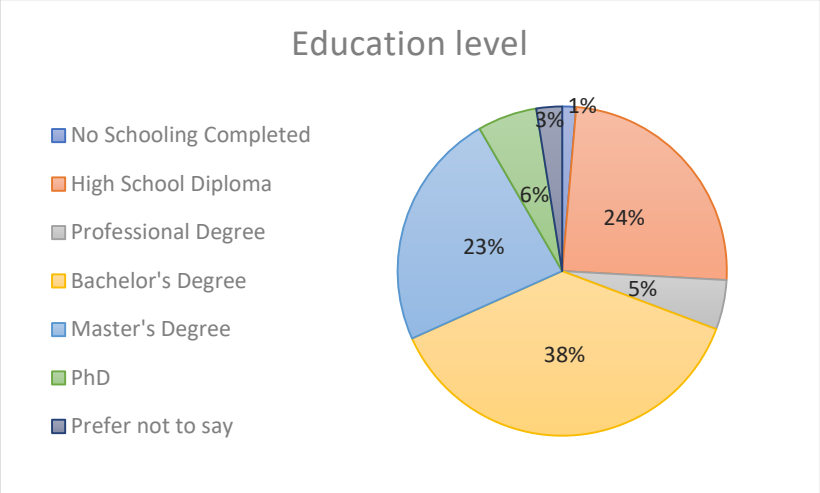


Figure 2. Survey respondents' education level

3.3.2. General knowledge and behaviours

Although the most respondents (74%) have indicated that they have never participated in any formal training/workshop/studies on cybersecurity or phishing specifically, more than a half of the respondents (56%) have researched this subject themselves. These results may indicate that cybersecurity and phishing topics are relevant in all the surveyed countries, and while respondents may not necessarily have the opportunity to study the topic in a formal setting, they are willing to spent time researching the topic to improve their knowledge and skills themselves.

61% of respondents answered that they have phishing knowledge, 27% are not sure, and 12% do not know what phishing is. When asked to choose the correct phishing definition, 72% of surveyed people

Funded by the Erasmus+ Programme of the European Union

have chosen it correctly. In Malta and Estonia, the number of respondents, who claim that they know what phishing is, is the same. In Lithuania, Cyprus and Latvia, more people have selected the correct answer than those who indicated they know what phishing is. These results may indicate that more respondents from these countries are aware of phishing, but they are not confident in their knowledge.

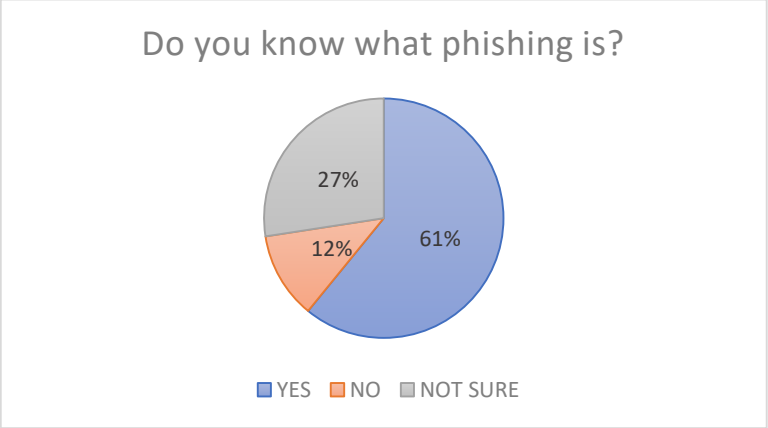


Figure 3. Survey respondents' awareness of phishing

Almost half of the respondents (46%) indicated that they are often afraid to open the link or attachment in the email, thinking it could be fake, while 13% are always afraid. Only 3% of respondents are never afraid to open links/attachments, and 8% are rarely afraid.

Almost one-third of respondents (32%) are often afraid to become targets of phishing attacks, and 19% are always scared. Only 5% of respondents indicated that they are never afraid to become a target of the phishing attack, while 17% are rarely afraid.

The results above show that most respondents are aware of the possibility of cyber-attacks and the main tools used by hackers (malicious links and attachments). Furthermore, even though 39% of respondents indicated that they do not know or are not sure what phishing is, still 51% of respondents are often or always afraid to become targets of phishing attacks. These results may mean that even those respondents who have indicated to know what phishing is, not necessarily have the necessary knowledge to protect themselves or confidence in their skills.

When asked about the different phishing types they know, the respondents in all the surveyed countries indicated that they are most aware of these phishing types: "Spray and Pray", "Cat phishing", and "Malvertising". The respondents in all the surveyed countries, except Lithuania, are also most aware of the "Advanced fee scam" phishing type.

Funded by the Erasmus+ Programme of the European Union

Figure 4. Types of phishing respondents are most aware of

On the other hand, the respondents are the least aware of these phishing types: "Whaling", "Clone phishing" and, except respondents from Cyprus, "Smishing"[15]. Respondents from Malta, Cyprus, Lithuania and Latvia are also the least aware of "Content injection", while respondents in Estonia indicated that they are mostly aware of this fishing type.

Figure 5. Types of phishing respondents are the least aware of

When asked what kind of consequences are most likely or definitely going to occur after the successful phishing attack on person or company, the majority of respondents from all the surveyed countries named these consequences – "theft of sensitive data", "credit card fraud", "theft of client information", "reputational damage" and "loss of usernames and passwords" (except Malta). The respondents from all the surveyed countries, except Cyprus[16], also tend to believe that after a successful phishing attack, their data are most likely will be sold to criminal third parties.

Figure 6. Consequences most likely to occur after the successful phishing attack according to respondents

On the other hand, respondents from all the surveyed countries believe that "loss of intellectual property" is unlikely to occur after a successful phishing attack. Lithuanian, Maltese, and Estonian respondents are also sceptical about the "theft of funds from business/client accounts" occurring after the phishing attack.

Considering the behavioural aspect, the respondents are most likely to click on the link or attachment in the email or message as well as provide sensitive information if it: "is sent by their boss or colleague", "is sent by the company which services they use", "is sent by the bank or any

[15] Except for the respondents in Cyprus
[16] Except for the respondents in Cyprus

Funded by the Erasmus+ Programme of the European Union

governmental institution". In Cyprus, respondents would also more likely do that if the email/message "asks them to clarify details such as their address for order shipment (e.g., amazon order)". At the same time, the opinions are mixed in Latvia and Malta, with an almost equal number of respondents that would be highly likely and the very unlikely do that. There are no mixed opinions among Estonia and Lithuania respondents, where most of them would very unlikely do that.

Figure 7. Types of emails respondents are most likely to click on the link or attachment in the email or message and/or provide sensitive information

The results are not so surprising if we would take a look at the six principles of persuasion described before. As previously mentioned, people tend to follow and trust more authority or experts. Thus, many hackers aim to impersonate either credible governmental institution/authority and banks or CEOs. This tendency was visible in the survey as well, where 34% of respondents claimed that they very often or always trust messages that appear to come from an important entity or look important, while 30% do that sometimes.

The "Liking principle" also plays an important role, meaning that people are much more likely to respond to request even if they sound unusual from their colleagues/bosses.

Furthermore, people are "creatures of habit" and tend to like consistency. Suppose the email is sent by the company they know and which services they use and probably have received emails or messages before. In that case, they will be more likely to open it, click on links/attachments, etc., than they would do with the company which services they do not use.

In all partner countries, the respondents are least likely to click on the link or attachment in the email or message and/or provide sensitive information if it: "offers them confidential information (e.g., information about competitors)", "asks them to fill in the survey/ provide your email or phone contacts in order to participate in the contest to win a prize" or "is sent by the company/organisation they know but don't use their services".

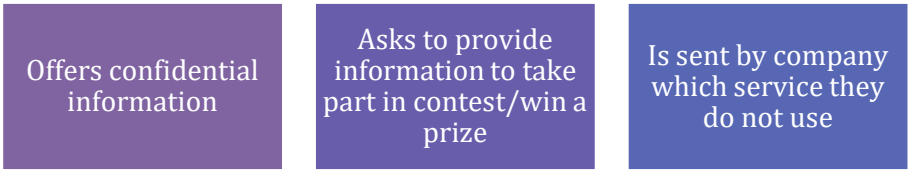


Figure 8. Types of emails respondents are least likely to click on the link or attachment in the email or message and/or provide sensitive information

The majority of respondents from Estonia, Cyprus and Malta, would also unlikely provide sensitive information if the email or message "asks them to help/ donate to local or international charities".

Funded by the Erasmus+ Programme of the European Union

Respondents from Cyprus would also more likely click on the link/attachment and provide sensitive information if it "will invite them to specific event online or offline (e.g., zoom meeting). Contrary, Lithuanian, Latvian, Estonian and Maltese respondents would rather unlikely do that.

3.3.3. Personal experience with phishing attacks

19,8% of respondents or almost every fifth respondent have been phished in the past. The most common way the respondents have been phished is by clicking the link in the email or message, followed by opening an attachment in the email, and answering the email or message and providing sensitive information. Surprisingly, only respondents in Estonia and Cyprus have indicated that they have been phished by entering their login details in the fake website. Among "other" answers, the most popular were "combination of several phishing techniques" and "providing information to fake survey".

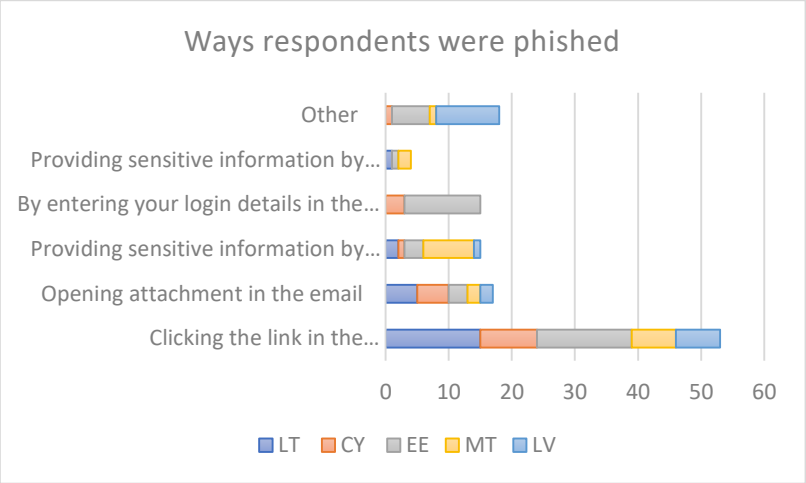


Figure 9. Ways survey respondents were phished in the past

When asked to indicate why they believe they have been phished, the majority of respondents indicated that they were distracted, curious or in a hurry.

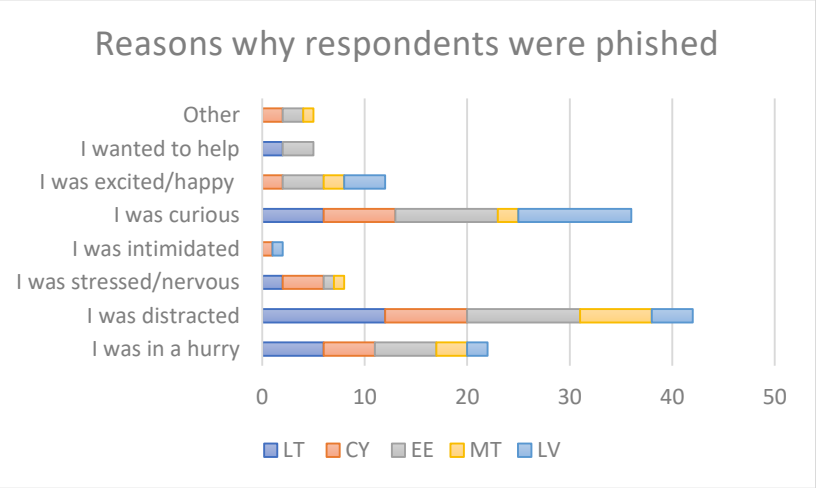


Figure 10. Reasons why respondents think they were phished

Funded by the Erasmus+ Programme of the European Union

3.3.4. Recognising phishing attacks

In the survey, respondents were asked to evaluate and indicate the most important criteria in recognising a suspicious email, text message or phone call, and social media message.

Email

When it comes to recognising suspicious emails, the respondents in all countries had a unified opinion about the most important criteria to consider. The main criteria indicated are as follows: 1) The sender's domain (email) does not look genuine (does not match the organisation, contain a concealed spelling mistake, extra numbers, letters in it, etc.); 2) The embedded links in the email is not the same as a genuine hyperlink; 3) The sender is asking to confirm/ provide sensitive information (login credentials, bank details) via email; 4) There are visible inconsistencies in email addresses, links & domain names; 5) The email contains an unexpected/unusual attachment.

The least important criteria indicated by respondents were 1) Generic greeting in the email; 2) There is no signature or contact information; 3) The email message creates curiosity, need to find out more; 4) The email message is too good to be true. Respondents from Malta also chose the style of writing and spelling and grammar mistakes as least important, too.

Text message or phone call

The almost unified opinion was also seen between the respondents in all surveyed countries when it came to identifying the most important criteria in recognising a suspicious text message or phone call, too. The respondents from all the countries agreed on these most important "red flags" – 1) Sender/Caller asks to verify details or provide sensitive information or send money; 2) Number with the different country code; and 3) Caller does not introduce himself/herself properly (name, position, company). Respondents from all surveyed countries, except Estonia, also agreed the unusually long number is one of the most important "red flags". Furthermore, all survey respondents, except the ones from Cyprus, also indicated that message containing a warning (e.g., expiring account) and putting pressure on the receiver to make an urgent decision is also one of the most important major red flags.

The less important criterion indicated by respondents in Malta, Estonia, Lithuania, and Cyprus was spelling and grammar mistakes. On the contrary, Latvian respondents chose spelling and grammar mistakes as one of the most important criteria. The respondents from surveyed countries also answered that it is not so important if the caller does not refer to them by name and surname, except respondents from Cyprus, who thought it would be one of the most important criteria in recognising a suspicious call.

Funded by the Erasmus+ Programme of the European Union

A message in social media channels

Respondents had an almost unified opinion when it comes to identifying suspicious messages in social media as well. The majority of respondents agreed on these most important criteria: 1) The message asks for money; 2) The message asks to verify details or provide sensitive information; 3) Message contains a doubtful link and 4) The social media profile of the sender looks suspicious (e.g., new account, no friends, etc.). Respondents, except the ones from Malta, also believe that the message asking you to install some programme is one of the major red flags indicating suspicious activity.

The spelling and grammar mistakes, not having any business relations with the sender or not knowing the sender were identified as the respondents' least important criteria.

RECOGNISING PHISHING ATTACK	MOST IMPORTANT CRITERIA	LEAST IMPORTANT CRITERIA
EMAIL	• The sender's domain (email) does not look genuine; • The embedded links in the email are not the same as a real hyperlink; • The sender is asking to confirm/ provide sensitive information; • There are visible inconsistencies in email addresses, links & domain names; • There is an unexpected/ unusual attachment.	• Generic greeting; • No signature or contact information; • The email itself creates curiosity, need to find out more.
TEXT MESSAGE OR PHONE CALL	• Sender/Caller asks to verify details or provide sensitive information or send money; • Number with the different country code; • The caller does not introduce himself/herself properly (name, position, company); • Unusual long number;[17] • The message contains a warning.[18]	• Spelling and grammar mistakes;[19] • The caller does not refer to you by name, surname.[20]
MESSAGE IN SOCIAL MEDIA	• The message asks for money; • The message asks to verity details or provide sensitive information; • The message contains a doubtful link; • The social media profile of the sender looks suspicious (e.g., new account, no friends, etc.); • The message asks you to install some programme[21]	• Spelling and grammar mistakes; • Not having any business relations with the sender; • Unknown sender.

Table 3. The most and the least important criteria in recognising phishing attacks

[17] Except for the respondents in Estonia
[18] Except for the respondents in Cyprus
[19] Except for the respondents in Latvia
[20] Except for the respondents in Cyprus
[21] Except for the respondents in Malta

Funded by the Erasmus+ Programme of the European Union

In general, when it comes to indicating the main criteria, respondents are mainly focused on "technical criteria", e.g., links, domains, attachments, country code, etc., rather than on human emotions (social engineering) when identifying suspicious emails or messages. Spelling or grammar mistakes or generic greeting are among the last points to be evaluated by the respondents.

However, it is important to note that while "technical criteria" are among the first points to get noticed and inspected by respondents, they do not mean that they do not consider social engineering when evaluating the emails and messages. When asked to identify the phishing emails/messages and the main "red flags" in the survey, the majority of respondents from all the surveyed countries chose both "technical criteria" and criteria focused on human emotions (social engineering).

3.3.5. Critical thinking skills

The majority of respondents are quite optimistic about their critical thinking skills. More than half of the respondents (57%) stated that they very often or always have sufficient focus and attention to detail when opening an email or message. In comparison, 12% stated that they have never or rarely have enough focus.

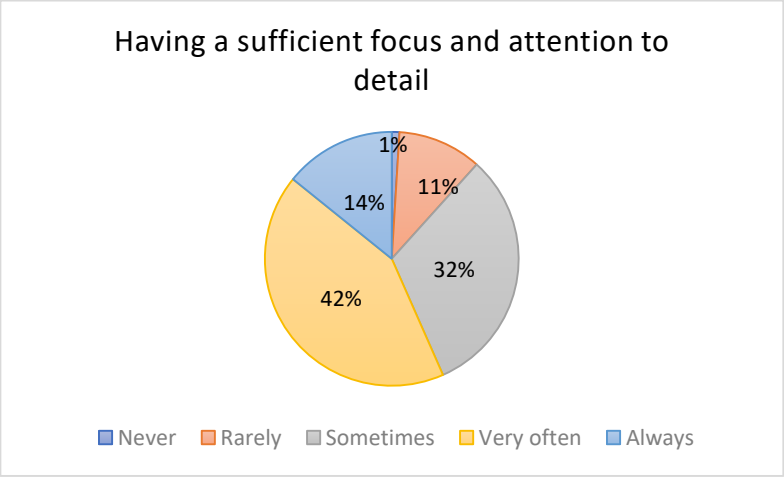


Figure 11. Respondents' focus and attention to details when opening a message/email

71% of respondents claim that they often are mindful when clicking on the link or attachment, while 11% claimed that they never or rarely are mindful when doing that.

Funded by the Erasmus+ Programme of the European Union

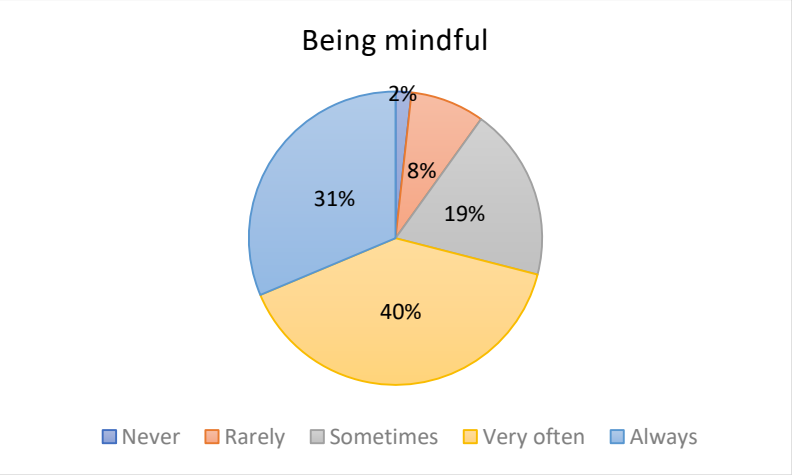


Figure 12. Respondents being mindful when clicking on the link/attachment

67% of respondents stated that they very often or always can visualise possible implications/consequences of their decisions, based on evidence when receiving a suspicious-looking email or message, while only 5% of respondents stated that they could never or rarely visualise it.

77% of respondents also very often or always are able to draw conclusions, based on evidence, when receiving a suspicious-looking email or message, while only 3% of respondents can never or rarely do it.

The difference between the percentage of respondents who can visualise the consequences and are able to draw conclusions may indicate. In contrast, not all respondents are aware of the consequences of being phished. They are still able to draw conclusions and recognise phishing email/message.

However, it is important to emphasise that despite the quite good results, around one-third of respondents yet are only sometimes able to visualise consequences and draw conclusions.

3.3.6. Avoiding phishing attacks

Survey respondents were also asked to indicate the main reasons that, in their opinion, contribute to successful phishing attacks. Respondents from all the surveyed countries have chosen 5 main reasons: 1) People are not aware/ have no knowledge on such attacks and how to prevent them; 2) Attackers exploit human nature, they rely on interaction and playing human emotions and needs; 3) Attackers are really good at replication of messages and emails from legit companies, making them very believable and convincing; 4) People are not paying enough attention/are ignorant[22]; 5) Attackers are becoming more advanced, targeting specific individuals while using emails are highly personalised and use specific information[23].

[22] Except the respondents in Malta
[23] Except the respondents in Cyprus

Funded by the Erasmus+ Programme of the European Union

Figure 13. Main reasons why phishing attacks are successful according to respondents

The respondents' least chosen reasons were: 1) People are using outdated software; 2) Phishing tools are low-cost and widespread; and 3) Malware itself is becoming more sophisticated[24].
The respondents agreed that hackers usually exploit human emotions, needs and desires, specifically through enhancing their motivation by offering "gifts" or free vouchers, raising their curiosity, and causing concern/anxiety.

The majority of respondents believe that to avoid phishing attacks, it is crucial to approach this matter from different perspectives: 1) technical factor - by using web filter to block malicious websites, multifactor authentication/changing passwords frequently as well as double-checking all-important details (senders email, links, attachments, etc.), and 2) human factor – by keeping sensitive information about oneself out of social media, being cautions when opening the emails/messages/answering the phone and continuously educating oneself in this area.'

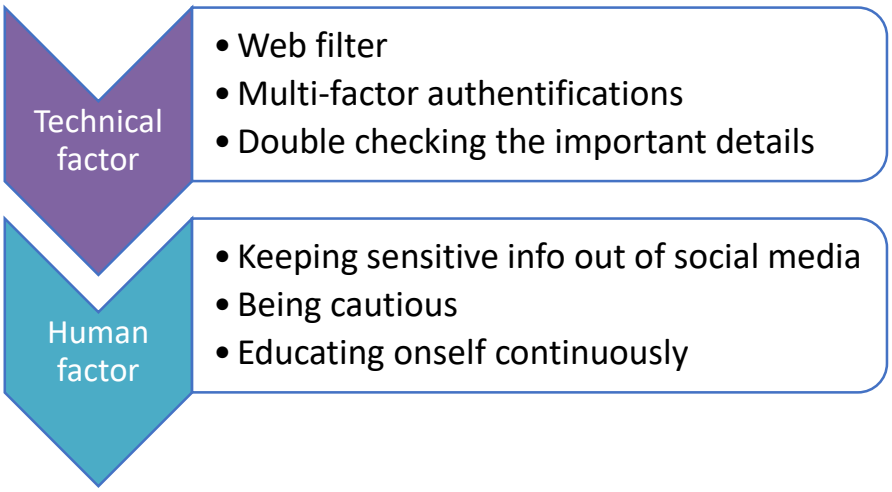


Figure 14. Actions to take to prevent phishing attacks according to respondents

The least important actions that should be taken to avoid phishing attacks according to the respondents are using an up-to-date browser, keeping up with the newest software & tools available

[24] Except the respondents in Malta

Funded by the Erasmus+ Programme of the European Union

or using an up-to-date operational system[25] as well as having regular cybersecurity trainings/workshops

The areas majority respondents feel the most confident are as follows: being able to find the relevant & trustworthy information online, identify phishing attacks and use the security software, multifactor authentication as well as a web filter.

Fewer respondents feel confident with their knowledge of cybersecurity/phishing terminology and using it and as being able to encrypt all sensitive company information.

Figure 15. Areas respondents feel most confident in

[25] Except respondents in Estonia

Funded by the Erasmus+ Programme of the European Union

4. SUMMARY AND MAIN FINDINGS

Socio-demographics of respondents

- 514 people took part in the survey, out of which 259 are women, 248 men and seven people prefer not to identify their gender.
- The majority of respondents are students (304), followed by employees (139), business owners (53), unemployed people (10) and self-employed people (8).
- The majority of survey respondents are highly educated – with the majority of respondents (38%) having a bachelor's degree, followed by a master's degree (23%) and PhD (6%).

General knowledge and behaviours

- Although 74% of respondents have never participated in any training/workshop or studies in cybersecurity in a formal setting, more than half of the respondents (54%) have researched this topic themselves (read an article, watched videos, etc.). These results indicates that while respondents may not necessarily always have an opportunity to study a topic in a formal setting, they are motivated to improve their knowledge and skills independently.
- 61% of respondents claimed to know what phishing is, while 27% were not sure, and 12% did not know. When asked to choose the correct phishing definition, more respondents from Lithuania, Latvia and Cyprus chose the correct answer than the number of people who indicated to know what phishing is. These findings may indicate that more respondents from these countries are aware of phishing, however, they may not have sufficient knowledge or confidence.
- 59% of surveyed people are very often or always afraid to open the link or attachment, thinking it could be malicious. In comparison, while 51% are very often or always afraid to become a target of phishing attacks. The questionnaire results mentioned shows that even the respondents who claimed to know what phishing is are afraid of being phished, indicating insufficient knowledge or lack of confidence in one's skills.
- Respondents are mostly aware of "Spray and pray", "Cat phishing", and "Malvertising" phishing types. Contrary they have less knowledge about "Whaling", "Clone phishing" and "Smishing" phishing attacks.

Funded by the Erasmus+ Programme of the European Union

- Respondents believe that after a successful phishing attack these consequences are most likely to occur – theft of one's sensitive data or client information, credit card fraud and reputational damage. The majority of respondents, except the Maltese ones, also believe successful phishing attacks may lose one's usernames and passwords. Furthermore, data sold to third criminal parties was also named most likely by respondents from all survey countries except Cyprus. Contrary, respondents believe that the loss of one's intellectual property is less likely to occur after successful phishing attack.

- Lithuanian, Maltese, and Estonian respondents are also sceptical about the "theft of funds from business/client accounts" occurring after the phishing attack.

- Respondents are more likely to click on the link or attachment in the email or message if it is sent by a boss or colleague, the company which services they use or bank or governmental institution. It seems that "authority", and "liking" principles of persuasion are the ones that respondents would most likely respond to.

- Respondents are less likely to click on the link or attachment in the email or message if it offers confidential information, asks to provide information to take part in the contest to win a prize or is sent by the company which service they do not use. It seems that the "reciprocation" principle of persuasion is the one that respondents would less likely to respond to.

Respondents' experience with phishing

- Almost every 5th respondent has been phished in the past. The main ways respondents were phished were by clicking on the link or providing sensitive information by email or message. Only respondents in Cyprus and Estonia indicated that they had been phished by entering their details into a fake website.

- The main reasons they have been phished are that they indicated that they were distracted, curious, or in a hurry. Some of the respondents also mentioned that they did not know of what phishing is.

Funded by the Erasmus+ Programme of the European Union

Recognising phishing attacks

- When it comes to the main criteria used to indicate the phishing attack, respondents were in general more focused on "technical criteria" such as sender's domain, embedded links, attachments and visible inconsistencies between them as well as unusually long number or different country code. Respondents also indicated that sender/caller asking for sensitive information or money is one of the major criterion. Spelling or grammar mistakes and generic greeting in most cases are the last points to be evaluated by the respondents.

- However, while "technical criteria" are first to get noticed and inspected by respondents, they do take "human criteria" (social engineering) into consideration when evaluating the emails and messages as well. When asked to identify the phishing emails/messages and the main "red flags" in the survey, the majority of respondents from all the surveyed countries chose both "technical criteria" and criteria focused on human emotions (social engineering).

Critical thinking skills

- The majority of respondents are quite positive about their critical thinking skills. 57% of respondents stated that they very often or always have sufficient focus when opening emails or messages. In comparison, 71% claimed to very often or always be mindful when clicking on the link or attachment.

- 67% of respondents said that they are very often or always able to visualise possible consequences on their actions when receiving suspicious email or message. In comparison, 77% of respondents are very often or always able to draw conclusions. The difference between the percentage of respondents who can visualise the consequences and are able to draw conclusions may indicate while not all the respondents are aware of the consequences of being phished, they are still able to draw conclusions and recognise the phishing email/message.

- However, it is important to emphasise that despite the quite good results, around one -third of respondents, yet are only sometimes able to visualise consequences and draw conclusions.

Funded by the Erasmus+ Programme of the European Union

Avoiding phishing attacks

- The respondents chose these main reasons that, in their opinion, lead to successful phishing attacks – people are not aware of phishing and how to prevent it, attackers exploit human nature. They are also good at replicating emails and messages from legit companies and people are not paying enough attention or are ignorant. Fewer respondents believe that people using outdated software, phishing tools being low-cost or widespread, and malware becoming more sophisticated are the main reasons behind phishing attacks.
- The respondents believe that hackers mainly exploit human's curiosity, concern or anxiety, and use incentives such as "free gifts" or "vouchers".
- To avoid phishing attacks, respondents believe that it is important to approach it from 2 different perspectives, such as "technical factor" and "human factor" using the appropriate tools and strategies to cover both. For example, the "technical factor" involves using a web filter, a multifactor authentication and checking important details such as the sender's email, links and attachments, etc. The "human factor" consists in keeping sensitive information out of social media, being cautions and educating oneself continuously.
- Interestingly, while most respondents believe that it is important to educate oneself in this area continuously, fewer respondents believe that regular cybersecurity training or workshops are needed. This, however, corresponds to data that almost half of the respondents do study this topic on their own.
- In general, respondents emphasise on human ability to evaluate and identify phishing attacks instead of counting on computer operational system, software and available tools.
- The areas majority respondents feel the most confident in are being able to find the relevant & trustworthy information online, identify phishing attacks and use the security software, multifactor authentication as well as web filter.
- Fewer respondents feel confident with their knowledge of cybersecurity/phishing terminology and using it as well as being able to encrypt all sensitive company information.

Funded by the Erasmus+ Programme of the European Union

5. BIBLIOGRAPHY

1. EU Commission (2020): Special Eurobarometer 499: Europeans' attitudes towards cyber security, URL https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG
2. European Union Agency for Cybersecurity (2020): ENISA threat landscape 2019-2020
3. EUROSTAT (2020): Is internet use safer today?, URL https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_pb/default/table?lang=en (accessed 11.02.2021)
4. Proofpoint (2019): Human Factor Report 2019, URL https://www.proofpoint.com/us/resources/threat-reports/human-factor (accessed 12.02.2021)
5. European Union Agency for Cybersecurity (2020): Phishing - ENISA threat landscape 2019-2020
6. Deloitte (2019): Understanding Phishing Techniques, URL https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-part10.pdf (accessed 112.02.2021)
7. EUROPOL (2020): Internet Organised Crime Threat Assessment 2020
8. NCC group (2020) :Psychology of the Phish: Leveraging the Seven Principles of Influence, URL: https://www.mynewsdesk.com/nccgroup/blog_posts/psychology-of-the-phish-leveraging-the-seven-principles-of-influence-95433 (accessed 12.02.2021)
9. Council of Europe (2020): Cybercrime and Covid, URL: https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19 (accessed 12.02.2021)
10. EUROPOL (2020): Pandemic profiteering - how criminals exploit the COVID-19 crisis

Funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

ANNEX 1. Survey "Evaluation of skills and recognition of phishing attacks"

SECTION 1: Personal data

1. **Name:**..... *(optional)*

2. **Email address:**..... *(optional - If you would like to receive the updates about the project and participate in the pilot testing of the training programme please submit your email.)*

3. **Gender**

- Male
- Female
- Prefer not to say

4. **Education Level**

- No Schooling Completed
- High School Diploma
- Professional Degree (Technical/ Vocational Training)
- Bachelor's Degree
- Master's Degree
- Doctoral degree
- Prefer not to say
- Other:.....

5. **Employment Status**

- Business Owner
- Employed
- Self Employed
- Student
- Retired
- Unemployed
- Other:.....

SECTION 2: General knowledge & behaviours

6. **How likely are you to click on the link or attachment in the email or message and/or provide sensitive information if it:**

Funded by the Erasmus+ Programme of the European Union

	Very unlikely	Unlikely	Neutral	Likely	Very likely
Offers voucher or discounts on some purchases					
Offers you access to some exclusive offers					
Invites you to specific event online or offline (e.g., zoom meeting)					
Asks you to fill in the survey/ provide your email or phone contacts in order to participate in the contest to win a prize					
Offers you confidential information (e.g., information about your competitors)					
Asks you to clarify your personal and/or account details for it not be closed/deactivated (e.g., bank account, Netflix account, Facebook account, etc.)					
Ask you to clarify your details such as your address for your order shipment (e.g., Amazon deliver)					
Updates you on the newest developments regarding important social issues and natural disasters (e.g., updates on COVID-19 situation)					
Asks you to help/ donate to local or international charities'					
Includes information about your hobbies					
Is sent by the bank or any governmental institution					
Is sent by your boss or colleague					
Is sent by the company which services you use					
Is sent by the company/organisation you know but don't use their services					

7. **Have you ever participated in any formal training/workshop/studies on cybersecurity or phishing specifically?**

- Yes
- No

Funded by the Erasmus+ Programme of the European Union

8. **Have you researched/ studied cybersecurity or phishing specifically by yourself? (read an article, watched videos, etc.)**

- Yes
- No

9. **Do you know what phishing is?**

- Yes
- No
- Not sure

10. **Which of these examples do you think fits the phishing definition?**

- A cybercrime in which a target is contacted by email to lure an individual into providing sensitive data about his accounts
- It is a kind of sport for pleasure or competition
- Unwanted and/or repeated emails by an individual or company offering products or services
- A cybercrime in which a target is contacted by email, telephone or text message to lure an individual into providing sensitive data.

11. **Are you aware of these types of phishing?'**

1) Spray and pray – malicious emails that are sent to any and all email addresses in attempt to attempt to steal sensitive information;
2) Advanced fee scam – common fraud associated with nationals from Nigeria, e.g. asking for assistance in moving large amount of money;
3) Cat phishing – luring someone in relationship by adopting a fictional online persona;
4) Spear fishing - malicious emails that are specially crafted and sent to specific individual or organisation in attempt to steal sensitive information
5) Whaling - an attempt to steal sensitive information and is often targeted at senior management;
6) Vishing - refers to phishing scams that take place over the phone;
7) Smishing - refer to phishing by using SMS messages as opposed to emails to target individuals;
8) Clone Phishing - type of phishing where a legitimate and previously delivered email is used to create an identical email with malicious content.
9) Content Injection - cybercriminals hack a familiar website and include a fake website login page or pop-up that directs website visitors to a fake website.
10) Malvertising - This phishing type uses online advertisements or pop-ups to compel people to click a valid-looking link that then installs malware on their computer.

	Not at all aware	Slightly aware	Moderately aware	Very aware	Extremely aware
Spray and pray					
Advanced fee scam					
Cat phishing					
Spear phishing					
Whaling					
Whishing					
Smishing					
Clone phishing					
Content Injection					
Malvertising					

Funded by the Erasmus+ Programme of the European Union

12. What kind of consequences are likely to occur after a successful phishing attack on a person or company?

	Definitely not	Probably not	Probably	Very probably	Definitely
Identity theft					
Credit card fraud					
Theft of sensitive data					
Loss of usernames and passwords					
Installation of malware and ransomware					
Loss of intellectual property					
Theft of client information					
Theft of funds from business and client accounts					
Access to systems to launch future attacks					
Data sold on to criminal third parties					
Reputational damage					

SECTION 3- Personal experience

13. Have you ever feared to open a link in an email or message, thinking that it could be fake?

1 – Never
2 – Rarely
3 – Sometimes
4 – Often
5 – Always

14. Are you, in general, afraid of becoming a target of a phishing attack?

1 – Never
2 – Rarely
3 – Sometimes
4 – Often
5 – Always

15. Have you ever been phished?

Description: By phished we mean - clicked on the malicious link/ attachment/ provided sensitive data, etc.

- Yes
- No

Funded by the Erasmus+ Programme of the European Union

SECTION 4 - Phishing attack (only for those who answered 'yes' in question 15)

16. How have you been phished?

- By clicking the link in the email or message
- By answering the email or message and providing sensitive information (e.g., login details)
- By opening attachment in the email
- By providing sensitive information by phone
- Other.....

17. Why do you think it happened?

- I was in a hurry
- I was distracted/not paying attention
- I was stressed/nervous
- I was intimidated
- I was curious
- I was excited/happy (e.g., thought I won the prize)
- I wanted to help
- Other.....

SECTION 5 - Recognising phishing attack

19. How important are these criteria in recognising a suspicious email?

	Not important	Slightly important	Moderately important	Important	Very important
Generic greeting in the email (e.g., Dear customer)					
The sender is asking you to confirm/ provide sensitive information (login credentials, bank details) via email or phone					
The sender's domain (email) does not look genuine (does not match the organisation, contain a concealed spelling mistake, extra numbers, letters in it, and etc.)					
The embedded links in the email is not the same as real hyperlink					
There are visible inconsistencies in email addresses, links & domain names					
The email contains an unexpected/unusual attachment					
There are spelling and grammar mistakes in the email					

Funded by the Erasmus+ Programme of the European Union

The style of the writing in the email does not match a person/company that usually sends you such emails					
There is no signature or contact information					
The email message creates a sense of urgency, demands immediate action, and makes you panic and feel stressed					
The email message creates curiosity, need to find out more					
The email message is too good to be true					

20. How important are these criteria in recognising a suspicious text message/phone call?

	Not important	Slightly important	Moderately important	Important	Very important
Unusually long number					
Number with the different country code					
Sender/Caller asks you to verify details or provide sensitive information or send money					
Caller does not introduce himself/herself properly (name, position, company)					
Caller does not refer to you by name, surname					
Text message contains a link					
You are not client of the sender/caller (company)					
You do not have any relationship or business relations with the sender/caller					
Message contains another phone number to call					
Spelling/grammar mistakes					
Message itself contains a warning (e.g. expiring account) and puts pressure on receiver to make an urgent decision					

Funded by the Erasmus+ Programme of the European Union

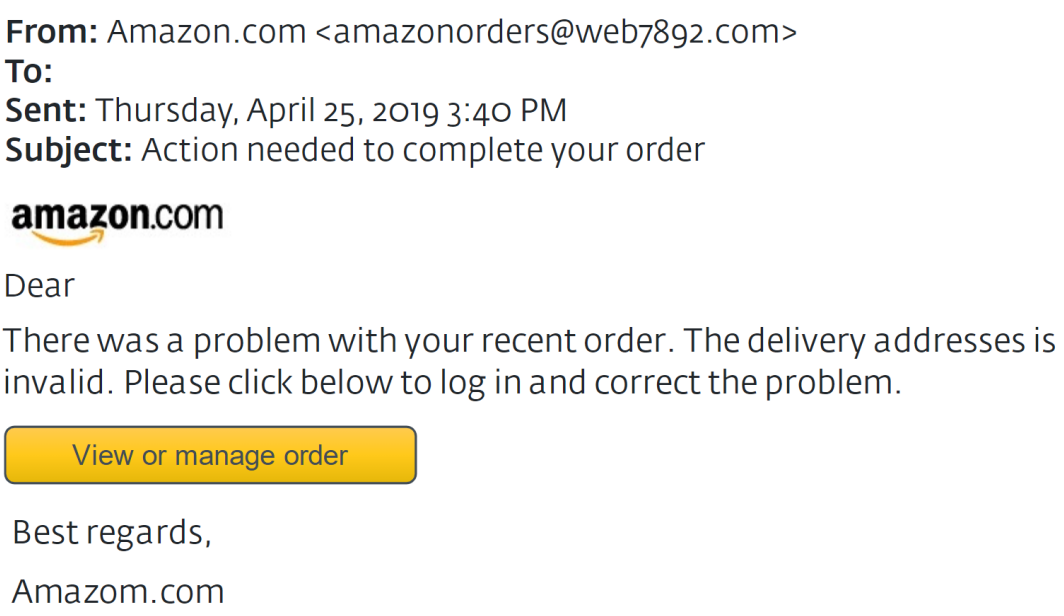
21. How important are these criteria in recognising a suspicious message in Social Media channels?

	Not important	Slightly important	Moderately important	Important	Very important
The message asks you to verity details or provide sensitive information					
The message asks you for money					
The message asks you to install some programme					
Message contains a doubtful link					
You do not know the sender					
You do not have any business relations with the sender					
The social media profile of the sender looks suspicious (e.g. new account, no friends, etc.)					
Message contains attention-grabbing title (e.g. You won't believe this video!)					
The message style does not match the sender (too formal/informal, etc.)					
Spelling/grammar mistakes					

Funded by the Erasmus+ Programme of the European Union

SECTION 6 – Phishing examples

Phishing Example 1



From: Amazon.com <amazonorders@web7892.com>
To:
Sent: Thursday, April 25, 2019 3:40 PM
Subject: Action needed to complete your order

amazon.com

Dear

There was a problem with your recent order. The delivery addresses is invalid. Please click below to log in and correct the problem.

View or manage order

Best regards,

Amazom.com

22. Is the image above a real email or phishing email?

- Real Email
- Phishing Email

SECTION 7

Example 1 (only if answered 'Phishing Email' in previous question)

23. Why have you decided that this is a phishing email? Choose the "red flags"

- Generic greeting
- Request for confirmation/verification/details of sensitive information
- The sender's domain/email
- Suspicious links
- Inconsistencies in email addresses, links & domain names
- Spelling and grammar mistakes
- Suspicious style of writing
- Sense of urgency/need for immediate actions
- Too good to be true

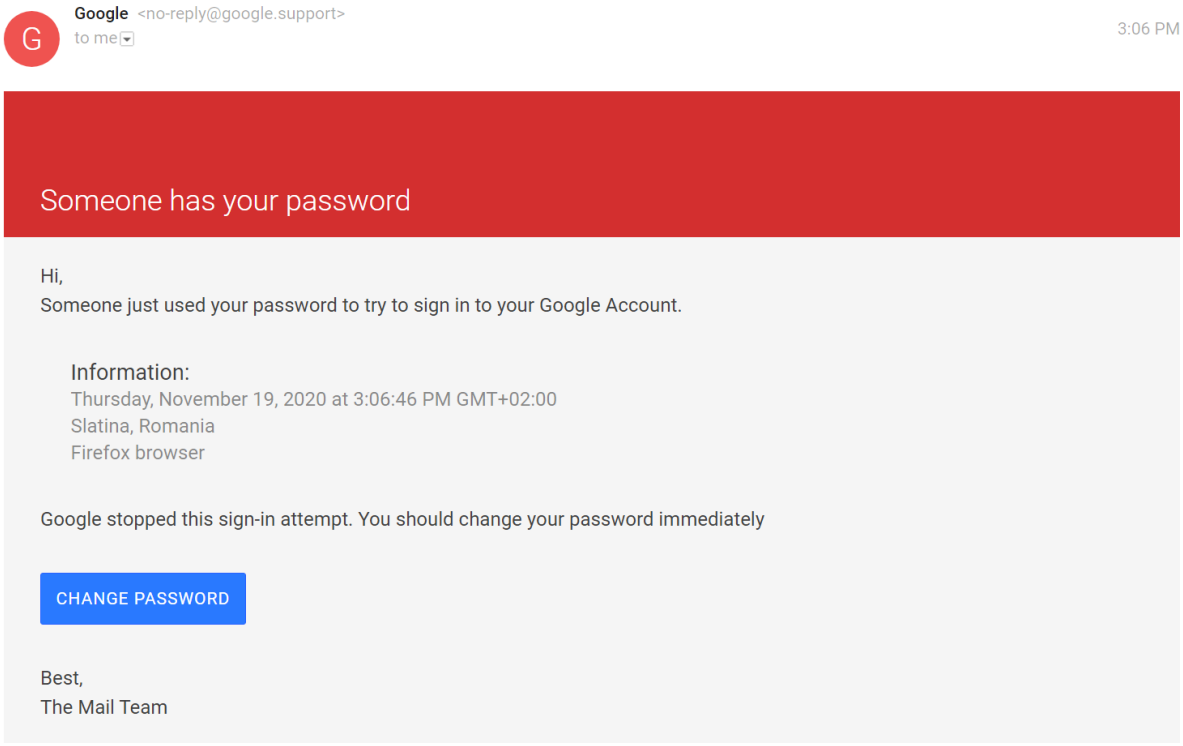
Other.....

Funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

SECTION 8

Phishing Example 2



24. Is the image above a real email or phishing email?

- Real email
- Phishing email

SECTION 9

Example 2 (only if answered 'Phishing Email' in previous question)

25. Why have you decided that this is a phishing email? Choose the "red flags"

- Generic greeting
- Request for confirmation/verification/details of sensitive information
- The sender's domain/email
- Suspicious links
- Inconsistencies in email addresses, links & domain names
- Spelling and grammar mistakes
- Suspicious style of writing
- Sense of urgency/need for immediate actions
- Too good to be true

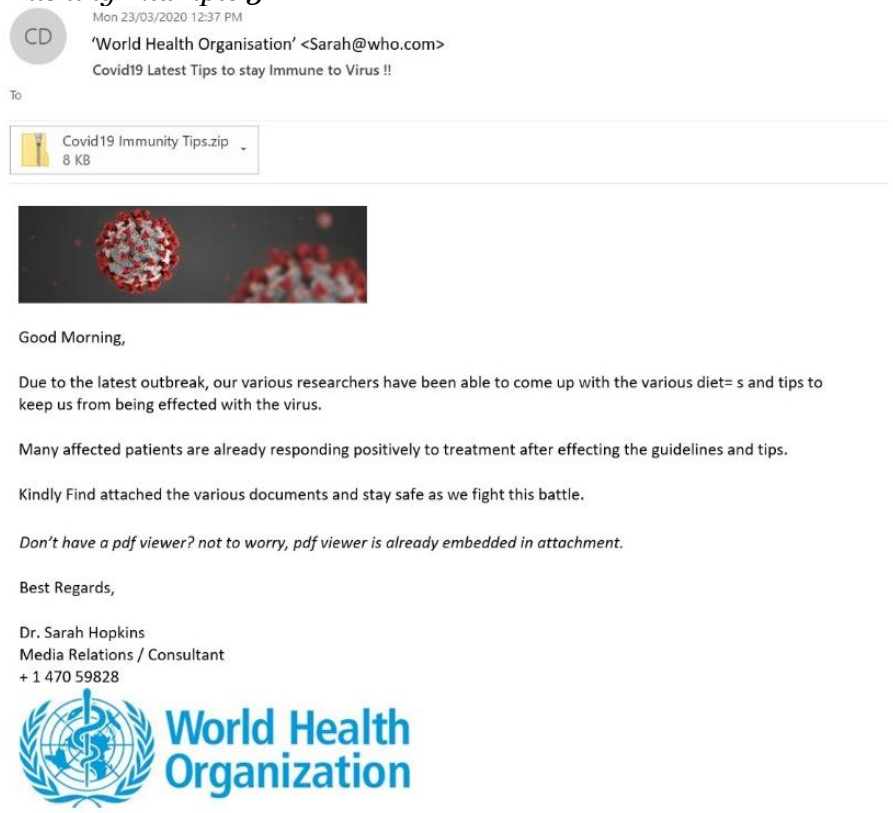
Other.....

Funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

SECTION 10

Phishing Example 3



CD

Mon 23/03/2020 12:37 PM

'World Health Organisation' <Sarah@who.com>

Covid19 Latest Tips to stay Immune to Virus !!

To

Covid19 Immunity Tips.zip
8 KB

Good Morning,

Due to the latest outbreak, our various researchers have been able to come up with the various diet= s and tips to keep us from being effected with the virus.

Many affected patients are already responding positively to treatment after effecting the guidelines and tips.

Kindly Find attached the various documents and stay safe as we fight this battle.

Don't have a pdf viewer? not to worry, pdf viewer is already embedded in attachment.

Best Regards,

Dr. Sarah Hopkins
Media Relations / Consultant
+ 1 470 59828

World Health Organization

26. Is the image above a real email or phishing email?

- Real email
- Phishing email

SECTION 11

Example 3 (only if answered 'Phishing Email' in previous question)

27. Why have you decided that this is a phishing email? Choose the "red flags"

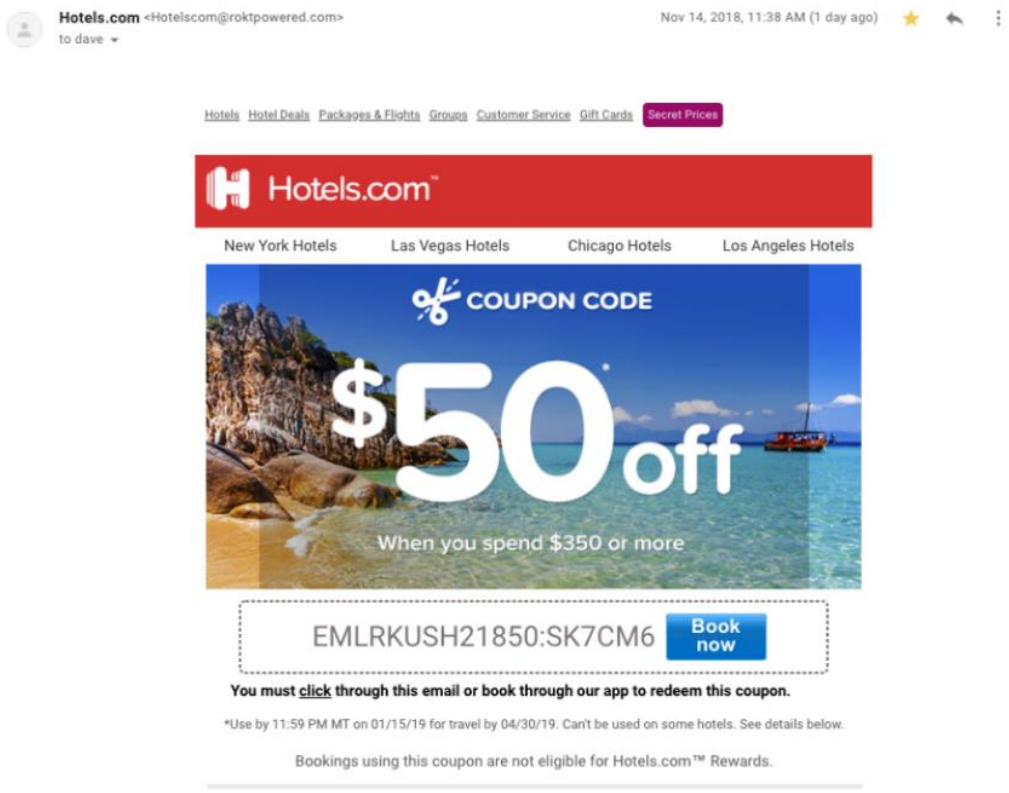
- Generic greeting
- Request for confirmation/verification/details of sensitive information
- The sender's domain/email
- Suspicious links
- Inconsistencies in email addresses, links & domain names
- Spelling and grammar mistakes
- Suspicious style of writing
- Sense of urgency/need for immediate actions
- Too good to be true

Other.....

Funded by the Erasmus+ Programme of the European Union

SECTION 12

Phishing Example 4



28. Is the image above a real email or phishing email?

- Real email
- Phishing email

SECTION 13

Example 4 (only if answered 'Phishing Email' in previous question)

29. Why have you decided that this is a phishing email? Choose the "red flags"

- Generic greeting
- Request for confirmation/verification/details of sensitive information
- The sender's domain/email
- Suspicious links
- Inconsistencies in email addresses, links & domain names
- Spelling and grammar mistakes
- Suspicious style of writing
- Sense of urgency/need for immediate actions
- Too good to be true

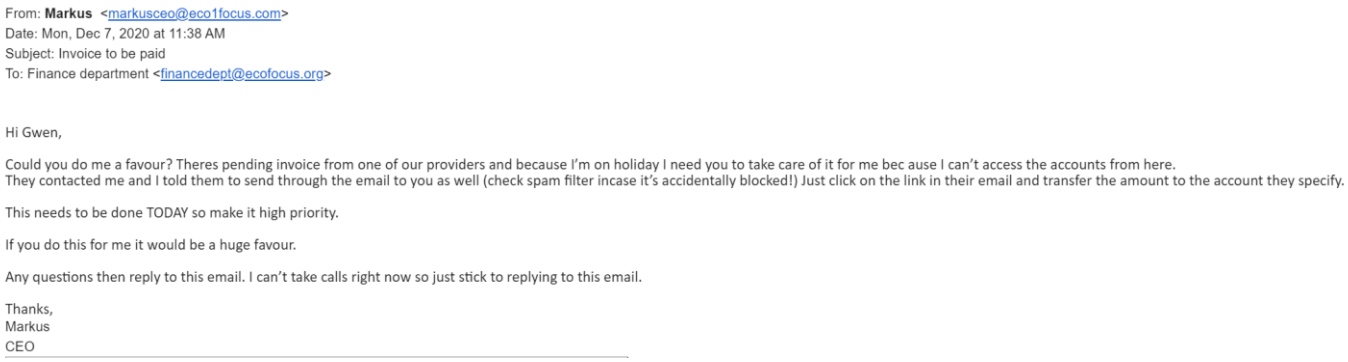
Other .....

Funded by the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. (Project Nº.: 2020-1-LT01-KA203-078070)

SECTION 14

Phishing Example 5



From: **Markus** <markusceo@eco1focus.com>
Date: Mon, Dec 7, 2020 at 11:38 AM
Subject: Invoice to be paid
To: Finance department <financedept@ecofocus.org>

Hi Gwen,

Could you do me a favour? Theres pending invoice from one of our providers and because I'm on holiday I need you to take care of it for me bec ause I can't access the accounts from here.
They contacted me and I told them to send through the email to you as well (check spam filter incase it's accidentally blocked!) Just click on the link in their email and transfer the amount to the account they specify.

This needs to be done TODAY so make it high priority.

If you do this for me it would be a huge favour.

Any questions then reply to this email. I can't take calls right now so just stick to replying to this email.

Thanks,
Markus
CEO

30. Is the image above a real email or phishing email??

- Real email
- Phishing email

SECTION 15

Example 5 (only if answered 'Phishing Message' in previous question)

31. Why have you decided that this is a phishing email? Choose the "red flags"

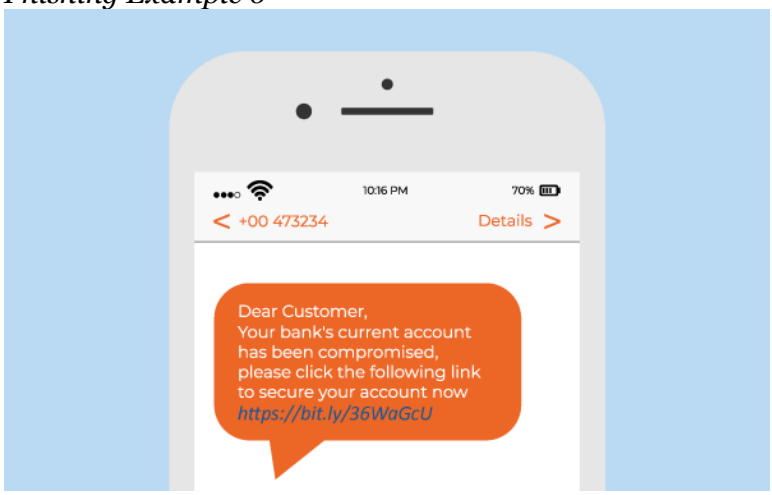
- Generic greeting
- Request for confirmation/verification/details of sensitive information
- The sender's domain/email
- Suspicious links
- Inconsistencies in email addresses, links & domain names
- Spelling and grammar mistakes
- Suspicious style of writing
- Sense of urgency/need for immediate actions
- Too good to be true

Other .....

Funded by the Erasmus+ Programme of the European Union

SECTION 16

Phishing Example 6



32. Is the image above a real text or phishing text?

- Real text
- Phishing text

SECTION 17

Example 6 (only if answered 'Phishing Text' in previous question)

33. Why have you decided that this is a phishing text message? Choose the "red flags"

- Generic greeting
- Request for confirmation/verification/details of sensitive information
- The sender's domain/email
- Suspicious links
- Inconsistencies in email addresses, links & domain names
- Spelling and grammar mistakes
- Suspicious style of writing
- Sense of urgency/need for immediate actions
- Too good to be true

Other.....

SECTION 18 - Self-evaluation: Critical thinking

34. Use the scale from 1 till 5 to evaluate:

1) Never
2) Rarely
3) Sometimes
4) Very Often
5) Always

Funded by the Erasmus+ Programme of the European Union

	Never	Rarely	Sometimes	Very often	Always
Do you normally trust messages that appear to come from an important entity or look important?					
When you open an email/ message do you have a sufficient focus and attention to detail?					
Are you mindful of what you click on when you receive an email/message with the link/ attachment?					

35. When you receive a suspiciously looking email, do you evaluate:

	Never	Rarely	Sometimes	Very often	Always
Who is sender					
Sender's email					
Subject line					
Style of email (formal, non-formal, words used)					
Images					
Grammar and spelling mistakes					
Links/attachments					
Signature and credentials					

36. When you receive a suspicious looking email/message, are you able to visualise possible implications/consequences of your decision, based on evidence?

- Never
- Rarely
- Sometimes
- Very Often
- Always

37. When you receive a suspicious looking email/message, are you able to draw the conclusions, based on evidence?

- Never
- Rarely
- Sometimes
- Very Often
- Always

Funded by the Erasmus+ Programme of the European Union

SECTION 19 - Avoiding phishing attacks

38. Why phishing attacks are successful? (Choose top 5 reasons)

- Attackers are really good at replication of messages and emails from legit companies, making them very believable and convincing
- Attackers exploit human nature, they rely on interaction and playing human emotions and needs
- Attackers can easily access personal details and information about the specific person or company in social media/company webpages, press, etc.
- Attackers are becoming more advanced, targeting specific individuals while using emails are highly personalised and use specific information
- People are not paying enough attention/are ignorant
- People are not aware/ have no knowledge on such attacks and how to prevent them
- People are using outdated software
- Organisations/Companies are not doing enough to prevent these attacks
- There is a lack of training provided in regard to cybersecurity and phishing
- Phishing tools are low-cost and widespread
- Malware itself is becoming more sophisticated
- Other.....

39. What emotions, needs and desires are usually exploited by attackers?

- Fear
- Concern/Anxiety
- Panic
- Curiosity
- Greediness
- Motivation (Gift / Free voucher)
- Desire for emotional fulfilment
- Trusting nature
- Helpfulness
- Other.....

40. What actions are important to take in order to avoid phishing attacks?

	Not important	Slightly important	Moderately important	Important	Very important
Using up-to-date browser					
Using up-to-date operational system					
Keeping up with the newest software & tools available					
Using security software					
Keeping sensitive information about yourself out of social media					
Using multifactor authentication/changing passwords frequently					

Funded by the Erasmus+ Programme of the European Union

Using web filter to block malicious websites					
Having regular cybersecurity trainings/workshops					
Develop a security policy					
Encrypting all sensitive company information					
Being cautions when opening the emails/messages/answering the phone					
Double-checking all-important details (senders' email, links, attachments, etc.)					
Trusting your instincts and using good judgement					
Continuously educating yourself on the topic					

41. To what extent do you agree with the statements. I feel confident in:

	Not confident at all	Slightly confident	Somewhat confident	Fairly confident	Completely confident
Knowing cybersecurity/phishing terminology and using it					
Finding the relevant & trustworthy information online					
Taking right actions/measures to prevent phishing attacks					
Identifying phishing attacks					
Keeping my software/programmes up to date					
Using multifactor authentication					
Using the security software					
Using web filter to block malicious websites					
Encrypting all sensitive company information					

Funded by the Erasmus+ Programme of the European Union

42.Other comments/ suggestions

Funded by the Erasmus+ Programme of the European Union