



Co-funded by the
Erasmus+ Programme
of the European Union

Safeguarding against Phishing in the age of 4th Industrial Revolution

Project duration:

November, 2020 – November, 2022

www.cyberphish.eu

Šis projektas finansuojamas remiant Europos Komisijai.

Šis leidinys [pranešimas] atspindi tik autoriaus požiūrį, todėl Komisija negali būti laikoma atsakinga už bet kokį jame pateikiamos informacijos naudojimą.



Website:

<https://cyberphish.eu/>

CyberPhish: Safeguarding against Phishing in the age of 4th Industrial Revolution

ABOUT THE PROJECT THE PROJECT PARTNERS NEWS PUBLICATIONS PROJECT RESULTS EVENTS CONTACT

CyberPhish
Safeguarding your digital future

About the 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 digital environment. Digital devices and information systems increasingly become attractive for cyber-attacks.

Eurostat states, that in 2019, approximately 1 in 3 EU citizens aged 16 to 74 reported security-related incidents and the phishing was the most frequent security incident.

CyberPhish on Facebook

CyberPhish
230 followers
Erasmus+
ERASMUS+ Project about Cyber Security
Follow Page

CyberPhish
about 3 months ago

Read our full article here:
<https://tech.mt/.../cyber-phishing-towards-safeguarding-your.../>
#cyberphish

TECH.MT
Cyber Phishing: Towar...
Would you open your attach...



Kaunas Faculty



HOW PEOPLE RECOGNISE PHISHING ATTACKS [SURVEY]

The aim is to identify and summarize what are the main reasons why people trust phishing attacks.



Kauno fakultetas



514 people



from 5 countries
Cyprus
Estonia
Latvia
Lithuania
Malta

participated in our

40-QUESTIONS SURVEY



304
students



139
employees



53
business owners



10
unemployed people



8
self-employed people



Co-funded by the Erasmus+ Programme of the European Union

https://cyberphish.eu/wp-content/uploads/2021/07/IO1-A1_EN_CYBERPHISH-REPORT_survey-results.pdf

Hotels.com <Hotelscom@roktpowered.com> Nov 14, 2018, 11:38 AM (1 day ago)
to dave ▾

[Hotels](#) [Hotel Deals](#) [Packages & Flights](#) [Groups](#) [Customer Service](#) [Gift Cards](#) [Secret Prices](#)



[New York Hotels](#) [Las Vegas Hotels](#) [Chicago Hotels](#) [Los Angeles Hotels](#)

COUPON CODE

\$50 off

When you spend \$350 or more

EMLRKUSH21850:SK7CM6

[Book now](#)

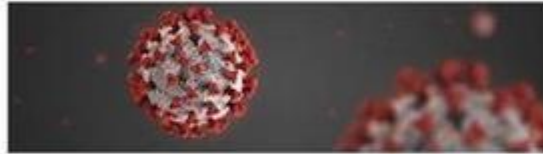
You must click through this email or book through our app to redeem this c



Mon 23/03/2020 12:37 PM

'World Health Organisation' <Sarah@who.com>
Covid19 Latest Tips to stay Immune to Virus !!

To



Good Morning,

Due to the latest outbreak, our various research
keep us from being effected with the virus.

Many affected patients are already responding

Kindly Find attached the various documents an

Don't have a pdf viewer? not to worry, pdf view

Best Regards,

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



World Health
Organizat

10:16 PM 70%

< +00 473234

Details >

Dear Customer,
Your bank's current account
has been compromised,
please click the following link
to secure your account now
<https://bit.ly/36WaGcU>



Google <no-reply@google.support>
to me ▾

Someone has your password

Hi,
Someone just used your password to try to sign in to your Google Account.

Information:
Thursday, November 19, 2020 at 3:06:46 PM GMT+02:00
Slatina, Romania
Firefox browser

Google stopped this sign-in attempt. You should change your password immediately

[CHANGE PASSWORD](#)

Best,
The Mail Team

[KEY FINDINGS]

CYBERSECURITY TRAININGS



- Respondents (100%)
- Never participated in the trainings (73.93%)
- Self trained (54.09%)

HAVE YOU BEEN PHISHED?



Every 5th respondent has been phished in the past.

The main reasons:
distraction,
being in a hurry,
curiosity.

GENERAL KNOWLEDGE AND BEHAVIOURS



Respondents from three countries (Lithuanian, Maltese, and Estonian) are skeptical about the “theft of funds from business/client accounts” occurring after the phishing attack.



Respondents from all the surveyed countries believe that the “loss of intellectual property” is unlikely to occur after a successful phishing attack.

https://cyberphish.eu/wp-content/uploads/2021/07/IO1-A1_EN_CYBERPHISH-REPORT_survey-results.pdf

WHY PEOPLE TEND TO BE PHISHED?



Case study No1: 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.

SOURCE:

< CyberPhish Project <https://cyberphish.eu> >

https://cyberphish.eu/wp-content/uploads/2021/07/IO1-A1_EN_CYBERPHISH-REPORT_survey-results.pdf

THE CURRICULUM (E-LEARNING MODULE) STRUCTURE

1. Introduction to Cybersecurity
2. Overview of Cybersecurity within the EU
3. Cyber-attacks – Social Engineering and Phishing
4. Understanding and Handling Cyberattacks

https://cyberphish.eu/wp-content/uploads/2021/07/IO2-A1_EN_Cyberphish-Short-Curriculum-Final.pdf

Intellectual Outputs of CyberPhish

1

Study analysis and recommendations:
Avoiding phishing attacks and improving critical thinking

2

Course Curriculum

3

Online learning material

4

Simulations for education (gamification)

5

Self-evaluation knowledge evaluation system

6

Methodological guidelines for trainers and for implementation

Invitation

We kindly invite you to participate in the online course about phishing!

Registration to online training: [<link>](#)



Duration of pilot training **4-6 week**



You will learn about **phishing attacks** through an online training material and a scenarios in which you will have to recognise whether or not it is a phishing case and what actions you would take in such a situation.



The scenarios tool will help you **better understand fraud** and **gain knowledge interactively**.



All course participants completed the course will be **awarded certificates**.

Participants completed course with highest scores will be **awarded prizes**.

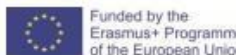


Course participants will develop competences that will help them to highlight threats and take appropriate preventive measures.



More information about the **CyberPhish project**: <https://cyberphish.eu/>

Trainings are organized in the framework of the CyberPhish (Safeguarding against Phishing in the age of 4th Industrial Revolution) project which is funded under the Erasmus+ programme.



Questionnaire before trainings:

<https://forms.gle/xBs6HCDE4qRz3xWJA>



Funded by the
Erasmus+ Programme
of the European Union



CyberPhish pilot training

Welcome to the Cyberphish pilot training. This questionnaire is the first step of the pilot training. The results of the questionnaire will not affect your training, it is a tool to measure your progress after the training.

The questionnaire will take between 20-25 minutes. Before completing the questionnaire, please provide your email address, which we also ask you to use when registering for the course training environment (please use a valid email address).

The trainer will shortly send you a link to the CyberPhish training environment, which contains material on phishing attacks and how to avoid them. You will test your knowledge by solving scenarios in which you will have to recognise whether it is a fraud and what you would do in such a situation.

The scenarios will help you to better understand fraud and gain knowledge in an interactive way.

The estimated duration of the training is 4 weeks.

Certificates will be awarded to all participants upon completion of the course.

If you have any questions, you can contact kestutis.driaunys@knf.vu.lt

Thank you for your cooperation and your time.

We kindly invite you to participate in the
online course about phishing!

Registration to online training: <link>



Duration of pilot training **4-6 week**



You will learn about **phishing attacks** through an online training material and a scenarios in which you will have to recognise whether or not it is a phishing case and what actions you would take in such a situation.



The scenarios tool will help you **better understand fraud** and **gain knowledge interactively**.



All course participants completed the course will be **awarded certificates**.
Participants completed course with highest scores will be **awarded prizes**.



Course participants will develop competences that will help them to highlight threats and take appropriate preventive measures.



More information about the **CyberPhish project**:
<https://cyberphish.eu/>

Trainings are organized in the framework of the CyberPhish (Safeguarding against Phishing in the age of 4th Industrial Revolution) project which is funded under the Erasmus+ programme.



Funded by the
Erasmus+ Programme
of the European Union

E-LEARNING MODULE



The screenshot shows the CyberPhish website interface. At the top, there is a navigation bar with the CyberPhish logo on the left and menu items: Home, Learning Material, Ranks, Sign In, Sign Up, and Language (with a dropdown arrow). Below the navigation bar is a large banner featuring a network diagram background. The banner contains the CyberPhish logo (a stylized 'S' inside a circle) and the text 'CyberPhish' in a large, blue, sans-serif font, followed by the tagline 'Safeguarding your digital future' in a smaller, grey font. Below the banner, the page has a white background with the heading 'About CyberPhish' in a bold, blue font. Underneath the heading is a paragraph of text: '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 digital environment. Digital devices and information systems increasingly become attractive for cyber-attacks.' At the bottom of this section is a blue button with the text 'More About us' in white.

Website:
<https://cyberphish.vuknf.it/>




Co-funded by the
Erasmus+ Programme
of the European Union

Create an Account

Kauno
fakultetas

https://cyberphish.vuknf.lt/register



Sukurkite paskyrą!


Use your (student) email

Slaptažodis

Pakartokite slaptažodį

Šalis

Aš ne robotas


reCAPTCHA
Privatumas • Sąlygos

Aš sutinku su naudojimo sąlygomis

<https://cyberphish.vuknf.lt/register>

Signe up

**Kauno
fakultetas**



Welcome Back!

Login

[Forgot Password?](#)

[Create an Account!](#)

<https://cyberphish.vuknf.lt/login>

Learning material

Kauno
fakultetas

Students have to read and understand all learning material

The image shows a screenshot of a learning management system (LMS) interface. On the left, a blue arrow labeled "Topics" points to a sidebar menu. The sidebar menu is titled "Simulations" and contains a list of topics: "INTRODUCTION TO CYBERSECURITY", "CYBERSECURITY WITHIN THE EU", "CYBER-ATTACKS; SOCIAL ENGINEERING AND PHISHING", and "UNDERSTANDING AND HANDLING CYBER-ATTACKS". Each topic has a list of sub-topics. The main content area displays a slide titled "Introduction to Cybersecurity Background – Challenges of the 4th Industrial Revolution". The slide includes the European Union logo and the text "Co-funded by the Erasmus+ Programme of the European Union". Below the slide, there is a "Download slides" button. A blue arrow labeled "Press" points to a "Mark as Completed!" button in the top right corner of the slide area. The top left of the interface shows "Course Progress" at 0%.

Course Progress 0%

Background - Challenges of the 4th Industrial Revolution

✓ Mark as Completed!

Topics

Press

Simulations

INTRODUCTION TO CYBERSECURITY

- Background - Challenges of the 4th Industrial Revolution
- History of Cybersecurity
- Definitions of Cybersecurity

CYBERSECURITY WITHIN THE EU

- Fostering Cybersecurity within the European Union
- Legal Aspects of Cybersecurity
- Overview on the tendencies of Cybersecurity landscape

CYBER-ATTACKS; SOCIAL ENGINEERING AND PHISHING

- Introduction to Cyber-attacks
- Social Engineering Modules and Manipulation
- Different Types of Phishing Attacks and Techniques
- Case Studies

UNDERSTANDING AND HANDLING CYBER-ATTACKS

Introduction to Cybersecurity

Background – Challenges of the 4th Industrial Revolution

Safeguarding against Phishing in the age of 4th Industrial Revolution
www.cyberphish.eu
This project has been funded with support from the European Commission.
The publication (re)presentation reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Download slides

Self-Evaluation Tests

Kauno
fakultetas

Students have to solve four Self-evaluation tests.
Students have to answer at least 4 questions correct in each test.



The screenshot displays a course management interface. On the left, a sidebar shows 'Course Progress' at 10% and a 'Simulations' button. Below this, a list of topics is shown, with 'INTRODUCTION TO CYBERSECURITY' and its sub-topics 'Background—Challenges of the 4th Industrial Revolution', 'History of Cybersecurity', and 'Definitions of Cybersecurity' highlighted with a red box. The main content area features a 'Self Evaluation Test' button (also highlighted with a red box) and a 'Definitions of Cybersecurity' section marked as 'Completed!'. Below this, a video player shows a slide titled 'Definitions of Cyber Security' with the text 'Introduction to Cybersecurity' and 'Definitions of Cyber Security'.

Simulations

Students have to solve at least 20 Simulations

The image shows a course interface with two main panels. The top panel displays 'Course Progress' at 10% and a 'Self Evaluation Test' button. Below this, a 'Simulations' button is highlighted with a red box. The left sidebar lists course topics: 'INTRODUCTION TO CYBERSECURITY' (with sub-items: 'Background—Challenges of the 4th Industrial Revolution', 'History of Cybersecurity', 'Definitions of Cybersecurity'), 'CYBERSECURITY WITHIN THE EU' (with sub-items: 'Fostering Cybersecurity within the European Union', 'Legal Aspects of Cybersecurity', 'Overview on the tendencies of...'). The bottom panel shows a 'Background - Challenges of the 4th Industrial Revolution' section marked as 'Completed'. Below it, a 'Simulations' section is highlighted with a red box, containing buttons for 'Unity', 'Liking', 'Consensus', 'Consistency', 'Authority', 'Scarcity', and 'Reciprocation'. The 'Course Progress' indicator in this panel also shows 10%.

Knowledge evaluation test

Kauno
fakultetas

Students have to solve Final test with score at least 75%

The image displays a screenshot of a course management system interface. The top left shows 'Course Progress' at 10%. A 'Self Evaluation Test' button is visible. Below it, a 'Simulations' button is highlighted with a red box. The main content area shows 'Background - Challenges of the 4th Industrial Revolution' with a 'Completed!' status. A larger inset window shows a 'Simulations' section with a 'Course Progress' at 10% and a 'Simulations' button. The simulation content is highlighted with a red box and includes buttons for 'Unity', 'Liking', 'Consensus', 'Consistency', 'Authority', 'Scarcity', and 'Reciprocation'. The left sidebar lists course topics: 'INTRODUCTION TO CYBERSECURITY' (with sub-items: 'Background—Challenges of the 4th Industrial Revolution', 'History of Cybersecurity', 'Definitions of Cybersecurity'), 'CYBERSECURITY WITHIN THE EU' (with sub-items: 'Fostering Cybersecurity within the European Union', 'Legal Aspects of Cybersecurity', 'Overview on the tendencies of...').