Funded by the
Erasmus+ Programme
of the European Union

Introduction to Cybersecurity

# Definitions of Cyber Security

**Safeguarding against Phishing in the age of 4th Industrial Revolution**
**www.cyberphish.eu**

*This project has been funded with support from the European Commission. This publication [communication] 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.*

CyberPhish
Safeguarding your digital future

# *Learning Goals*

To become familiar with the very notion of cybersecurity

**What is cybersecurity**

**What is cyberattack**

Funded by the
Erasmus+ Programme
of the European Union

# *Student Workload*

| | |
|---|---|
| Lecture | 0.5 h |
| Further reading | 4 h |
| Preparation for exam | 1 h |

Funded by the
Erasmus+ Programme
of the European Union

# Cyberspace Definition

- First of all we need to define what the cyberspace is.
- The popular definition is provided by NIST:

*A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers*

*Source: https://csrc.nist.gov/glossary/term/cyberspace*

Funded by the
Erasmus+ Programme
of the European Union

# *What is Cybersecurity?*

- In recent years, “Cyber Security” has emerged as a widely-used term with increased adoption by practitioners and public.
- However, as with many fashionable phenomena exact definition of cyber security isn’t so clear.
- E.g. early in 2000s the terms regularly used in this context would be “Computer Security”, “IT Security,” or “Information Security.”

- The term cybersecurity became so popular only in 2010s.

Funded by the
Erasmus+ Programme
of the European Union

# *What is Cybersecurity?*

- The rising popularity of the term cybersecurity often is associated with US President Barack Obama.
- In 2009 Barack Obama proclaimed: *“I call upon the people of the United States* ***to recognize the importance of cybersecurity*** *and to observe this month with appropriate activities, events, and trainings to enhance our national security and resilience”* (https://obamawhitehouse.archives.gov/the-press-office/presidential-proclamation-national-cybersecurity-awareness-month).

- “Cyber Security” is much more than “Computer Security”

Funded by the
Erasmus+ Programme
of the European Union

# *Cyber Security Definitions*

Industry definition:

*Cyber security is set of security practices related to the combination of offensive and defensive actions involving or relying upon information technology and/or operational technology environments and systems.*

*Cyber security is superset of security practices such as information security, IT security and other related practices*.

*Source: https://www.isaca.org/resources/isaca-journal/issues/2015/volume-6/developing-a-common-understanding-of-cybersecurity*

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

# Cyber Security Definitions

## Academic definition:

*Cybersecurity is the approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyber space. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection in cyber space.*

Source: https://www.isaca.org/resources/isaca-journal/issues/2015/volume-6/developing-a-common-understanding-of-cybersecurity

Funded by the
Erasmus+ Programme
of the European Union

# *What is Cyber Attack?*

- The cyber security is closely related to cyber threats.
- Popular definition provided by NIST:

*An attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information*

Source: https://csrc.nist.gov/glossary/term/cyber_attack

Funded by the Erasmus+ Programme of the European Union

# *Some Types of Cyberattacks*

- **Malware** describes malicious software, including spyware, ransomware, viruses, and worms. It breaches a network through some type of vulnerability. Most often clicking dangerous link or email attachment with  risky software.
- **Phishing** denotes sending fraudulent communications. The goal is to simulate coming from a reputable source. Typically sending done through email. The aim is to steal sensitive data like login information or to install malware on the victim’s machine.
- **Man-in-the-middle (MitM)** attacks, aka eavesdropping attacks, occur when attackers insert themselves into a two-party transaction.

Funded by the
Erasmus+ Programme
of the European Union

# *Some Types of Cyberattacks*

- **A denial-of-service attack** aims to overcrowd computer and network resources with unnecessary traffic. As a result, the system is unable to fulfil legitimate requests.
- **A Structured Query Language (SQL) injection** occurs inserting malicious code into a server using SQL, The goal is to reveal information that normally would not be exposed.
- **DNS tunnelling** using DNS protocol to communicate non-DNS traffic
- **A zero-day exploit** is the exploitation of the vulnerability when it was found and announced but still not patched. Attackers using information about the vulnerability this window of time.

Funded by the Erasmus+ Programme of the European Union

# *Some Types of Cyberattacks*

- Different types of cyber attacks may requires different actions.

- Some cyber attacks may need deep technical knowledge.
- Part of cyber attacks may exploit human psychology and manipulations.

- **Remember**: the weakest element in cyber chain is human.

Funded by the
Erasmus+ Programme
of the European Union

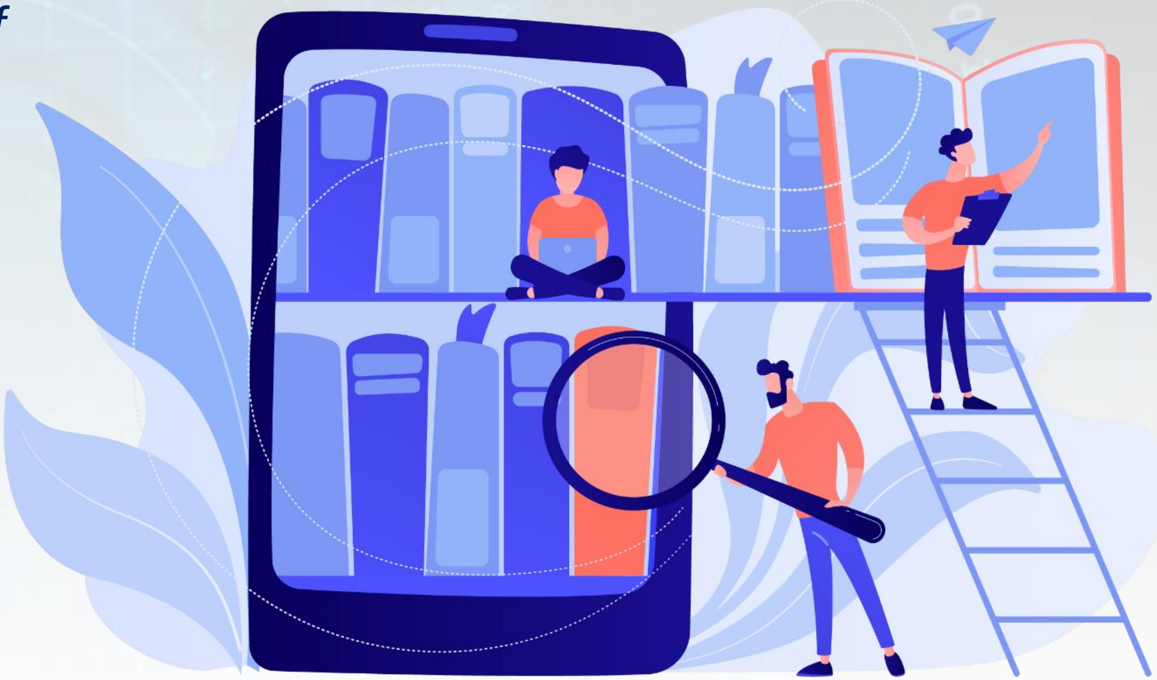
# Some Types of Phishing

- ***Email phishing***: most popular way for phishing. The crook will use a fake domain similar to existing and reliable organization's that mimics a genuine organization and sending many requests.
- ***Spear phishing***:  malicious emails sent to a specific person usually high value target. Attackers typically will gather some information about the victim.
- ***Whaling attacks*** are even more targeted, taking aim at senior executives.
- ***Smishing and vishing***: telephones used as a primary way of attack instead of email. Smishing involves text messages such as SMS while vishing performed via spoken conversation.
- ***Angler phishing:*** social media capabilities are used to persuade people to expose sensitive information or download malware. Data that people post on social media to create highly targeted attacks could be used too.

Funded by the
Erasmus+ Programme
of the European Union

# Further Reading

- *Daniel Schatz, Rabih Bashroush, Julie Wall. Towards a More Representative Definition of Cyber Security. Journal of Digital Forensics, Security and Law. Number 2, volume 12, 2017*
- *Dan Craigen, Nadia Diakun-Thibault, Randy Purse. Defining Cybersecurity. Technology Innovation Management Review. Number 4, volume 10, 2014*
- *Defining Cybersecurity. Emerging technologies and problem definition uncertainty: The case of cybersecurity. Regulation @ Governance, July 2020*



Funded by the
Erasmus+ Programme
of the European Union

# Thank you!

CyberPhish
Safeguarding your digital future

www.cyberphish.eu
Project Implementation Period
02 11 2020 – 02 11 2022

CyberPhish Project
#CyberPhish

Funded by the
Erasmus+ Programme
of the European Union