Funded by the Erasmus+ Programme of the European Union

Introduction to Cybersecurity

History of Cybersecurity

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

Learn a brief history of how approaches to cyber-attacks have changed over time, leading to increased measures and hence the counter measures against cyber-attacks

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

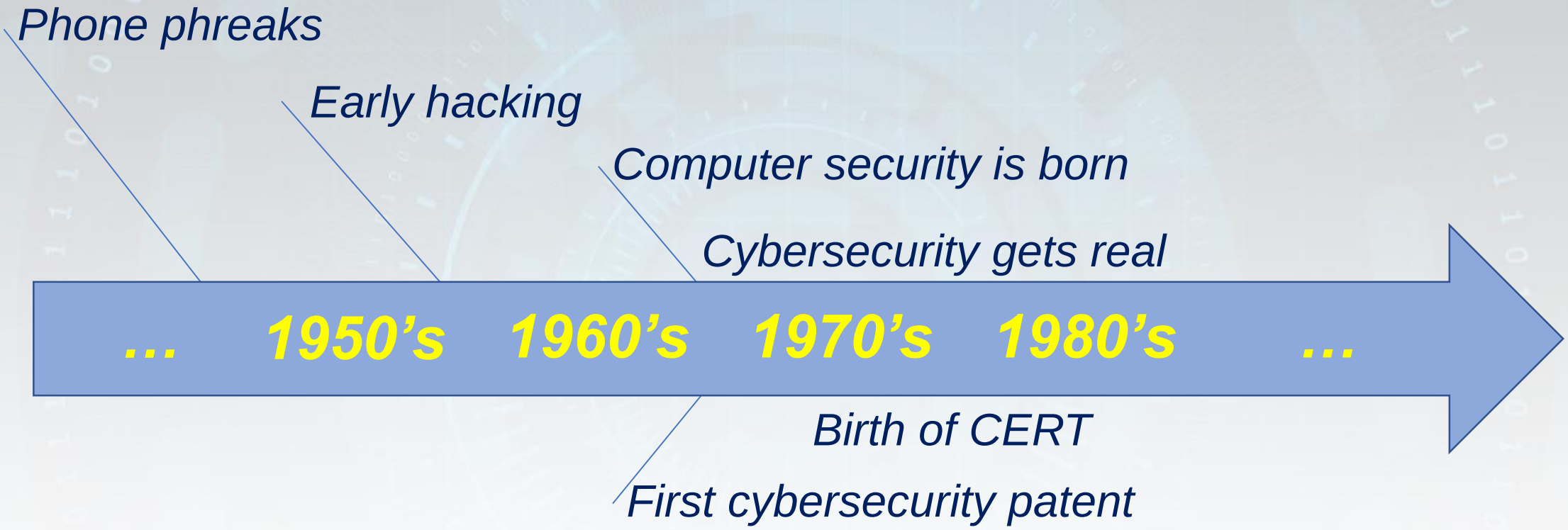
Student Workload

Lecture	1 h
Audio and video material	1 h
Case studies	1 h
Further reading	2 h
Preparation for exam	1 h

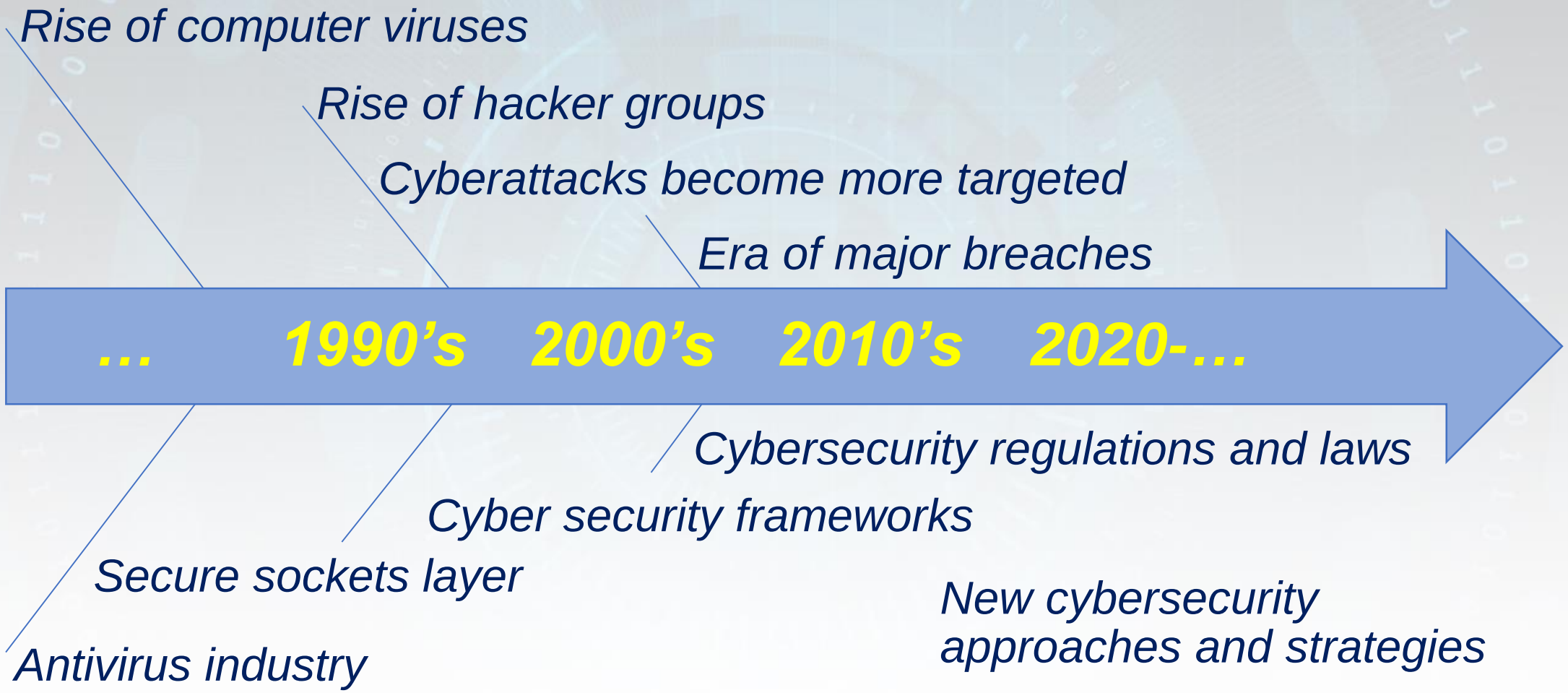
CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Contents


Phone phreaks
Early hacking
Computer security is born
Cybersecurity gets real
… 1950's 1960's 1970's 1980's …
Birth of CERT
First cybersecurity patent

Contents



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Phone Phreaks

In the 1950's, phones were the cutting-edge of technology

- **Phone phreaks**
  - Learned to control the phone lines by listening to the sounds as calls were connected by operators
  - Read phone company technical journals
  - Breaking into offices to develop their own hardware

[*Lapsley, 2013*]

Phone phreaks were starting the hacking mindset before there was a computer around to hack

Early Hacking

In the 1960's, computers were giant mainframes, locked in rooms

Hacking developed as a positive practice intended to help computer systems improve

This resulted in some of the first ideas for defensive programs that could stop hackers

https://blog.avast.com/history-of-cybersecurity-avast

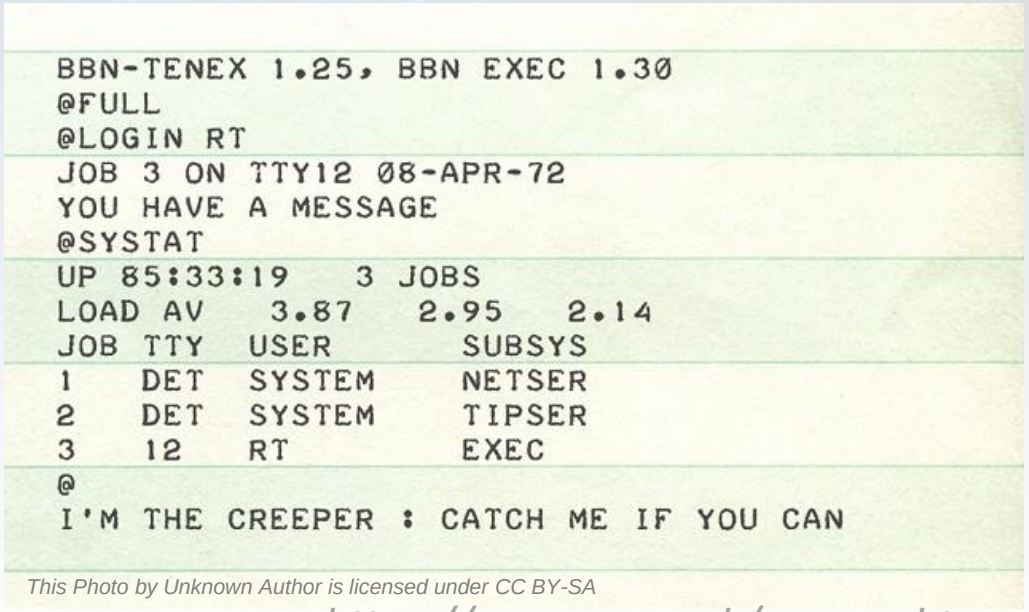
CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Computer Security is Born

1971: **I am the creeper: catch me if you can**

- Researcher **Bob Thomas** created a **Creeper** that could move across ARPA network
- **Ray Tomlinson** wrote the **Reaper**, which chased and deleted Creeper
  - Reaper was the very first example of antivirus software
  - Reaper was also the first self-replicating program, making it the first-ever computer worm



https://corewar.co.uk/creeper.htm

CyberPhish
Safeguarding your digital future

https://www.javatpoint.com/history-of-cyber-security

Funded by the Erasmus+ Programme of the European Union

First Cybersecurity Patent

1983: Cryptographic Communications System and Method

RSA

- Granted to the Massachusetts Institute of Technology (MIT)
  - **RSA** (Rivest-Shamir-Adleman) algorithm, which was one of the first public key cryptosystems

CyberPhish
Safeguarding your digital future

https://www.secureworld.io/industry-news/historic-hacking-brief-history-cybersecurity

Funded by the Erasmus+ Programme of the European Union

Cybersecurity Gets Real

Hacking became an issue of national security in the 1980's

- In 1986, **Marcus Hess**, a German citizen, hacked into **400 military computers**
  - He intended to sell secrets to the KGB
- Attack method
  - Used Lawrence Berkeley Laboratory (LBL) to "***piggyback***" to ARPANET and MILNET
- An astronomer, **Clifford Stoll**, used ***honeypot*** to detect the intrusion and foil the plot

Birth of CERT

1988: Morris worm or Internet worm – the first network virus

- **The Morris worm**
  - The program went through networks, invaded Unix terminals, and copied itself
  - Infected a computer multiple times
  - Each additional process would slow the machine down, eventually to the point of being damaged

- R. Morris was charged under the **Computer Fraud and Abuse Act**
  - The act itself led to the founding of the **Computer Emergency Response Team**, *a.k.a.*, **CERT**

https://www.javatpoint.com/history-of-cyber-security

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

The 1990's: Rise of Computer Viruses

This Photo by Unknown Author is licensed under CC BY-SA

- Inadequate security solutions caused a huge number of unintended victims to be affected
- Most of the virus attacks were primarily concerned with financial gains or strategic objectives

Funded by the Erasmus+ Programme of the European Union

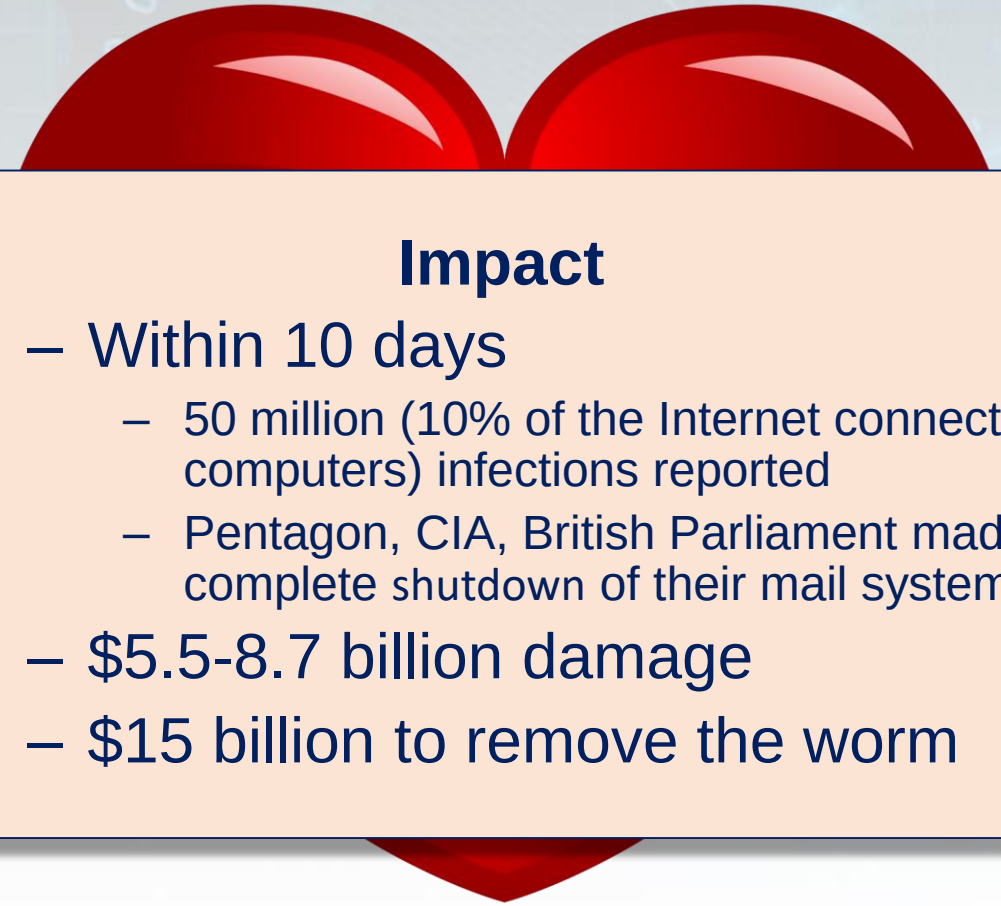
May 2000: *I LOVE YOU*

- **An email message**
  - subject line "ILOVEYOU" and
  - attachment "LOVE-LETTER-FOR-YOU.txt.vbs"
- **Opening the attachment**
  - activates the Visual Basic script
    - Overwriting image files,
    - Sent a copy of itself to the first 50 addresses in the Windows Address Book used by Microsoft Outlook

https://en.wikipedia.org/wiki/ILOVEYOU

Funded by the Erasmus+ Programme of the European Union

May 2000: *I LOVE YOU*



Impact

- Within 10 days
  - 50 million (10% of the Internet connected computers) infections reported
  - Pentagon, CIA, British Parliament made a complete shutdown of their mail systems
- $5.5-8.7 billion damage
- $15 billion to remove the worm

Success

- Scripting engine is enabled
- Advantage of Microsoft algorithm to hiding file extensions
- Social engineering
- Microsoft design weakness
  - Access to operating systems
  - Secondary storage

Pet Shop Boy's "E-mail"
https://youtu.be/AEF8hAAm_sg

Funded by the Erasmus+ Programme of the European Union

Antivirus Industry

The early 1990s: a sharp growth of antivirus products

Growth of malware programs
from **few thousands** in the 1990s to **at least 5 million** by the year 2007

- First commercial antivirus programs in 1987:
  - Antivirus for the Atari ST
  - The NOD antivirus
  - McAfee VirusScan
- Antivirus programs **scanned** and **tested** IT systems with ***signatures*** written in a database
  - An intensive use of resource
  - A large number of false positive

- **Endpoint protection platforms**
  - Identify ***malware families***
  - Premise: malware samples deviate from existing samples
  - Possible to detect and stop unknown malware since only a signature of other existing malware was required

CyberPhish
Safeguarding your digital future

https://cyberexperts.com/history-of-cybersecurity/

Funded by the Erasmus+ Programme of the European Union

Secure Sockets Layer

1995: SSL rears its head

- **SSL**
  - Developed by Netscape shortly after released of the first internet browser
  - Core for developing languages such as HyperText Transfer Protocol Secure (HTTPS)
  - Enables users to access the web securely and perform activities such as online purchases

Rise of Hacker Groups

2003: Anonymous – the first hacker group

Anonymous – October 1, 2003:

- First: hacked a website belonging to the *Church of Scientology* using **DDoS**
- Doesn't have a particular leader
- Members from different offline and online communities
- To date – linked to many high-profile attack incidents
- Main cause is protecting citizens' privacy
- Motivated other groups to execute large-scale cyberattacks
  - *Lazarus* and *Apt38*, etc

Credit Card Hacks

Between 2005 and 2007: cyberattacks more targeted

- **Albert Gonzales**:
  - Created a cybercriminal ring
  - Compromise credit card systems
  - Confidential information from at least ***45.7*** million cards
  - Loss amounting to ***$256*** million
  - Funds to compensate the affected victims

TJX was unprotected when the breach occurred and other organizations saw this as a cue for protecting themselves with sophisticated cybersecurity program

https://cyberexperts.com/history-of-cybersecurity/

Funded by the Erasmus+ Programme of the European Union

The 2010s: Era of Major Breaches

- **Snowden & The NSA, 2013**:
  - former CIA employee and contractor for the US Government – copied and leaked classified information from the National Security Agency (NSA)
  - highlighted the fact that the government was "spying" on the public
- **Yahoo, 2013 – 2014**:
  - Hackers used ***spear-phishing*** techniques to install malware on Yahoo's servers, allowing them unlimited backdoor access
  - Jeopardise the accounts and personal information of ***three billion*** users
  - Yahoo was fined ***$35*** million for failing to disclose news of the breach
  - Sale price decreased by ***$350*** million as a result
- **WannaCry ransomware cryptoworm, 2017**:
  - Targeted computers running the Microsoft Windows operating system
  - Demanded ransom payments in the Bitcoin cryptocurrency
  - In only one day, the worm infected over ***230.000*** across ***150*** countries

https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/

Funded by the Erasmus+ Programme of the European Union

May 12-15, 2017: *WannaCry*

- Microsoft design weakness
  - Propagated through EternalBlue
  - Took advantage of installing backdoors onto infected systems
- While Microsoft had released patches
  - Organizations had not applied these, or were using older Windows systems

https://www.avast.com/c-wannacry

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Cybersecurity Frameworks

- **Standards**
  - ISO/IEC 2700x series
  - NIST special publication
  - BSI standard 100 for information security
  - Common criteria
  - …
- **Techniques**
  - Misuse cases
  - Mal-activity diagrams
  - SecureUML
  - UMLsec
  - Agile security requirements engineering

- **Frameworks**
  - Framework for security requirements engineering: representation and analysis
  - Security-by-ontology: a knowledge-centric approach
  - …
- **Processes**
  - CC-based security engineering process
  - Security requirements for software product lines
  - Requirements reuse for improving system security
  - …
- **Methods**
  - Secure Troops
  - SQUARE
  - SREBP
  - …

Funded by the Erasmus+ Programme of the European Union

Cybersecurity Regulations and Laws

1996: **HIPPA** – Health Insurance Portability and Account Act

1999: **GLBA** – Gramm-Leach-Bliley Act

2003: **FISMA** – Federal Information Security Management Act

2018: **GDPR** – General Data Protection Regulation

2020: **CCPA** – California Consumer Privacy Act

New Cybersecurity Approaches and Strategies

- **MFA** – multi-factor authentication
- **NBA** – network behavioural analysis
  - identify malicious files based on behavioural deviations or anomalies
- **Threat intelligence** and update automation
- **Real-time protection**
  - on-access scanning, background guard, resident shield and auto-protect
- **Sandboxing**
  - an isolated test environment to execute a suspicious file or URL
- **Forensics**
  - replaying attacks to help security teams better mitigate future breaches
- **Back-up** and mirroring
- **WAF** – Web application firewalls
  - against cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection.

https://blog.avast.com/history-of-cybersecurity-avast

Funded by the Erasmus+ Programme of the European Union

Summary

- Phone phreaks
- Early hacking
- Cyber security is born
- Computer virus
- Hacker groups
- Major breaches
- Cybersecurity patent
- CERT
- Antivirus industry
- SSL
- Security frameworks
- Regulations and laws

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Assignments

Discuss what lessons should be learnt from the Phone Phreaks cases

Compare ***I LOVE YOU*** and ***WannaCry*** attacks

Which Cybersecurity frameworks have you studied or read about?

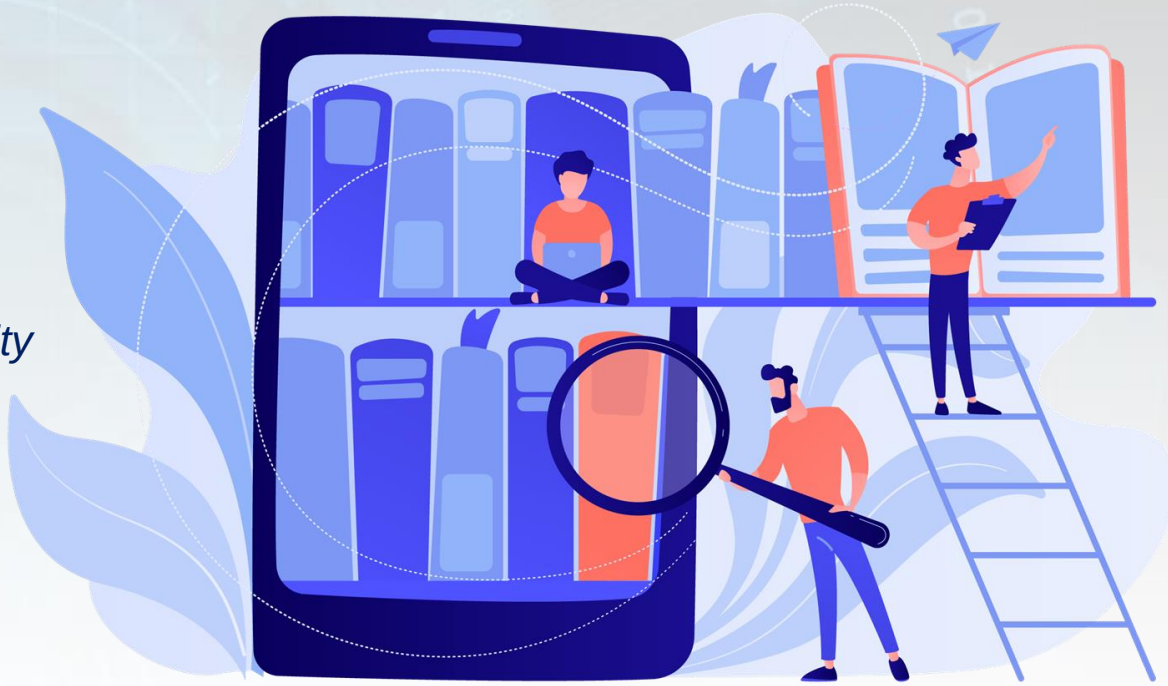
Funded by the Erasmus+ Programme of the European Union

Further Reading

History of Cybersecurity

Material used in preparation of this lecture

- *https://cyberexperts.com/history-of-cybersecurity/*
- *https://elevenfifty.org/blog/a-decade-by-decade-history-of-cybersecurity/*
- *https://www.secureworld.io/industry-news/historic-hacking-brief-history-cybersecurity*
- *https://www.jigsawacademy.com/blogs/cyber-security/cyber-security-history*
- *https://www.javatpoint.com/history-of-cyber-security*
- *https://blog.avast.com/history-of-cybersecurity-avast*
- *https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/*



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Short Videos

- A Brief History of Cybersecurity and Hacking
  https://youtu.be/V6p7lFsokXo
- History of Cybersecurity
  https://youtu.be/CFwmTzCVuFQ
- Evolution of Cybersecurity from 80s to Today
  https://youtu.be/wKaRdugeAPs
- Top Cyber Attacks In History
  https://youtu.be/fUeJtM1bgGo
  https://youtu.be/lJc3viPKXk4

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Thank you!