Funded by the
Erasmus+ Programme
of the European Union

Cybersecurity within the European Union (EU)

# Overview on the Tendencies of Cybersecurity Landscape

**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*

Get to know more about recent cyber security tendencies, emerging threats and realities as well as main cyber security incidents.

Funded by the
Erasmus+ Programme
of the European Union

# *Student Workload*

| | |
|---|---|
| Lecture | 1,5 h |
| Audio and video material | 1 h |
| Case studies | 1,5 h |
| Further reading | 2 h |
| Preparation for exam | 2 h |

Funded by the Erasmus+ Programme of the European Union

2019-2021

# *Cyber Security Threat Tendencies*

According to ENISA, two main facts have significantly contributed to significant changes in the EU cyber threat landscape

1. *Unique, abrupt transformation forces cause by COVID-19 pandemic*
2. *Continuous increasing trend in the advanced adversary capabilities of threat actors*

Funded by the Erasmus+ Programme of the European Union

2019-2021

# *Cyber Security Threat Tendencies*

1. Attack surface in cybersecurity continues to expand

2. Attacks will be a new social and economic norm after the *COVID-19 pandemic*

3. Serious trend - The use of *social media platforms* in targeted attacks

4. Finely targeted and persistent attacks on *high value data*

5. Massively distributed attacks with a short duration and wide impact

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

2019-2021

# *Cyber Security Threat Tendencies*

6. The motivation behind the majority of cyberattacks - *financial*

7. *Ransomware* remains widespread and costly

8. Many cybersecurity incidents go unnoticed or take a long time to be detected.

9. Organisations will invest more in preparedness to protect themselves

10. The number of *phishing victims* continues to grow

Funded by the
Erasmus+ Programme
of the European Union

| Top Threats 2018 | | Assessed Trends |
|---|---|---|
| 1 | Malware | - - - |
| 2 | Web-based attacks | ↗ |
| 3 | Web application attacks | - - - |
| 4 | Phishing | ↗ |
| 5 | Denial of service | ↗ |
| 6 | Spam | - - - |
| 7 | Botnets | ↗ |
| 8 | Data Breaches | ↗ |
| 9 | Insider threat | ↙ |
| 10 | Physical manipulation, damage, theft | - - - |
| 11 | Information leakage | ↗ |
| 12 | Identity theft | ↗ |
| 13 | Cryptojacking | ↗ |
| 14 | Ransomware | ↙ |
| 15 | Cyber espionage | ↙ |

| Top Threats 2019-2020 | | Assessed Trends | Change in Ranking |
|---|---|---|---|
| 1 | Malware | - - - | - - - |
| 2 | Web-based attacks | - - - | ↗ |
| 3 | Phishing | ↗ | ↗ |
| 4 | Web application attacks | - - - | ↙ |
| 5 | Spam | ↙ | ↗ |
| 6 | Denial of service | ↙ | ↙ |
| 7 | Identity theft | ↗ | ↗ |
| 8 | Data Breaches | - - - | - - - |
| 9 | Insider threat | ↗ | - - - |
| 10 | Botnets | ↙ | ↙ |
| 11 | Physical manipulation, damage, theft | - - - | ↙ |
| 12 | Information leakage | ↗ | ↙ |
| 13 | Ransomware | ↗ | ↗ |
| 14 | Cyber espionage | ↙ | ↗ |
| 15 | Cryptojacking | ↙ | ↙ |

Legend: **Trends:** ↙ Declining - - - Stable ↗ Increasing **Ranking:** ↗ Going up - - - Same ↙ Going down

*Source: ENISA "Threat Landscape 2019 -2020" report*

Funded by the
Erasmus+ Programme
of the European Union

# *Five Emerging Trends with Cyber Threats*

1. **Malware is getting upgraded**

   *Malware family strains are being upgraded into new versions with additional features, distribution and propagation mechanisms, e.g., Emotet*

2. **Threats will become fully mobile**

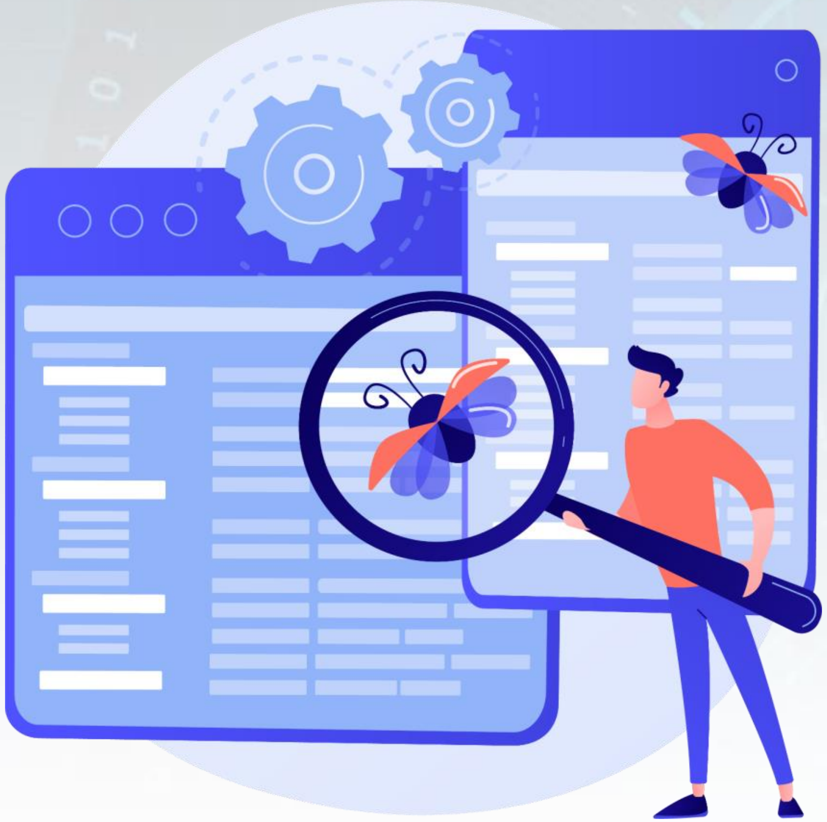
   *Users are increasingly dependent on mobile devices to secure their most sensitive accounts*

Source: https://www.freepik.com/

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

# Five Emerging Trends with Cyber Threats



Source: https://www.freepik.com/

3. **Use of new file types**

   *E.g., disc image files (ISO and IMG) for spreading malware*

   *DOC, PDF, ZIP and XLS files are still the most commonly used*

4. **Increase of coordinated and targeted ransomware attacks**

   *In 2019, it was an escalation of sophisticated and targeted ransomware exploits, e.g., health and public sector*

Funded by the Erasmus+ Programme of the European Union

# Five Emerging Trends with Cyber Threats

5. **Widespread of credential-stuffing attacks**

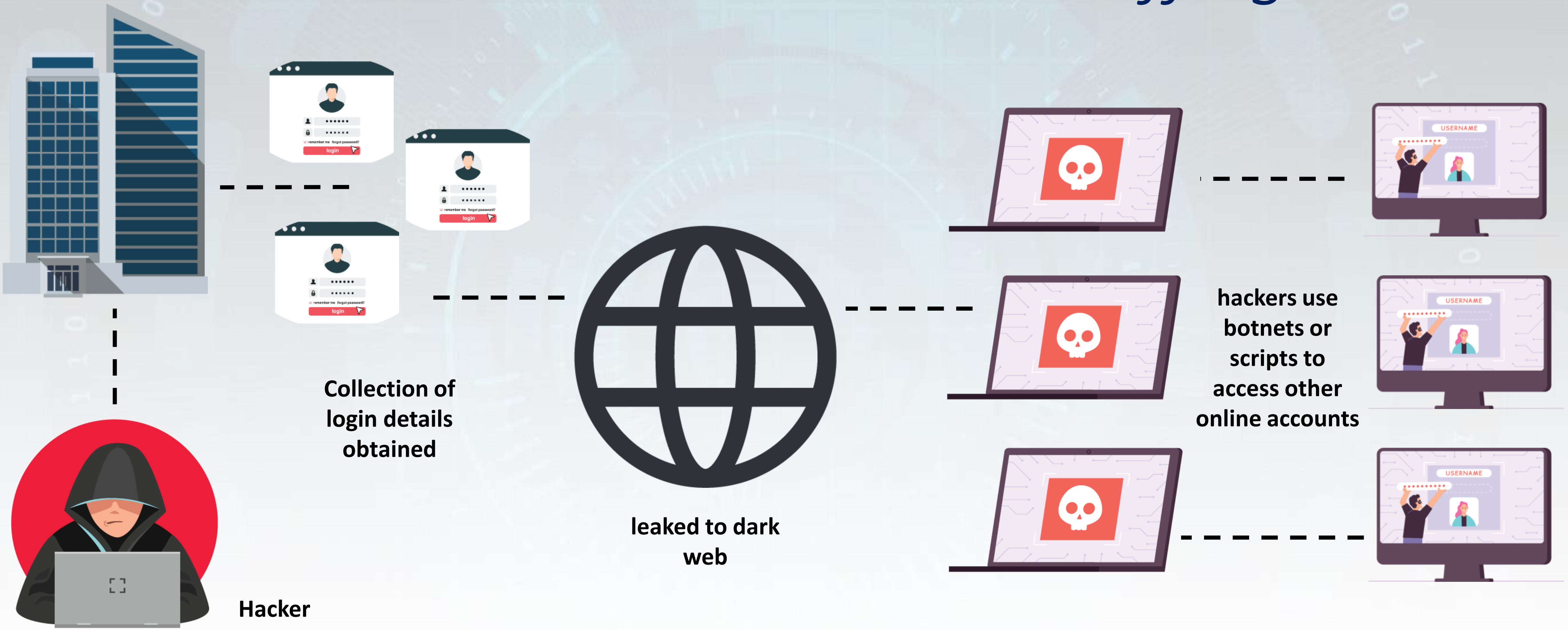
   *These attacks will proliferate as a result from a decade of an abnormal number of data breaches and trillions of personal data records stolen*

Source: https://www.freepik.com/

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

# *Credential Stuffing Attack*



Collection of login details obtained

leaked to dark web

hackers use botnets or scripts to access other online accounts

Hacker

*Adapted from Comparitech*

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

# *Ten Emerging Trends in Attack Vectors*

1. Attacks will be massively distributed with a short duration and a wider impact

2. Finely targeted and persistent attacks will be meticulously planned with well-defined and long-term objectives

3. Malicious actors will use digital platforms in targeted attacks

Source: https://www.freepik.com/

Funded by the Erasmus+ Programme of the European Union

# *Ten Emerging Trends in Attack Vectors*

4. The exploitation of business processes will increase

5. The attack surface will continue expanding

6. Teleworking will be exploited through home devices

7. Attackers will come better prepared

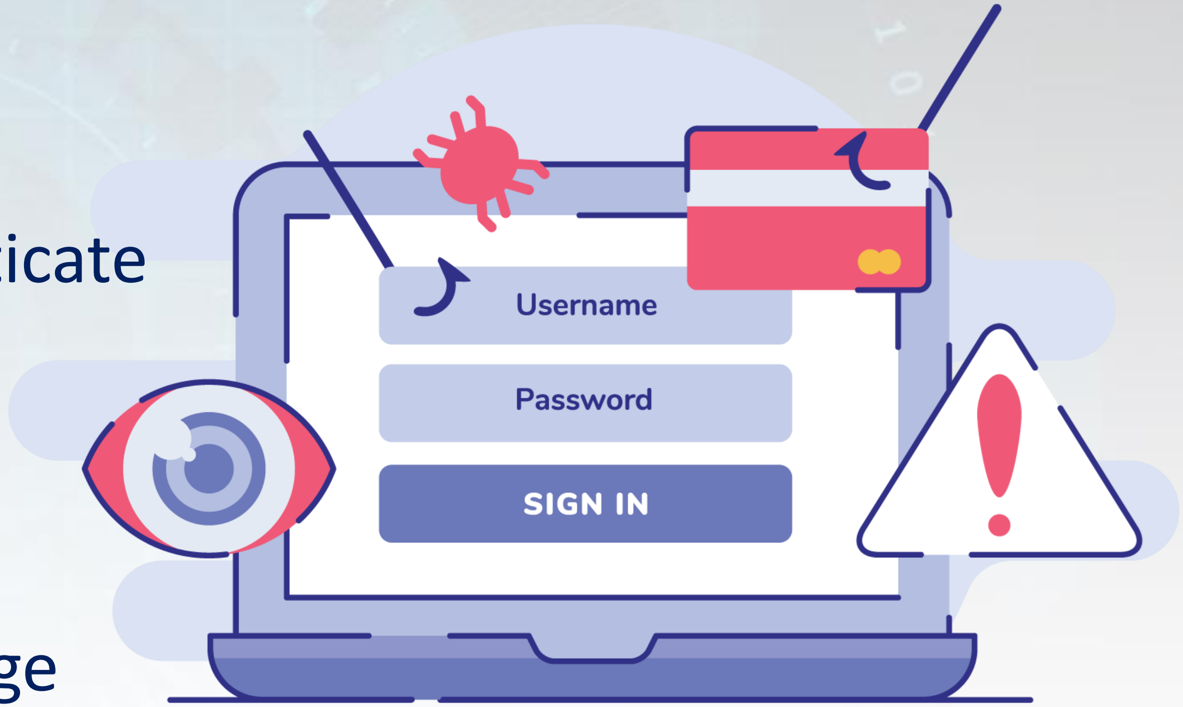
Source: https://www.freepik.com/

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

# *Ten Emerging Trends in Attack Vectors*

8. Obfuscation techniques will sophisticate
9. The automated exploitation of discontinued applications and unpatched systems will increase
10. Cyber threats are moving to the edge

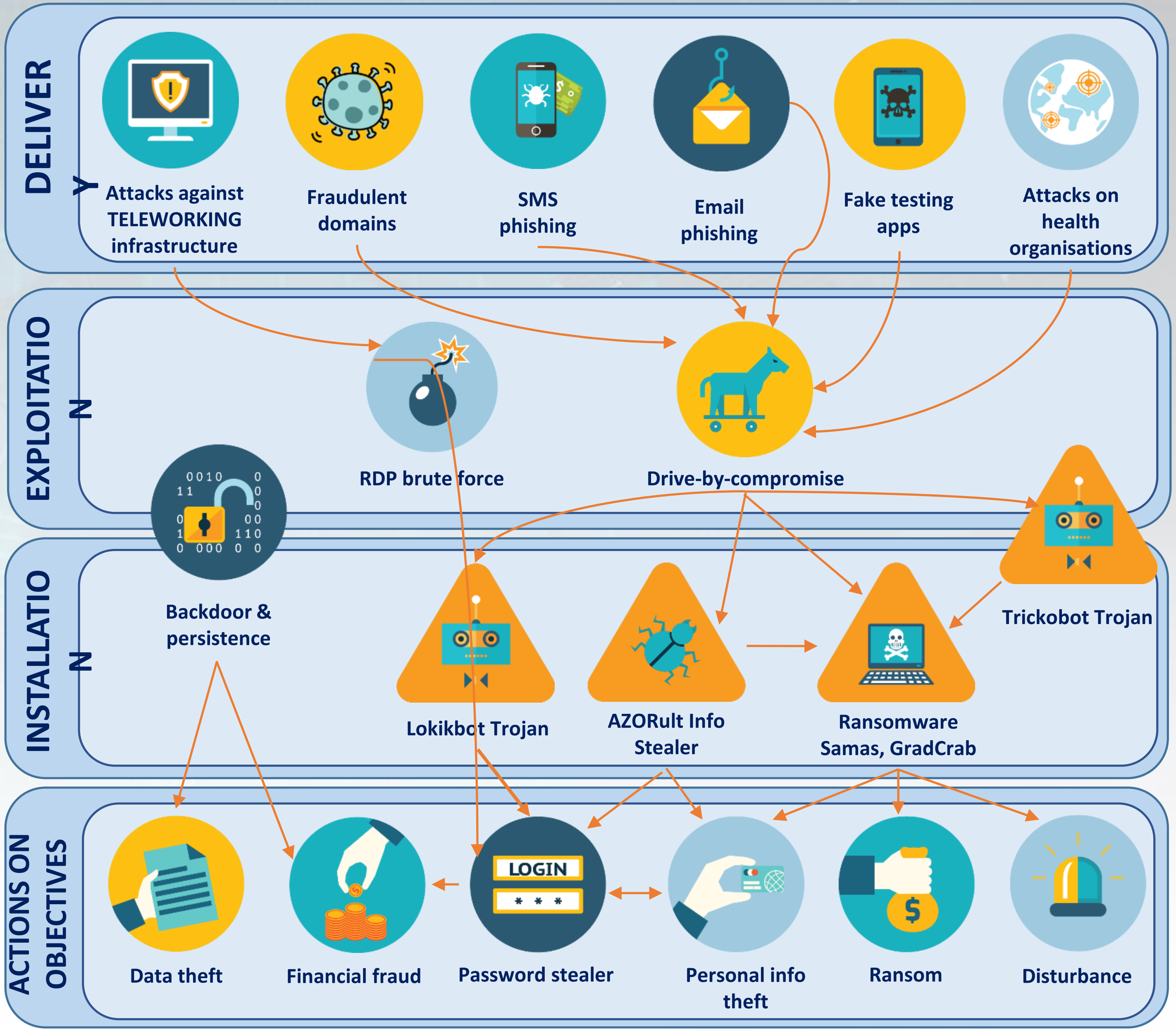


Source: https://www.freepik.com/

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

# *COVID-19 Threat Landscape by ENISA*



Source: https://www.enisa.europa.eu/

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

# Cybersecurity Realities: Citizens

70% of Internet user computers in the EU experienced at least one Malware-class attack

549 301 unique users in the EU were attacked by ransomware

1 523 148  unique users in the EU were attacked by miners

6.95 million new phishing and scam pages created worldwide, with the highest number of new phishing and scam sites in one month being 206,310 (73% increase from 2019)

Funded by the
Erasmus+ Programme
of the European Union

# Cybersecurity Realities: Business

87% of organization have experienced an attempted exploit of an already-known, existing vulnerability

46% of organizations have had at least one employee download a malicious mobile application which threatens their networks and data

It’s estimated that ransomware has cost businesses globally $20 billion in 2020, up from $11.5 billion in 2019

Research shows that in q3 2020, nearly half of all ransomware cases included the threat of releasing stolen data, and the average ransom payment was $233,817 - up 30% compared to q2 2020

Cybercrime will cost companies worldwide an estimated $10.5 trillion annually by 2025, up from $3 trillion in 2015

43% of cyber attacks are aimed at small businesses, but only 14% are prepared to defend themselves.

Funded by the
Erasmus+ Programme
of the European Union

# *Cybersecurity Realities in EU*

In 2019, the EU has registered around **450 attacks** on critical infrastructures in the energy and water supply sectors as well as information and communication technologies in the health, transport, and finance sectors

Source: https://www.freepik.com/

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

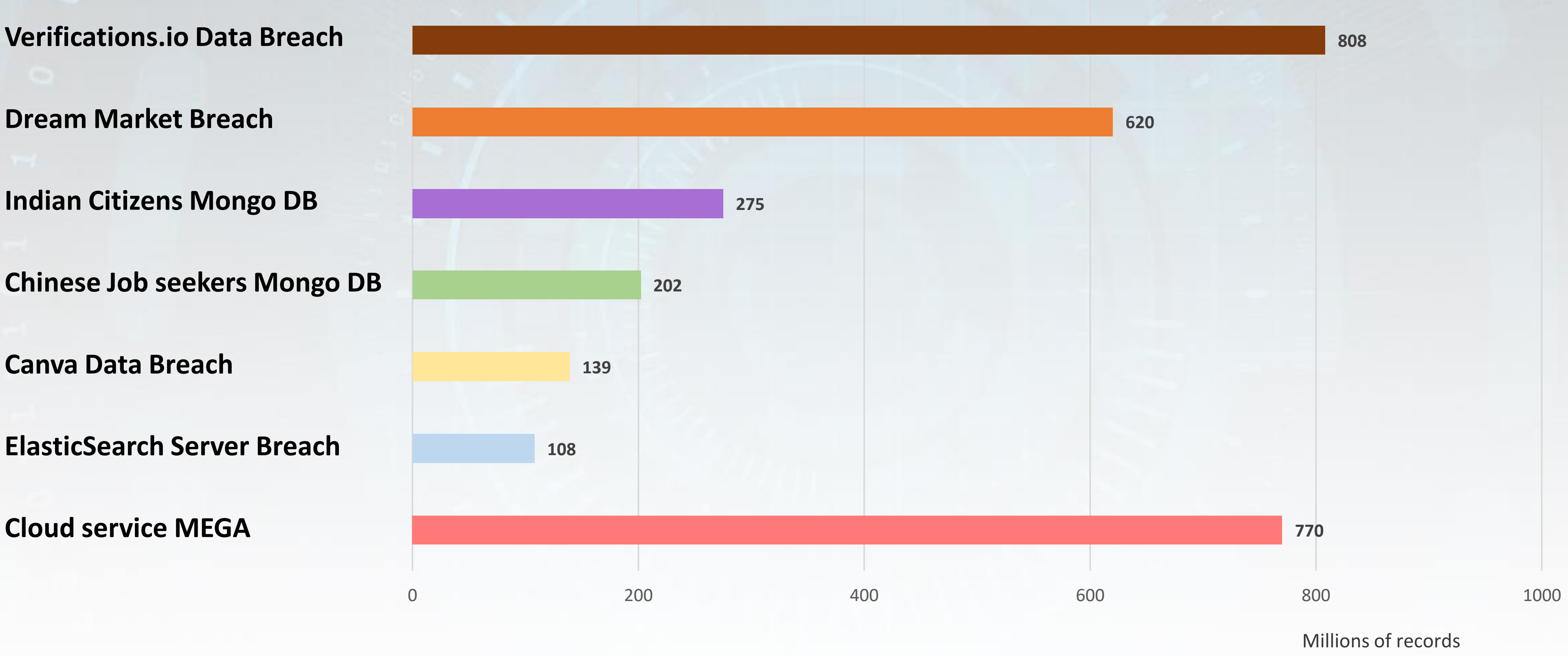
# *Main Cyber Security Incidents in 2019 - 2021*

ENISA Threat Landscape 2020

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

# Top Data Breaches Incidents



*Source: ENISA "Threat Landscape 2020"*

Funded by the Erasmus+ Programme of the European Union

# Data Breaches: Main Consequences

**Loss of information:** If a data breach has resulted in the loss of sensitive personal data, the consequences can be devastating

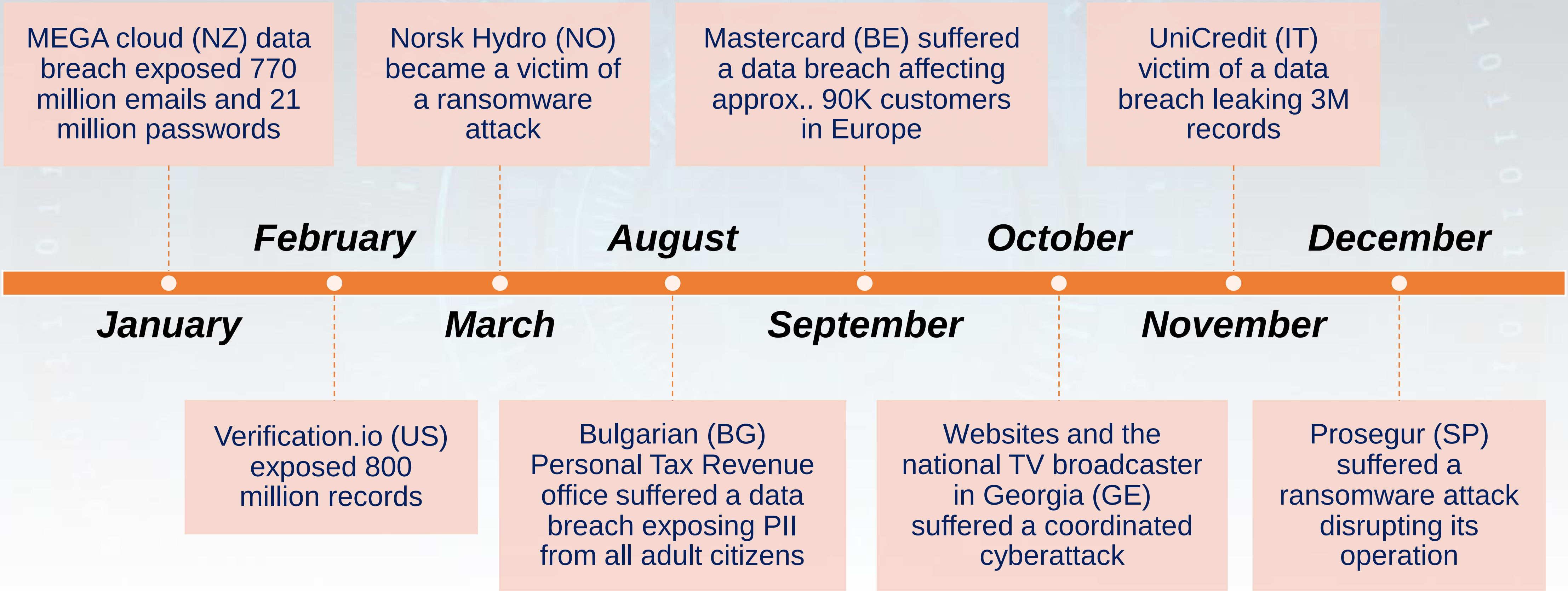
**Lawsuits and penalties**: The emergence of regulatory and class-action lawsuits against firms that fail to protect data, and new laws -- such as the EU's GDPR, can be used to impose heavy penalties

**Additional investments:** Organisations may need to spend funds on repairing systems and upgrading architectures as well as invest in new cybersecurity services and cyber forensics

**Damage to reputation:** A Forbes Insight report found that 46% of organisations had suffered reputational damage as a result of a data breach

Funded by the
Erasmus+ Programme
of the European Union

# *Main Cybersecurity Incidents in 2019*



***January***

MEGA cloud (NZ) data breach exposed 770 million emails and 21 million passwords

***February***

Verification.io (US) exposed 800 million records

***March***

Norsk Hydro (NO) became a victim of a ransomware attack

***August***

Bulgarian (BG) Personal Tax Revenue office suffered a data breach exposing PII from all adult citizens

***September***

Mastercard (BE) suffered a data breach affecting approx.. 90K customers in Europe

***October***

Websites and the national TV broadcaster in Georgia (GE) suffered a coordinated cyberattack

***November***

UniCredit (IT) victim of a data breach leaking 3M records

***December***

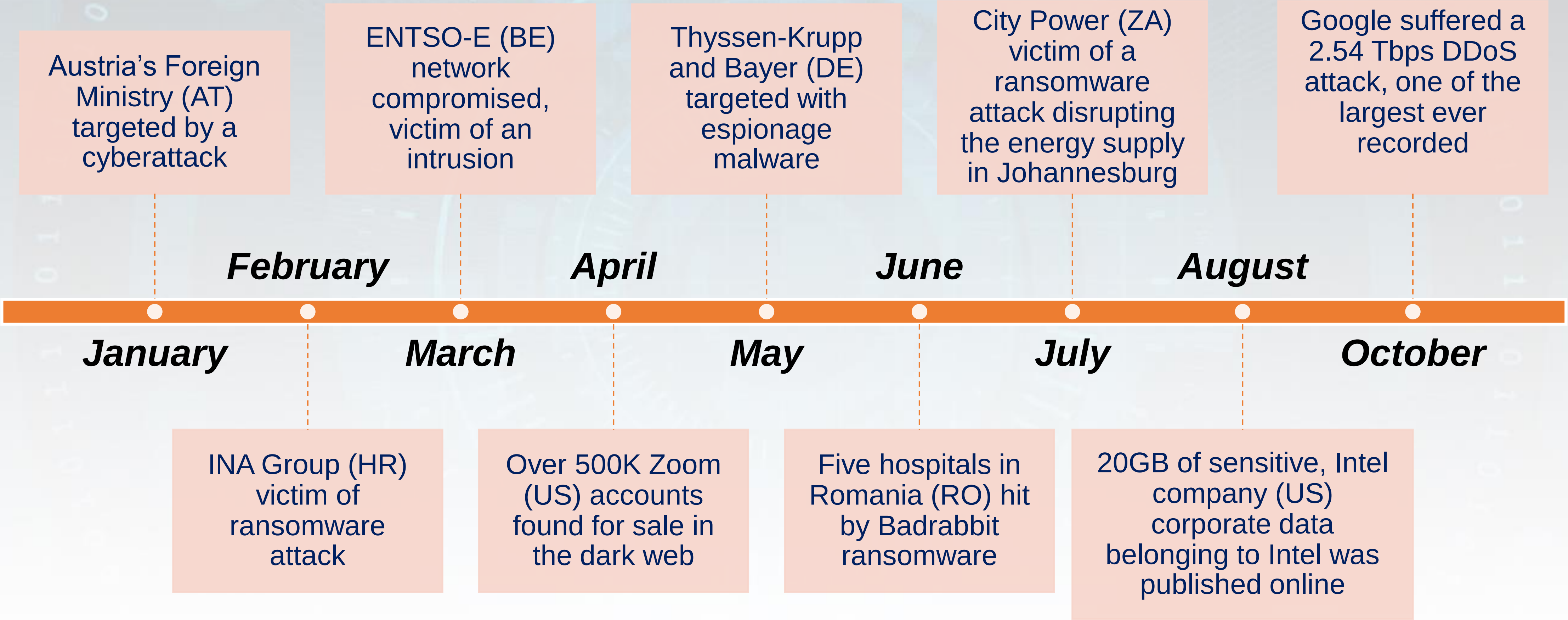
Prosegur (SP) suffered a ransomware attack disrupting its operation

CyberPhish

Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

# Main Cybersecurity Incidents in 2020



**January**

Austria's Foreign Ministry (AT) targeted by a cyberattack

**February**

INA Group (HR) victim of ransomware attack

**March**

ENTSO-E (BE) network compromised, victim of an intrusion

**April**

Over 500K Zoom (US) accounts found for sale in the dark web

**May**

Thyssen-Krupp and Bayer (DE) targeted with espionage malware

**June**

Five hospitals in Romania (RO) hit by Badrabbit ransomware

**July**

City Power (ZA) victim of a ransomware attack disrupting the energy supply in Johannesburg

**August**

20GB of sensitive, Intel company (US) corporate data belonging to Intel was published online

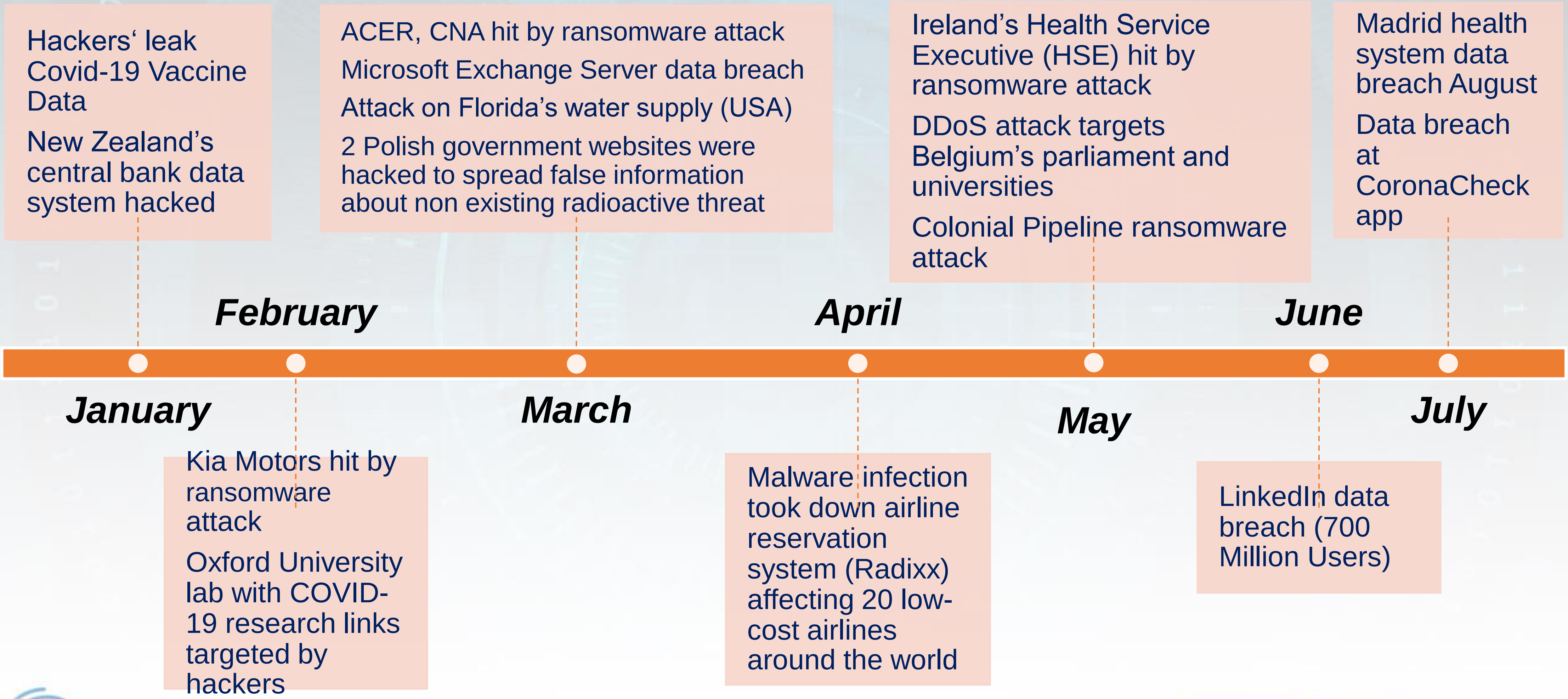
**October**

Google suffered a 2.54 Tbps DDoS attack, one of the largest ever recorded

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

# Example of Cybersecurity Incidents in 2021



**January**

Hackers‘ leak Covid-19 Vaccine Data

New Zealand’s central bank data system hacked

**February**

Kia Motors hit by ransomware attack

Oxford University lab with COVID-19 research links targeted by hackers

**March**

ACER, CNA hit by ransomware attack

Microsoft Exchange Server data breach

Attack on Florida’s water supply (USA)

2 Polish government websites were hacked to spread false information about non existing radioactive threat

**April**

Malware infection took down airline reservation system (Radixx) affecting 20 low-cost airlines around the world

**May**

Ireland’s Health Service Executive (HSE) hit by ransomware attack

DDoS attack targets Belgium’s parliament and universities

Colonial Pipeline ransomware attack

**June**

LinkedIn data breach (700 Million Users)

**July**

Madrid health system data breach August

Data breach at CoronaCheck app

CyberPhish

Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

# *Six Ways Cybercrime Affect Business*

- Increased Costs
- Operational Disruption
- Altered Business Practices
- Reputational Damage
- Lost Revenue
- Stolen Intellectual Property

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

# *Most Targeted Sectors 2019-2020*

Digital Services

Government Administration

Technology Industry

Financial industry

Healthcare industry

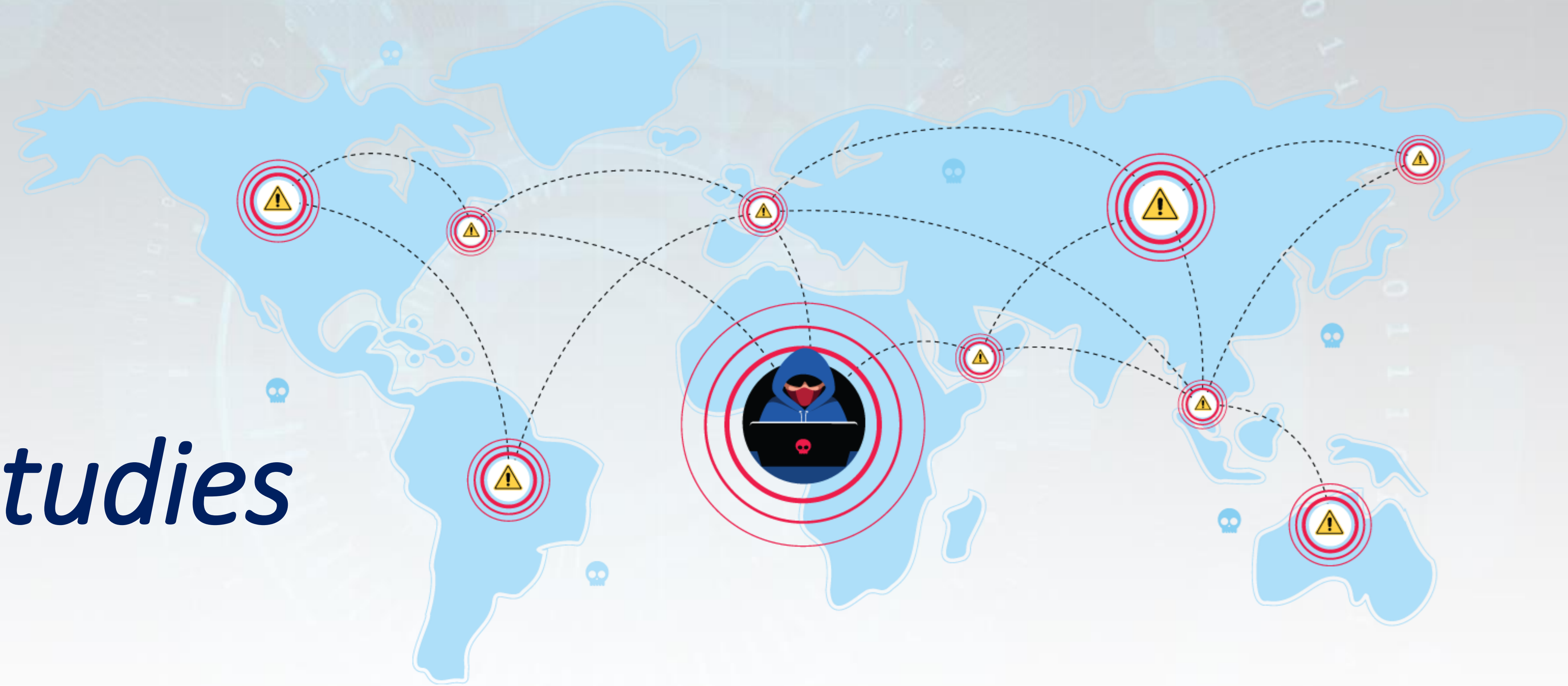
CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

# *Most popular phishing themes 2020*

- COVID-19
- REMOTE WORK
- ECOMMERCE
- RETAIL
- GAMING

Funded by the
Erasmus+ Programme
of the European Union



# Case Studies

Year 2020

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

# *Twitter*

Some of the most recognized and highly regarded global Twitter handles were compromised and used to **fraudulently tweet about Bitcoin**

Source: https://www.freepik.com/

Funded by the
Erasmus+ Programme
of the European Union

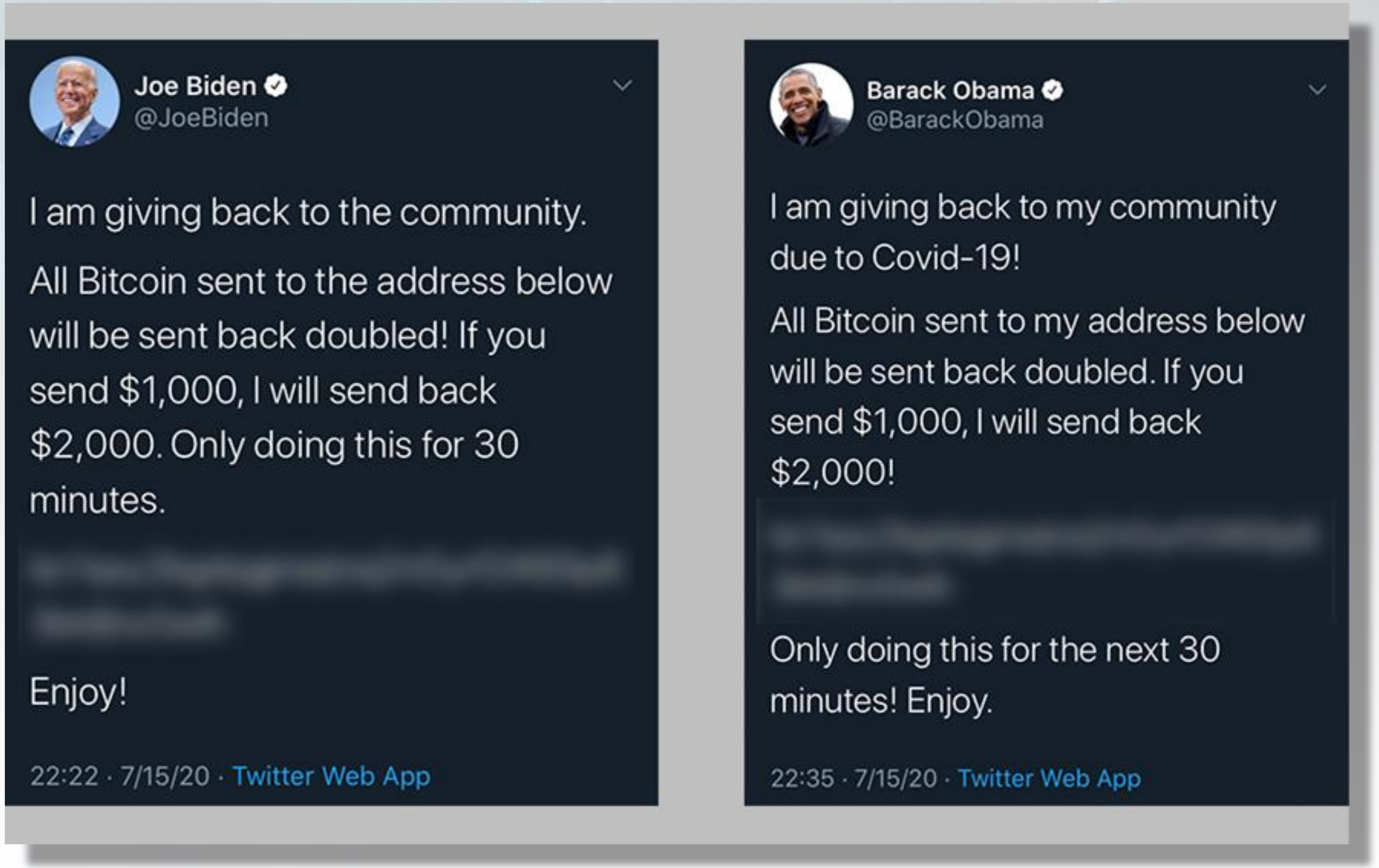
# *How It Was Done?*

- Perpetrators used a phone **spear phishing** attack to obtain the credentials of Twitter employees who had access to internal support tools
- Twitter issued a statement saying
  - *"We detected what we believe to be a coordinated social engineering attack by people who successfully targeted some of our employees with access to internal systems and tools"*
- Several suspects have been charged in relation to this attack

Funded by the
Erasmus+ Programme
of the European Union

# *Users Targeted*

Apple and Uber were among the company accounts targeted, as well as Bill Gates, Elon Musk, Jeff Bezos, Warren Buffett, Kanye West and Floyd Mayweather



Joe Biden
@JoeBiden

I am giving back to the community.

All Bitcoin sent to the address below will be sent back doubled! If you send $1,000, I will send back $2,000. Only doing this for 30 minutes.

[redacted]

Enjoy!

22:22 · 7/15/20 · Twitter Web App

Barack Obama
@BarackObama

I am giving back to my community due to Covid-19!

All Bitcoin sent to my address below will be sent back doubled. If you send $1,000, I will send back $2,000!

[redacted]

Only doing this for the next 30 minutes! Enjoy.

22:35 · 7/15/20 · Twitter Web App

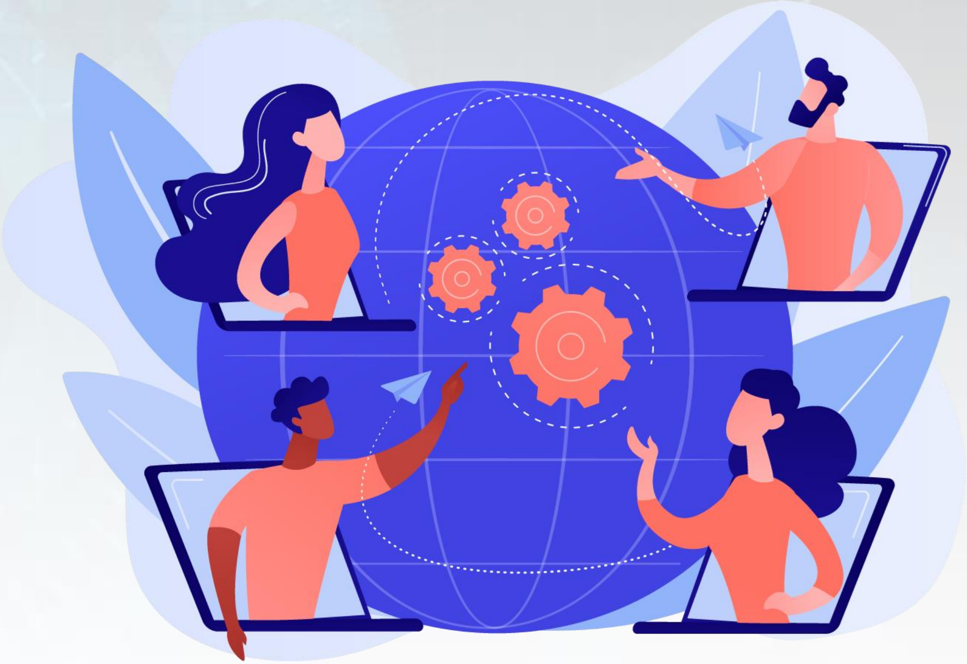
Source: BBC  News

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

zoom

Zoom did experience several security incidents, notably the approximately **500,000 user accounts that emerged for sale on a dark web forum**



Source: https://www.freepik.com/

Funded by the Erasmus+ Programme of the European Union

# *How It Was Done?*

Reportedly, the accounts were obtained by using user IDs and passwords that were exposed in previous breaches, which is also known as **credential stuffing**

Hackers could then gain access to important personal or corporate information that should have been kept secure. In addition, Zoom codes were easily guessable, so users could join meetings without an invitation and interrupt or share inappropriate materials, also known as **Zoom bombing**

Funded by the Erasmus+ Programme of the European Union

# *Greek Banks*

After a Greek travel website was hacked, Greece's four main banks followed security protocols and had to cancel and replace approximately 15,000 customer credit or debit cards

Source: https://www.freepik.com/

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

# *How Was It Done?*

- No definite answer
- A key source of the inquiry is whether or not the tourist website followed the Payment Card Industry Data Security Standards (PCI DSS)
- This is not the first time Greek banks are targeted – previously they have experienced DDoS and ransomware attacks, causing disruption to bank activities such as online banking

Funded by the Erasmus+ Programme of the European Union

# *Hospital in Czech Republic*

The Brno University Hospital in the city of Brno, Czech Republic, has been hit by a cyberattack right in the middle of a COVID-19 outbreak

Source: https://www.freepik.com/

Hospital needed to:

- *postpone urgent surgical interventions and re-route new acute patients to nearby St. Anne's University Hospital*
- *shut down its entire IT network during the incident*

Funded by the
Erasmus+ Programme
of the European Union

# *Summary*

- The sophistication of threat capabilities increased in 2019, with many cyber criminals  using exploits, credential stealing, and multistage attacks
- The number of data breach incidents remains very high, and the amount of stolen financial information and user credentials is growing
- ENISA predicts that in upcoming decade, cybersecurity risks and threats will become harder to detect and assess due to the growing complexity of the threat landscape and expansion of the attack surface

Funded by the Erasmus+ Programme of the European Union

# *Assignments*

Take a look at the case studies provided

- *Discuss what kind of possible consequences could happen to both companies attacked and the users?*
- *Discuss what cybersecurity incident trends we see in 2021? What should we expect for upcoming years?*
- *Discuss the importance of upskilling in the view of the possible risks brought by cyber attacks*

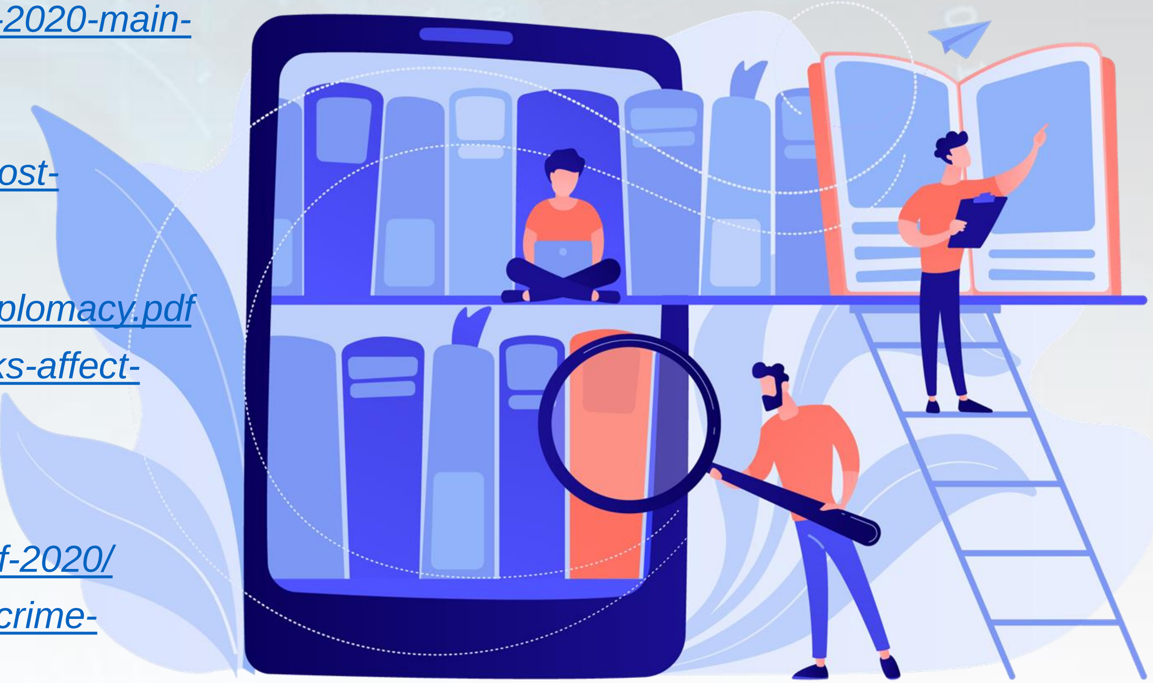
Funded by the Erasmus+ Programme of the European Union

# Further Reading

## Overview on the Tendencies of Cybersecurity Landscape

Material used in preparation of this lecture

- https://www.enisa.europa.eu/publications/year-in-review
- https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents
- https://www.enisa.europa.eu/publications/emerging-trends
- https://www.zdnet.com/article/todays-mega-data-breaches-now-cost-companies-392-million-in-damages-lawsuits/
- https://www.swp-berlin.org/publications/products/comments/2021C16_EUCyberDiplomacy.pdf
- https://www.securelink.com/blog/reputation-risks-how-cyberattacks-affect-consumer-perception/
- https://www.hiscox.co.uk/sites/uk/files/documents/2020-06/Hiscox_Cyber_Readiness_Report_2020_UK.PDF
- https://www.zdnet.com/article/the-biggest-hacks-data-breaches-of-2020/
- https://www.investopedia.com/financial-edge/0112/3-ways-cyber-crime-impacts-business.aspx
- https://www.isaca.org/resources/news-and-trends/industry-news/2020/top-cyberattacks-of-2020-and-how-to-build-cyberresiliency
- https://auth0.com/blog/what-is-credential-stuffing/



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

# *Short Videos*

- Martin Casado “The Latest in Cyber Attacks”

  ***[https://youtu.be/AQP0On85ZdQ](https://youtu.be/AQP0On85ZdQ)***

- The 5 Most Dangerous New Attack Techniques and How to Counter Them

  ***[https://youtu.be/xz7IFVJf3Lk](https://youtu.be/xz7IFVJf3Lk)***

- Ten Cyber Security Trends

  ***[https://youtu.be/kkP9URO8XJ8](https://youtu.be/kkP9URO8XJ8)***

Funded by the Erasmus+ Programme of the European Union

# Thank you!