Cyber Skills

Project Title: Cyber Skills

Ref. Number: 2021-1-CZ01-KA210-ADU-000035011

Rovnovazka, o.s.
Czech Republic

APS Brainery Academy
Italy

E-SCHOOL EDUCATIONAL
GROUP – Greece

Esquare
France

Co-funded by
the European Union

What is Social Engineering (and Phishing)?

Co-funded by
the European Union

Cyber Skills

What is Social Engineering (and Phishing)?

Social engineering refers to the manipulation and deception techniques used by individuals to exploit human psychology and manipulate others into performing actions or revealing sensitive information. It is a non-technical method employed to gain unauthorized access to systems, data, or confidential information.

Social engineers exploit various aspects of human behavior, including trust, authority, curiosity, greed, or helpfulness, to deceive their targets. They typically rely on psychological manipulation rather than technical skills to achieve their objectives.

Co-funded by
the European Union

Common techniques used in social engineering include:

1.Pretexting

2.Phishing

3.Baiting

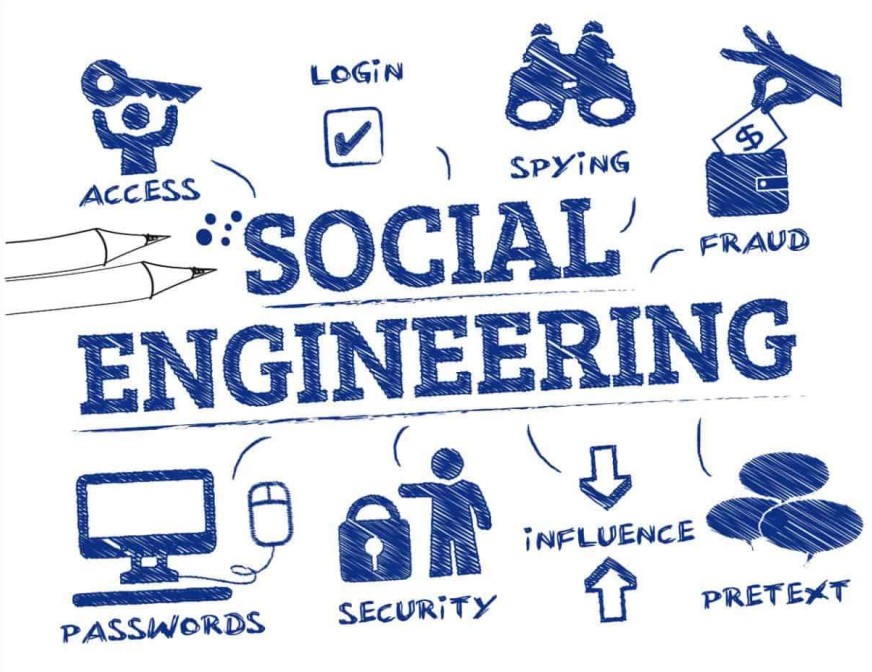
4.Impersonation

5.Reverse Social Engineering

Co-funded by the European Union

Cyber Skills

How Can We Protect Ourselves from Social Engineering?



Co-funded by the European Union

Cyber Skills

To protect against social engineering, it is essential to:

1. Be very skeptical
2. Practice caution online
3. Educate and raise awareness
4. Implement security measures
5. Report incidents

Co-funded by
the European Union

Cyber Skills

Software to Use to Avoid Social Engineering

Co-funded by
the European Union

Cyber Skills

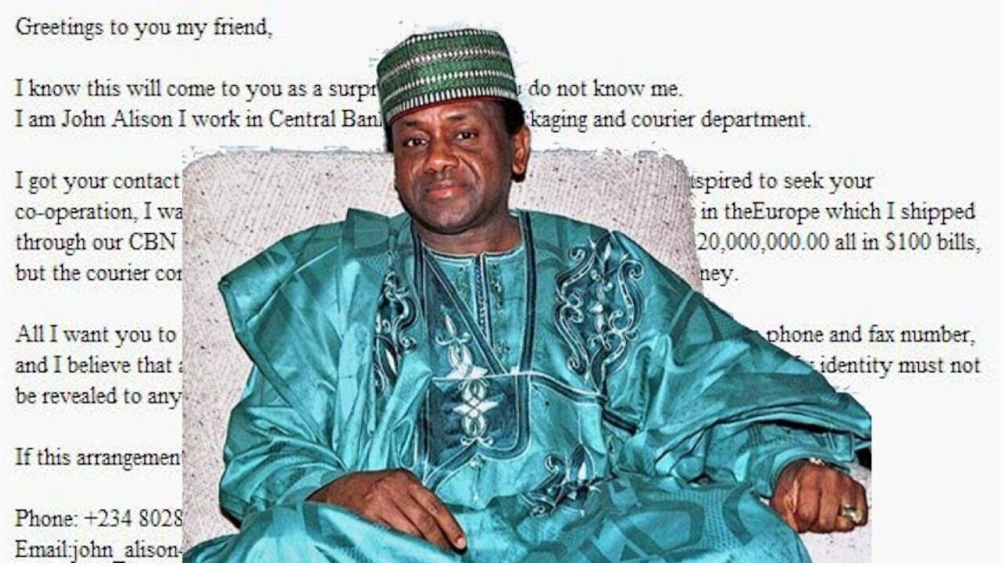
So, here is some software we can use to protect ourselves:

- Antivirus program
- Adblock
- Web-Of-Trust (WOT)
- Microsoft Office 365 Defender
- Virtual Machine (VM) Software
- ChatGPT
- Watch The Hater (2020)
- Linux! But not really.
- https://haveibeenpwned.com/

Co-funded by
the European Union

Cyber Skills

Common Phishing Messages to Avoid:



Co-funded by
the European Union

Cyber Skills

here are some common types of phishing messages you should learn to avoid:

1. Account Verification:
2. Urgent Threats or Security Alerts
3. Lottery or Prize Scams
4. Financial Requests or Charity Scams
5. Financial Requests or Charity Scams
6. Fake Shipping or Delivery Notifications
7. Employment Opportunities or Work-from-Home Scams
8. Suspicious/Strange messages from people you know

Co-funded by the European Union

Cyber Skills

Legal “Solutions” After Being Phished

1. Report the incident
2. Notify your bank or financial institution
3. Notify credit bureaus
4. Consult with an attorney
5. Civil litigation
6. Work with law enforcement and regulatory agencies

Co-funded by
the European Union

Cyber Skills


thank
you