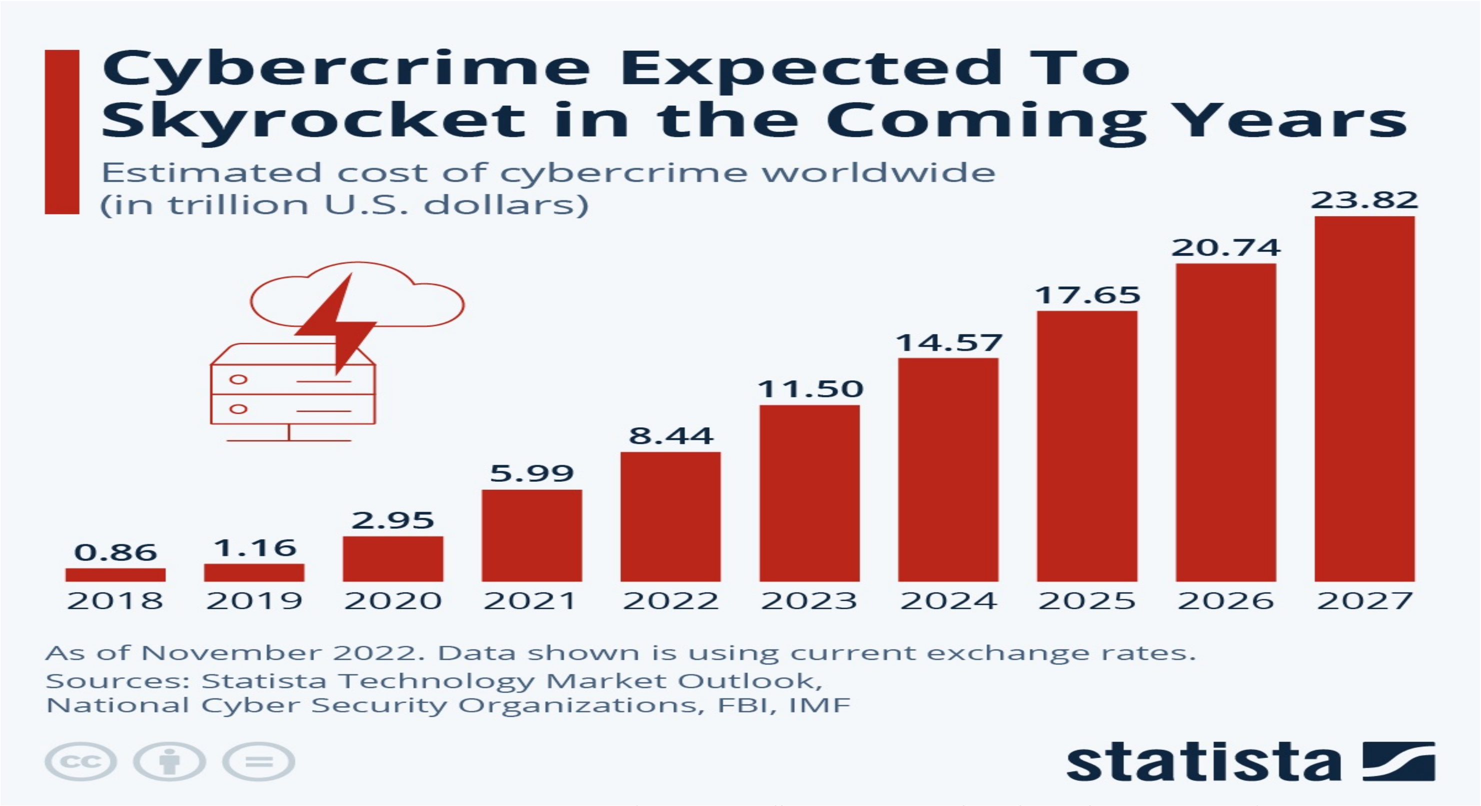
Information Security

User Awareness and Practices

JOSEPH BUGEJA

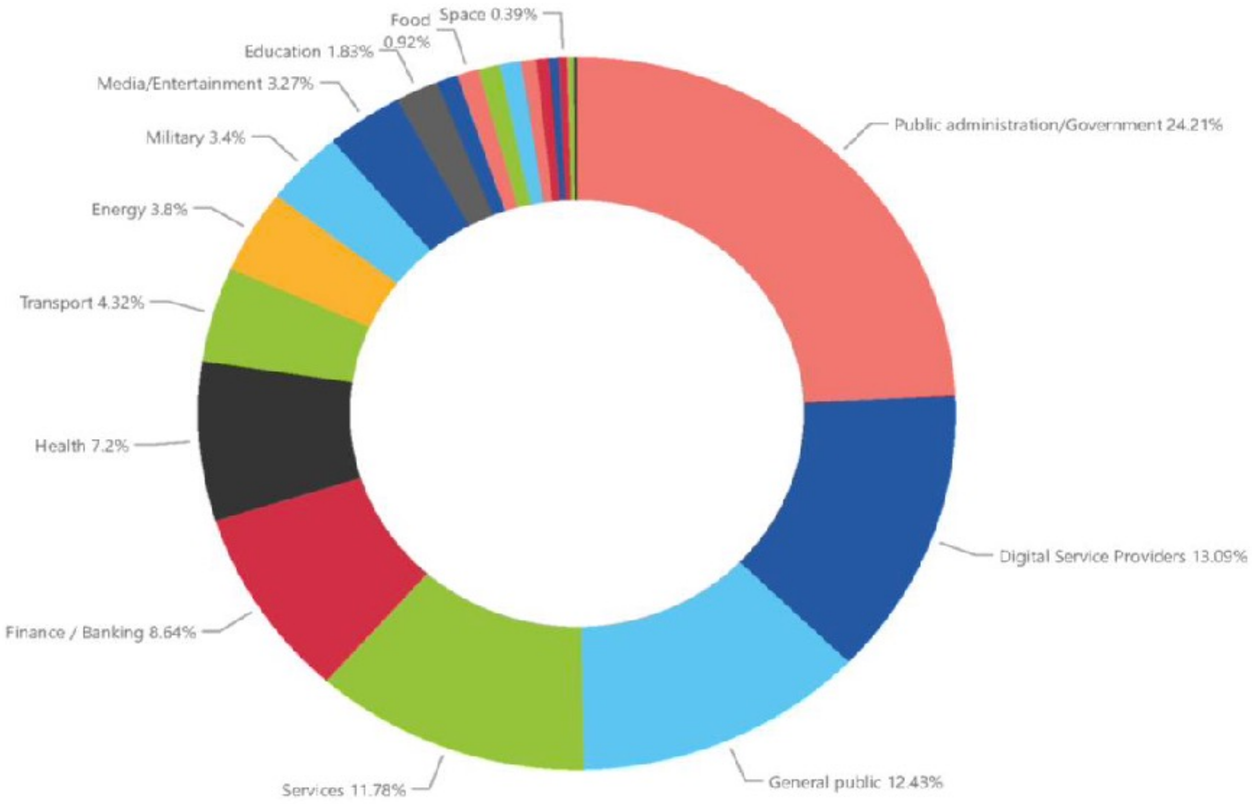
MALMÖ UNIVERSITET

Global Cybercrime Damage Costs



Source: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027

Incidents By Sector – Jul '21 to Jun '22

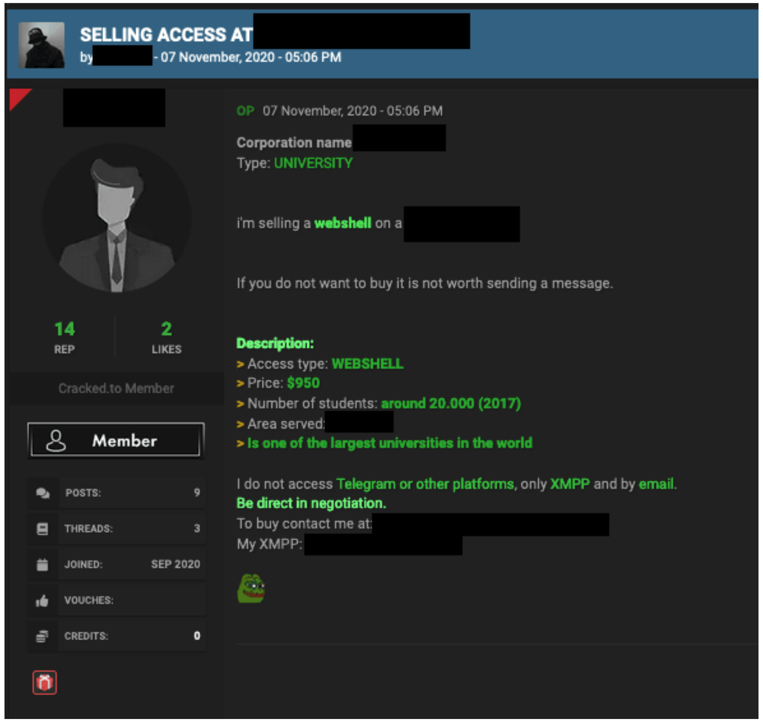


Source: ENISA Threat Landscape 2022.

MALMÖ UNIVERSITET

Information Security Threat Actors and Trends

- State-sponsored actors
- Cybercrime actors
- Hacker-for-hire actors
- Hacktivists



SELLING ACCESS AT [redacted]
by [redacted] - 07 November, 2020 - 05:06 PM

[redacted]

14 REP | 2 LIKES

Cracked.to Member

Member

POSTS: 9
THREADS: 3
JOINED: SEP 2020
VOUCHES:
CREDITS: 0

OP 07 November, 2020 - 05:06 PM

Corporation name [redacted]
Type: UNIVERSITY

i'm selling a **webshell** on a [redacted]

If you do not want to buy it is not worth sending a message.

Description:
> Access type: WEBSHELL
> Price: $950
> Number of students: **around 20.000 (2017)**
> Area served: [redacted]
> **Is one of the largest universities in the world**

I do not access Telegram or other platforms, only XMPP and by email.
Be direct in negotiation.
To buy contact me at: [redacted]
My XMPP: [redacted]

Prime Threats (2022)

Server-side

- Ransomware
- Malware
- Threats Against Data
- Denial-of-Service
- Supply Chain Attacks

Client-side

- Social Engineering
- Internet Threats
- Disinformation / Misinformation

Malware

- Malware is an overarching term used to describe any software or firmware intended to perform an unauthorized process adversely affecting a system
- Malware has seen an increase over the past two years
- Examples of malware include:
  - Viruses
  - Worms
  - Trojan horses
  - Spyware
  - Ransomware

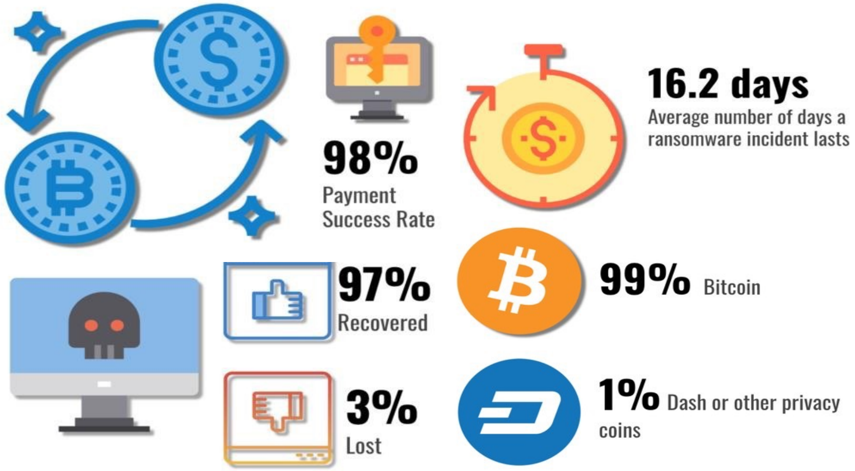
MALMÖ UNIVERSITET

Ransomware

- In 2022, ransomware has continued its upward trend

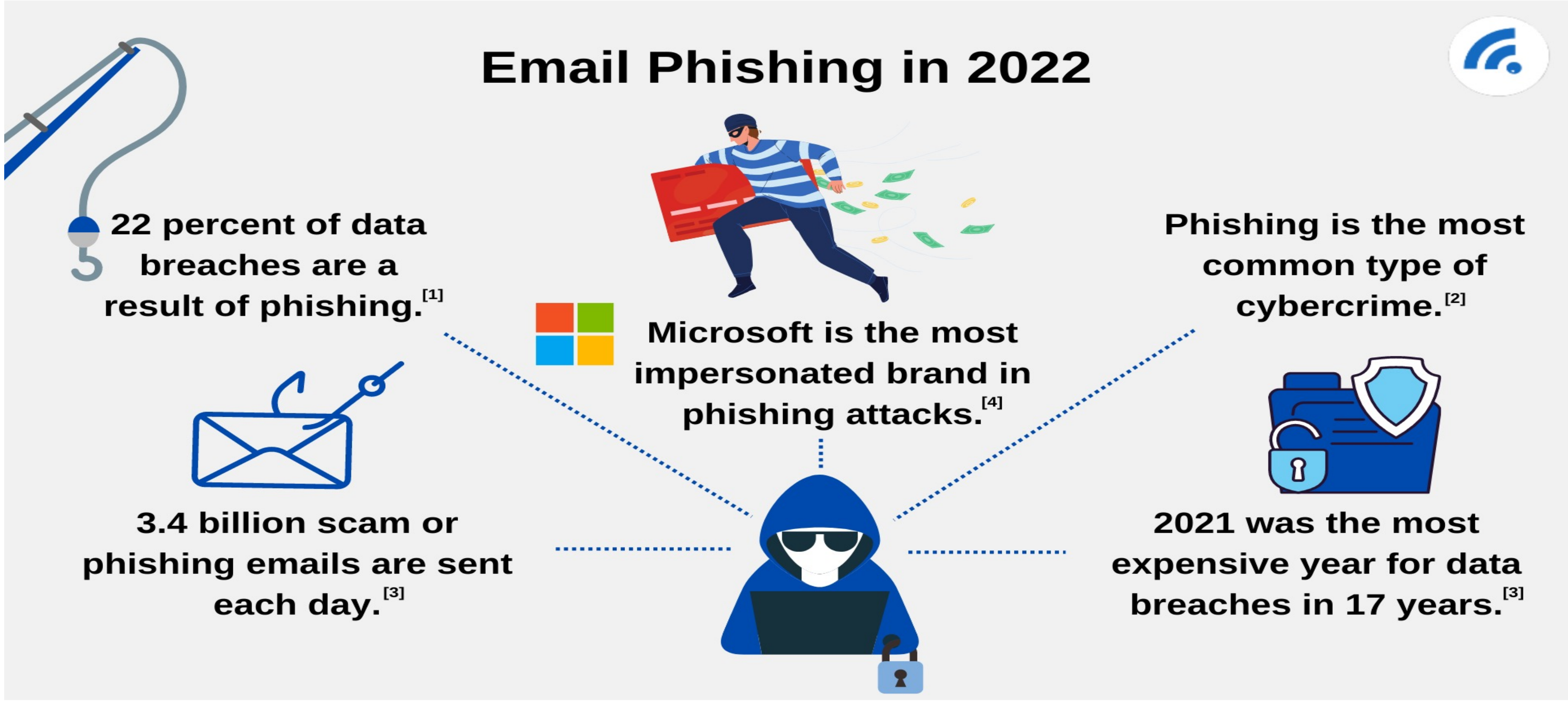
- Ransomware is a type of malware that restricts a person’s access to systems and files, typically by encryption and then demands a ransom to restore access

- Often, systems are infected by ransomware through a link in a malicious email



Phishing

A seemingly trustworthy entity asks for sensitive information, e.g., passwords, via e-mail



Email Phishing in 2022

22 percent of data breaches are a result of phishing.[1]

Microsoft is the most impersonated brand in phishing attacks.[4]

Phishing is the most common type of cybercrime.[2]

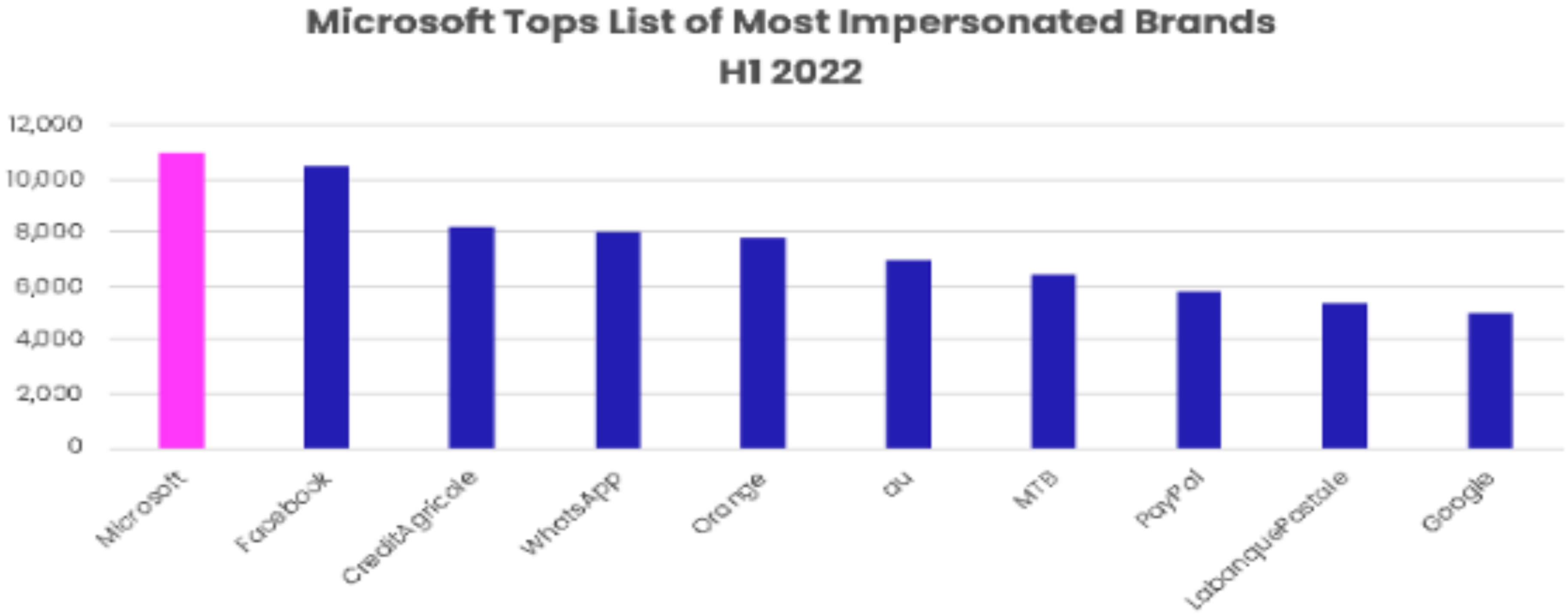
3.4 billion scam or phishing emails are sent each day.[3]

2021 was the most expensive year for data breaches in 17 years.[3]

Source: https://www.broadbandsearch.net/blog/popular-email-phishing-scams

OpenAI’s ChatGPT can be used to write sophisticated phishing emails

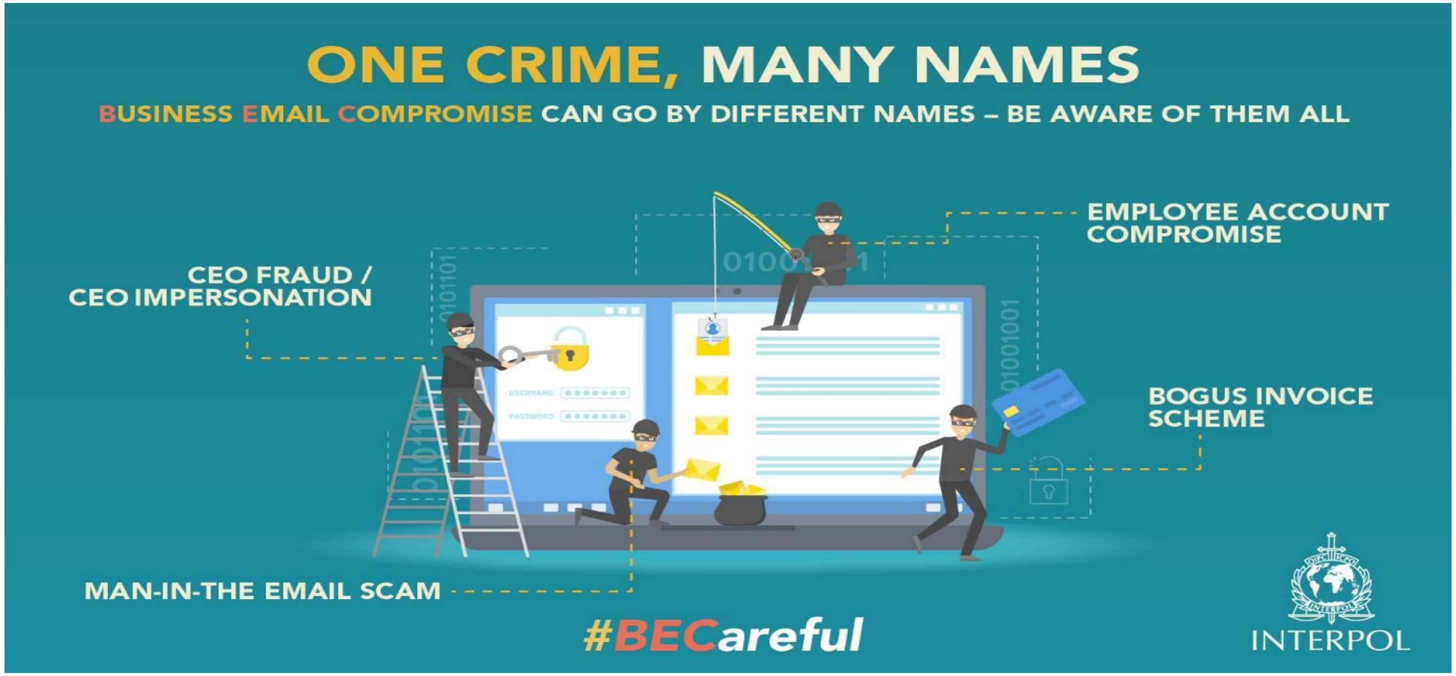
Phishing



Source: https://www.vadesecure.com/en/blog/phishers-favorites-top-25-h1-2022

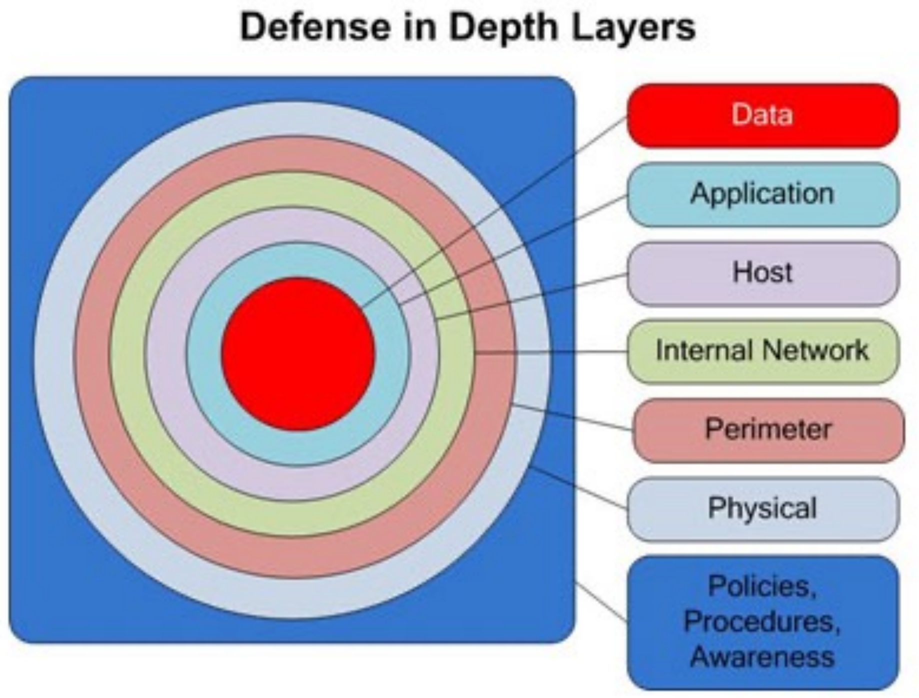
Business Email Compromise

The costliest crime recorded by the FBI was business email compromise and personal email compromise. In 2021, almost $2.4 billion were lost this way.


ONE CRIME, MANY NAMES
BUSINESS EMAIL COMPROMISE CAN GO BY DIFFERENT NAMES – BE AWARE OF THEM ALL
EMPLOYEE ACCOUNT COMPROMISE
CEO FRAUD / CEO IMPERSONATION
BOGUS INVOICE SCHEME
MAN-IN-THE EMAIL SCAM
#BECareful
INTERPOL

Best Practices to Avoid these Threats

Defense in depth uses multiple layers of defense to address technical, personnel and operational issues



Defense in Depth Layers

Data

Application

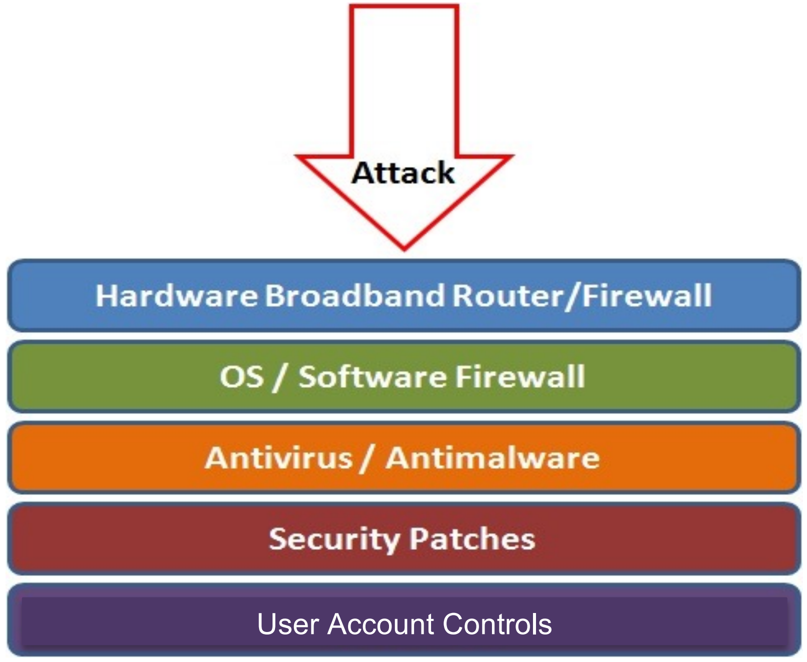
Host

Internal Network

Perimeter

Physical

Policies, Procedures, Awareness



Attack

Hardware Broadband Router/Firewall

OS / Software Firewall

Antivirus / Antimalware

Security Patches

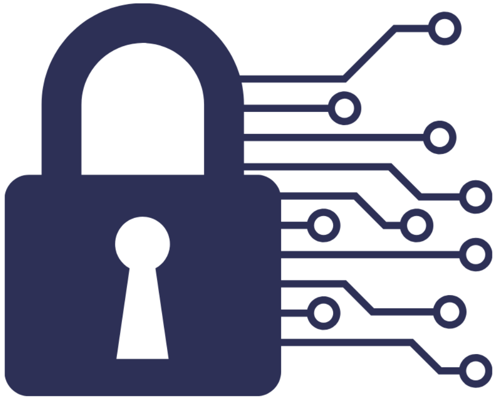
User Account Controls

Backup Important Information

- No security measure is 100% reliable
- Even the best hardware fails
- What information is important to you?
- Is your backup:
  - ➢ Recent?
  - ➢ Off-site & Secure?
  - ➢ Process Documented?
  - ➢ Encrypted?
  - ➢ Tested?

Preventing Supply Chain Attacks

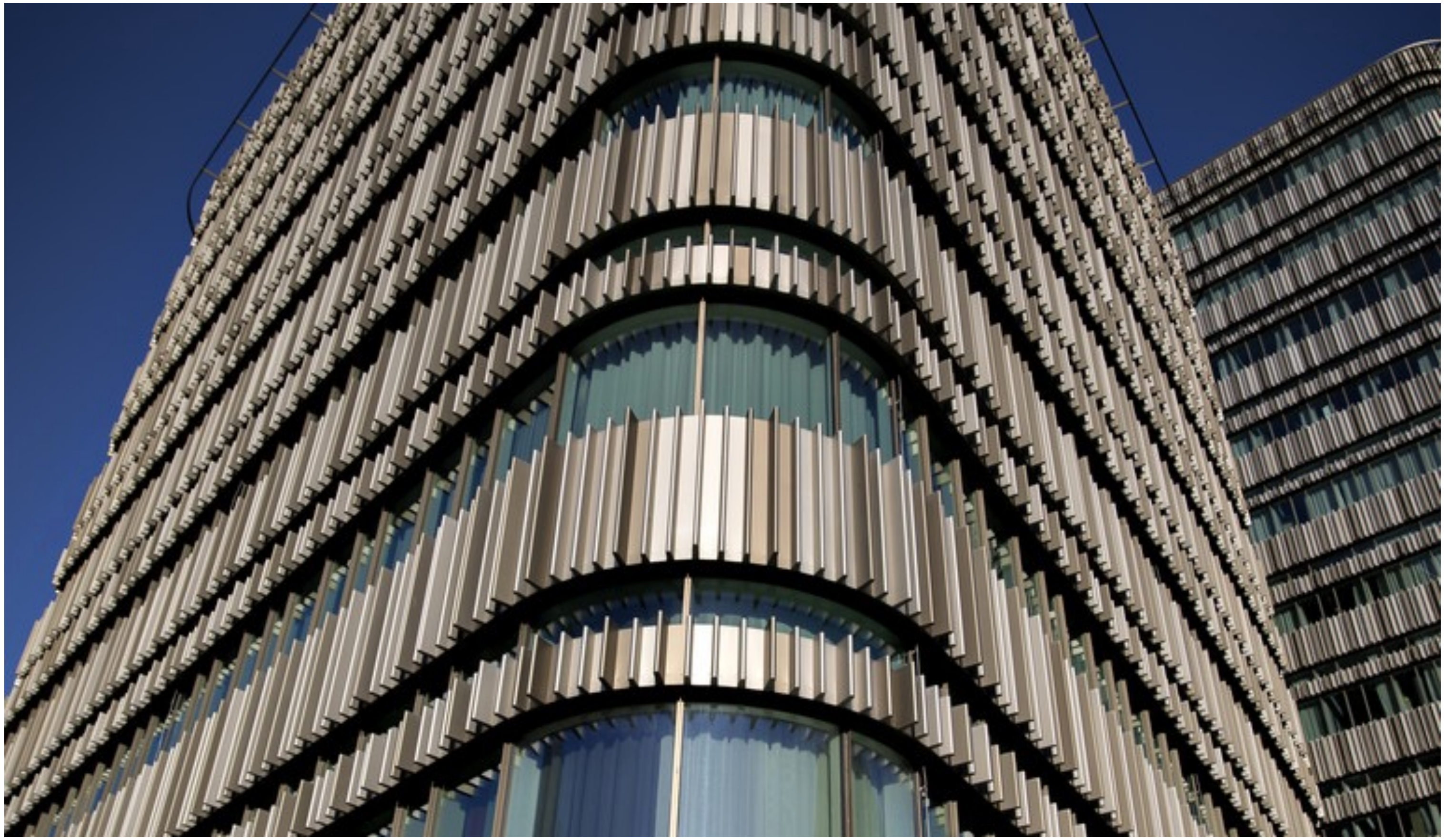
- Secure Privileged Access Management
- Implement a Zero Trust Architecture
- Minimize Access to Sensitive Data
- Send Regular 3rd Party Risk Assessments
- Monitor Vendor Network for Vulnerabilities



Information Security Starts and Ends With Us!

Commit to a disciplined practice of information security and continue to keep yourself updated to avoid being a weak link in the security defenses

Thank You For Your Attention!



Joseph Bugeja

joseph.bugeja@mau.se

MALMÖ UNIVERSITET