

# securitylabs

## INTRODUCTION TO CYBERSECURITY

Aleksander Gorkowienko

Senior Managing Consultant  
Spirent Communications

# Agenda

## Our meeting today



1. Hacking: origins, terminology, motivation
2. Computer networking 101
3. Why can we all be hacked?
4. Where are the security vulnerabilities coming from?
5. Common types of attacks (viruses, worms, botnets, APT, etc.)
6. How you or your company can be hacked?
7. Hackers' methodology and tools
8. Let's talk about phishing
9. Penetration testing vs hacking
10. What to do to prevent the disaster?
11. Q&A



# Introduction

---



# Disclaimer

- This course is for educational purposes only. It is intended to provide an insight into hacking for defensive purposes.
- This course is not an endorsement to undertake illegal or malicious activity in any form, unless such activity is properly authorised and you have obtained permission to do so.
- Spirent SecurityLabs takes no responsibility for any damage sustained to computer data, software or hardware through the use or misuse of tools referenced by this course.
- At the time of writing, Spirent SecurityLabs believes all information to be correct.
- Training material is (c) Spirent SecurityLabs and is for your own personal use only. The copying, recording, transcribing or photographing of any course materials, computer programs, computer code or digital information produced or supplied as part of any course is prohibited.

# Introduction to Cybersecurity

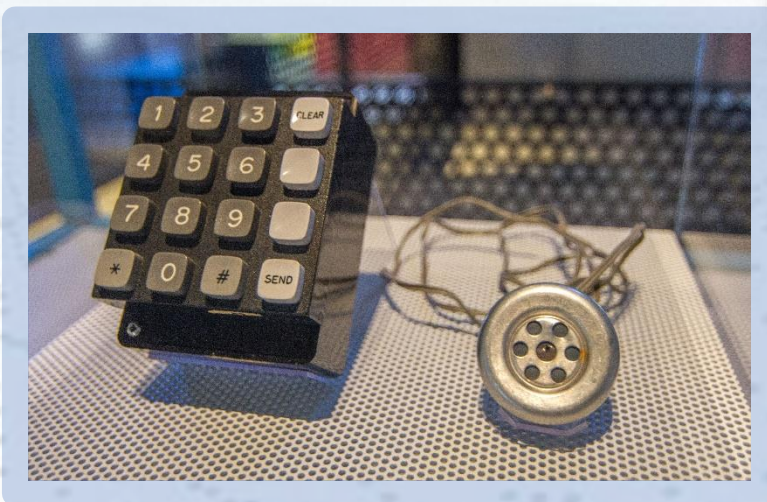
---

# Hacking origins

- Phreaking began as a hack for **getting free phone calls** by tricking phone companies back in the '60s to '70s.
- Hacking Cap'n Crunch cereal boxes in the late-1960s
- Blue boxes: first “automated” hacking tools



1. Dial a toll-free 1-800 number to get through a trunk line without getting charged.
2. Once the call goes through the toll-free number, play a **2600 Hz tone** from your whistle (or the “blue box” device or anything that produces a 2600Hz tone).
3. The 2600Hz tone will cause the trunk to hang up but it won't drop the call completely. As far as the telephone exchange knows, you're still on call with that toll-free number.
4. Dial the number you actually want to call. Since the telephone exchange thinks you're still on a toll-free call, you won't get charged.



**Blue box** designed and built by Steve Wozniak and sold by Steve Jobs before they founded Apple. Displayed at the Powerhouse Museum, from the collection of the Computer History Museum



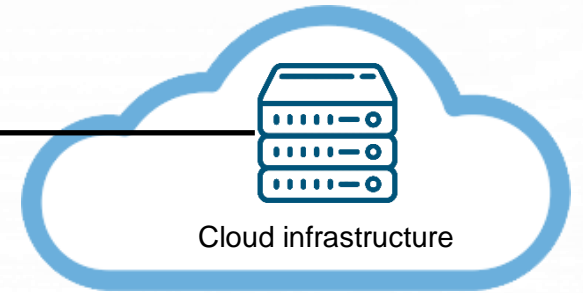
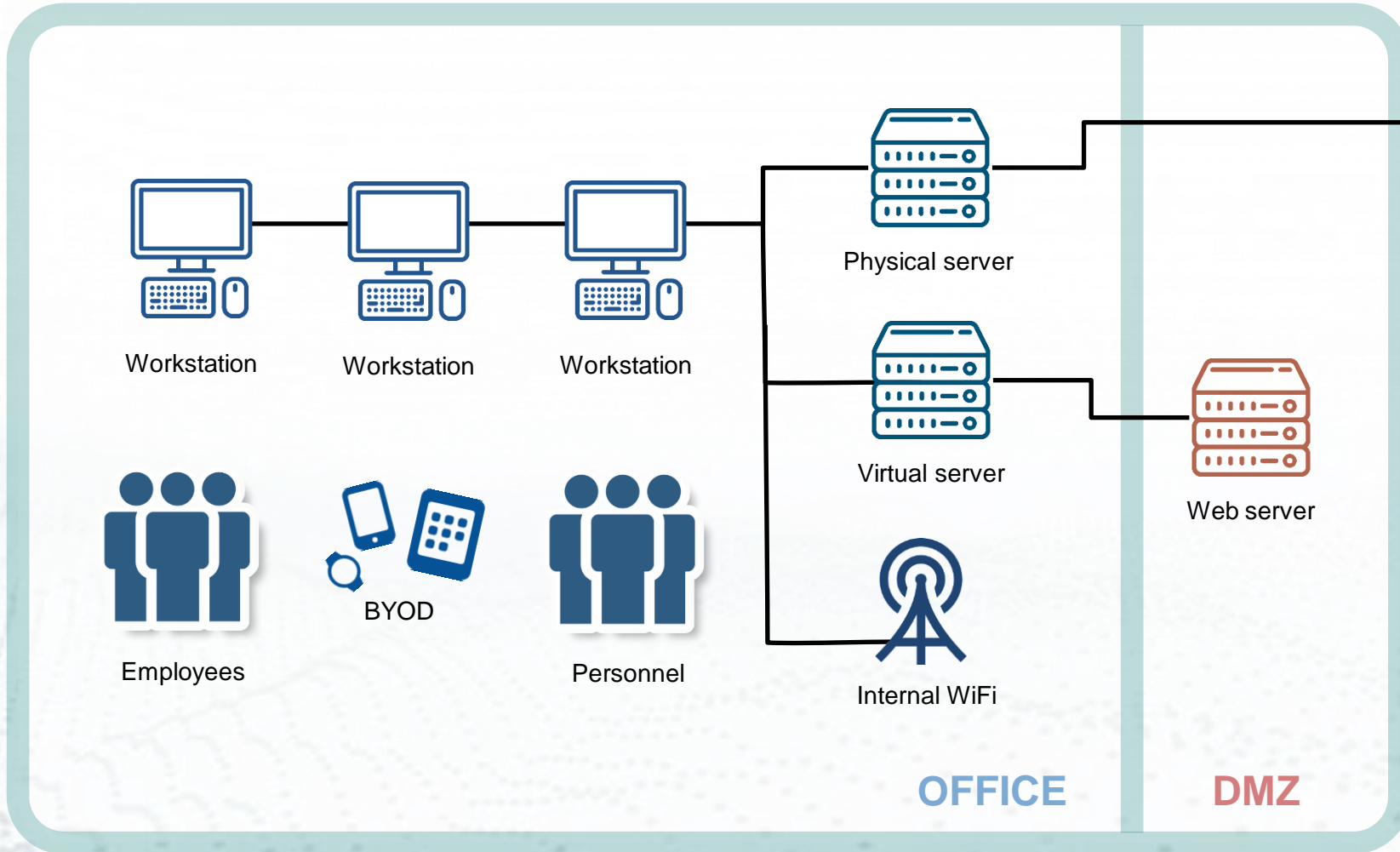
# Hacking origins (rewind it back)

The story goes back in time even more...

- The world's first national data network was constructed in France during the 1790s.
- Towers with different configurations of movable wooden arms = letters, numbers and other characters. Messages could now be sent much faster than letters, whizzing from one end of France to the other in minutes.
- The network was reserved for government use but in 1834 two bankers, François and Joseph Blanc, found a way to subvert it for their benefit.
- The Blanc brothers traded government bonds at the exchange in the city of Bordeaux, where information about market movements took several days to arrive from Paris (by coach). Traders who could get the information more quickly could make money by anticipating these movements!
- Blanc brothers **bribed the telegraph operator in the city of Tours to introduce deliberate errors** (included an additional “backspace” symbol) into routine government messages being sent over the network.
- The scam was only uncovered in 1836 (two years later). Blanc brothers were put on trial, though **they could not be convicted because there was no law against misuse of data networks**. The Blancs' pioneering misuse of the French network qualifies as the **world's first cyber-attack**.



# Computer networking 1-0-1



External users and customers





# Why can we all get hacked

## What is the “trophy”?



Motives in External actors by org size 2022 (by Verizon DBIR report)

There are multiple reasons why our IT systems could be under attack:

- Clear **financial gain** (e.g., an attempt to resell the stolen information, blackmail or get rid of the competitor)
- Access to sensitive information (e.g., corporate or nation-sponsored espionage). This information can be sold on black market.
- Disruption of communication
- Disruption of the critical national infrastructure (CNI)
- Hacktivism
- Political or ideological reasons
- Terrorist activities, blackmailing
- Fun/challenge



From FireEye M-Trends 2021 report

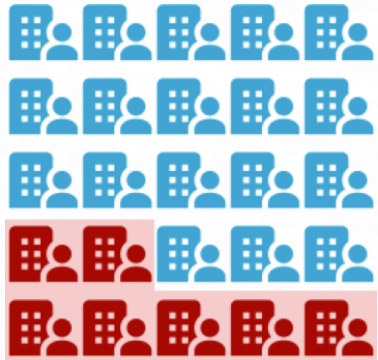
Top threat actor varieties in breaches 2021 (by Verizon DBIR report)





# Hacking and modern business life

## FireEye 2020 Security Trends Report



**27%** of organizations characterize their cyber security program as **semiformal approaches** where **efforts were mostly compliance driven** and focused on addressing mandatory regulations



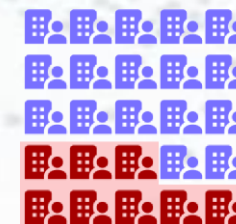
Over **40%** of organizations do not have or have only **very limited cyber security training** for their employees



Only **19%** of organizations identified their **security program as strategic** with intelligence data driving investment decisions, operational priorities and other critical cyber security factors.



**24%** saw their programs as informal with a focus is primarily on **addressing critical issues as they occur**



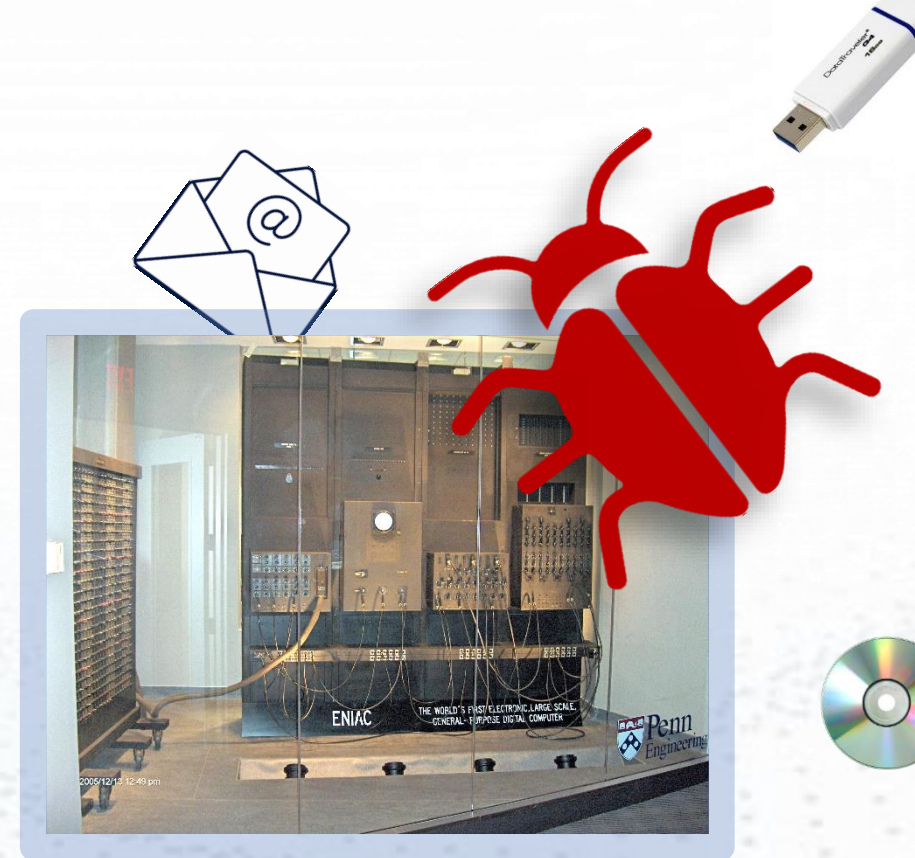
Nearly **29%** of organizations who have cyber attack and breach response plans **have not tested or updated their plans in 12 or more months**





# Where are the security vulnerabilities coming from?

- Mistake (or a “shortcut”) during software development, aka “**software bug**”.\*
- Not learning from past **mistakes** (“to err is human”, but...).
- Software/hardware/network **architecture design flaw**.
- **Misconfiguration** of software/hardware.
- **Time pressure** (e.g., to be the first on the market).
- **Lack of basic security knowledge** and understanding of security principles by personnel.
- **Complexity** of modern IT systems (multiple “single points of failure”).
- **Familiarity** (using common, well-known code, software, operating systems, and/or hardware).
- Deliberate **malicious activity** (creating malware, botnet management software or exploits for money)
- **Insider threat**
- **Weak cryptography** in use
- “**Security by obscurity**”



\* *First large computers were genuinely vulnerable to bugs infestation. Bugs could cause a sort circuit and easily put the whole system down.*

# Common types of attacks

- DoS and DDoS (using botnets)
  - Get rid of competitor
  - Mask other illegal activity
  - Demanding ransom
- Unauthorised access to information
  - Confidential data
  - Intellectual property
  - Credit card numbers
  - Personal Identifiable information
- Malware
- Ransomware (*what about “ransomware-as-a-service”?*)
- Scareware
- Spyware



Examples of ransomware and scareware

**YOUR COMPUTER HAS BEEN LOCKED!**

This operating system is locked due to the violation of the federal laws of the United States of America (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A., provides for a deprivation of liberty for four to twelve years.)

**WARNING!**

**SYSTEM MAY HAVE DETECTED VIRUSES ON YOUR COMPUTER**

System May Have Found (2) Malicious Virus  
Download Your Personal & Financial Information  
For Help Removing Viruses, Call  
**1(855) 555-1234**  
(TOLL-FREE, 24 HOURS)

**Cryptolocker 2.0**

**Your personal files are encrypted**

Your important files were encrypted on this computer: photos, videos, documents, etc. You can verify this by click on see files and try to open them.

Encryption was produced using unique public key **RSA-4096** generated for this computer. To decrypt files, you need to obtain private key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; the server will destroy the key within 72 hours after encryption completed. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

**Average Ransom Payment**  
Size of each known payment +8% from Q1/22

Average known Payout =

**USD \$228,125**

**BLACKFOG**  
Privacy. Security. Prevention.

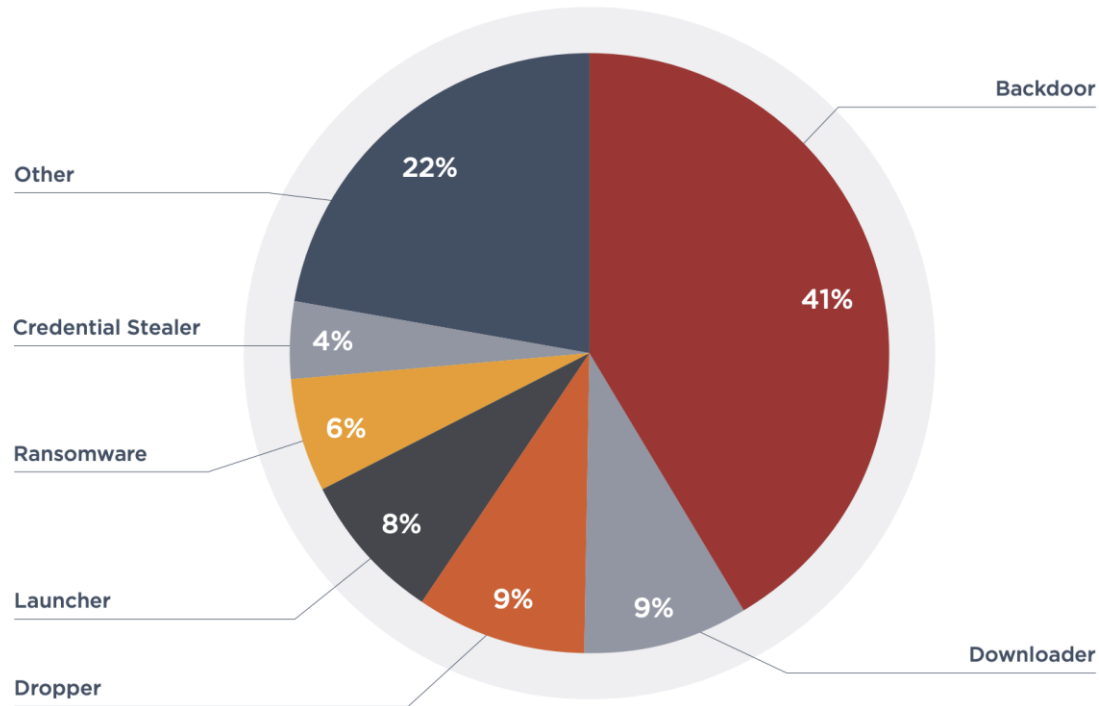
Published August 2022

“Fun fact”

# Malware

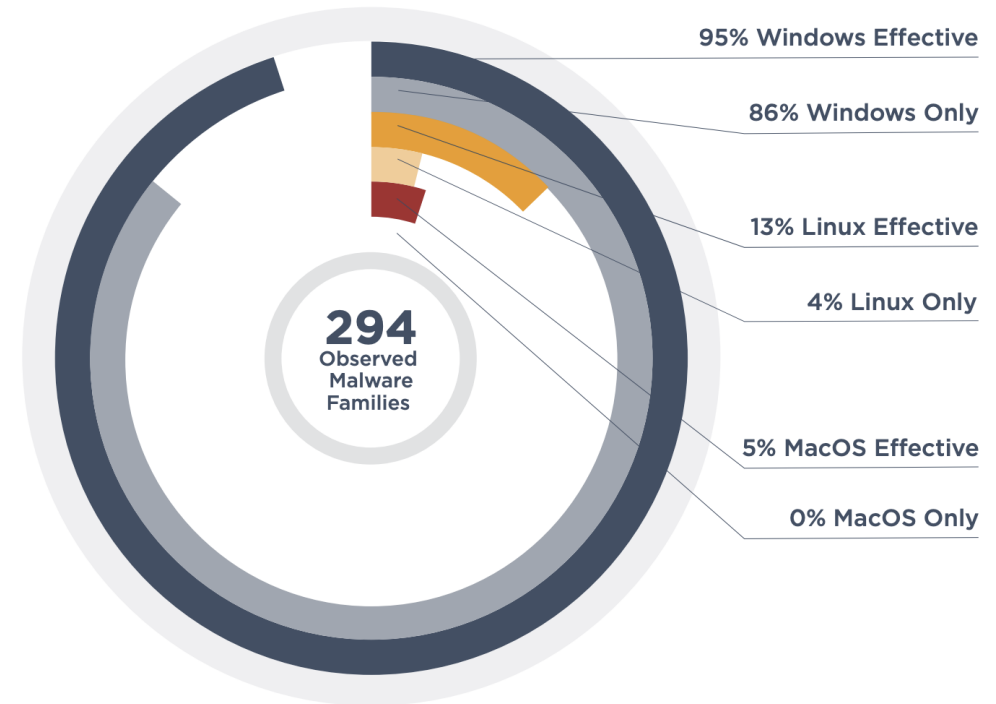
## Observed malware families by category, 2020

From FireEye M-Trends 2021 report



## Effectiveness of observed malware families by operating system, 2020

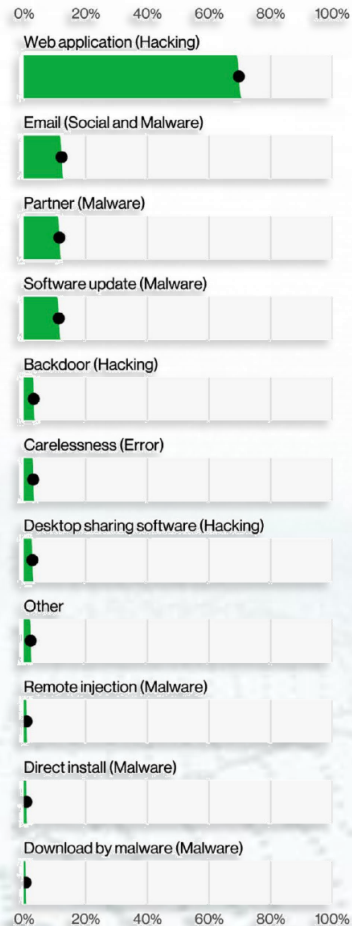
From FireEye M-Trends 2021 report





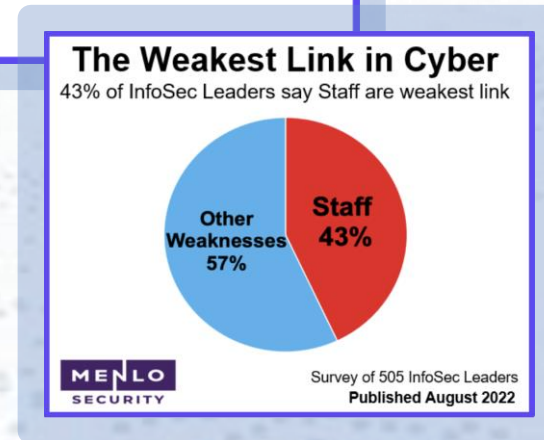
# How you or your company can be hacked?

## Easier than you think!



Top Action vectors in incidents 2022 (by Verizon DBIR report)

- Click the wrong web link
- Open an email with a malicious attachment
- Your software/hardware has “zero-day” vulnerability
- Connect to the wrong (malicious) WiFi access point
- Credentials can be stolen by a keylogger (software or hardware)
- An employee brings their own compromised device and connect to the corporate network (e.g., mobile phone or laptop)
- Someone can tailgate through the office back door
- You use software/hardware which has serious security vulnerabilities in it
- You use the software/hardware with embedded backdoor
- You have a rootkit installed in your system



# How else can you be hacked?

- Using “trojan horses”
- Malicious insiders (e.g., Snowden, the story with PRISM, etc.)
- Social engineering (read about Kevin Mitnick)
- Phishing attacks
- Phishing + digital attacks
- State-sponsored attacks (like Stuxnet)
- Ideology-driven attacks (Anonymous)





# Hackers' methodology and tools

Penetration testers and malicious hackers do similar things

1. **Information discovery** (analysis and research of the target)
2. **Scanning** (attempt to identify potential entry points)
3. **Vulnerability assessment** (looking for weaknesses)
4. **Exploitation of the weakness** (make use of the identified vulnerabilities)
5. **Privilege escalation** (increasing privileges for total access)
6. **Lateral movements** (aka “pivoting attacks”: hacking the adjacent systems, servers, workstations, etc.)
7. **Retaining access** (set up a backdoor to be able to return later)
8. **Covering tracks** (removing evidence of malicious activities)





# Penetration testing vs hacking



- **Penetration tester:** A person who has rights to simulate the attack on a computer system, performed to evaluate the security posture. The test is performed to identify the weaknesses and the potential for unauthorized parties to gain access to the system's features and data.
- **Intent:** Improve the security of the customer's IT infrastructure and applications.
- **Source of income:** salary, bug bounties.

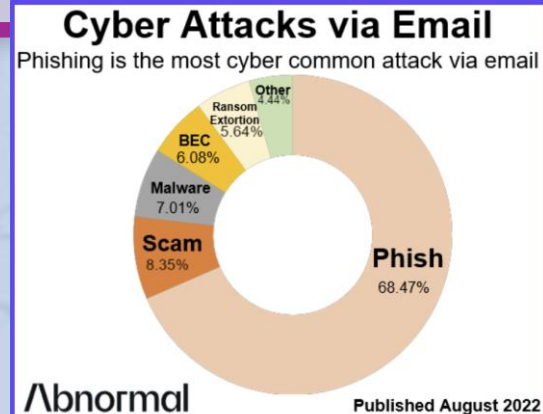


- **Hacker:** a person who illegally break the system security and application for their own malicious purposes.
- **Intent:** Earn money through illegal activities.
- **Source of income:** fraud, blackmailing, ransom, illegal transactions, etc.

# Let's talk about phishing



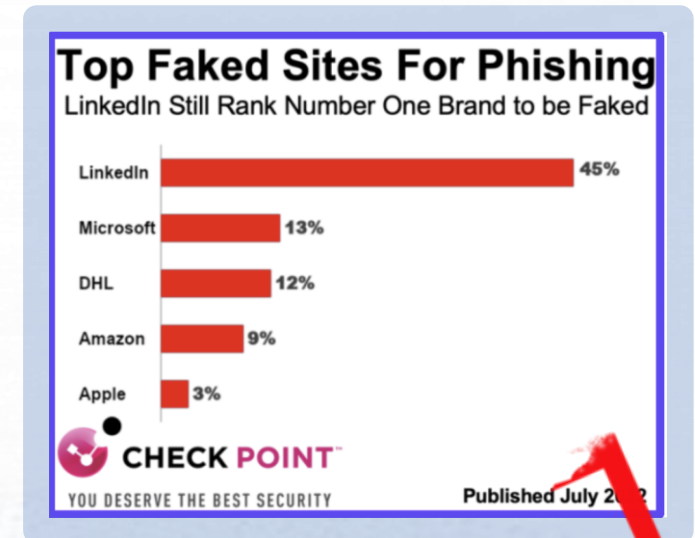
- “Phishing” is where fraudsters pose as a trusted organisation, e.g. your bank, social website, e-commerce, etc. in emails, calls or text messages.
- Phishing is widely carried out through the use of emails. Impersonators generally use this method to send emails that appear to have come from genuine sources.



- 🐟 **Mass Phishing:** Large-volume attack intended to reach as many people as possible
- 🐟 **Spear Phishing:** Targeted attack directed at specific individuals or companies. Some information is gathered before to personalize the message and make the scam more difficult to spot.
- 🐟 **Whaling:** Type of spear phishing attack. Targets “big fish,” including high-profile individuals or those with a great deal of authority or access (e.g., CEO, HR, etc.).
- 🐟 **Clone Phishing:** Attacker uses a spoofed copy of a legitimate and previously delivered email, where original attachments or hyperlinks replaced with malicious. The email is sent from a forged email address so it appears to come from the original sender.
- 🐟 **Filter Evasion:** Using images instead of text to make it harder for anti-phishing engines to detect keywords which are typically used in phishing emails
- 🐟 **Website Forgery:** Manipulating the web browser to hide the fact that the victim is navigating malicious URL

# Phishing – what information they are after?

- First and last name (yours and your family members)
- Passwords
- Email address
- Bank account / credit card info
- Personal Information (physical address)
- Phone number(s)
- Details about your employer and the work you do
- Technical details about your computer and network configuration
- .....



**TOP SECRET**



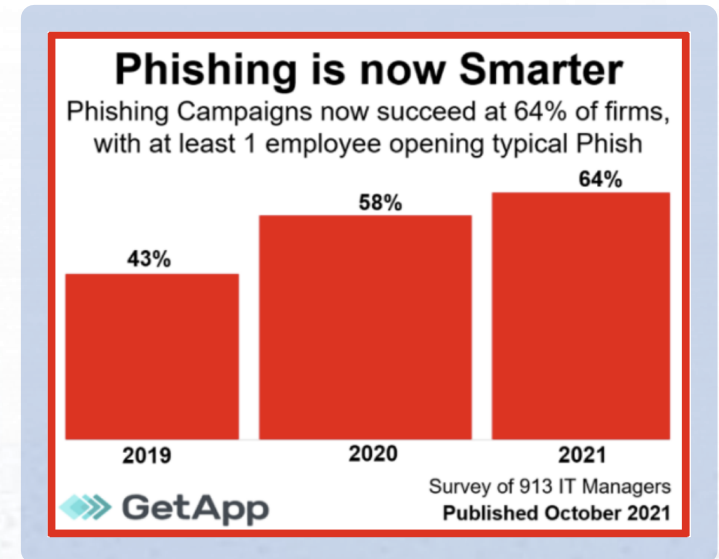
# Phishing – is it profitable?

Oh, very much so!

Let's review a sample phishing one day “campaign” \*:

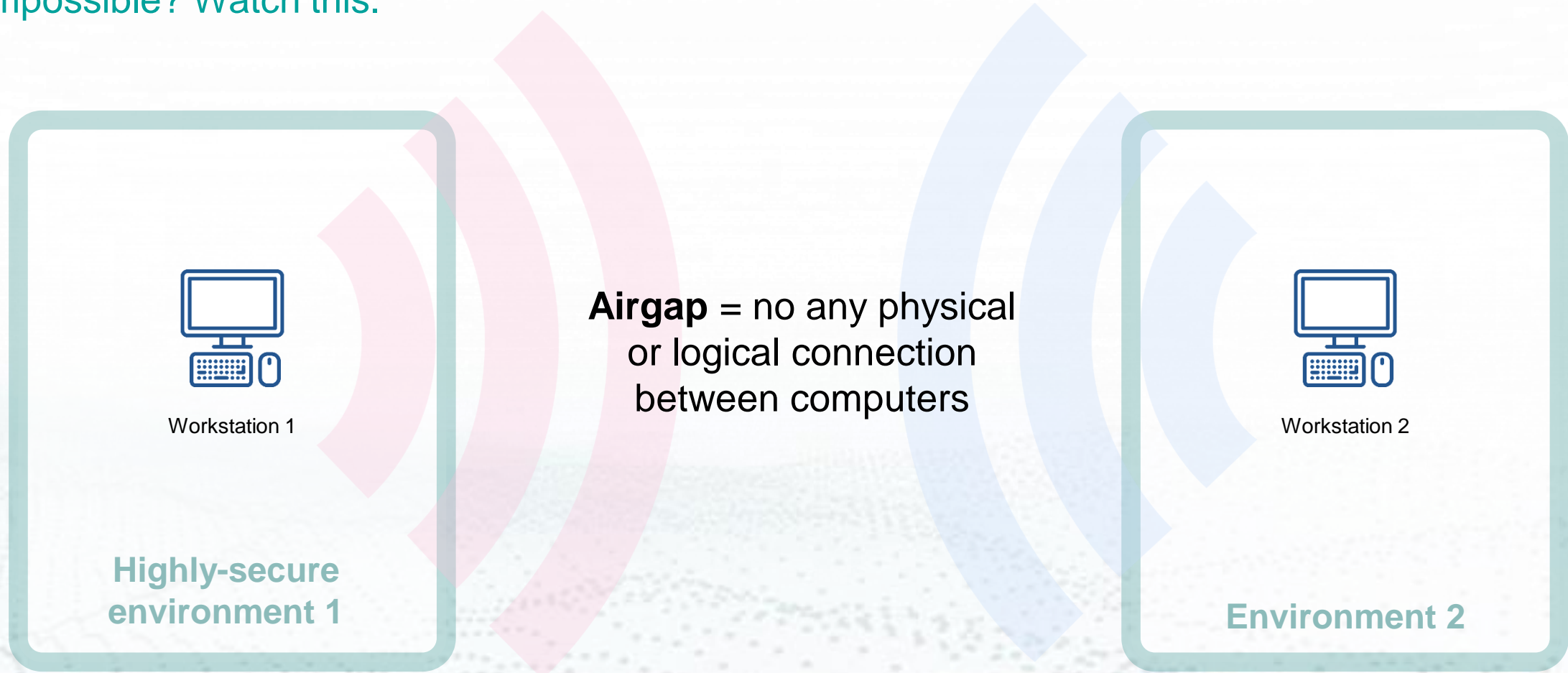
- 2,000,000 emails sent (100%)
- 100,000 emails successfully delivered to recipient (5%)
- 5,000 recipients clicked the phishing link (0.25%)
- 100 victims enter personal details (it's 0.05%)
- **£1,000** from each person who entered information
- Potential Reward: **£100,000**

\* based on real life example!



# Extracting data from “air-gapped” computers

Impossible? Watch this.



# Extracting data from “air-gapped” computers

Impossible? Watch this.



Workstation 1

Highly-secure  
environment 1

## Electromagnetic

- AirHopper exploit: control the electromagnetic emissions from computer displays or screen cables (so they become a transmitter)

## Magnetic

- Low frequency magnetic signals generated by the computer's CPU cores
- Covert signals generated by using magnetic head of hard disk drives to generate magnetic emission (detected by mobile phone).

## Optical

- Data exfiltration through PC keyboard LEDs, router/switch LEDs
- Data exfiltration through fast blinking low-contrast images on the screen
- Using IR LEDs in security cameras for transmitting data

## Thermal

- The heat generated by the CPU/GPU of a computer is received by temperature sensors that are integrated into the motherboard of the nearby computer

## Acoustic

- Data is transmitted via inaudible, ultrasonic sound waves
- Noise intentionally generated by the computer's cooling fan
- Turn headphones or speakers to a microphone (jack re-tasking technique)
- Acoustic signals emitted from the hard disk drive (HDD) moving arm



Workstation 2

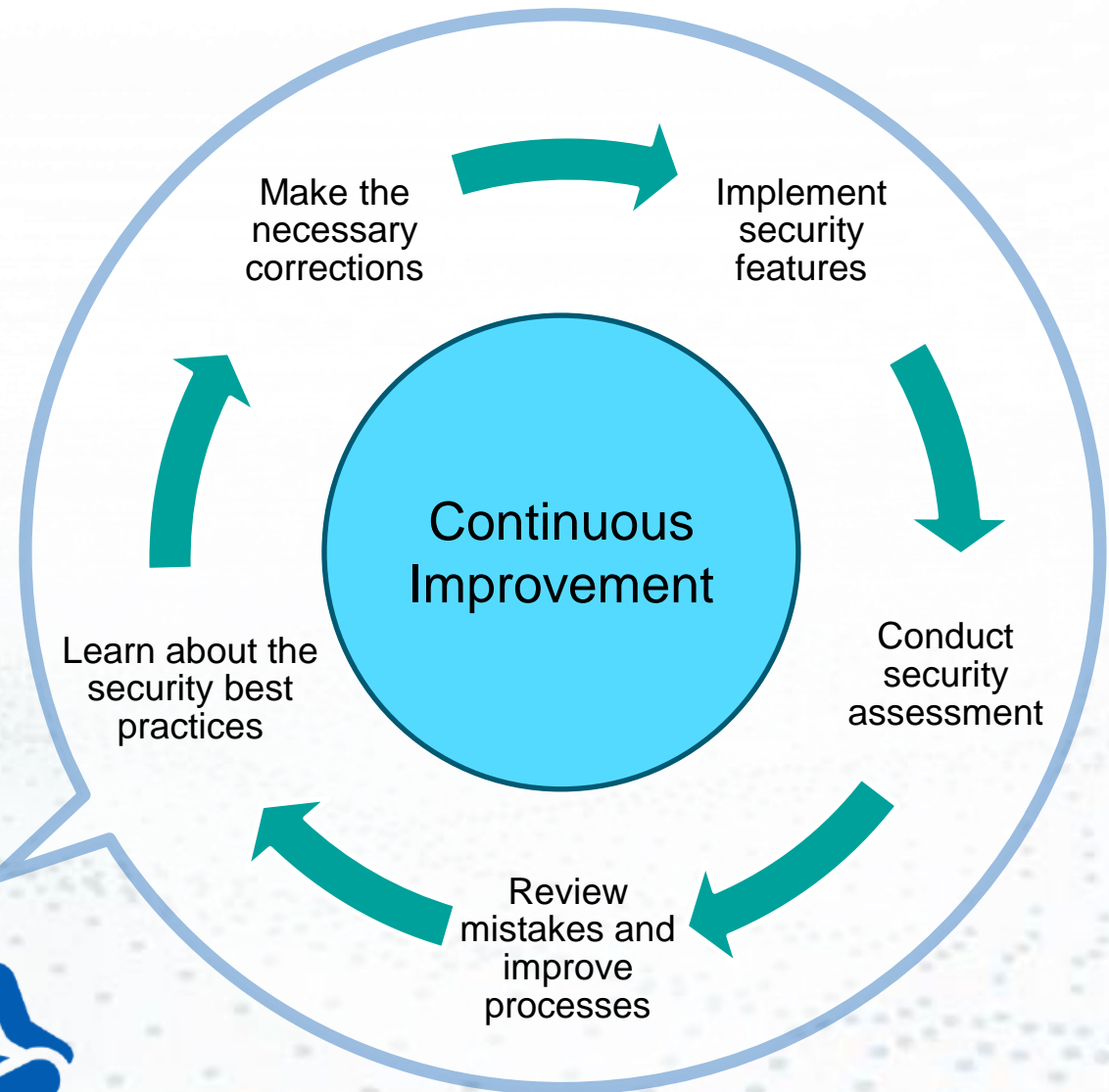
Environment 2



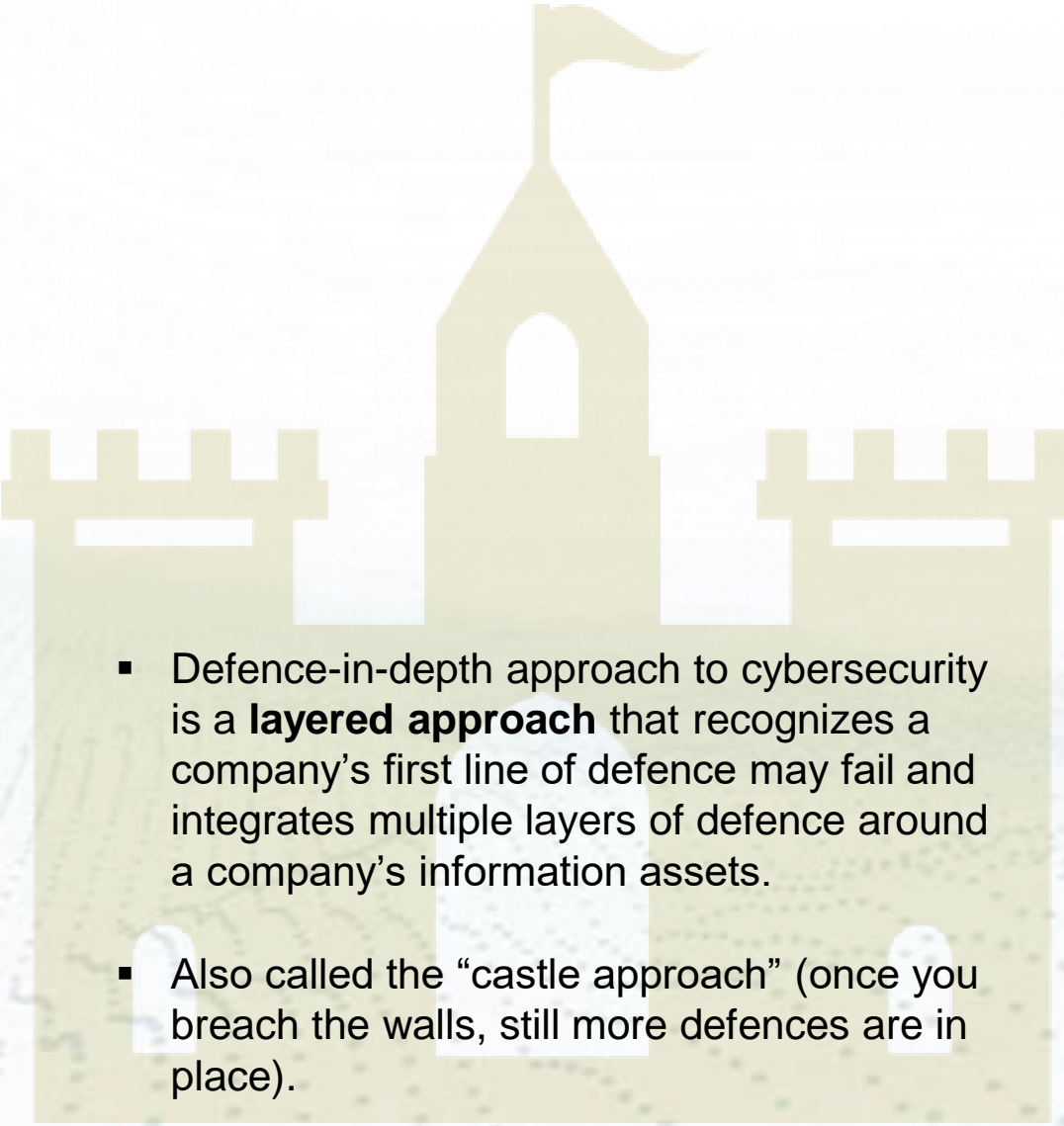
# Takeaways: what to do to prevent the disaster?

## Change your mindset first

- Security is a **continuous process**, where an organization is learning and improving their processes and the security posture all the time.
- A system can be called “secure” only in a specific moment in time. It cannot be “always secure”, therefore **regular testing is imperative**.
- Security is a **system property**, not a feature.
- Security is a **continual process**, not a product.



# Defence-in-depth

- 
- Defence-in-depth approach to cybersecurity is a **layered approach** that recognizes a company's first line of defence may fail and integrates multiple layers of defence around a company's information assets.
  - Also called the “castle approach” (once you breach the walls, still more defences are in place).



## People

Humans remain one of the weakest links in security chain. Ensure you have a strong security awareness training program.



## Processes

It is important to ensure that best practice processes and associated management frameworks are in place. Regular audits and reviews are important.



## Technology

The continuously increasing sophistication and rate of attacks means that constant upkeep and tracking of technology changes is essential.

# Takeaways: DOs and DON'Ts

## This is what you **SHOULD NOT** do:

- DO NOT CLICK ANYTHING YOU SEE IN THE WEB. STOP AND THINK.
- Never give out your password or any other sensitive information via email. Beware of links in emails that ask for personal information.
- If you are unsure do not open the attachments and links. Never open email attachments from unknown sender.
- Do not connect BYOD without authorisation.
- Be vigilant: report strange behaviour and unknown individuals in the office.





# Takeaways: DOs and DON'Ts

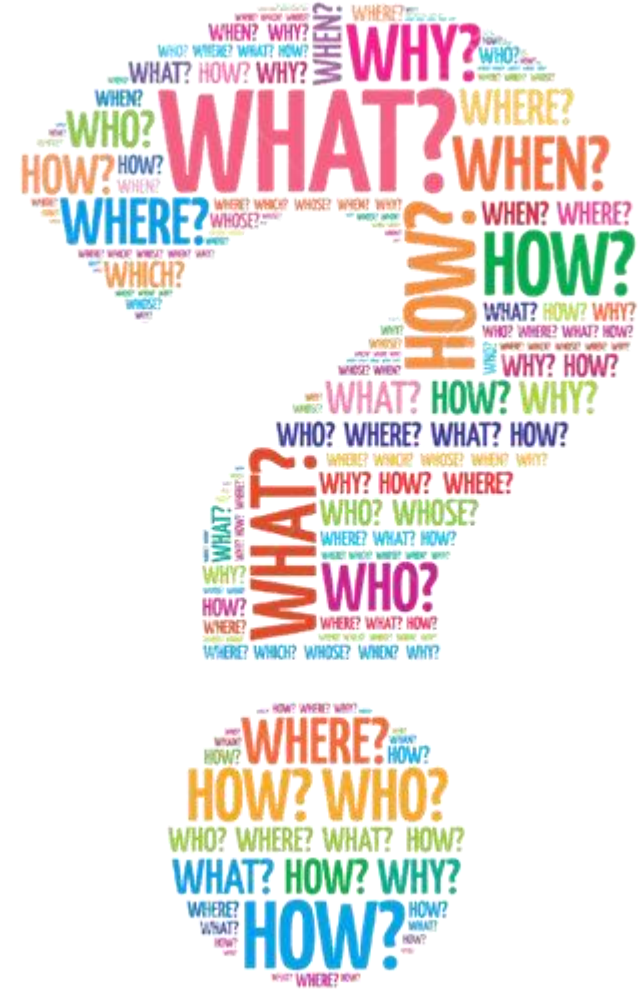
## This is what you SHOULD do:

- If you see phishing email – warn the others! Stay vigilant and let the others also be aware of the threat.
- If you have doubts - call the sender to confirm the information and also warn them if needed.
- Check your online accounts and bank statements regularly to ensure that no unauthorised transactions have been made on your behalf.
- Any deviation from the routine = warning sign!
- Contact your IT department – they will be happy to help in either case: with your corporate or personal problem.
- Learn about cybersecurity and conduct penetration testing exercises in your organisation regularly.



# Questions

---





# Thank you!

<https://www.spirent.com/Products/SecurityLabs>

[securityLabs@spirent.com](mailto:securityLabs@spirent.com)

**securitylabs**

Aleksander Gorkowienko  
e: [aleksander.gorkowienko@spirent.com](mailto:aleksander.gorkowienko@spirent.com)  
m: +44 (0) 7974431025



