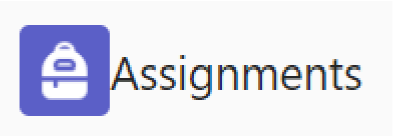
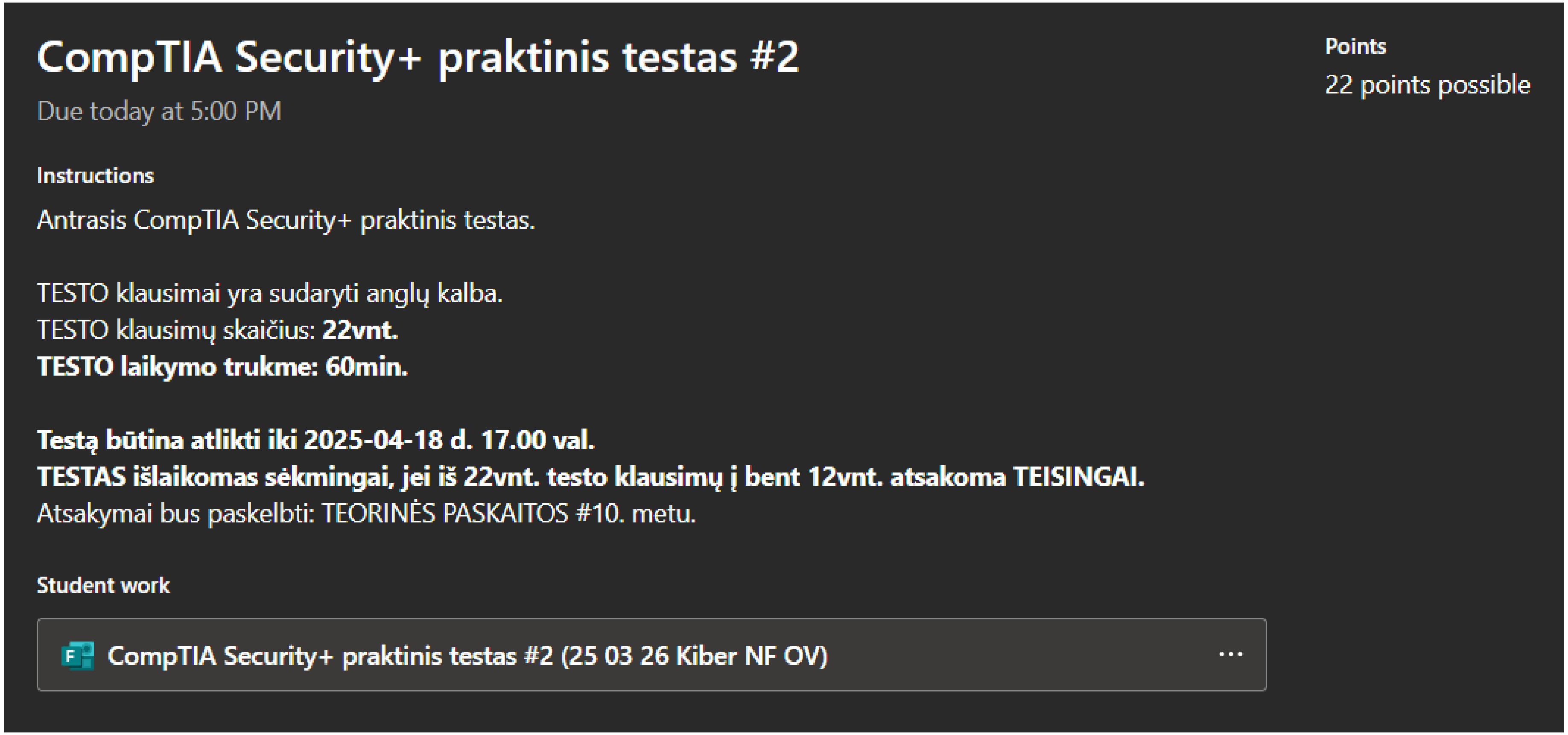
# Cyber Security
# Lession 10

# Labs


Assignments

11 Students – Turned in
0 Student – Viewed
0 Student – Not turned in



## CompTIA Security+ praktinis testas #2

Due today at 5:00 PM

**Points**
22 points possible

**Instructions**

Antrasis CompTIA Security+ praktinis testas.

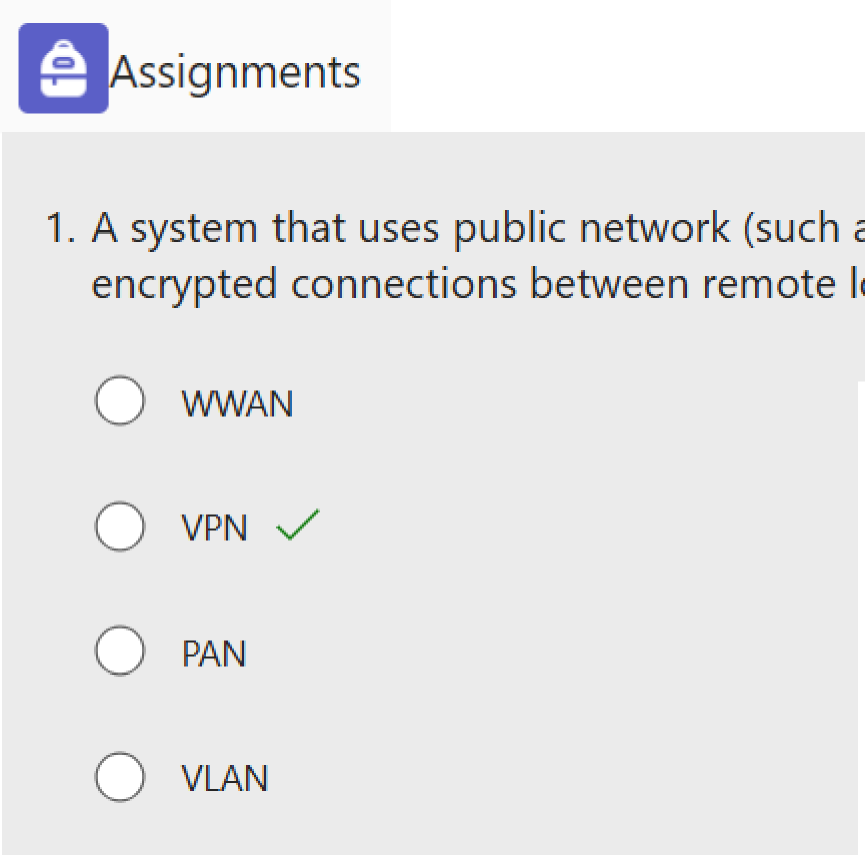
TESTO klausimai yra sudaryti anglų kalba.
TESTO klausimų skaičius: **22vnt.**
**TESTO laikymo trukme: 60min.**

**Testą būtina atlikti iki 2025-04-18 d. 17.00 val.**
**TESTAS išlaikomas sėkmingai, jei iš 22vnt. testo klausimų į bent 12vnt. atsakoma TEISINGAI.**
Atsakymai bus paskelbti: TEORINĖS PASKAITOS #10. metu.

**Student work**

CompTIA Security+ praktinis testas #2 (25 03 26 Kiber NF OV)

# Labs



Assignments

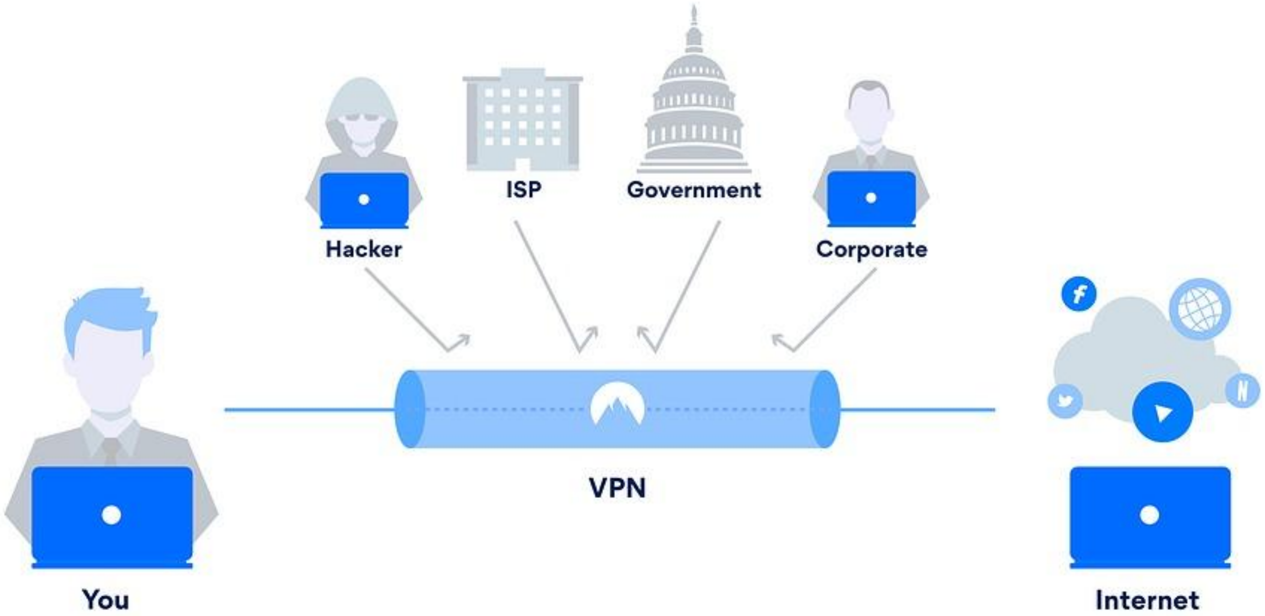
1. A system that uses public network (such as the Internet) as a means for creating private encrypted connections between remote locations is referred to as: * (1 Point)

○ WWAN

○ VPN ✓

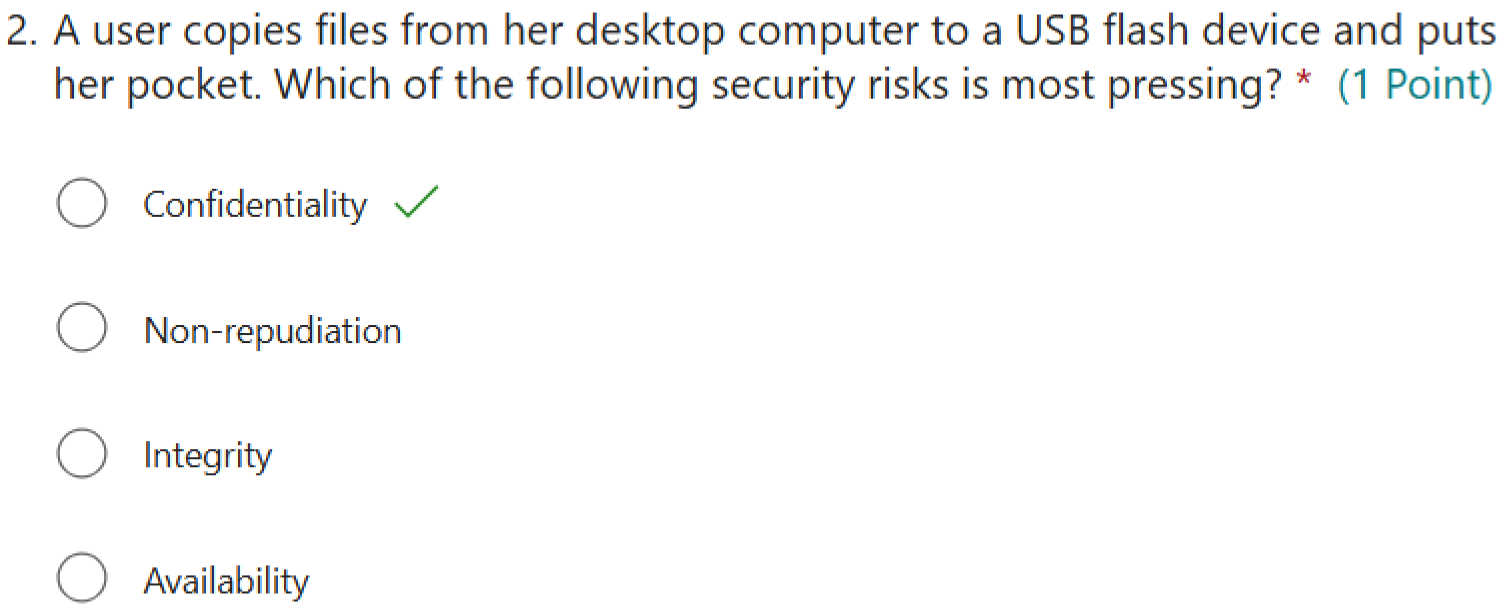
○ PAN

○ VLAN



# Labs

Assignments



2. A user copies files from her desktop computer to a USB flash device and puts the device into her pocket. Which of the following security risks is most pressing? * (1 Point)

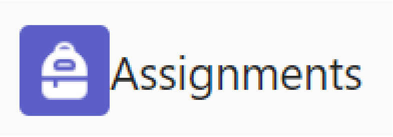
○ Confidentiality ✓

○ Non-repudiation

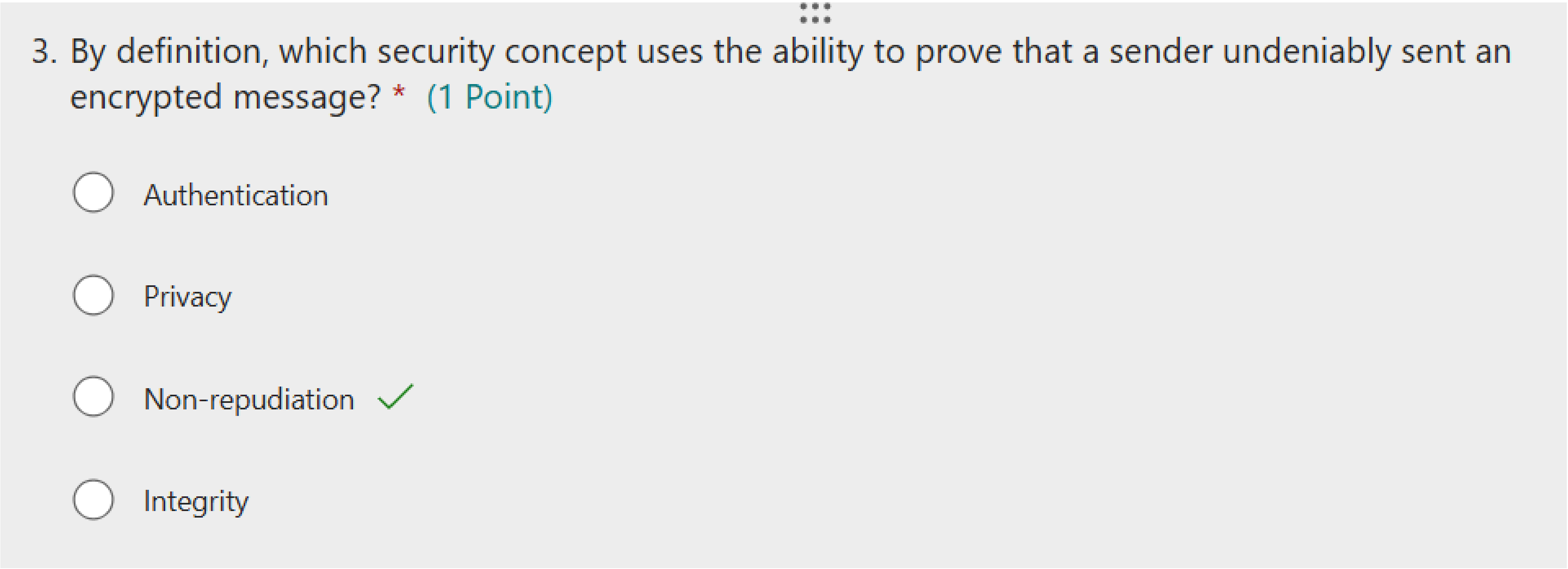
○ Integrity

○ Availability

# Labs



Assignments



3. By definition, which security concept uses the ability to prove that a sender undeniably sent an encrypted message? * (1 Point)

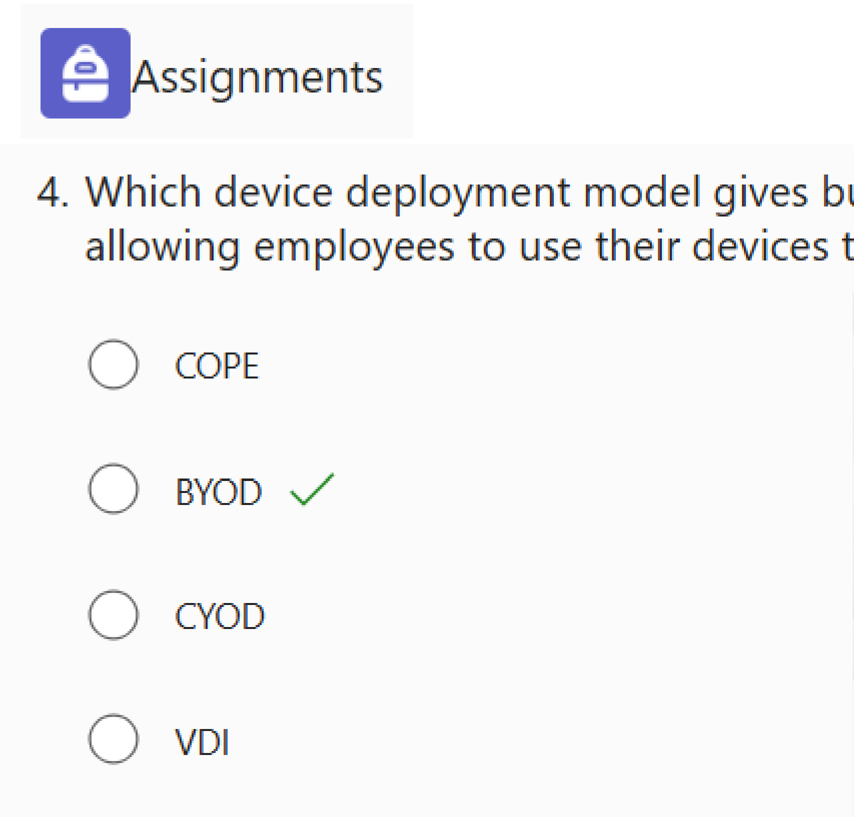
○ Authentication

○ Privacy

○ Non-repudiation ✓

○ Integrity

# Labs



Assignments

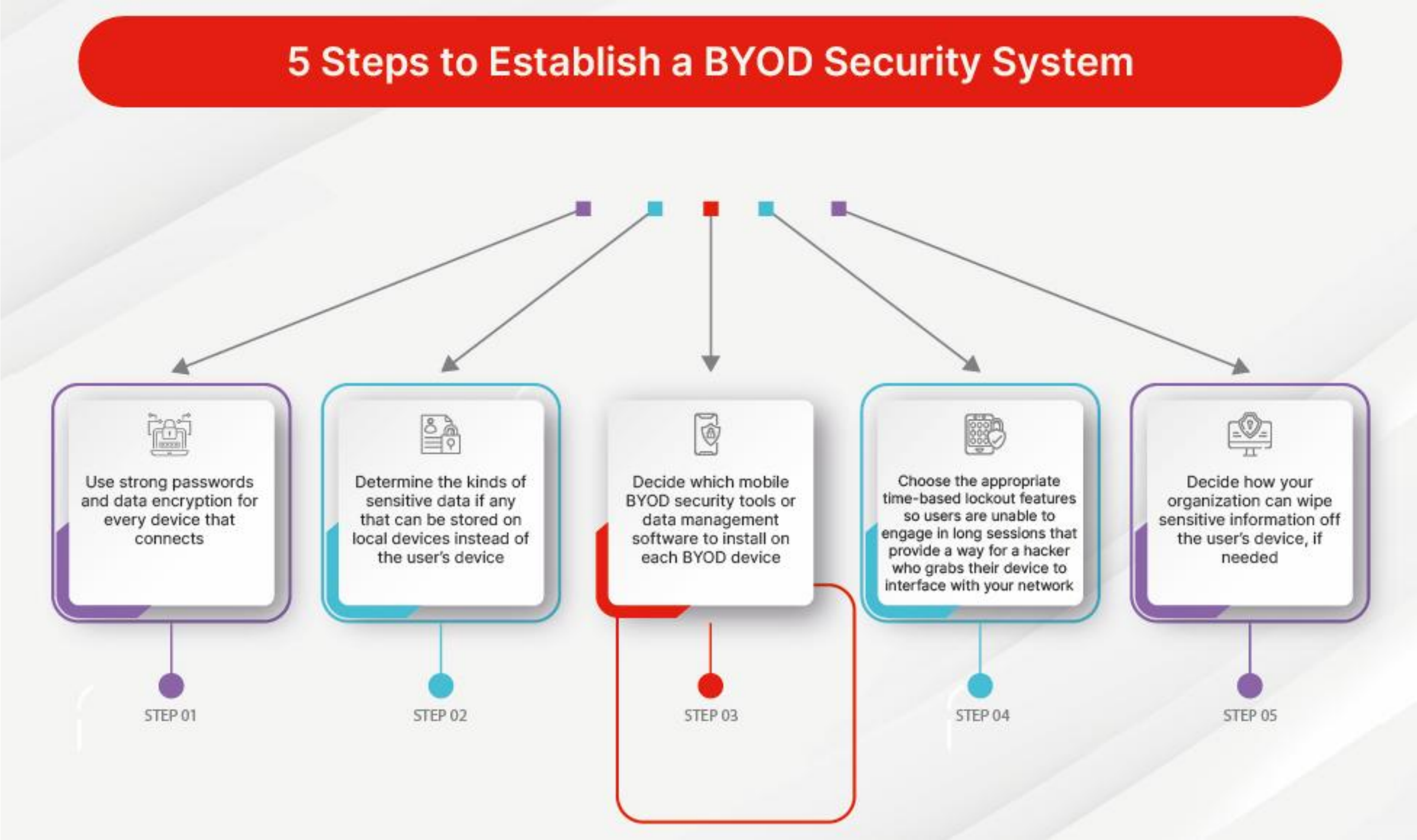
4. Which device deployment model gives businesses significant control over device security while allowing employees to use their devices to access both corporate and personal data? * (1 Point)

○ COPE

○ BYOD ✓

○ CYOD

○ VDI



5 Steps to Establish a BYOD Security System

STEP 01: Use strong passwords and data encryption for every device that connects

STEP 02: Determine the kinds of sensitive data if any that can be stored on local devices instead of the user's device

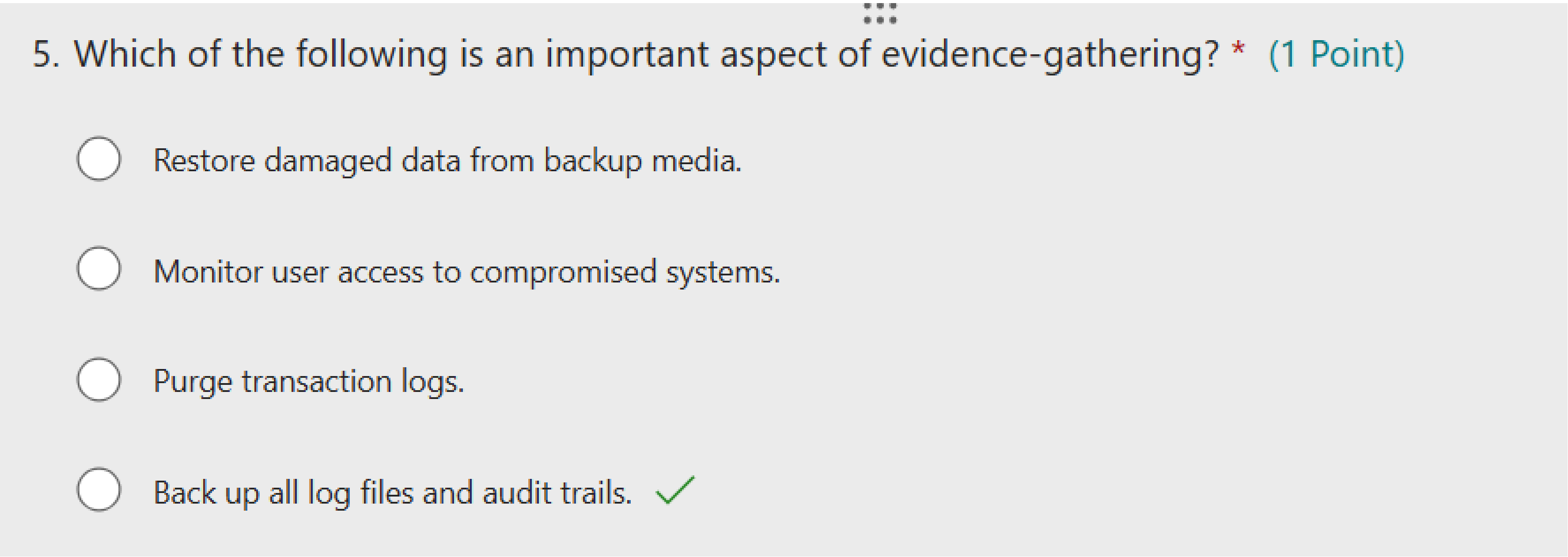
STEP 03: Decide which mobile BYOD security tools or data management software to install on each BYOD device

STEP 04: Choose the appropriate time-based lockout features so users are unable to engage in long sessions that provide a way for a hacker who grabs their device to interface with your network

STEP 05: Decide how your organization can wipe sensitive information off the user's device, if needed

# Labs

Assignments



5. Which of the following is an important aspect of evidence-gathering? * (1 Point)

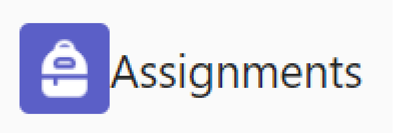
○ Restore damaged data from backup media.

○ Monitor user access to compromised systems.

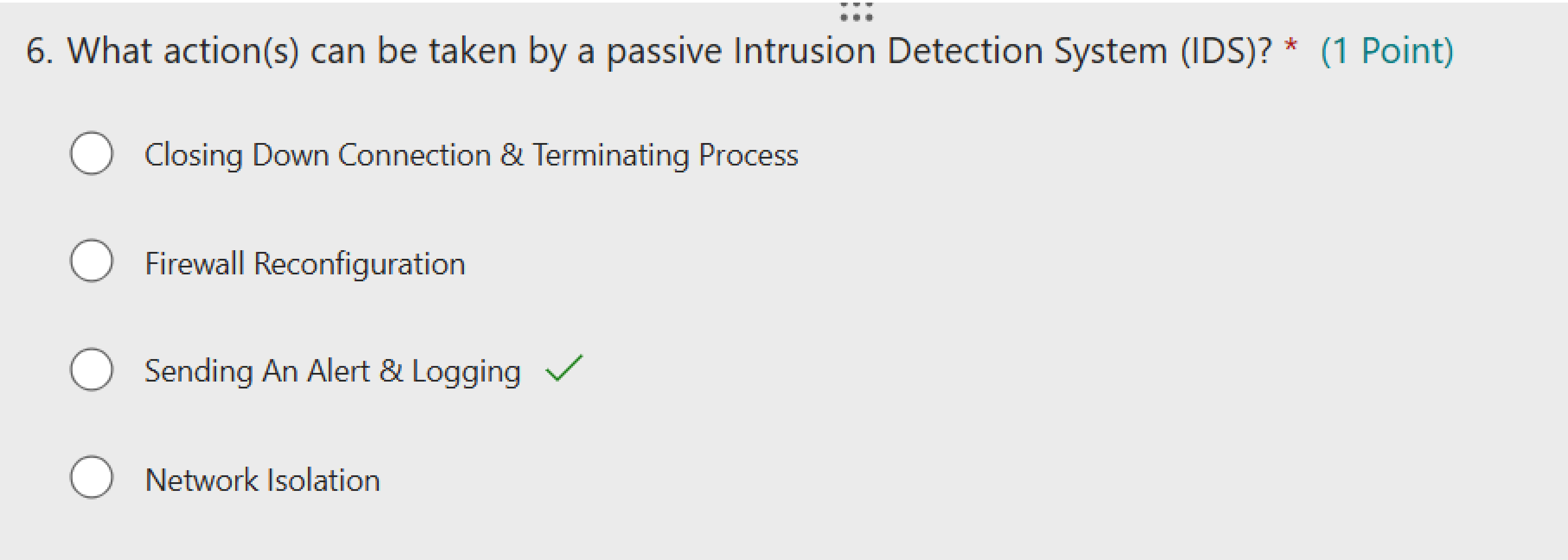
○ Purge transaction logs.

○ Back up all log files and audit trails. ✓

# Labs



Assignments



6. What action(s) can be taken by a passive Intrusion Detection System (IDS)? * (1 Point)

○ Closing Down Connection & Terminating Process

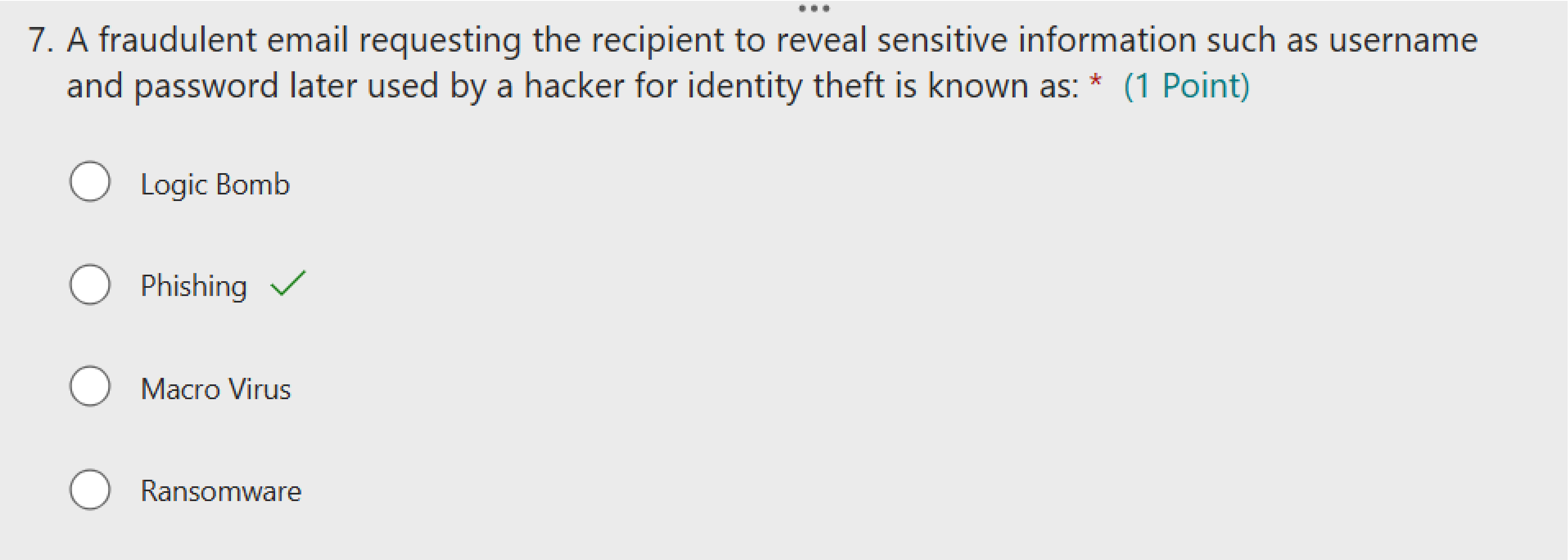
○ Firewall Reconfiguration

○ Sending An Alert & Logging ✓

○ Network Isolation

# Labs

Assignments



7. A fraudulent email requesting the recipient to reveal sensitive information such as username and password later used by a hacker for identity theft is known as: * (1 Point)

○ Logic Bomb

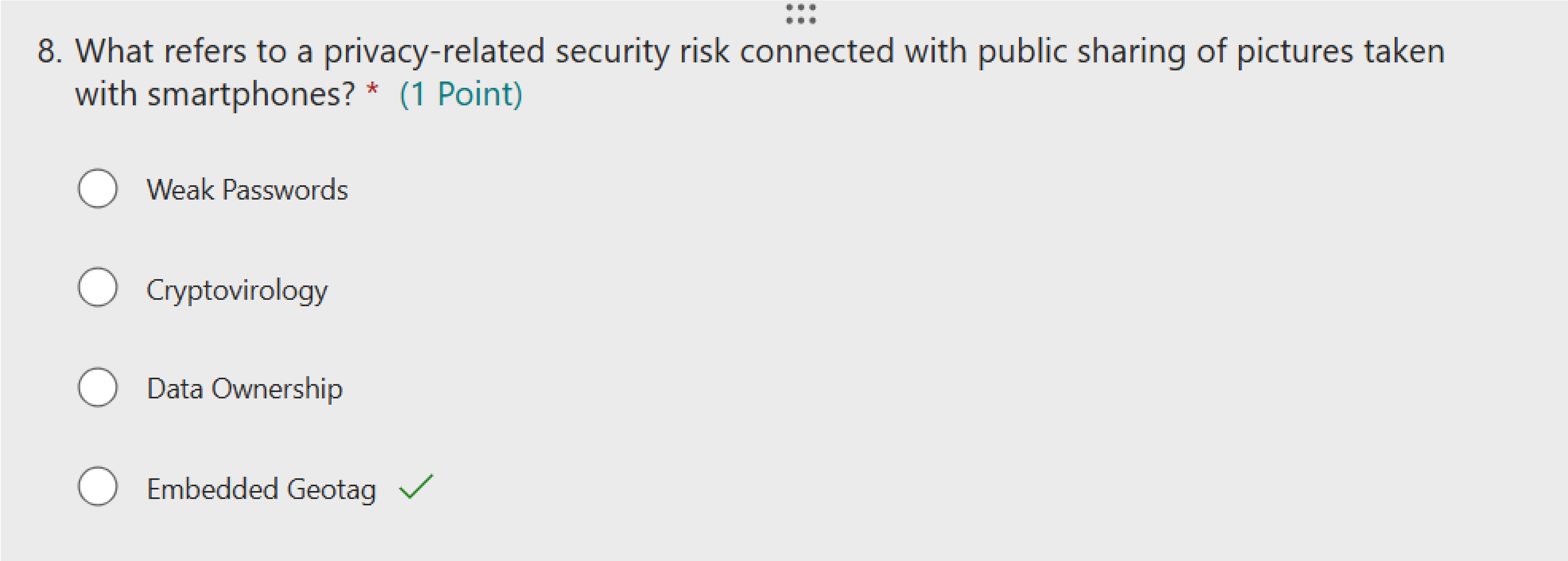
○ Phishing ✓

○ Macro Virus

○ Ransomware

# Labs

Assignments



8. What refers to a privacy-related security risk connected with public sharing of pictures taken with smartphones? * (1 Point)

○ Weak Passwords

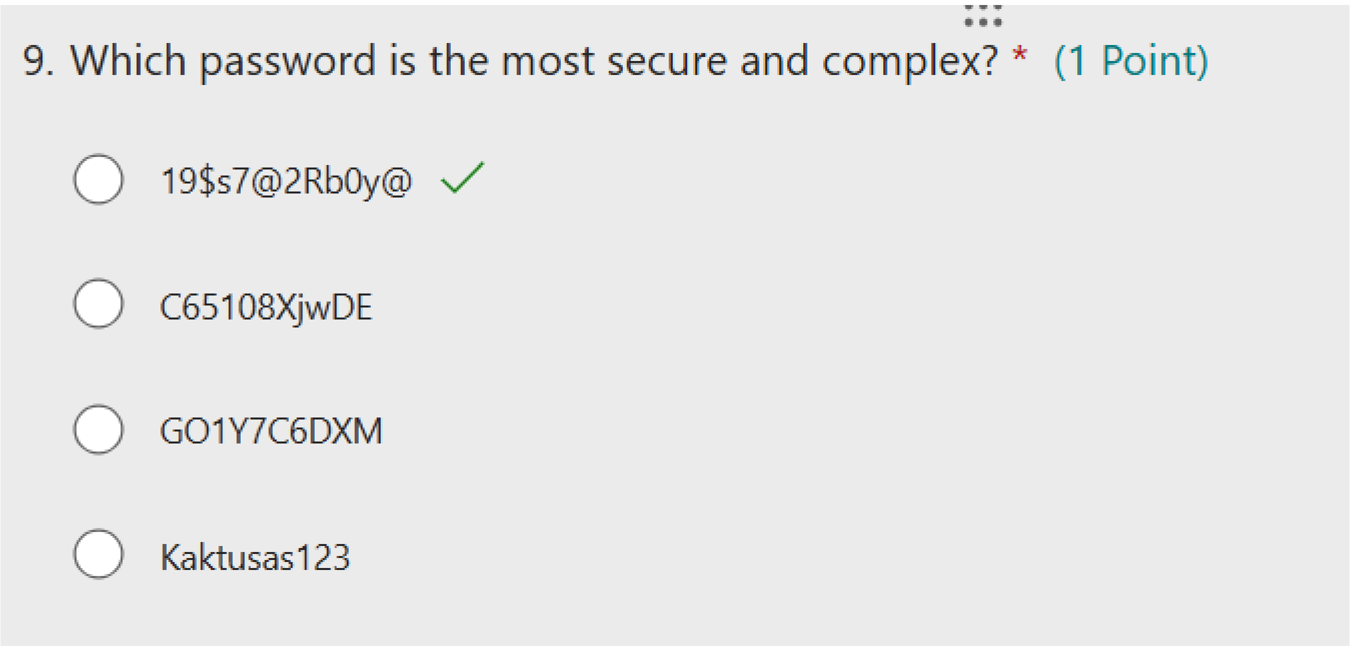
○ Cryptovirology

○ Data Ownership

○ Embedded Geotag ✓

# Labs

Assignments



9. Which password is the most secure and complex? * (1 Point)

○ 19$s7@2Rb0y@ ✓

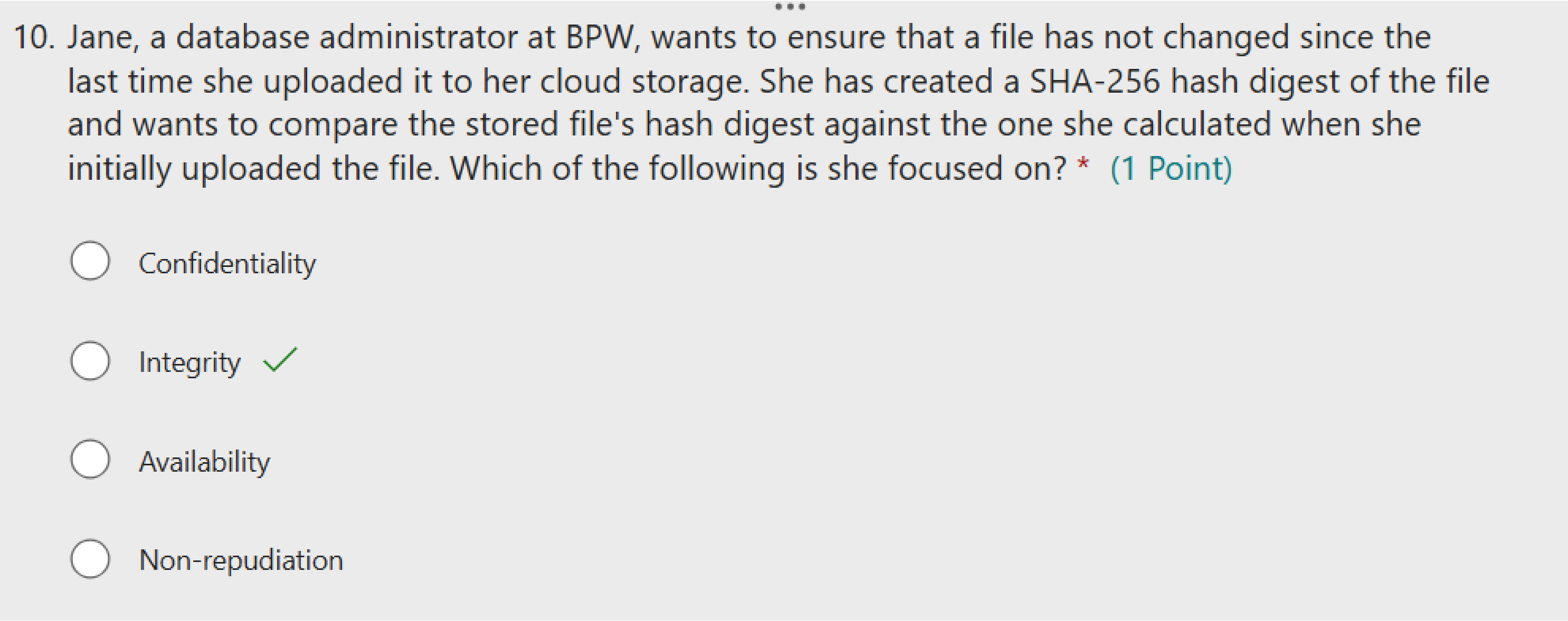
○ C65108XjwDE

○ GO1Y7C6DXM

○ Kaktusas123

# Labs

Assignments



10. Jane, a database administrator at BPW, wants to ensure that a file has not changed since the last time she uploaded it to her cloud storage. She has created a SHA-256 hash digest of the file and wants to compare the stored file's hash digest against the one she calculated when she initially uploaded the file. Which of the following is she focused on? * (1 Point)

○ Confidentiality

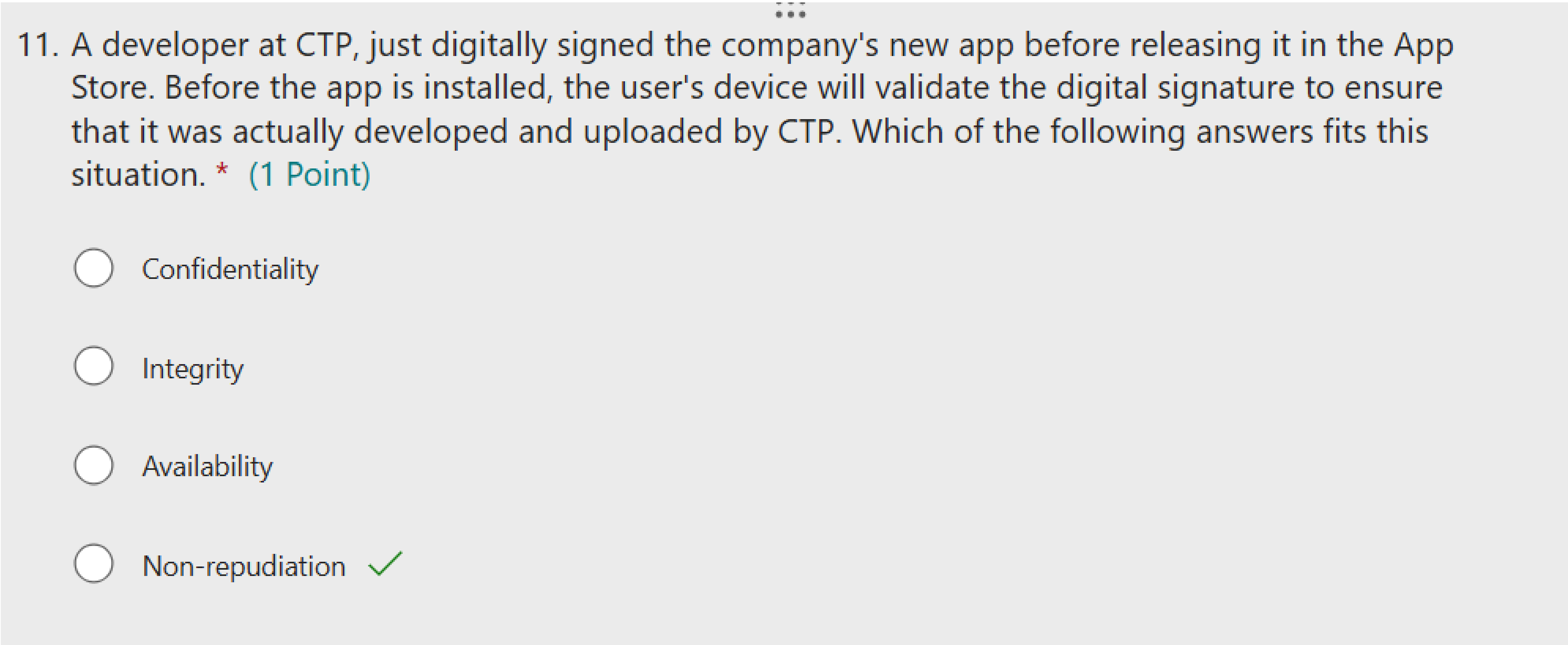
○ Integrity ✓

○ Availability

○ Non-repudiation

# Labs

Assignments



11. A developer at CTP, just digitally signed the company's new app before releasing it in the App Store. Before the app is installed, the user's device will validate the digital signature to ensure that it was actually developed and uploaded by CTP. Which of the following answers fits this situation. * (1 Point)

○ Confidentiality

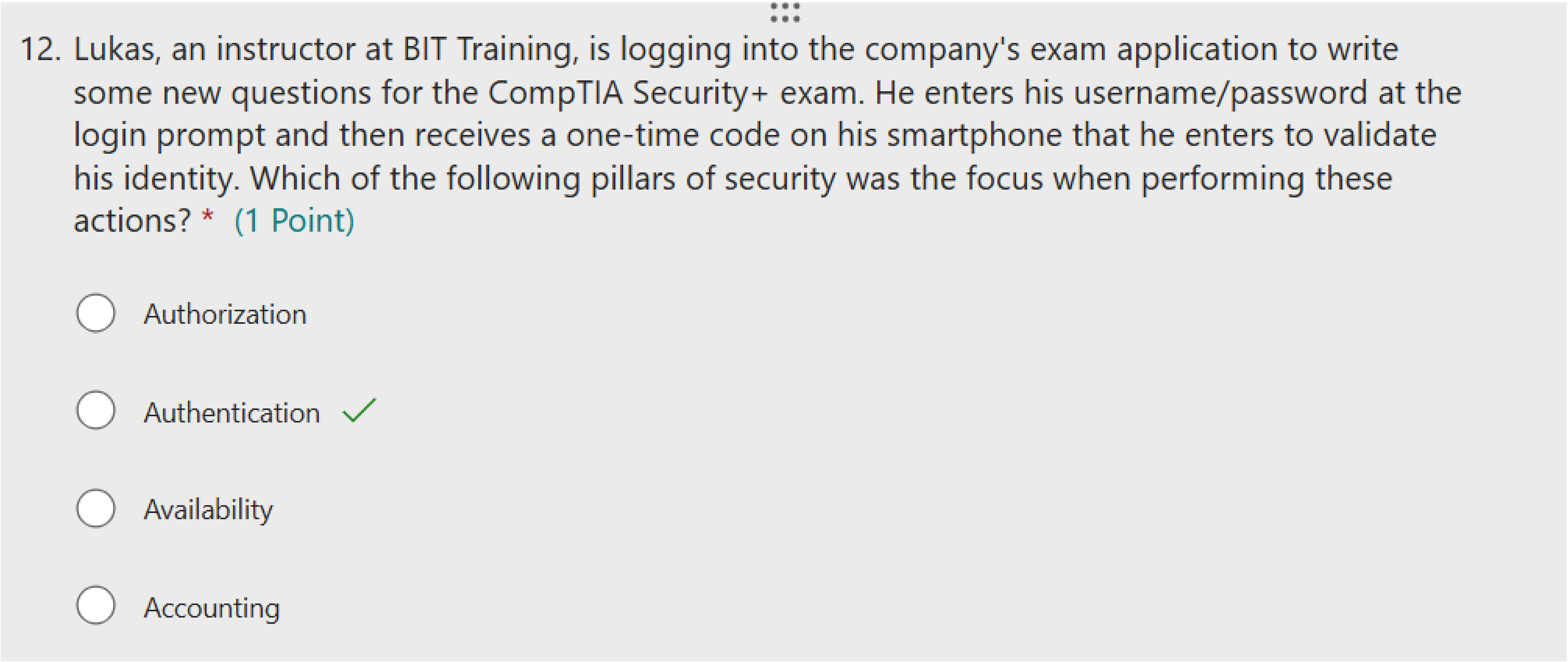
○ Integrity

○ Availability

○ Non-repudiation ✓

# Labs

Assignments



12. Lukas, an instructor at BIT Training, is logging into the company's exam application to write some new questions for the CompTIA Security+ exam. He enters his username/password at the login prompt and then receives a one-time code on his smartphone that he enters to validate his identity. Which of the following pillars of security was the focus when performing these actions? * (1 Point)

○ Authorization

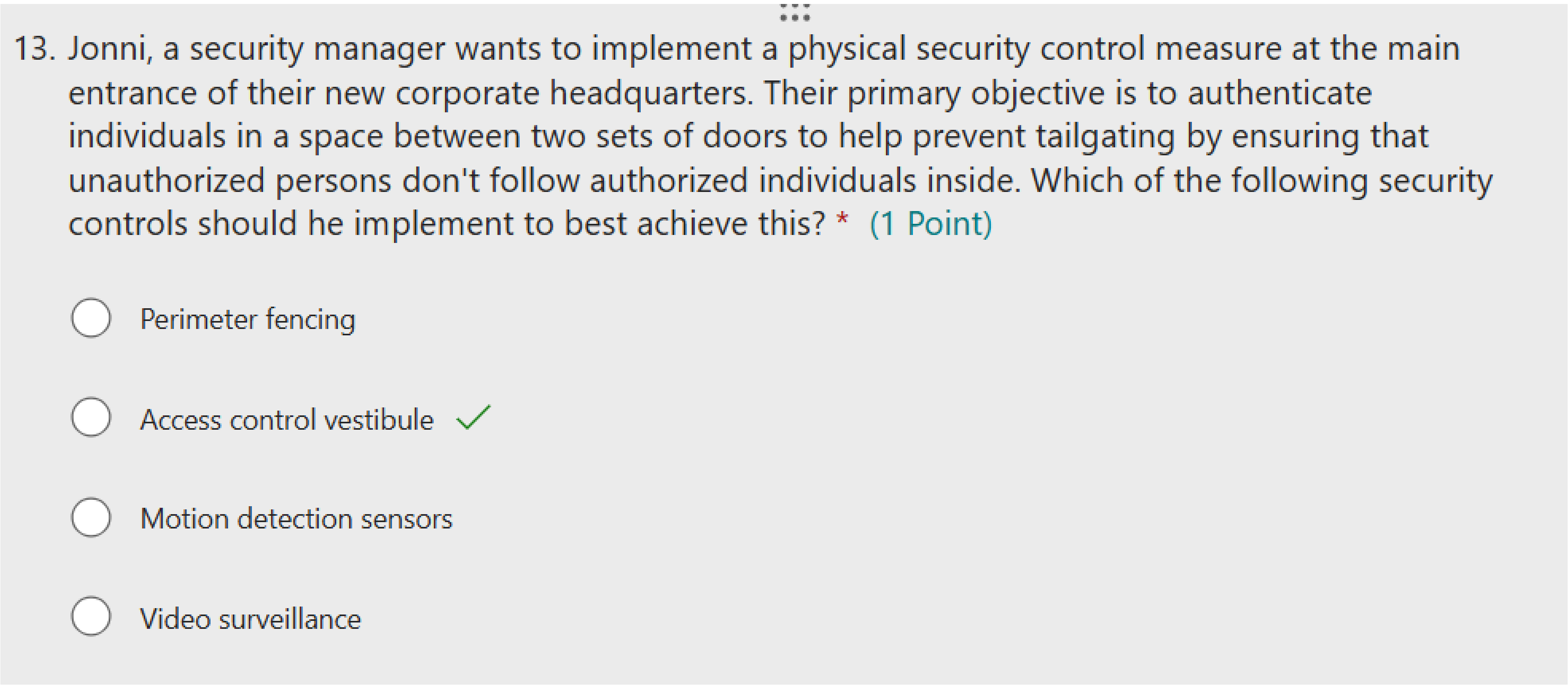
○ Authentication ✓

○ Availability

○ Accounting

# Labs

Assignments



13. Jonni, a security manager wants to implement a physical security control measure at the main entrance of their new corporate headquarters. Their primary objective is to authenticate individuals in a space between two sets of doors to help prevent tailgating by ensuring that unauthorized persons don't follow authorized individuals inside. Which of the following security controls should he implement to best achieve this? * (1 Point)

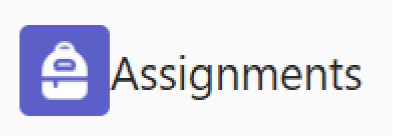
○ Perimeter fencing

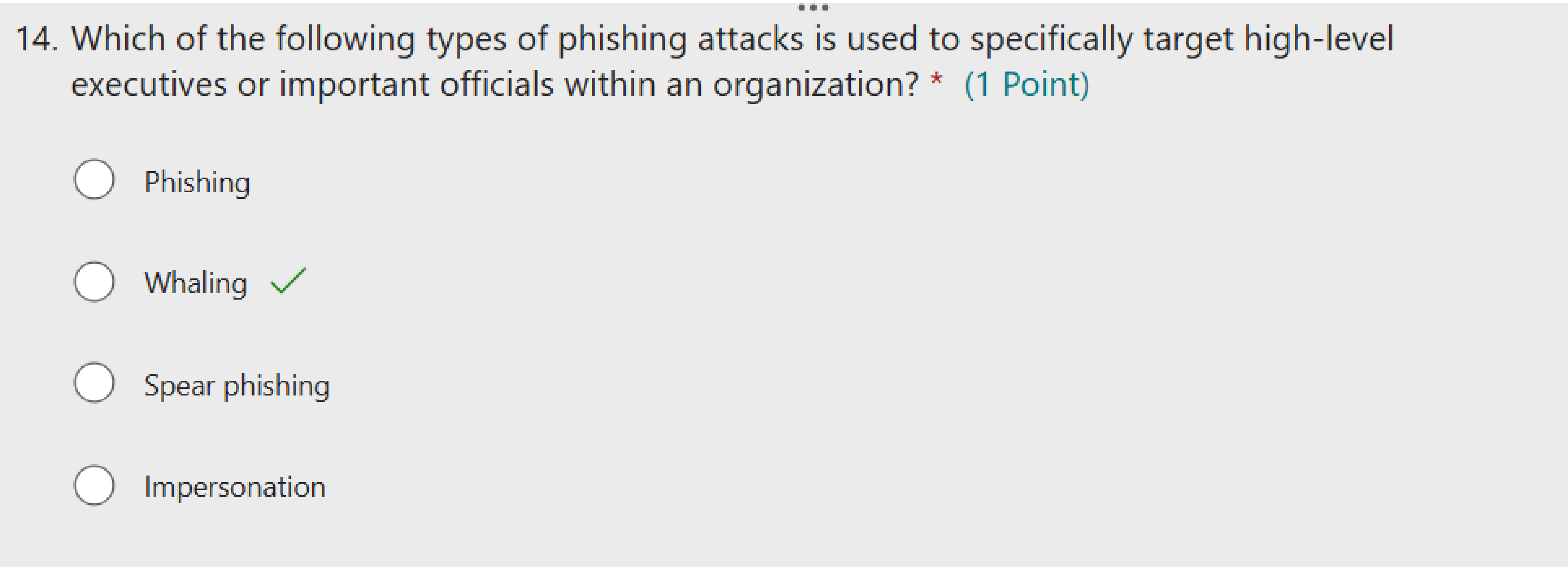
○ Access control vestibule ✓

○ Motion detection sensors

○ Video surveillance

# Labs


Assignments


14. Which of the following types of phishing attacks is used to specifically target high-level executives or important officials within an organization? * (1 Point)

○ Phishing

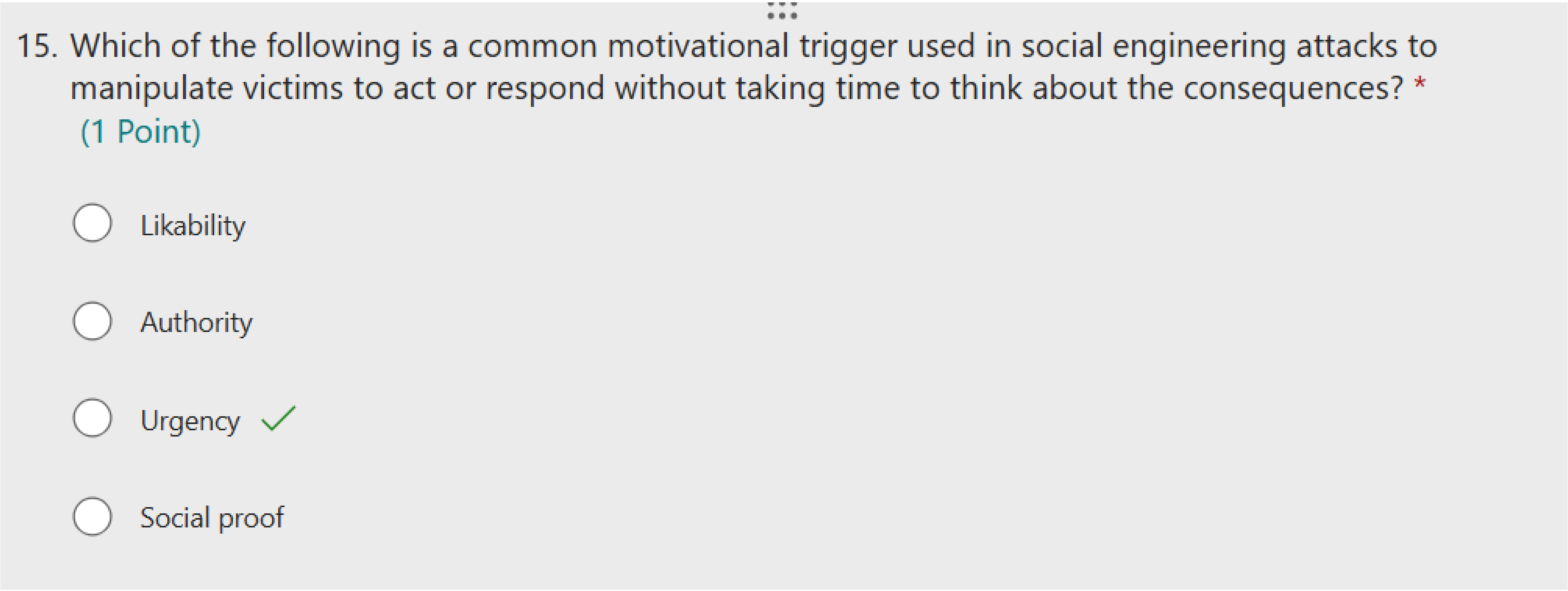
○ Whaling ✓

○ Spear phishing

○ Impersonation

# Labs

Assignments



15. Which of the following is a common motivational trigger used in social engineering attacks to manipulate victims to act or respond without taking time to think about the consequences? *
(1 Point)

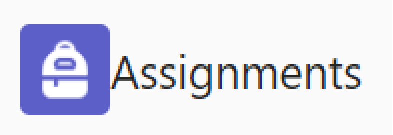
○ Likability

○ Authority

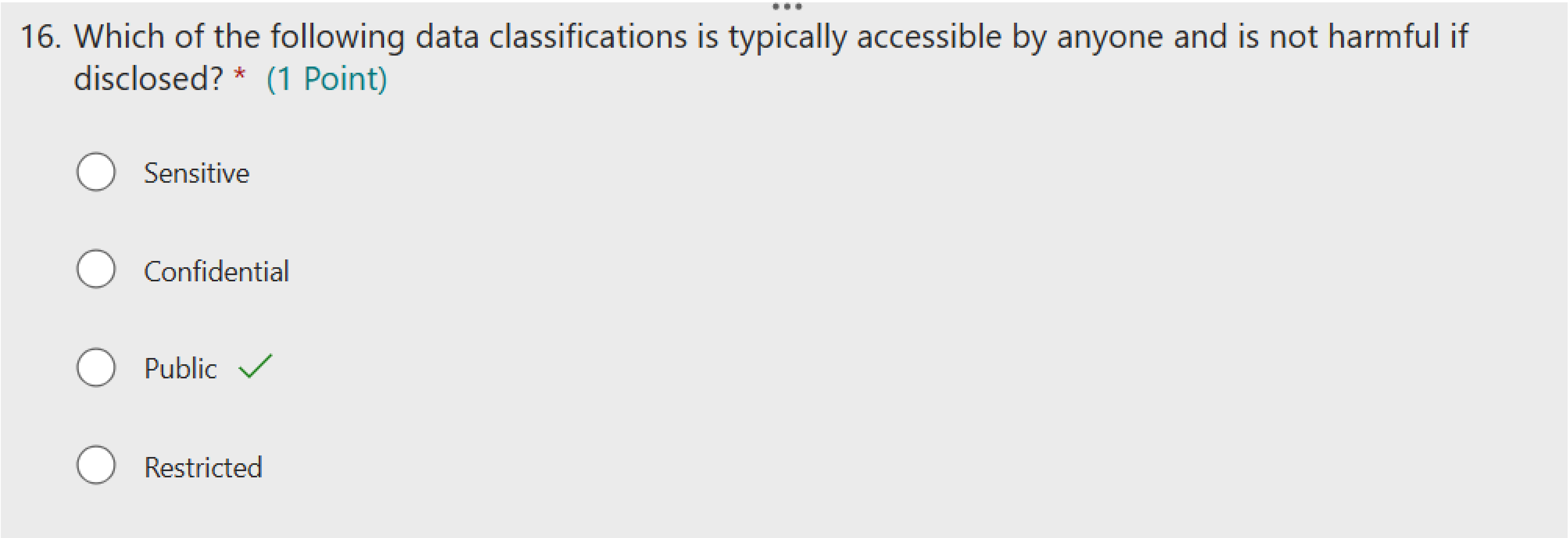
○ Urgency ✓

○ Social proof

# Labs



Assignments



16. Which of the following data classifications is typically accessible by anyone and is not harmful if disclosed? * (1 Point)

○ Sensitive

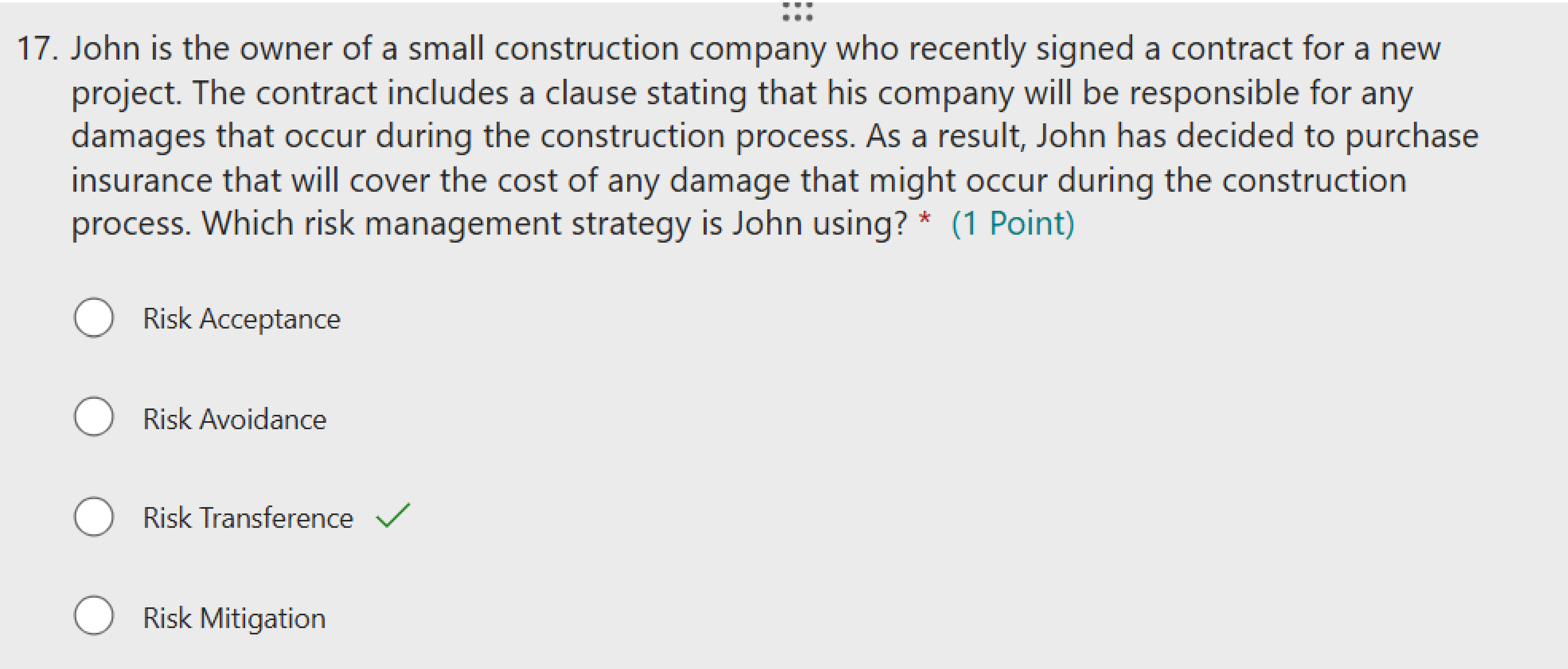
○ Confidential

○ Public ✓

○ Restricted

# Labs

Assignments



17. John is the owner of a small construction company who recently signed a contract for a new project. The contract includes a clause stating that his company will be responsible for any damages that occur during the construction process. As a result, John has decided to purchase insurance that will cover the cost of any damage that might occur during the construction process. Which risk management strategy is John using? * (1 Point)

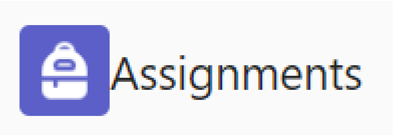
○ Risk Acceptance

○ Risk Avoidance

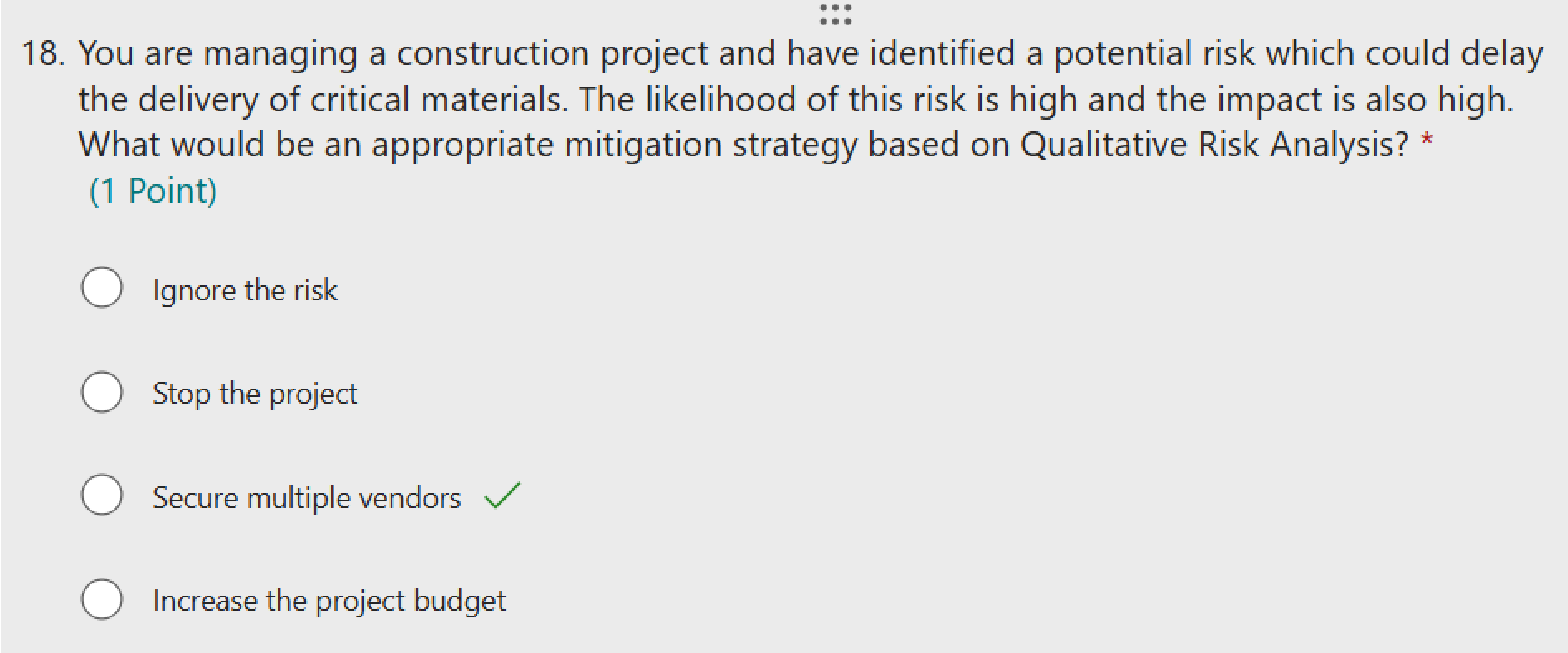
○ Risk Transference ✓

○ Risk Mitigation

# Labs



Assignments



18. You are managing a construction project and have identified a potential risk which could delay the delivery of critical materials. The likelihood of this risk is high and the impact is also high. What would be an appropriate mitigation strategy based on Qualitative Risk Analysis? *
(1 Point)

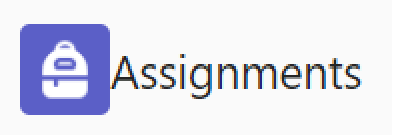
○ Ignore the risk

○ Stop the project

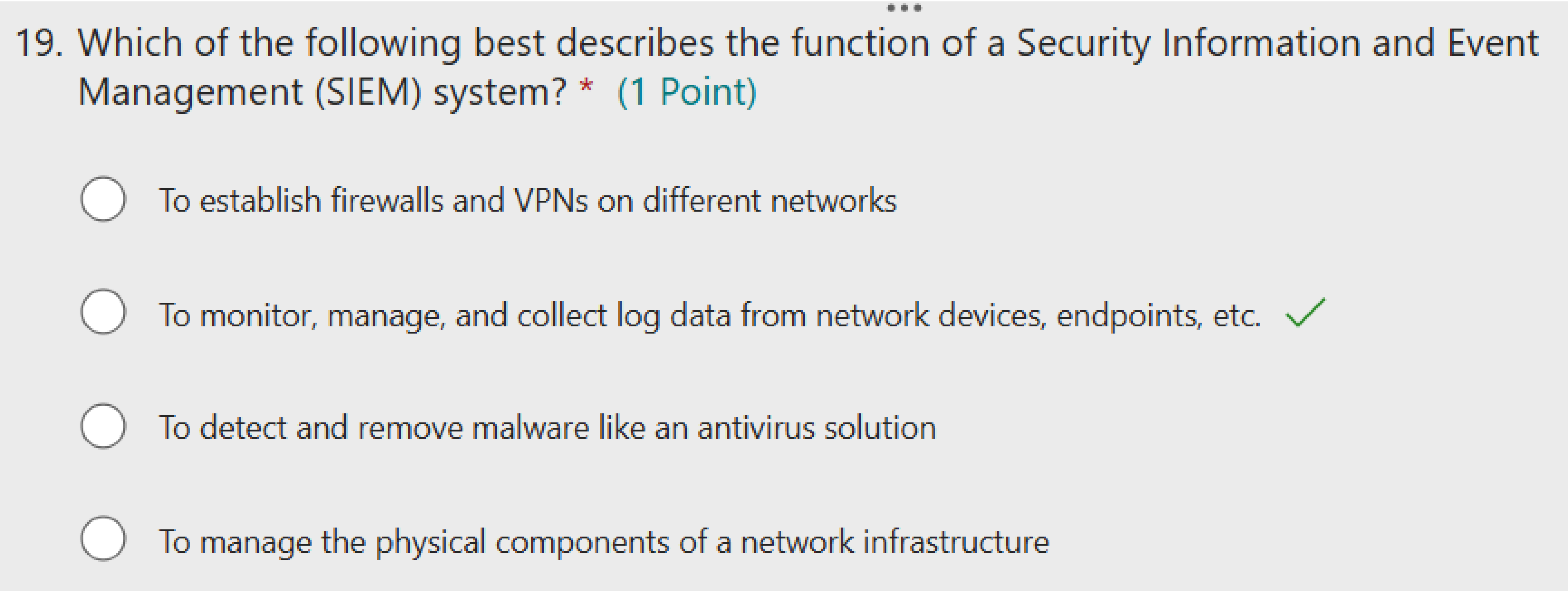
○ Secure multiple vendors ✓

○ Increase the project budget

# Labs



Assignments



19. Which of the following best describes the function of a Security Information and Event Management (SIEM) system? * (1 Point)

○ To establish firewalls and VPNs on different networks

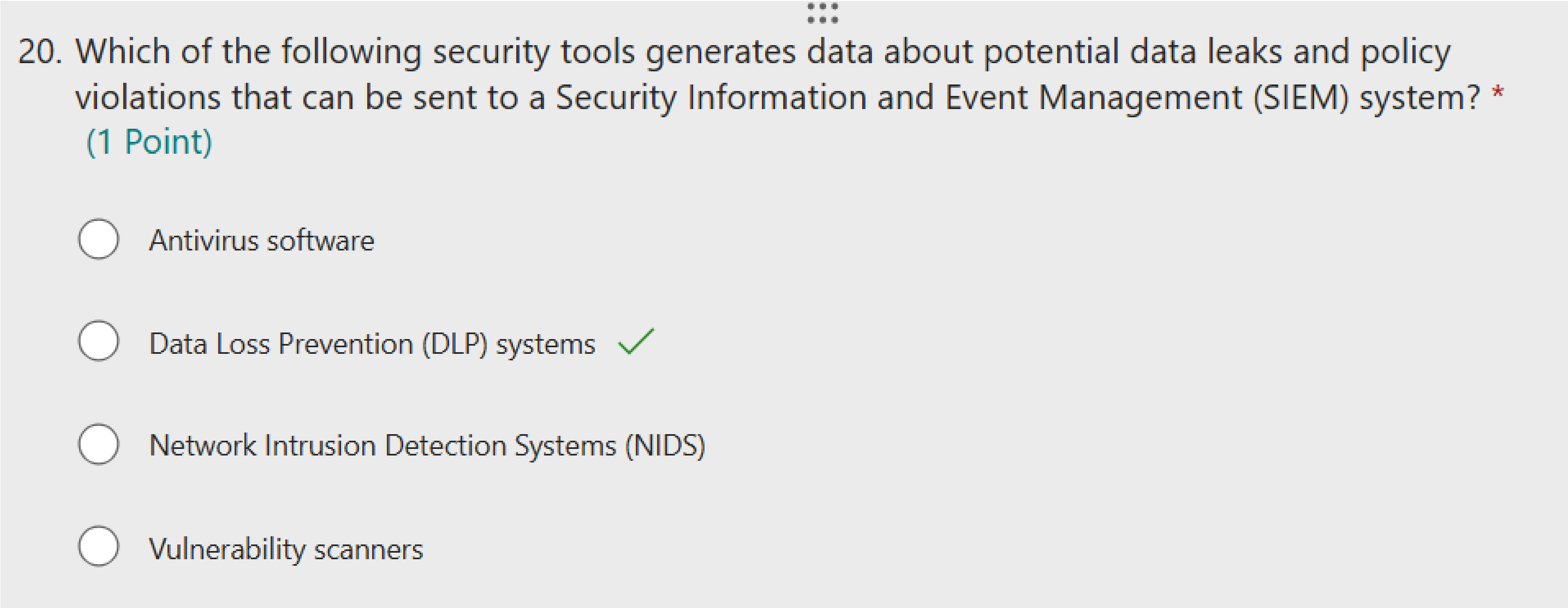
○ To monitor, manage, and collect log data from network devices, endpoints, etc. ✓

○ To detect and remove malware like an antivirus solution

○ To manage the physical components of a network infrastructure

# Labs

Assignments



20. Which of the following security tools generates data about potential data leaks and policy violations that can be sent to a Security Information and Event Management (SIEM) system? * (1 Point)

○ Antivirus software

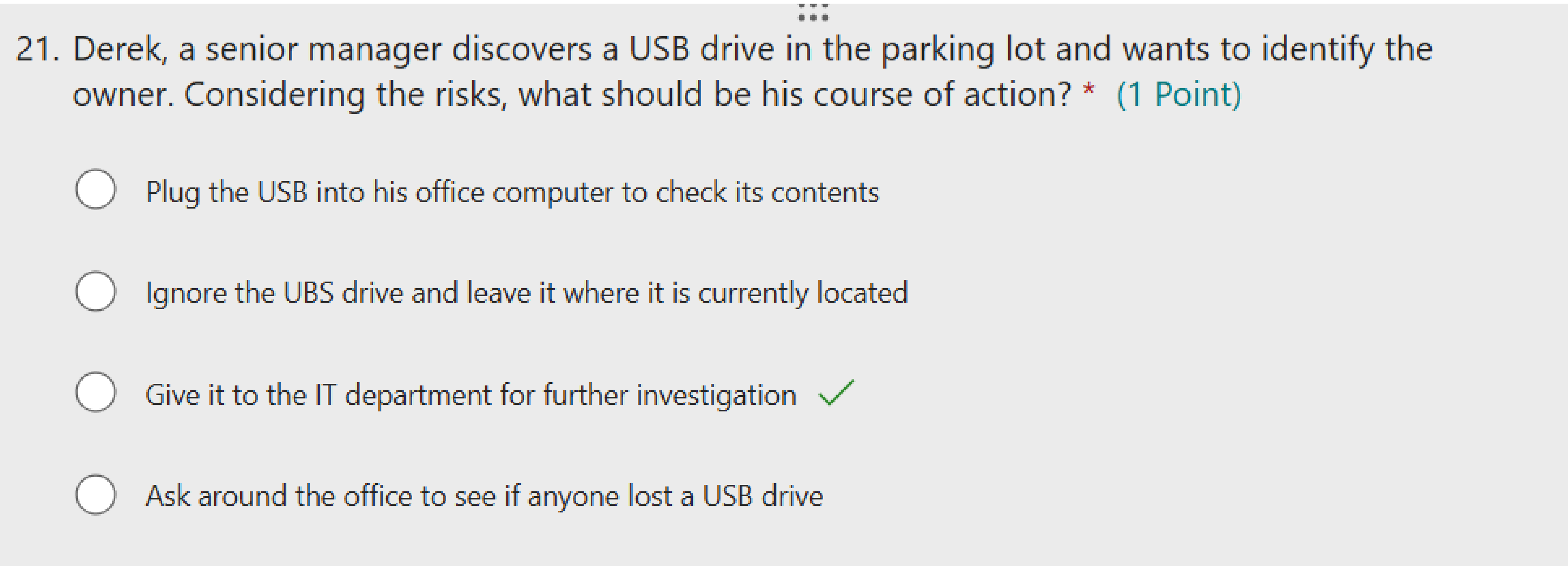
○ Data Loss Prevention (DLP) systems ✓

○ Network Intrusion Detection Systems (NIDS)

○ Vulnerability scanners

# Labs

Assignments



21. Derek, a senior manager discovers a USB drive in the parking lot and wants to identify the owner. Considering the risks, what should be his course of action? * (1 Point)

○ Plug the USB into his office computer to check its contents

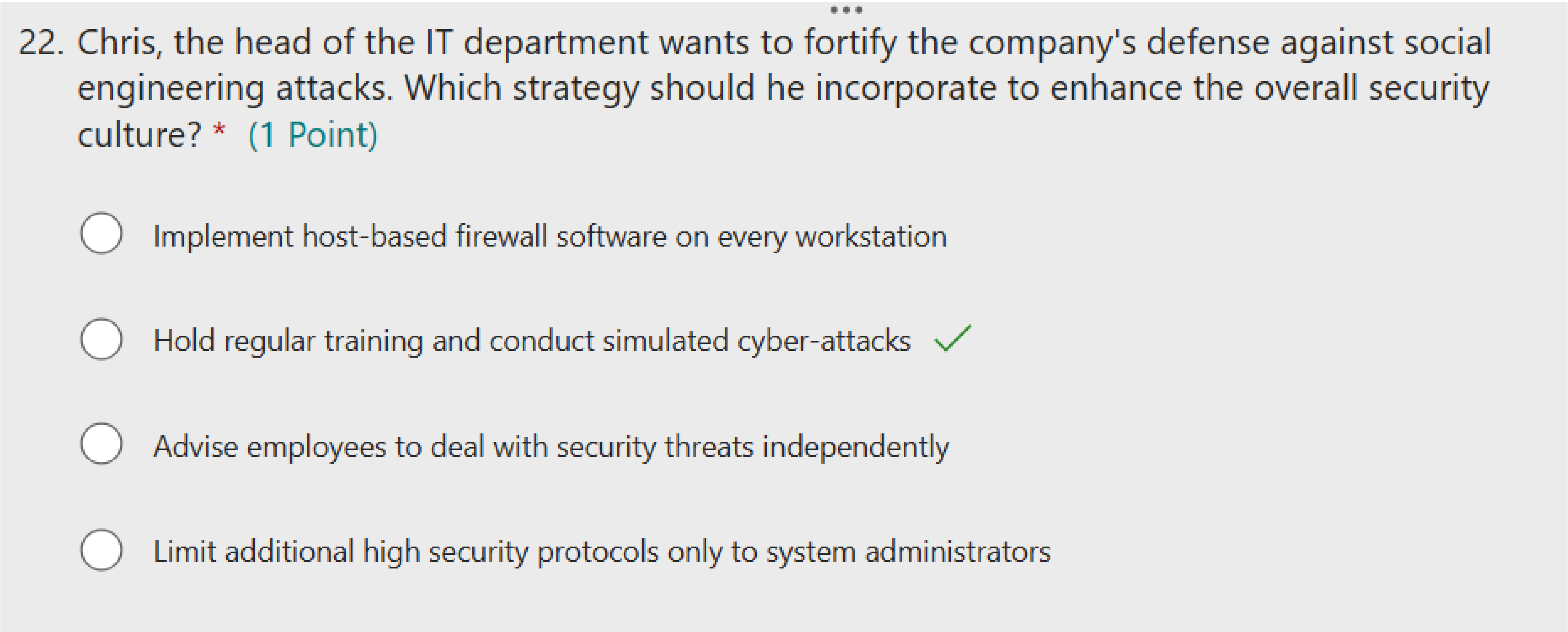
○ Ignore the UBS drive and leave it where it is currently located

○ Give it to the IT department for further investigation ✓

○ Ask around the office to see if anyone lost a USB drive

# Labs

Assignments



22. Chris, the head of the IT department wants to fortify the company's defense against social engineering attacks. Which strategy should he incorporate to enhance the overall security culture? * (1 Point)

○ Implement host-based firewall software on every workstation

○ Hold regular training and conduct simulated cyber-attacks ✓

○ Advise employees to deal with security threats independently

○ Limit additional high security protocols only to system administrators

# In the previous lession…

# NIS2 (TIS2)

**NIS2 –** The second Network and Information Security Directive

**TIS2 -** Antroji ES tinklų ir informacinių sistemų saugumo direktyva

# NIS2 (TIS2)

**LIETUVOS RESPUBLIKOS**

**KIBERNETINIO SAUGUMO ĮSTATYMO**

**NR. *XII-1428***

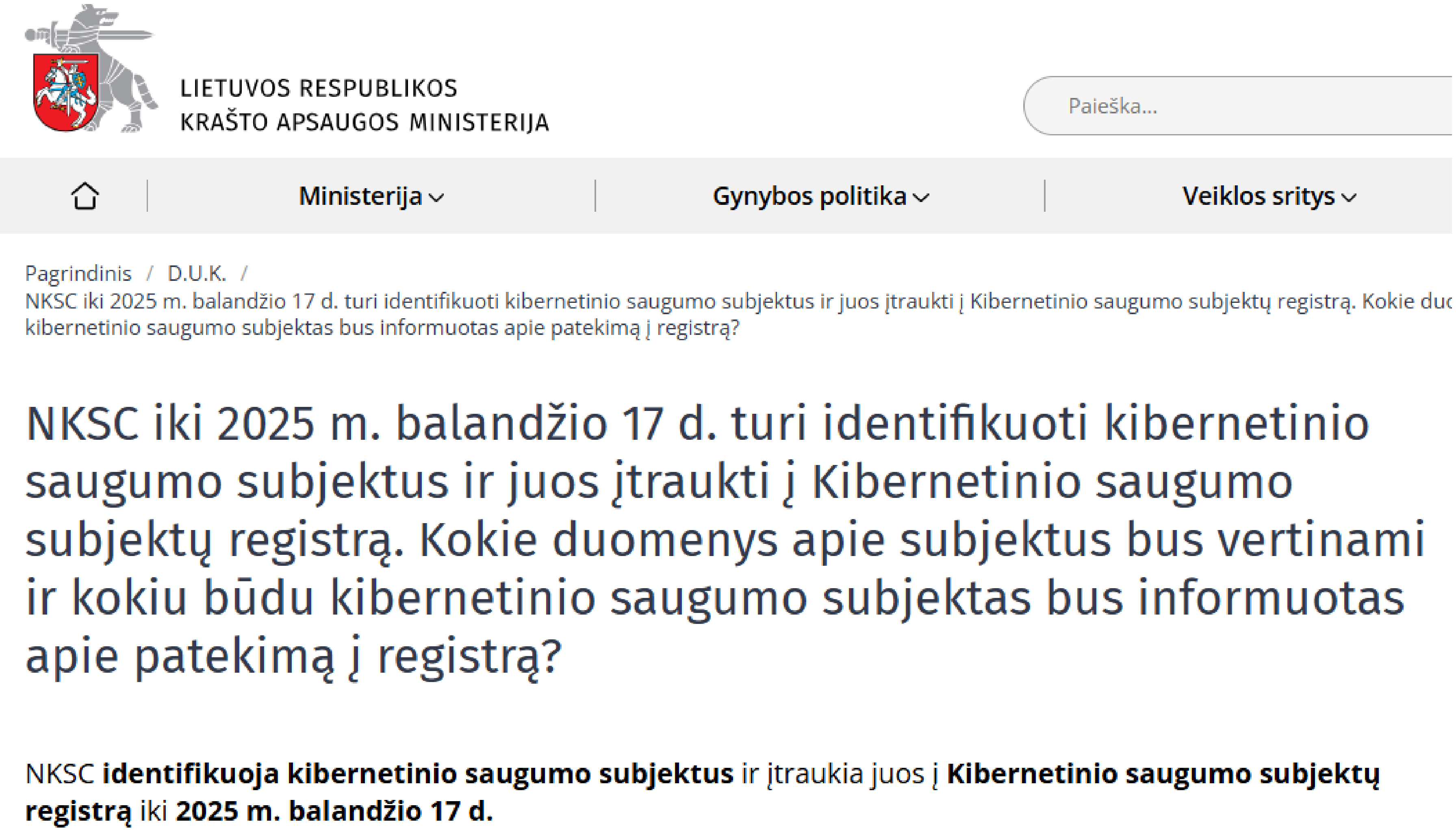
**PAKEITIMO ĮSTATYMAS**

2024 m. liepos 11 d. Nr. XIV-2902

Įsigaliojo nuo 2024 m. spalio 18 d.

LIETUVOS
RESPUBLIKOS
KRAŠTO APSAUGOS
MINISTERIJA

# NIS2 (TIS2)

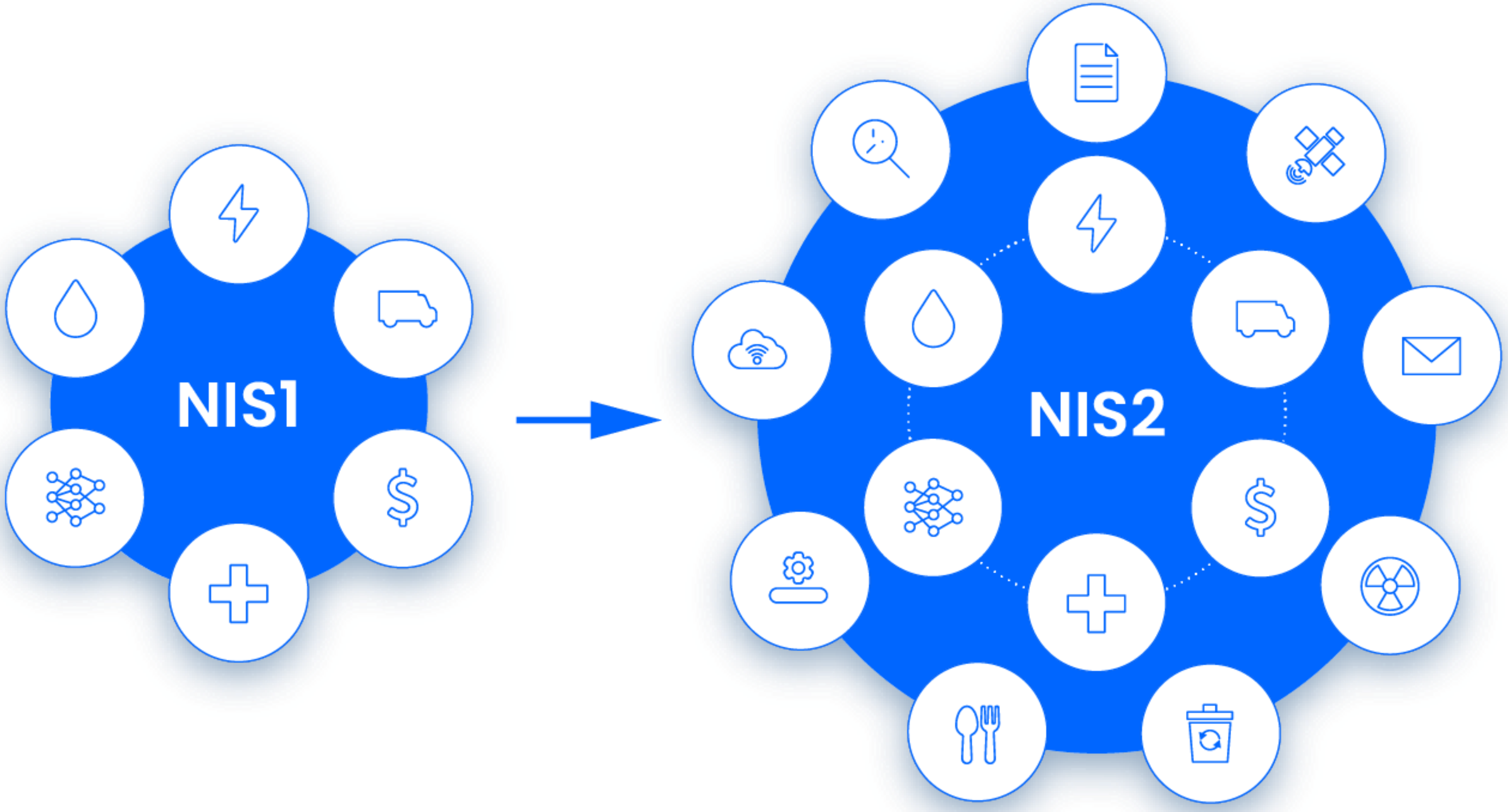


Pagrindinis / D.U.K. /
NKSC iki 2025 m. balandžio 17 d. turi identifikuoti kibernetinio saugumo subjektus ir juos įtraukti į Kibernetinio saugumo subjektų registrą. Kokie duc
kibernetinio saugumo subjektas bus informuotas apie patekimą į registrą?

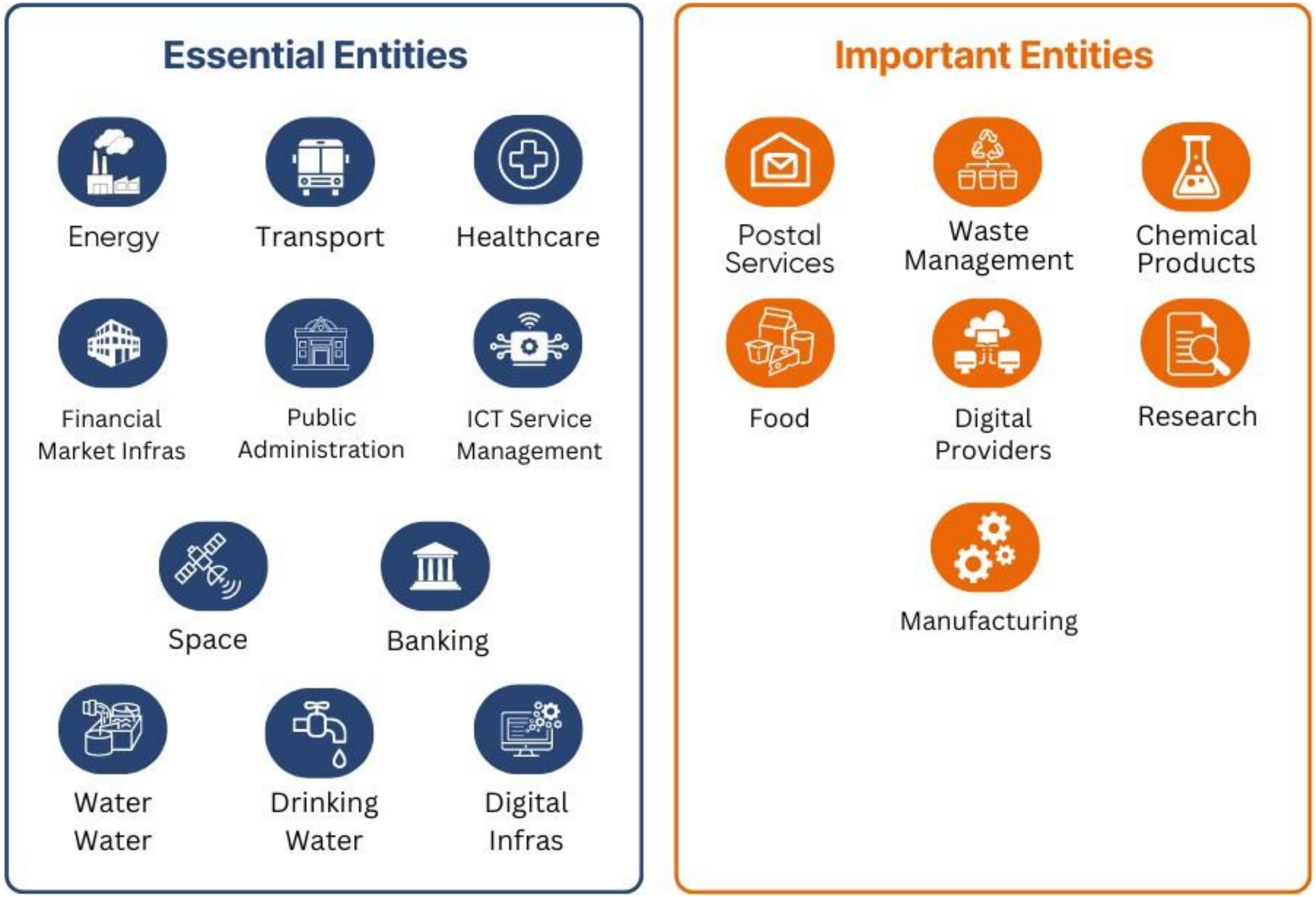
## NKSC iki 2025 m. balandžio 17 d. turi identifikuoti kibernetinio saugumo subjektus ir juos įtraukti į Kibernetinio saugumo subjektų registrą. Kokie duomenys apie subjektus bus vertinami ir kokiu būdu kibernetinio saugumo subjektas bus informuotas apie patekimą į registrą?

NKSC **identifikuoja kibernetinio saugumo subjektus** ir įtraukia juos į **Kibernetinio saugumo subjektų registrą** iki **2025 m. balandžio 17 d.**

# NIS1 vs NIS2



# Essential and Important Entities



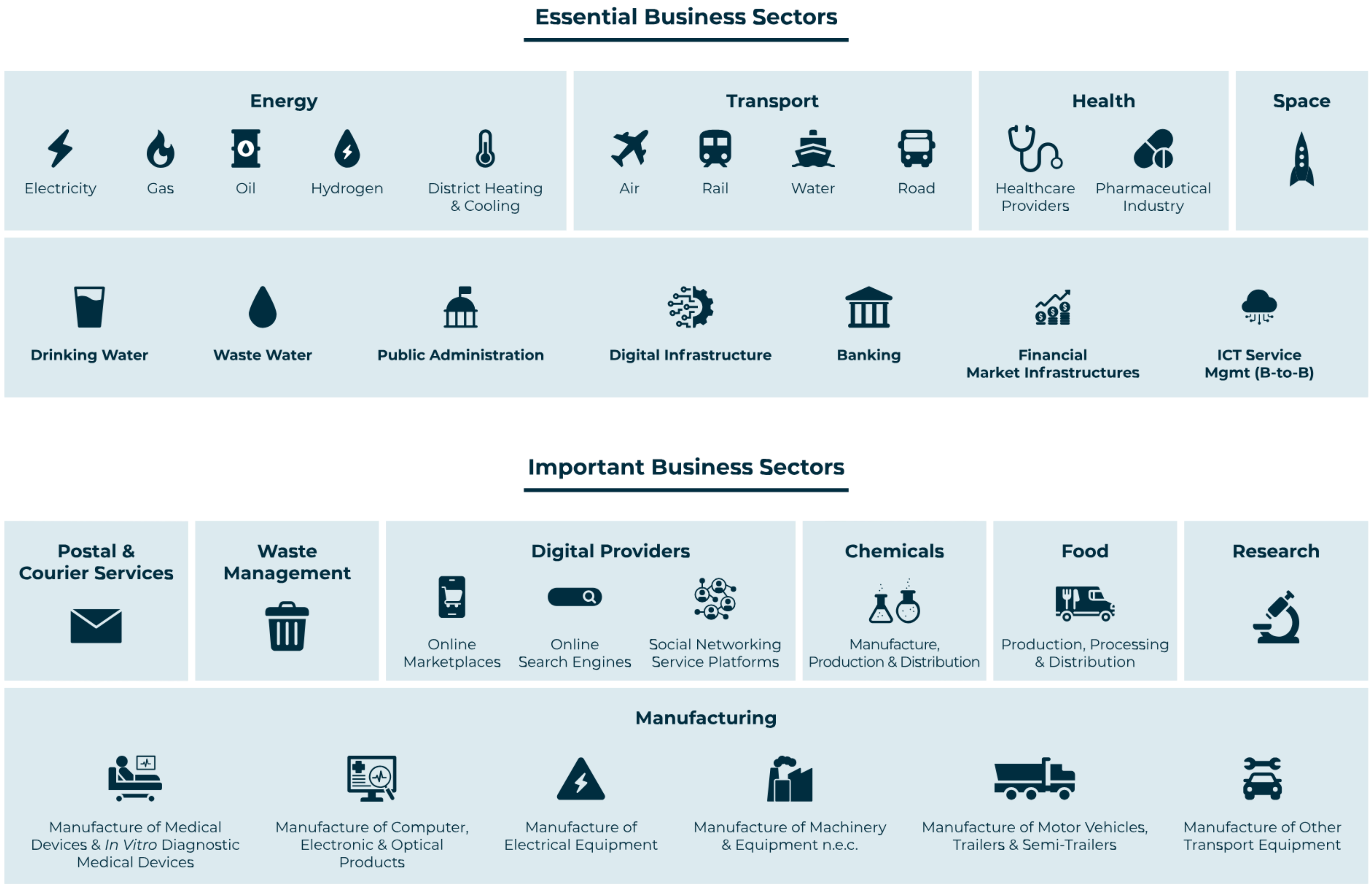
## Essential Entities

- Energy
- Transport
- Healthcare
- Financial Market Infras
- Public Administration
- ICT Service Management
- Space
- Banking
- Water Water
- Drinking Water
- Digital Infras

## Important Entities

- Postal Services
- Waste Management
- Chemical Products
- Food
- Digital Providers
- Research
- Manufacturing

# Essential and Important Entities



## Essential Business Sectors

### Energy
- Electricity
- Gas
- Oil
- Hydrogen
- District Heating & Cooling

### Transport
- Air
- Rail
- Water
- Road

### Health
- Healthcare Providers
- Pharmaceutical Industry

### Space

- **Drinking Water**
- **Waste Water**
- **Public Administration**
- **Digital Infrastructure**
- **Banking**
- **Financial Market Infrastructures**
- **ICT Service Mgmt (B-to-B)**

## Important Business Sectors

### Postal & Courier Services

### Waste Management

### Digital Providers
- Online Marketplaces
- Online Search Engines
- Social Networking Service Platforms

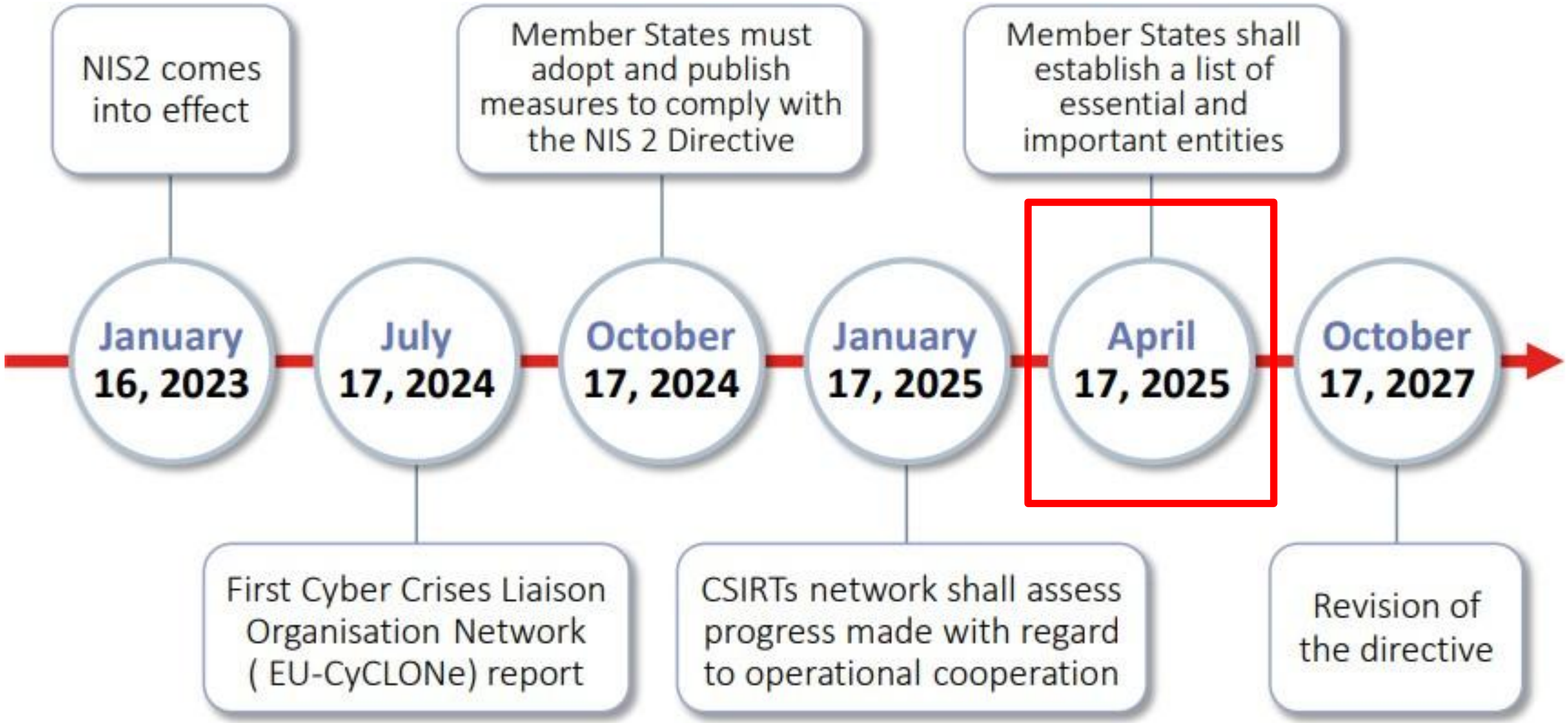
### Chemicals
- Manufacture, Production & Distribution

### Food
- Production, Processing & Distribution

### Research

### Manufacturing
- Manufacture of Medical Devices & *In Vitro* Diagnostic Medical Devices
- Manufacture of Computer, Electronic & Optical Products
- Manufacture of Electrical Equipment
- Manufacture of Machinery & Equipment n.e.c.
- Manufacture of Motor Vehicles, Trailers & Semi-Trailers
- Manufacture of Other Transport Equipment

# NIS2 Timeline



January 16, 2023 – NIS2 comes into effect

July 17, 2024 – First Cyber Crises Liaison Organisation Network ( EU-CyCLONe) report

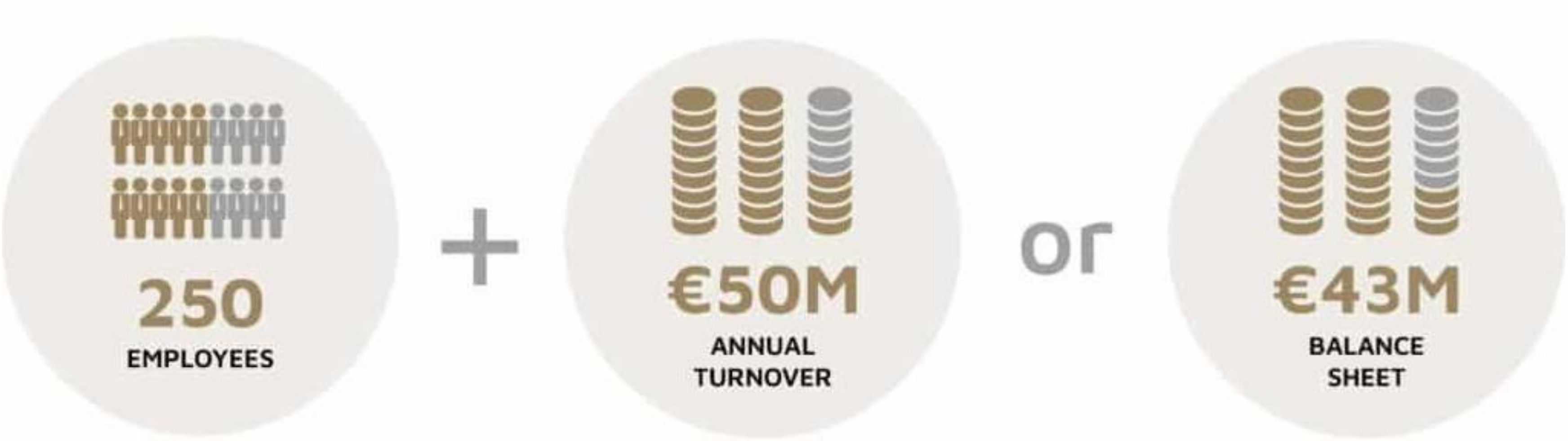
October 17, 2024 – Member States must adopt and publish measures to comply with the NIS 2 Directive

January 17, 2025 – CSIRTs network shall assess progress made with regard to operational cooperation

April 17, 2025 – Member States shall establish a list of essential and important entities

October 17, 2027 – Revision of the directive

# Essential Entity Thresholds



250

EMPLOYEES

+

€50M

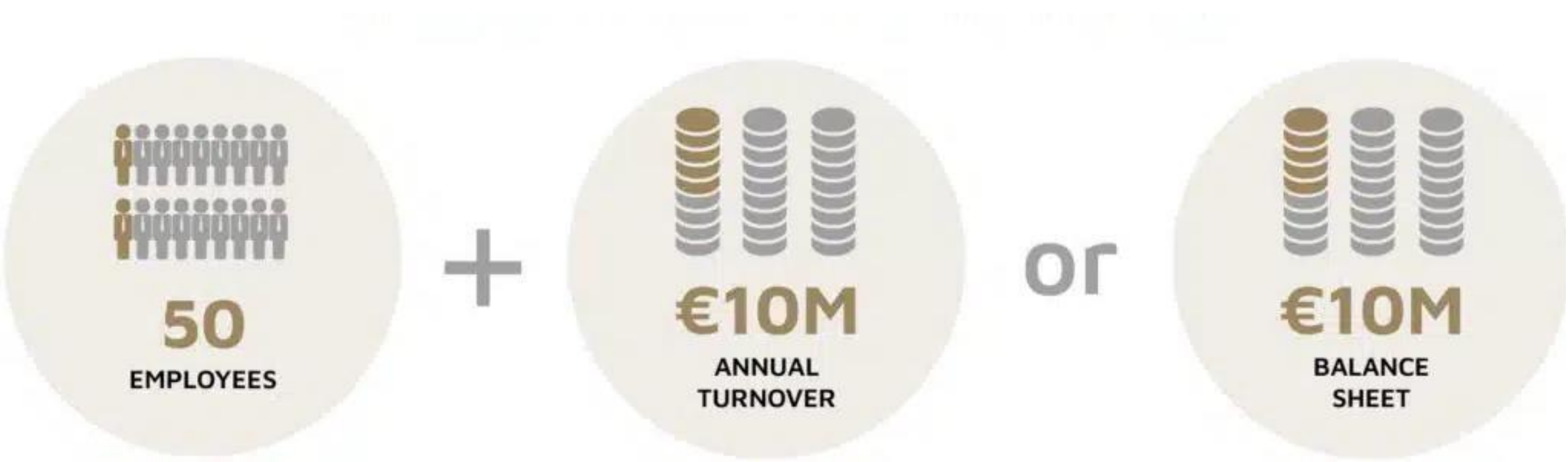
ANNUAL TURNOVER

or

€43M

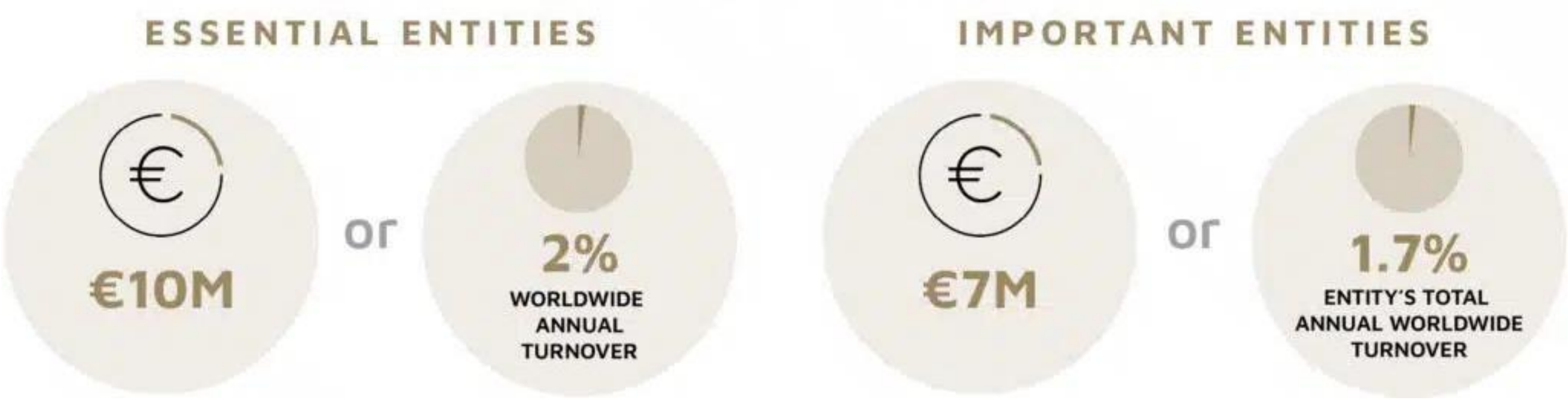
BALANCE SHEET

# Important Entity Thresholds



Exclusions*

# NIS2 Penalties



ESSENTIAL ENTITIES

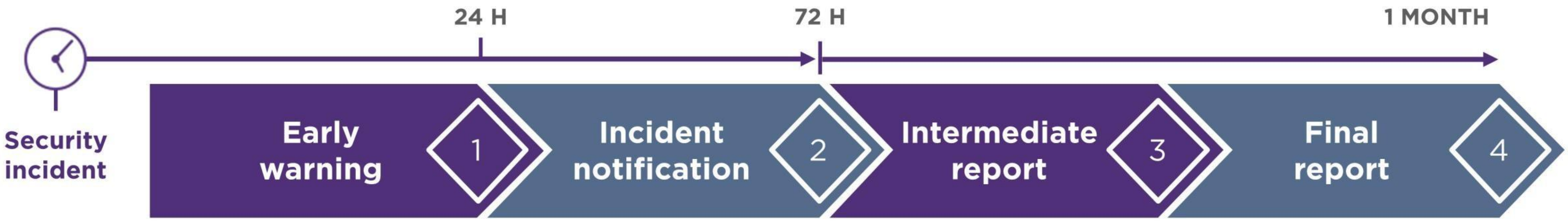
€10M or 2% WORLDWIDE ANNUAL TURNOVER

IMPORTANT ENTITIES

€7M or 1.7% ENTITY'S TOTAL ANNUAL WORLDWIDE TURNOVER

Exclusions*

# Security incident reporting



24 H

72 H

1 MONTH

Security incident

Early warning 1

Incident notification 2

Intermediate report 3

Final report 4

Indicating whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact

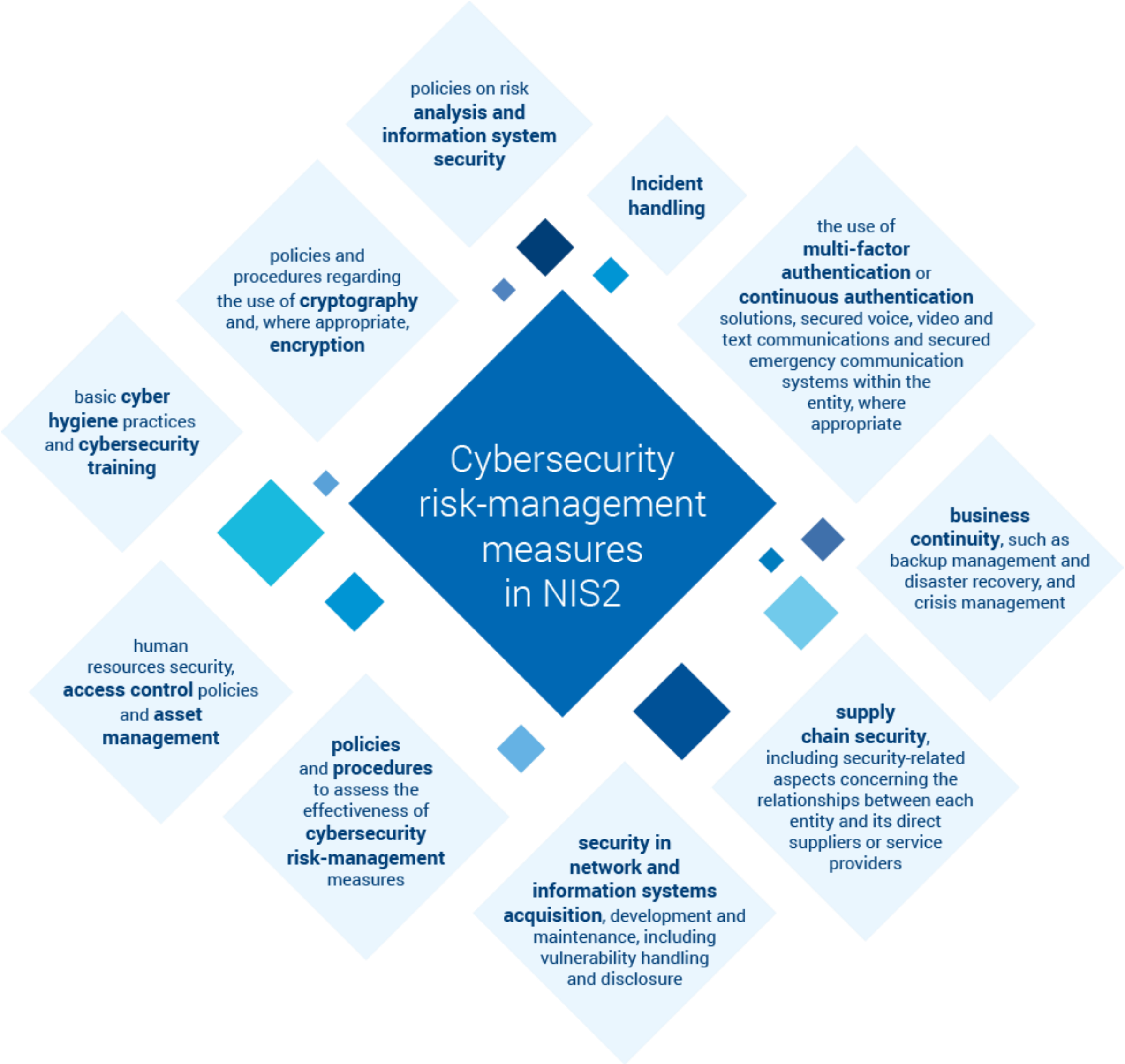
Updating the previous warning and indicating an initial assessment of the significant incident, including its severity and impact and the indicators of compromise

Upon request and concerning relevant status updates

Including :

- Detailed description of the incident
- Type of threat or root cause
- Mitigation measures
- Cross-border impact

# NIS2 Measures



Cybersecurity risk-management measures in NIS2

policies on risk **analysis and information system security**

**Incident handling**

policies and procedures regarding the use of **cryptography** and, where appropriate, **encryption**

the use of **multi-factor authentication** or **continuous authentication** solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate

basic **cyber hygiene** practices and **cybersecurity training**

**business continuity**, such as backup management and disaster recovery, and crisis management

human resources security, **access control** policies and **asset management**

**policies and procedures** to assess the effectiveness of **cybersecurity risk-management** measures

**supply chain security**, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers

**security in network and information systems acquisition**, development and maintenance, including vulnerability handling and disclosure

# NIS2 Compliance

Kibernetinio saugumo subjektai nustatytus organizacinius kibernetinio saugumo reikalavimus privalo įgyvendinti ne vėliau kaip per 12 mėnesių nuo jų įtraukimo į Kibernetinio saugumo subjektų registrą.

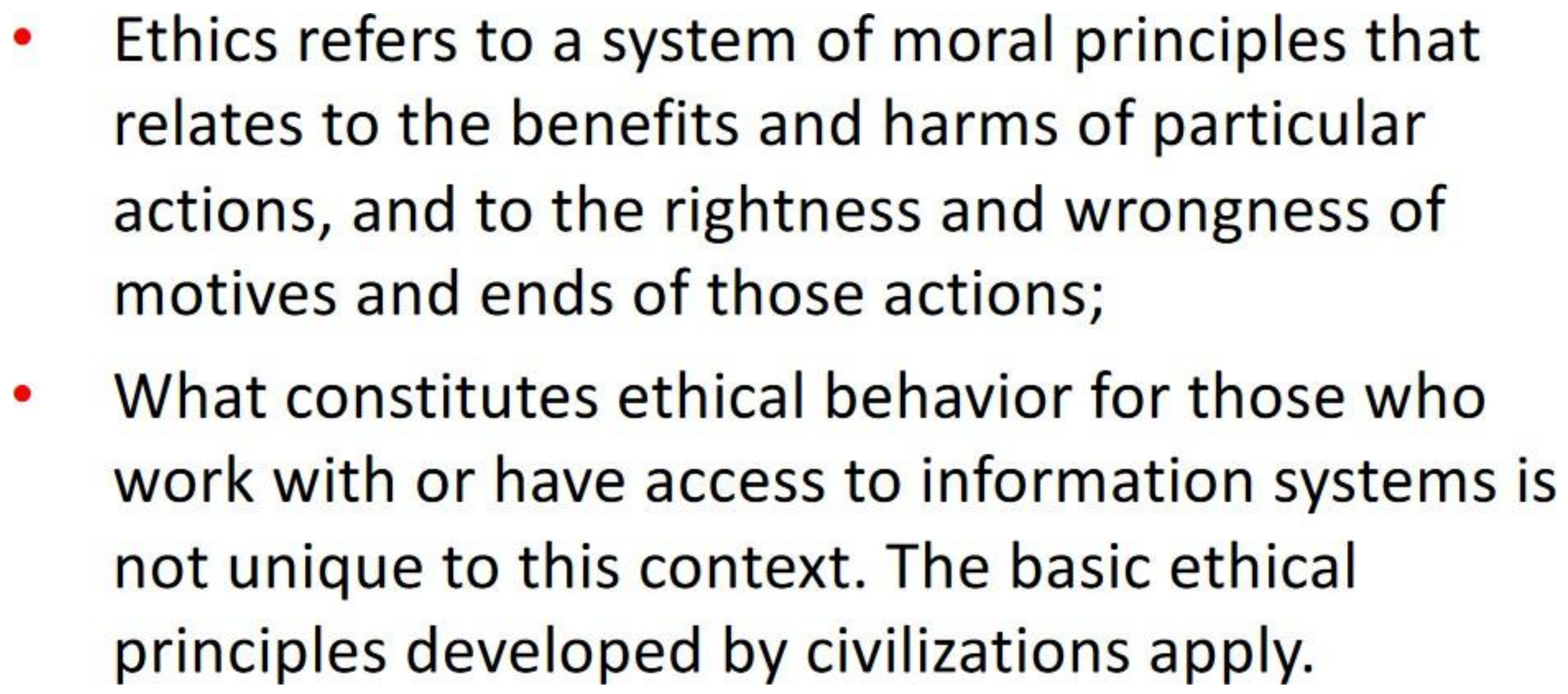
Kibernetinio saugumo subjektai nustatytus techninius kibernetinio saugumo reikalavimus privalo įgyvendinti ne vėliau kaip per 24 mėnesius nuo jų įtraukimo į Kibernetinio saugumo subjektų registrą.

# Lession 10

# Legal aspects of cyber security

(Ethical Issues)

# Ethical Issues

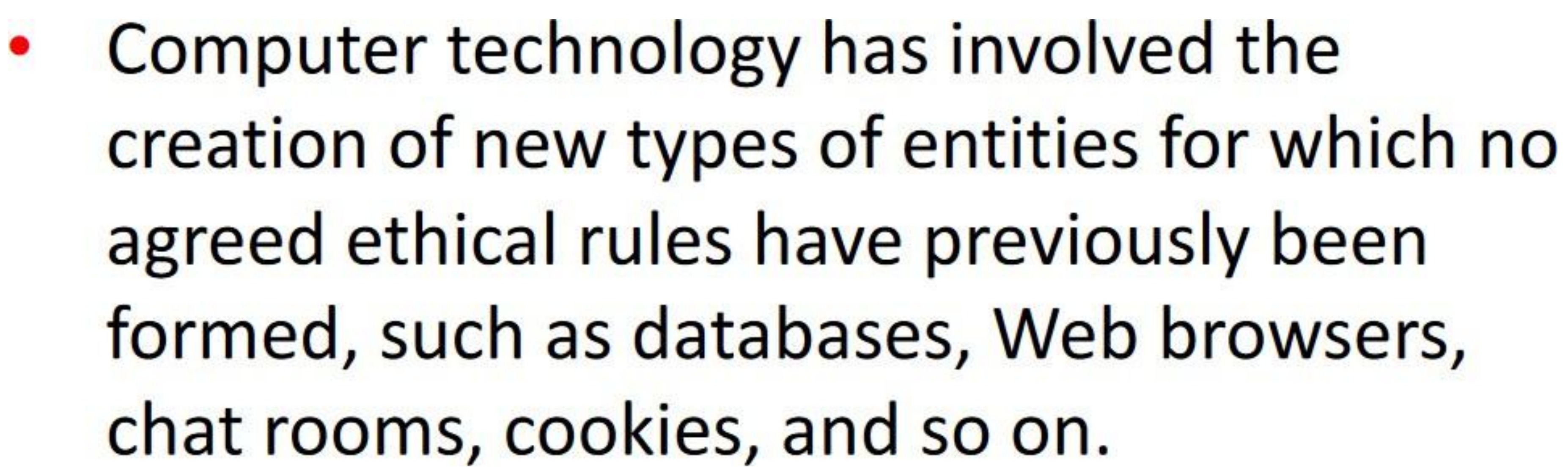


- Ethics refers to a system of moral principles that relates to the benefits and harms of particular actions, and to the rightness and wrongness of motives and ends of those actions;
- What constitutes ethical behavior for those who work with or have access to information systems is not unique to this context. The basic ethical principles developed by civilizations apply.

# Ethical Issues

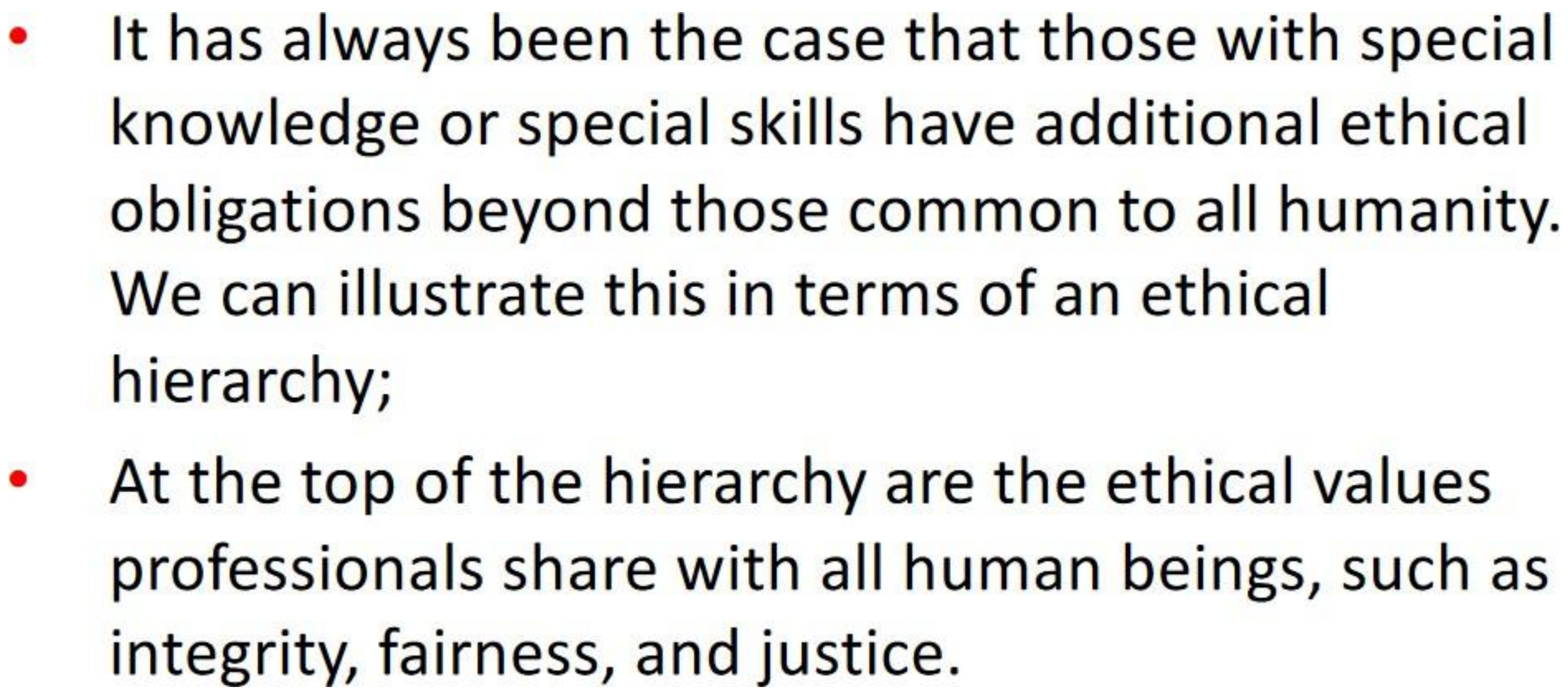
- Ethics is a system of moral principles relating benefits and harms of particular actions to rightness and wrongness of motives and ends of them;
- Have potential misuses/abuses of information and electronic communication that create privacy and security problems;
- Ethical behavior here not unique, but do have some unique considerations in scale of activities, in new types of entities.

# Ethical Issues



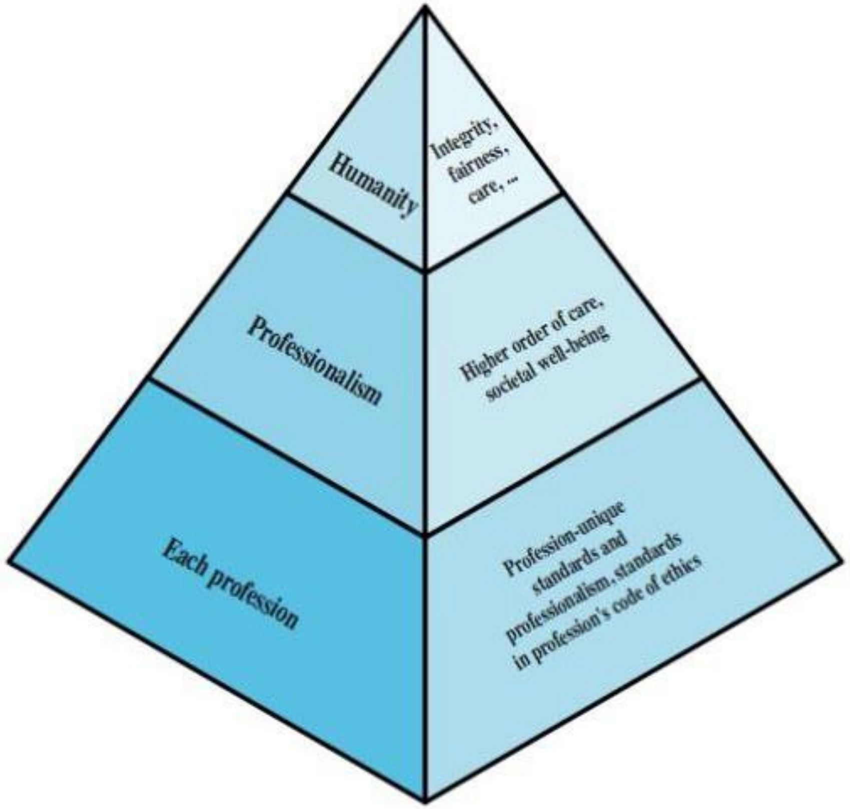
- Computer technology has involved the creation of new types of entities for which no agreed ethical rules have previously been formed, such as databases, Web browsers, chat rooms, cookies, and so on.

# Ethical Hierarchy

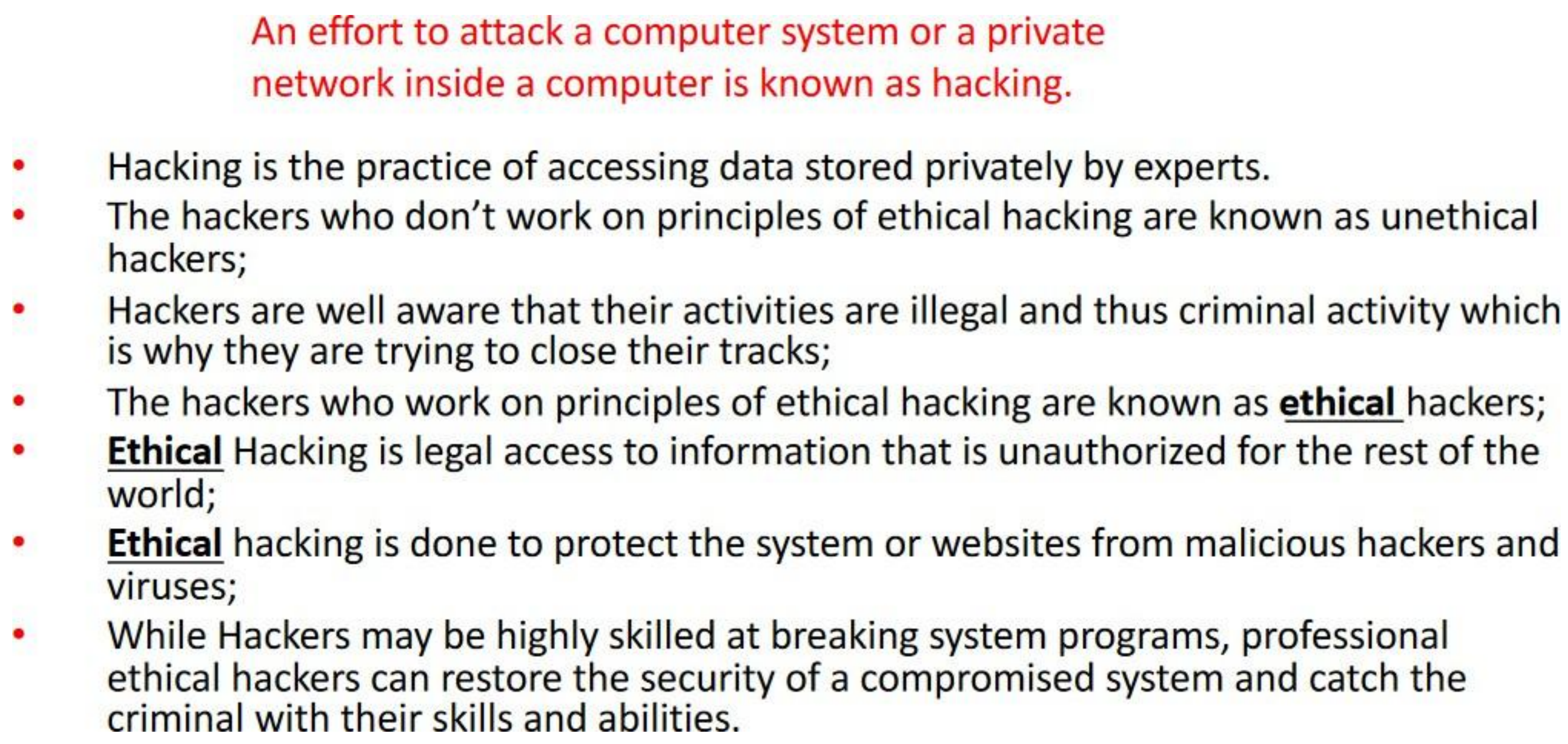


- It has always been the case that those with special knowledge or special skills have additional ethical obligations beyond those common to all humanity. We can illustrate this in terms of an ethical hierarchy;
- At the top of the hierarchy are the ethical values professionals share with all human beings, such as integrity, fairness, and justice.

# Ethical Hierarchy


Humanity
Integrity, fairness, care, ...
Professionalism
Higher order of care, societal well-being
Each profession
Profession-unique standards and professionalism, standards in profession's code of ethics

# Ethical hacking vs hacking

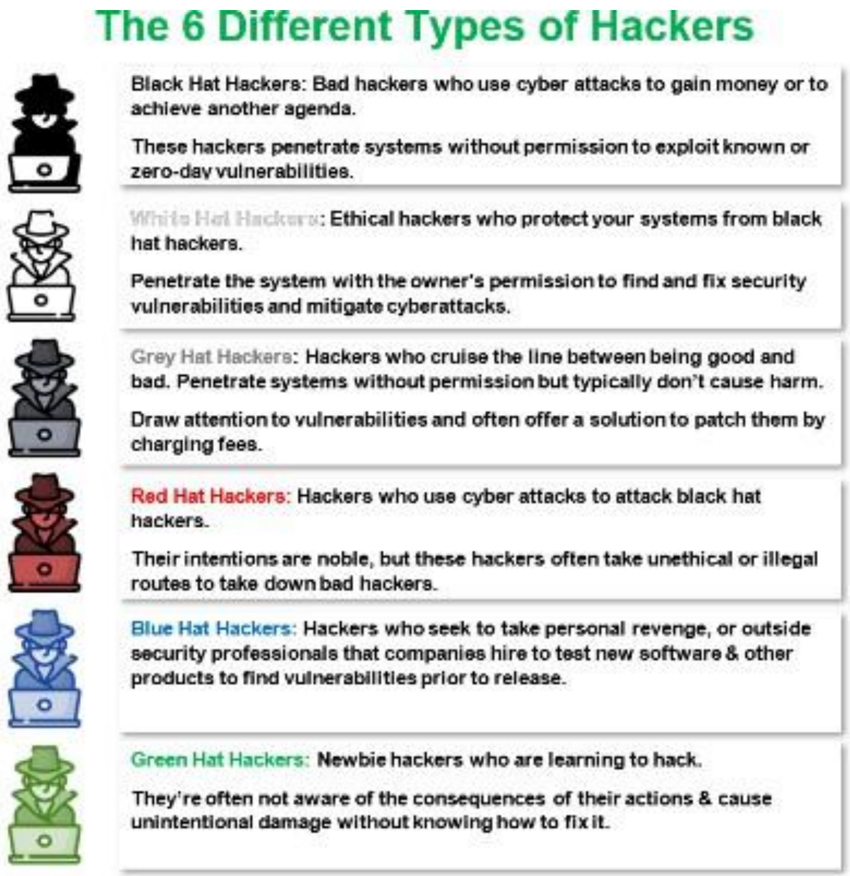


An effort to attack a computer system or a private network inside a computer is known as hacking.

- Hacking is the practice of accessing data stored privately by experts.
- The hackers who don’t work on principles of ethical hacking are known as unethical hackers;
- Hackers are well aware that their activities are illegal and thus criminal activity which is why they are trying to close their tracks;
- The hackers who work on principles of ethical hacking are known as **ethical** hackers;
- **Ethical** Hacking is legal access to information that is unauthorized for the rest of the world;
- **Ethical** hacking is done to protect the system or websites from malicious hackers and viruses;
- While Hackers may be highly skilled at breaking system programs, professional ethical hackers can restore the security of a compromised system and catch the criminal with their skills and abilities.

# Hackers

- ✓ Suicide Hacker
- ✓ Script Kiddie
- ✓ Spy Hacker
- ✓ Cyber Terrorist
- ✓ State Sponsored Hacker
- ✓ Hacktivist
- ✓ Malicious Insider or Whistle-blower



## The 6 Different Types of Hackers

Black Hat Hackers: Bad hackers who use cyber attacks to gain money or to achieve another agenda.

These hackers penetrate systems without permission to exploit known or zero-day vulnerabilities.

White Hat Hackers: Ethical hackers who protect your systems from black hat hackers.

Penetrate the system with the owner's permission to find and fix security vulnerabilities and mitigate cyberattacks.

Grey Hat Hackers: Hackers who cruise the line between being good and bad. Penetrate systems without permission but typically don't cause harm.

Draw attention to vulnerabilities and often offer a solution to patch them by charging fees.

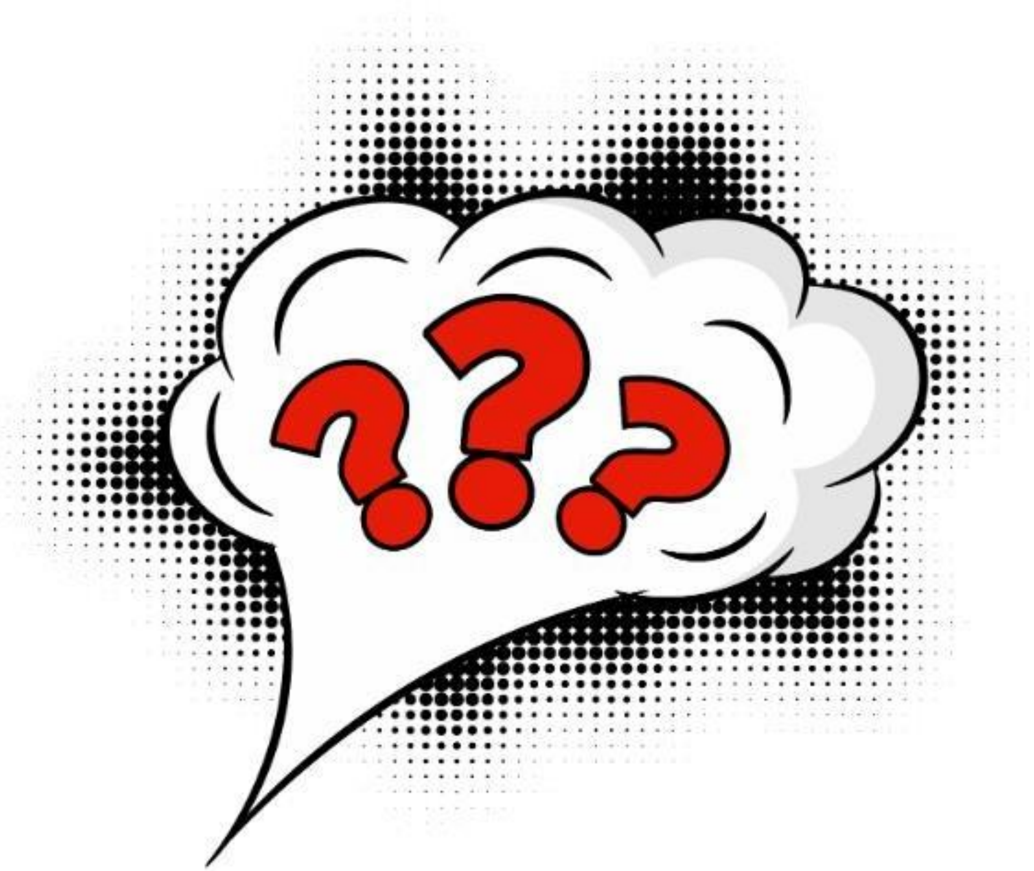
Red Hat Hackers: Hackers who use cyber attacks to attack black hat hackers.

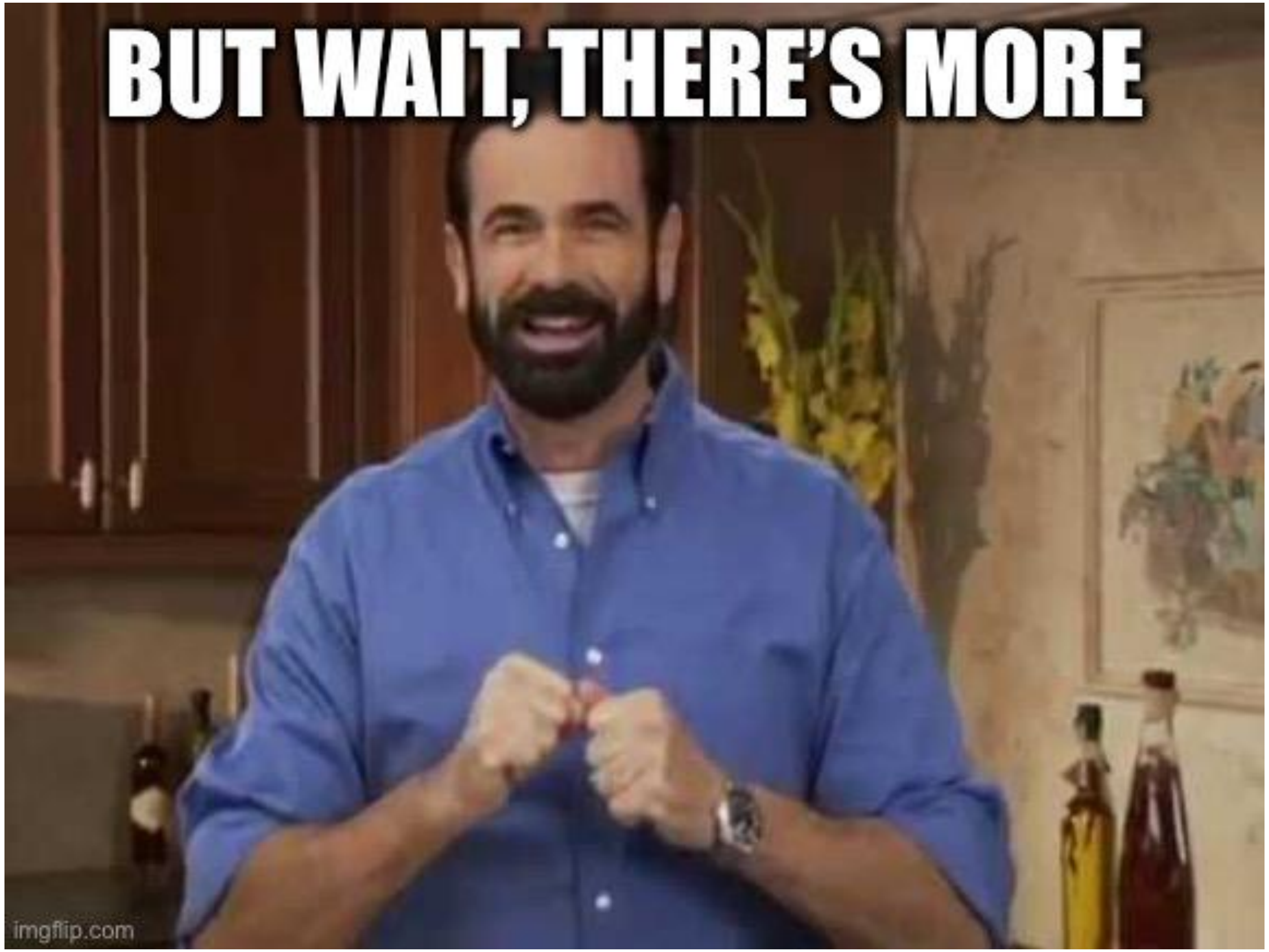
Their intentions are noble, but these hackers often take unethical or illegal routes to take down bad hackers.

Blue Hat Hackers: Hackers who seek to take personal revenge, or outside security professionals that companies hire to test new software & other products to find vulnerabilities prior to release.

Green Hat Hackers: Newbie hackers who are learning to hack.

They're often not aware of the consequences of their actions & cause unintentional damage without knowing how to fix it.




BUT WAIT, THERE'S MORE
imgflip.com

# Social engineering and neoro-linguistic programming

(Chapter 2)

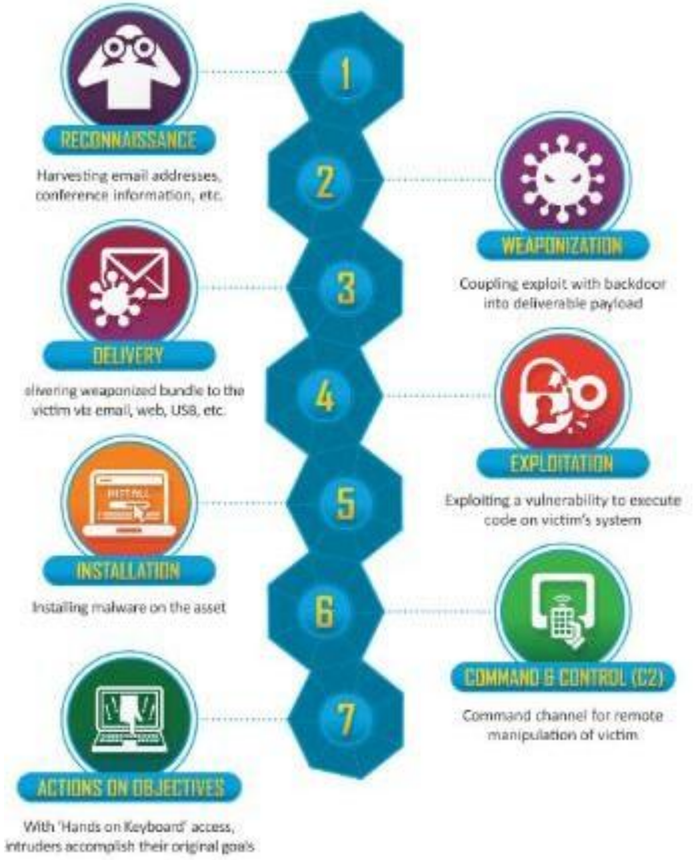
# Introduction

- What is social engineering;
- The most popular techniques (methods);
- Psychological attacks;
- Neurolinguistic programming and neurolinguistics;
- Hybrid attack.

# What is social engineering?

# Cyber attacks

- IT technologies are used, sometimes with psychological manipulations to enhance the effect;
- Less protected technological components or functionalities are exploited;
- Unmanaged or insufficiently well-managed risks are realized;
- Like psychological attacks, they can be predicted using price and value identification.



1 RECONNAISSANCE
Harvesting email addresses, conference information, etc.

2 WEAPONIZATION
Coupling exploit with backdoor into deliverable payload

3 DELIVERY
elivering weaponized bundle to the victim via email, web, USB, etc.

4 EXPLOITATION
Exploiting a vulnerability to execute code on victim's system

5 INSTALLATION
Installing malware on the asset

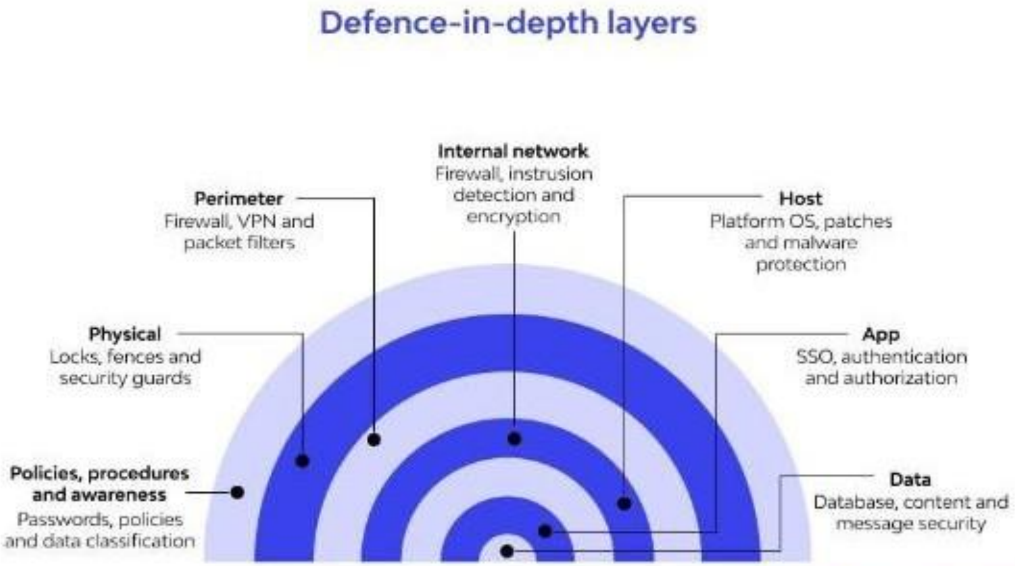
6 COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

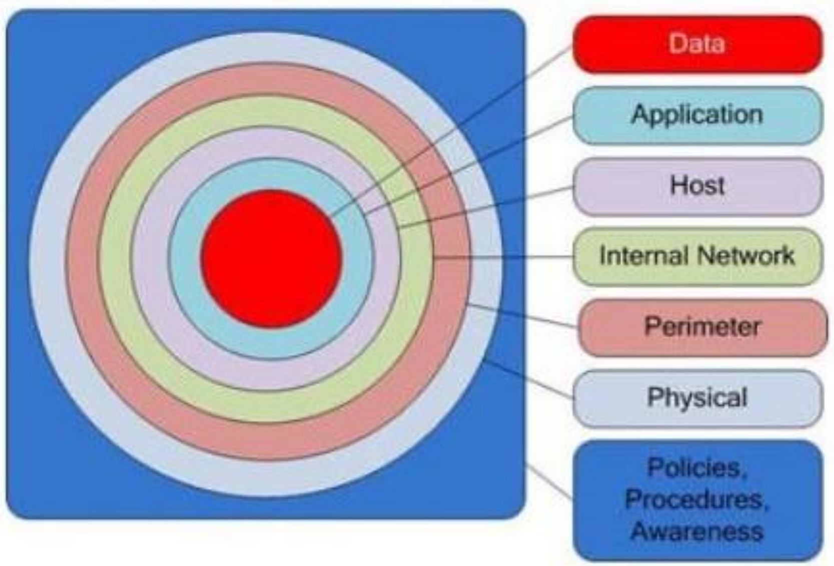
LOCKHEED MARTIN

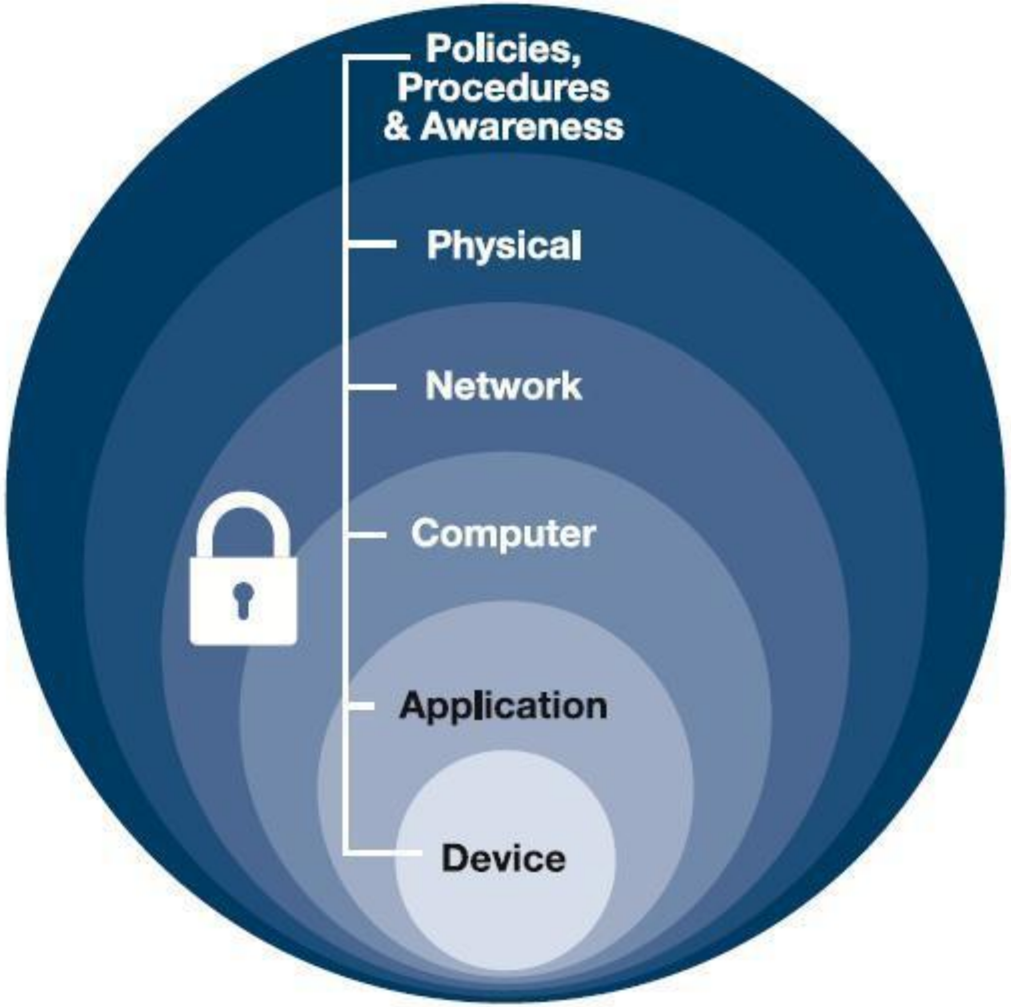
# Defense in depth



Defence-in-depth layers

Internal network
Firewall, instrusion detection and encryption
Perimeter
Firewall, VPN and packet filters
Host
Platform OS, patches and malware protection
Physical
Locks, fences and security guards
App
SSO, authentication and authorization
Policies, procedures and awareness
Passwords, policies and data classification
Data
Database, content and message security





# Not technological and out of management scope of victim attacks

# Nature

- Fires;
- Floods and flooding;
- High temperature and humidity;
- Lightning;
- Storms;
- Dust;
- Solar activity.

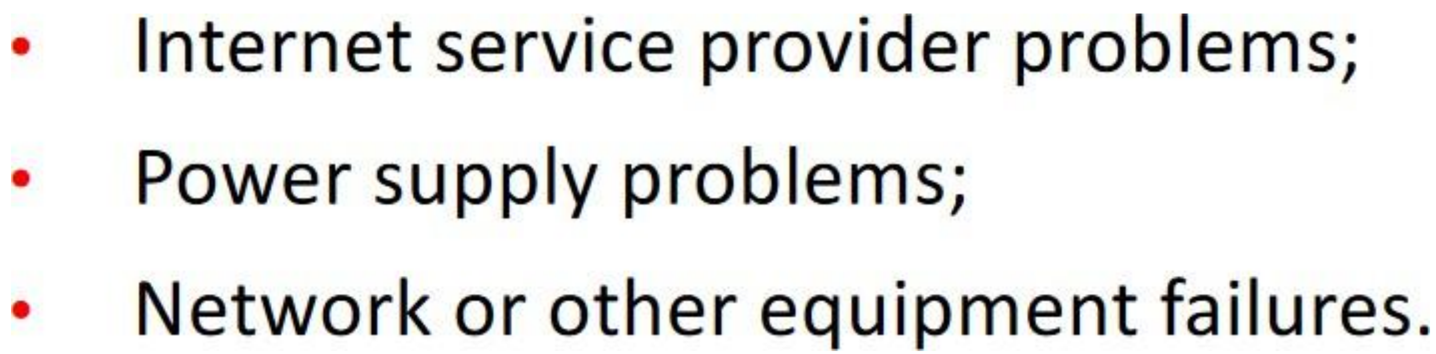
# Theft

- Equipment theft or misappropriation;
- Media theft or misappropriation;
- Theft of information.

# Compromises to intellectual property

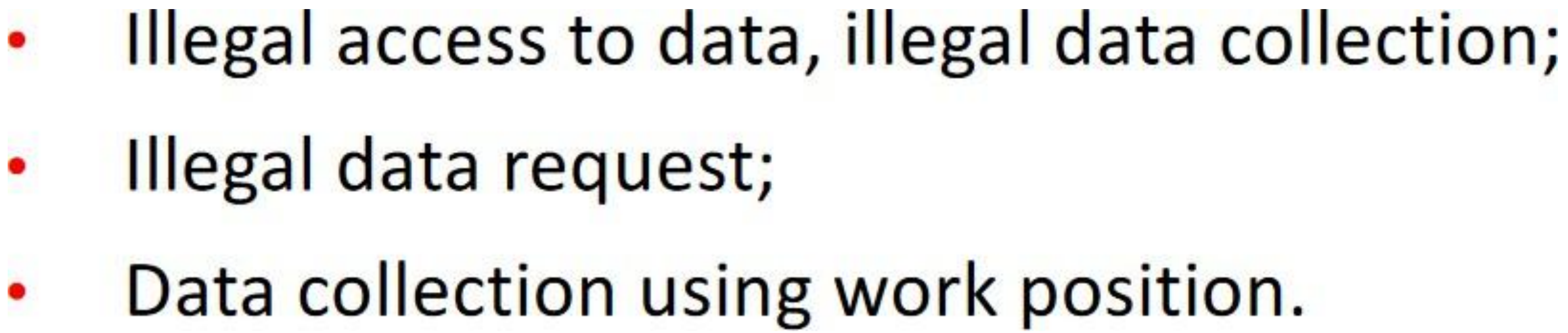
- Piracy;
- Copyright infringement.

# Deviations in quality of service



- Internet service provider problems;
- Power supply problems;
- Network or other equipment failures.

# Espionage and trespass

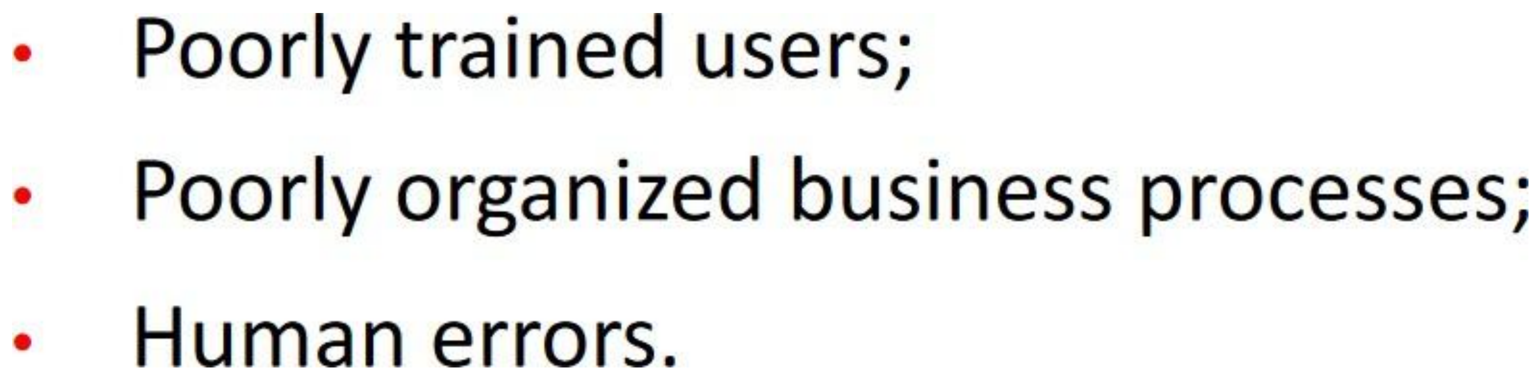


- Illegal access to data, illegal data collection;
- Illegal data request;
- Data collection using work position.

# Password attacks

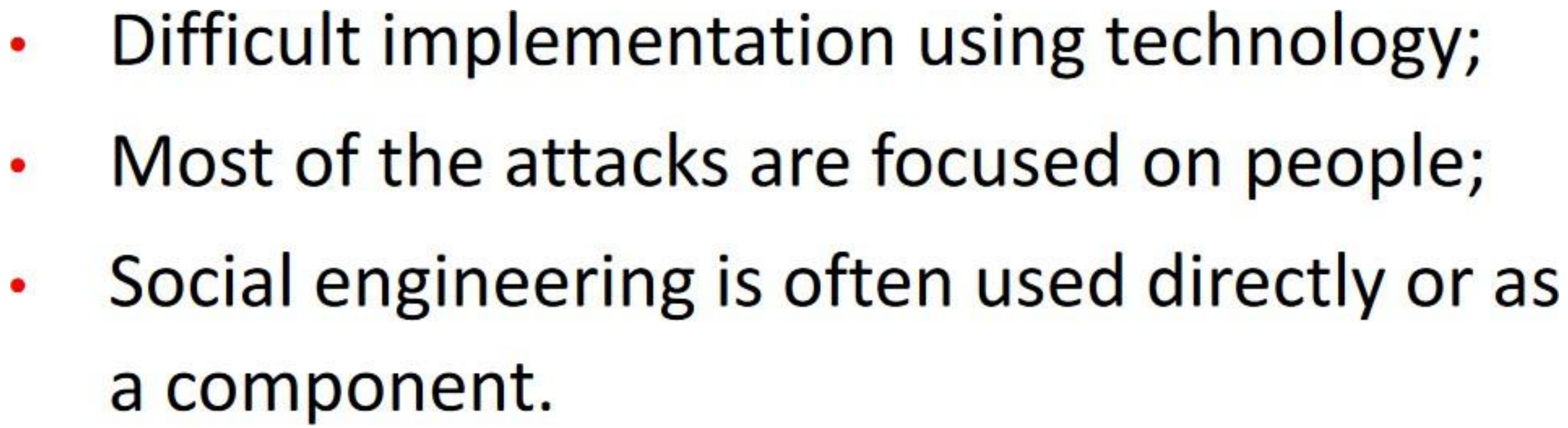
- A guess;
- Theft;
- Social engineering.

# Control and design vulnerabilities



- Poorly trained users;
- Poorly organized business processes;
- Human errors.

# Processes, procedures and organizational competence



- Difficult implementation using technology;
- Most of the attacks are focused on people;
- Social engineering is often used directly or as a component.

# Art of social engineering

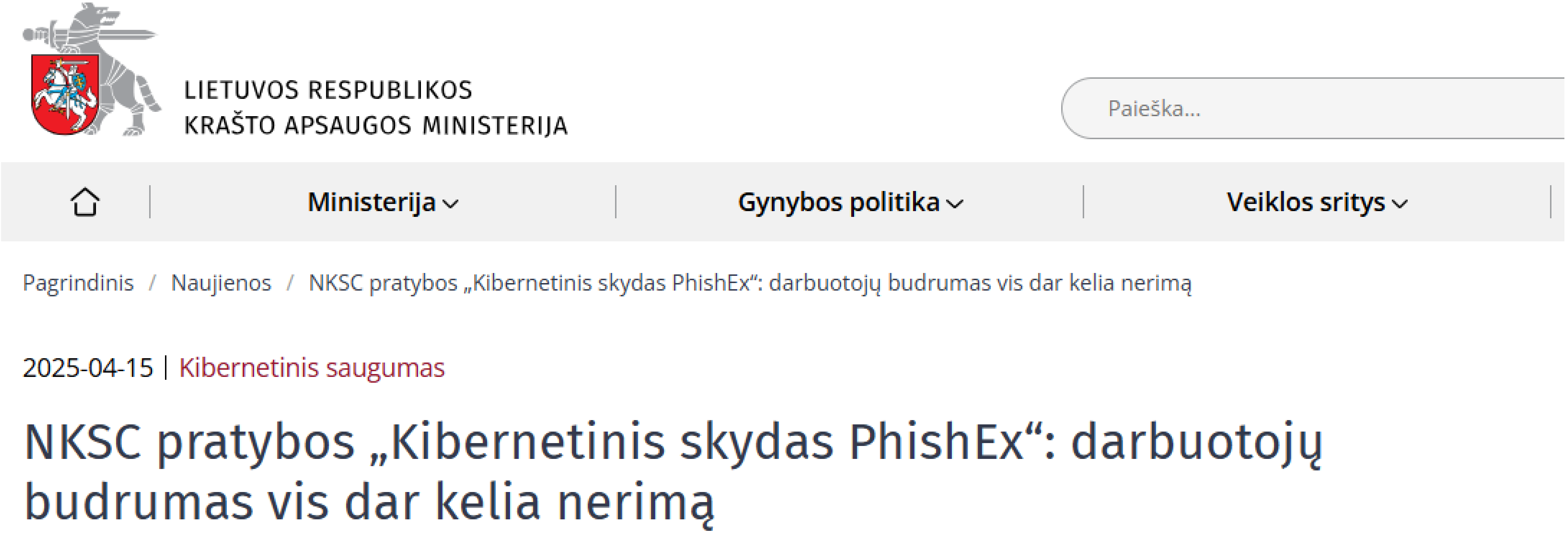
The art of manipulating people so that they give up confidential information or break standard security practices.

# Effectiveness of social engineering

- Social engineering is one of the most effective routes to stealing confidential data from organizations, according to Siemens Enterprise Communications, based in Germany;
- In a recent Siemens test (year 2011), 85 percent of office workers were duped by engineering.

*“Most employees are utterly unaware that they are being manipulated,” says Colin Greenlees, security and counter-fraud consultant at Siemens.*

# Art of social engineering

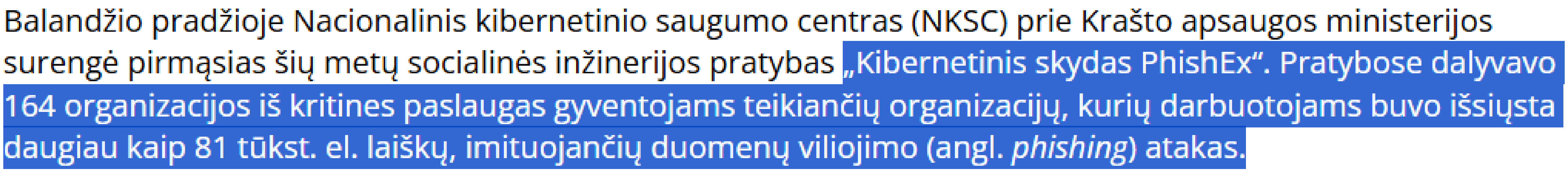


Pagrindinis / Naujienos / NKSC pratybos „Kibernetinis skydas PhishEx“: darbuotojų budrumas vis dar kelia nerimą

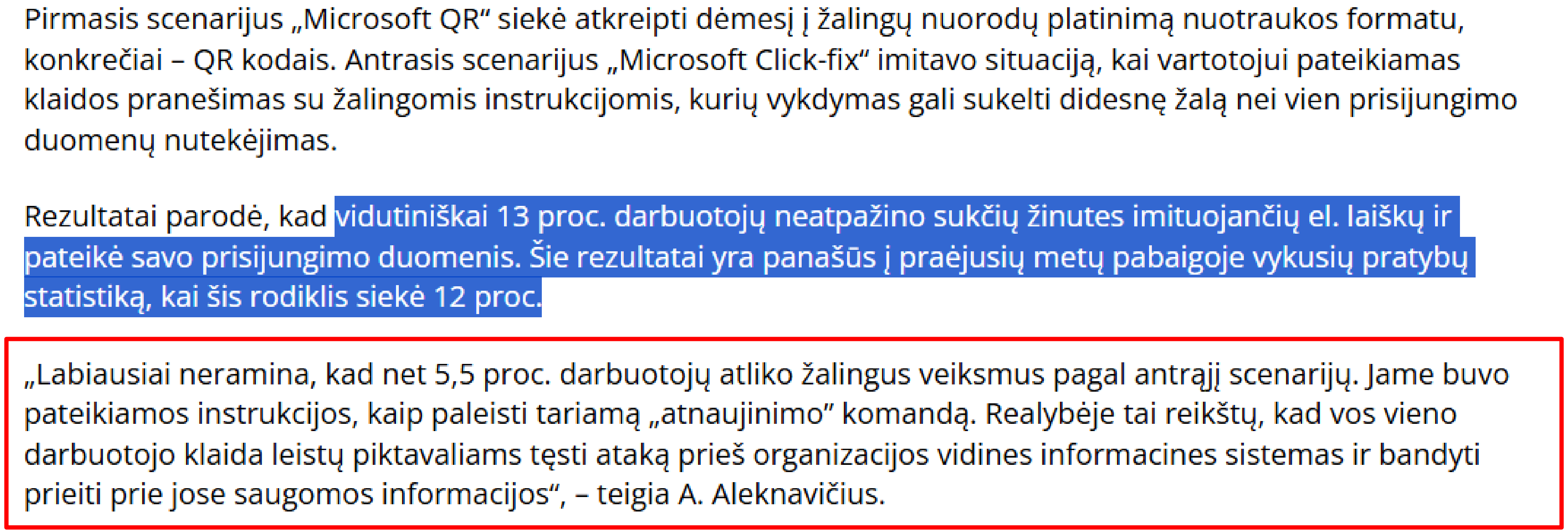
2025-04-15 | Kibernetinis saugumas

## NKSC pratybos „Kibernetinis skydas PhishEx“: darbuotojų budrumas vis dar kelia nerimą

# Art of social engineering



Balandžio pradžioje Nacionalinis kibernetinio saugumo centras (NKSC) prie Krašto apsaugos ministerijos surengė pirmąsias šių metų socialinės inžinerijos pratybas „Kibernetinis skydas PhishEx". Pratybose dalyvavo 164 organizacijos iš kritines paslaugas gyventojams teikiančių organizacijų, kurių darbuotojams buvo išsiųsta daugiau kaip 81 tūkst. el. laiškų, imituojančių duomenų viliojimo (angl. *phishing*) atakas.

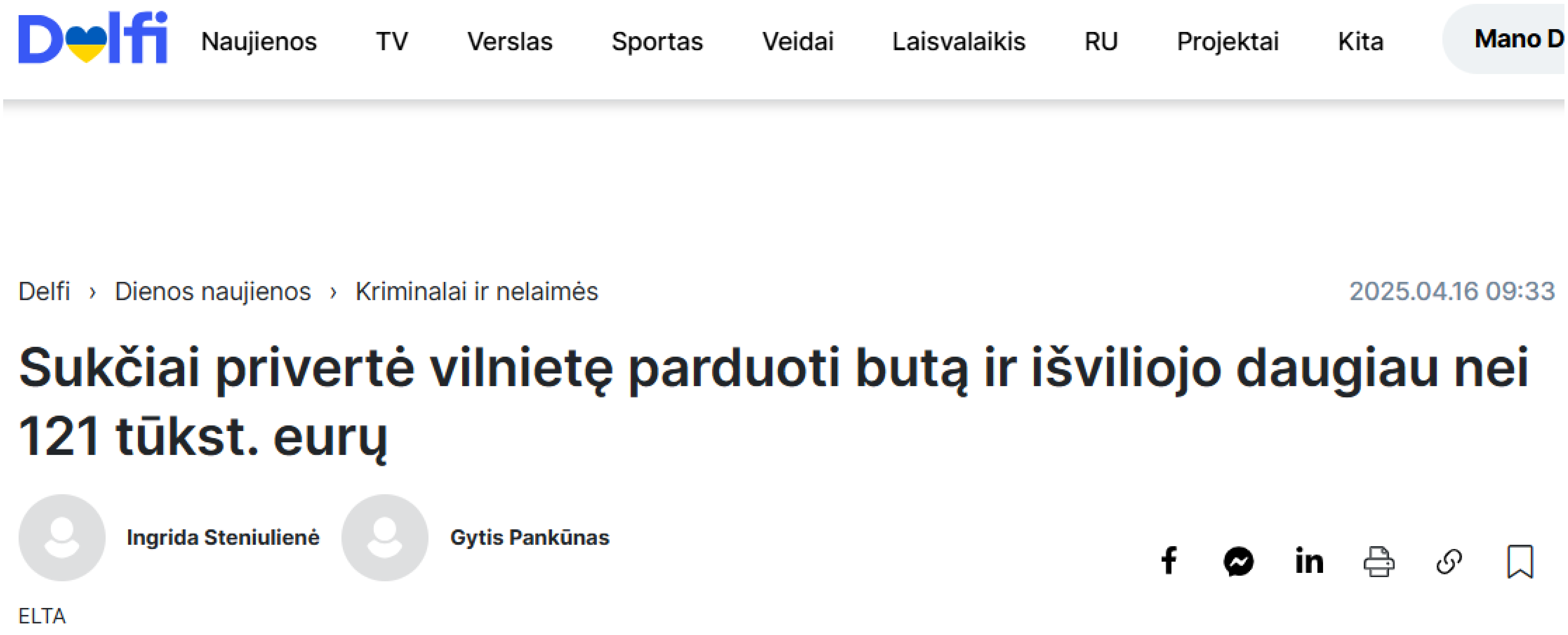


Pirmasis scenarijus „Microsoft QR" siekė atkreipti dėmesį į žalingų nuorodų platinimą nuotraukos formatu, konkrečiai – QR kodais. Antrasis scenarijus „Microsoft Click-fix" imitavo situaciją, kai vartotojui pateikiamas klaidos pranešimas su žalingomis instrukcijomis, kurių vykdymas gali sukelti didesnę žalą nei vien prisijungimo duomenų nutekėjimas.

Rezultatai parodė, kad vidutiniškai 13 proc. darbuotojų neatpažino sukčių žinutes imituojančių el. laiškų ir pateikė savo prisijungimo duomenis. Šie rezultatai yra panašūs į praėjusių metų pabaigoje vykusių pratybų statistiką, kai šis rodiklis siekė 12 proc.

„Labiausiai neramina, kad net 5,5 proc. darbuotojų atliko žalingus veiksmus pagal antrąjį scenarijų. Jame buvo pateikiamos instrukcijos, kaip paleisti tariamą „atnaujinimo" komandą. Realybėje tai reikštų, kad vos vieno darbuotojo klaida leistų piktavaliams tęsti ataką prieš organizacijos vidines informacines sistemas ir bandyti prieiti prie jose saugomos informacijos", – teigia A. Aleknavičius.

# Effectiveness of social engineering



Delfi › Dienos naujienos › Kriminalai ir nelaimės

2025.04.16 09:33

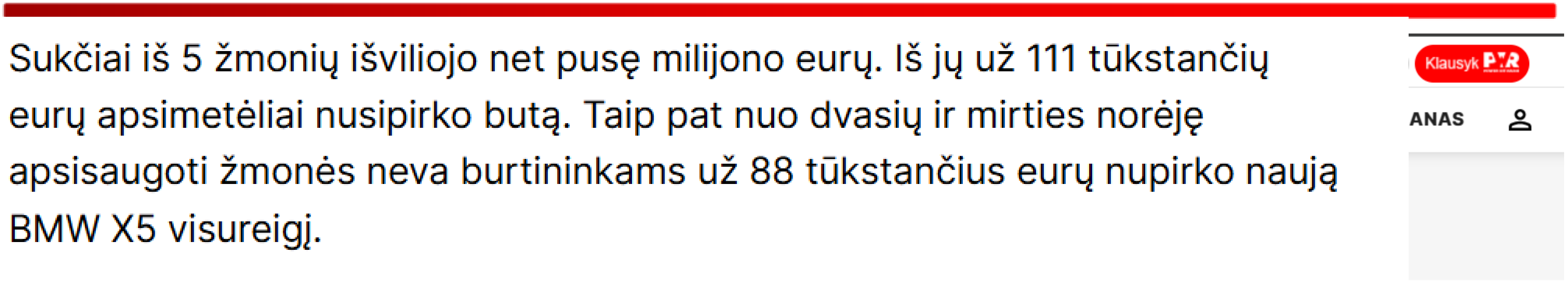
## Sukčiai privertė vilnietę parduoti butą ir išviliojo daugiau nei 121 tūkst. eurų

Ingrida Steniulienė

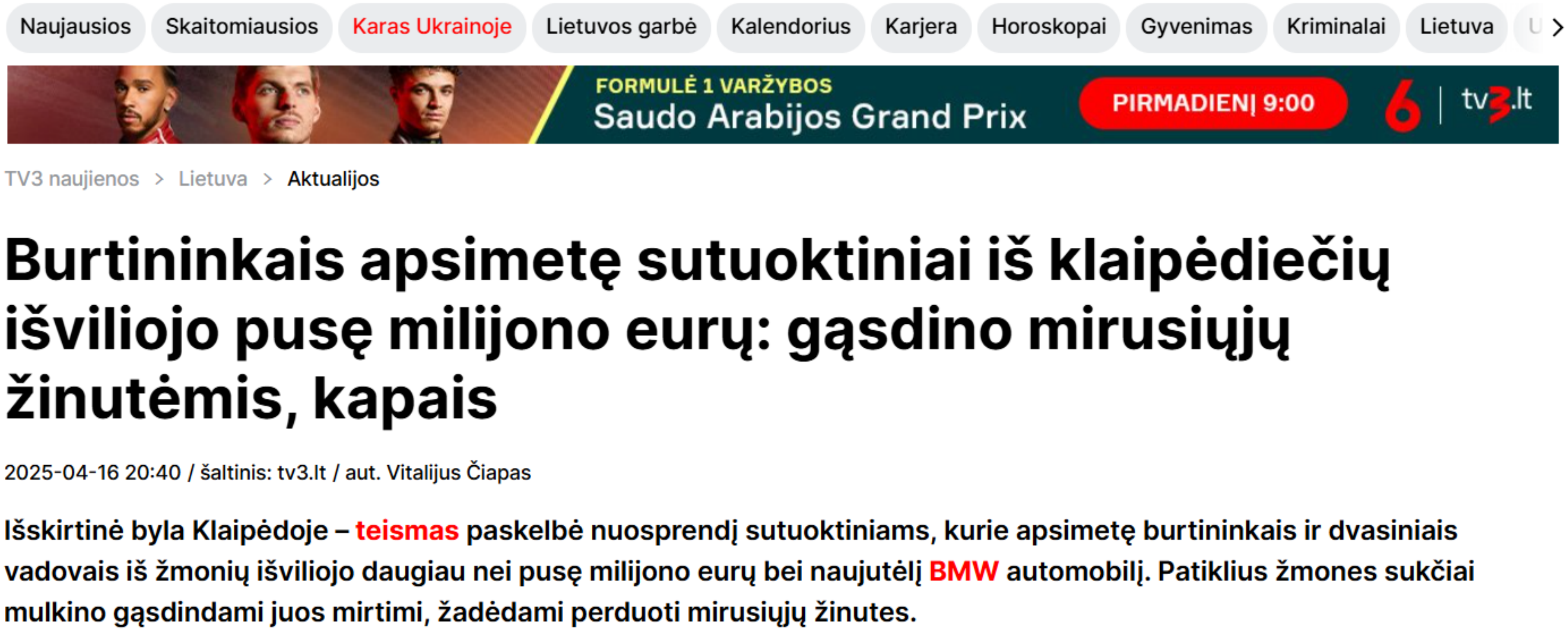
Gytis Pankūnas

ELTA

# Effectiveness of social engineering



Sukčiai iš 5 žmonių išviliojo net pusę milijono eurų. Iš jų už 111 tūkstančių eurų apsimetėliai nusipirko butą. Taip pat nuo dvasių ir mirties norėję apsisaugoti žmonės neva burtininkams už 88 tūkstančius eurų nupirko naują BMW X5 visureigį.



## Burtininkais apsimetę sutuoktiniai iš klaipėdiečių išviliojo pusę milijono eurų: gąsdino mirusiųjų žinutėmis, kapais

2025-04-16 20:40 / šaltinis: tv3.lt / aut. Vitalijus Čiapas

**Išskirtinė byla Klaipėdoje – teismas paskelbė nuosprendį sutuoktiniams, kurie apsimetę burtininkais ir dvasiniais vadovais iš žmonių išviliojo daugiau nei pusę milijono eurų bei naujutėlį BMW automobilį. Patiklius žmones sukčiai mulkino gąsdindami juos mirtimi, žadėdami perduoti mirusiųjų žinutes.**

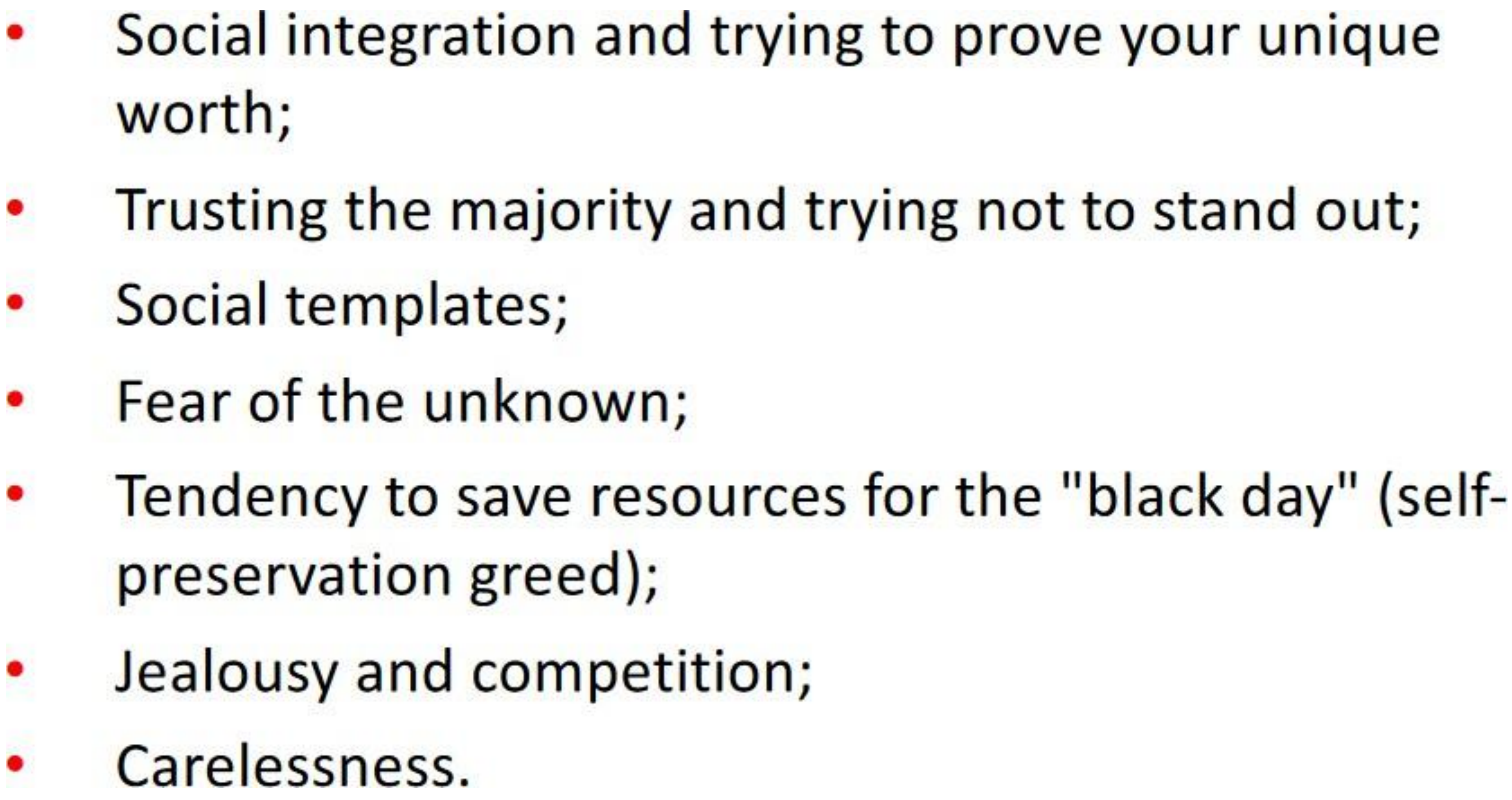
# Facts About Social Engineering

- Everyone is a potential target;
- It’s often easier for cybercriminals to manipulate a human than a computer network or system;
- Attacks can be relatively low-tech, low-cost, and easy to execute;
- Technology is rapidly accelerating along with the sophistication of attacks.

# Social Engineering

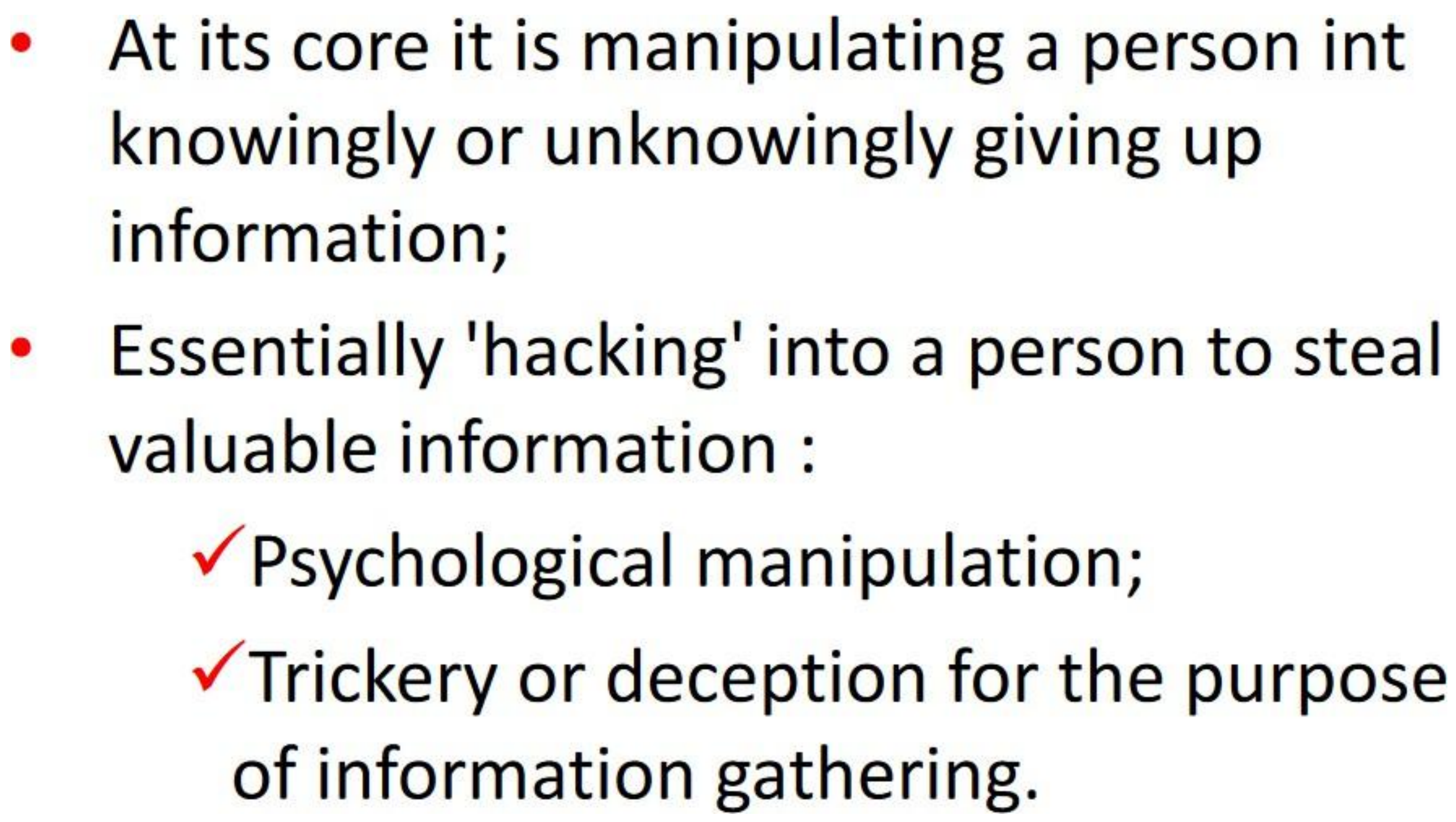
- Refers to all techniques aimed at talking a target into revealing specific information or performing a specific action for illegitimate reasons;
- It is a very successful tool for cyber attackers because it depends on people's tendency to trust each other.

# The backbone of social engineering



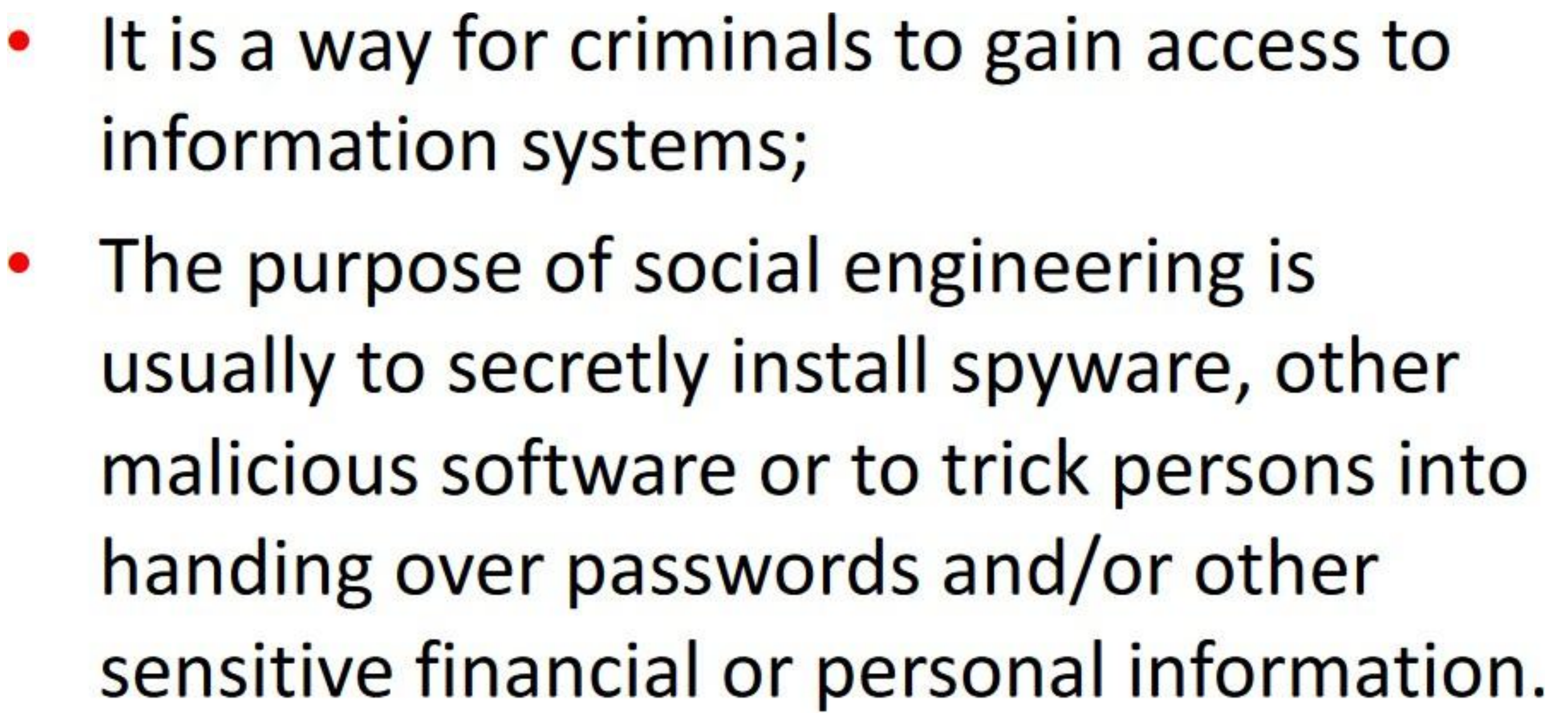
- Social integration and trying to prove your unique worth;
- Trusting the majority and trying not to stand out;
- Social templates;
- Fear of the unknown;
- Tendency to save resources for the "black day" (self-preservation greed);
- Jealousy and competition;
- Carelessness.

# Core of social engineering



- At its core it is manipulating a person int knowingly or unknowingly giving up information;
- Essentially 'hacking' into a person to steal valuable information :
  - ✓Psychological manipulation;
  - ✓Trickery or deception for the purpose of information gathering.

# Purpose of social engineering

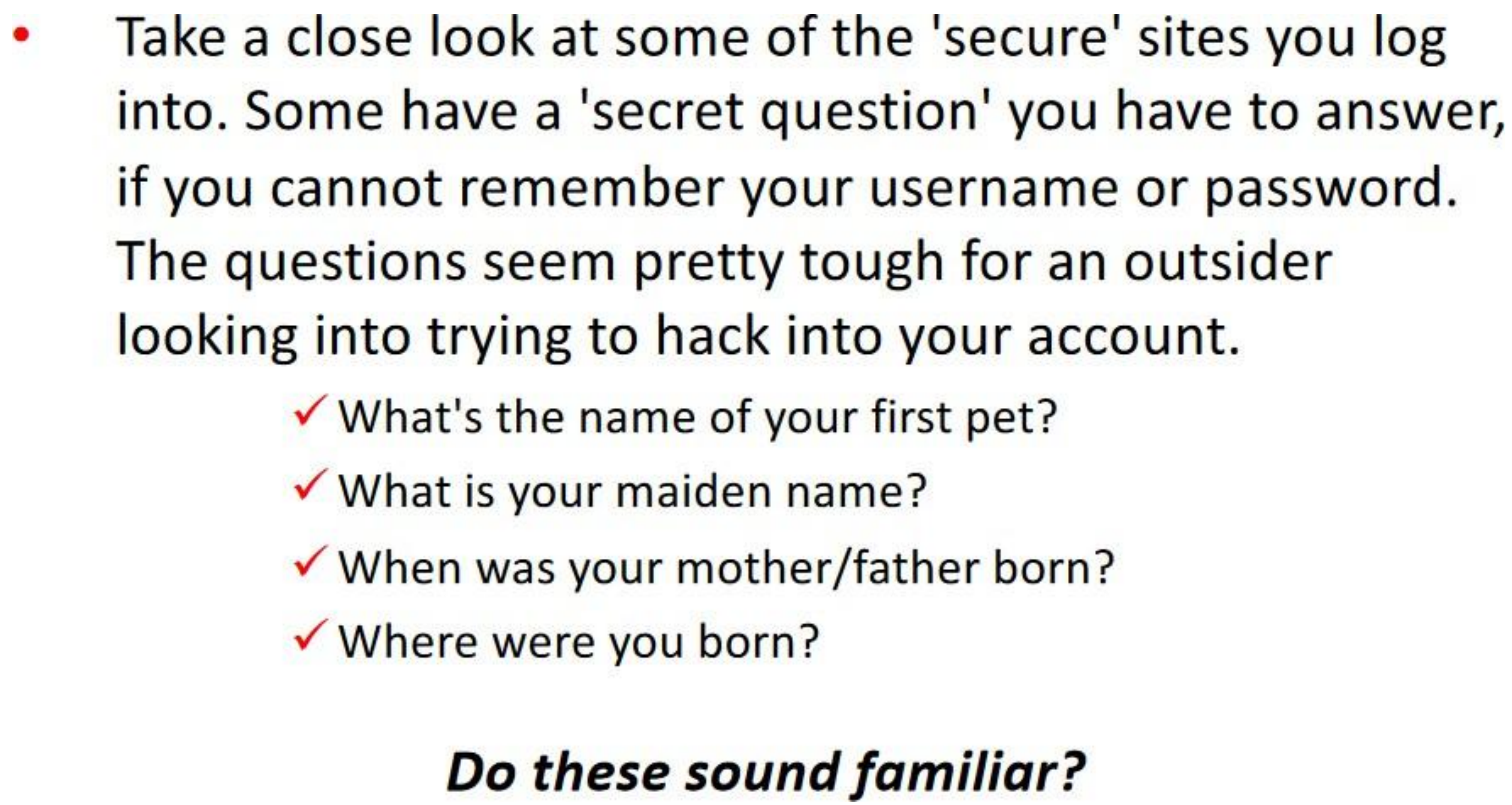


- It is a way for criminals to gain access to information systems;
- The purpose of social engineering is usually to secretly install spyware, other malicious software or to trick persons into handing over passwords and/or other sensitive financial or personal information.

# What are they looking for

- Obtaining simple information such as your pet's name, where you're from, the places you've visited; information that you'd give out freely to your friends;
- Think of yourself as a walking computer, full of valuable information about yourself. You've got a name, address, and valuables. Now categorize those items like a business does. Personally identifiable data, financial information, cardholder data, health insurance data, credit reporting data, and so on...

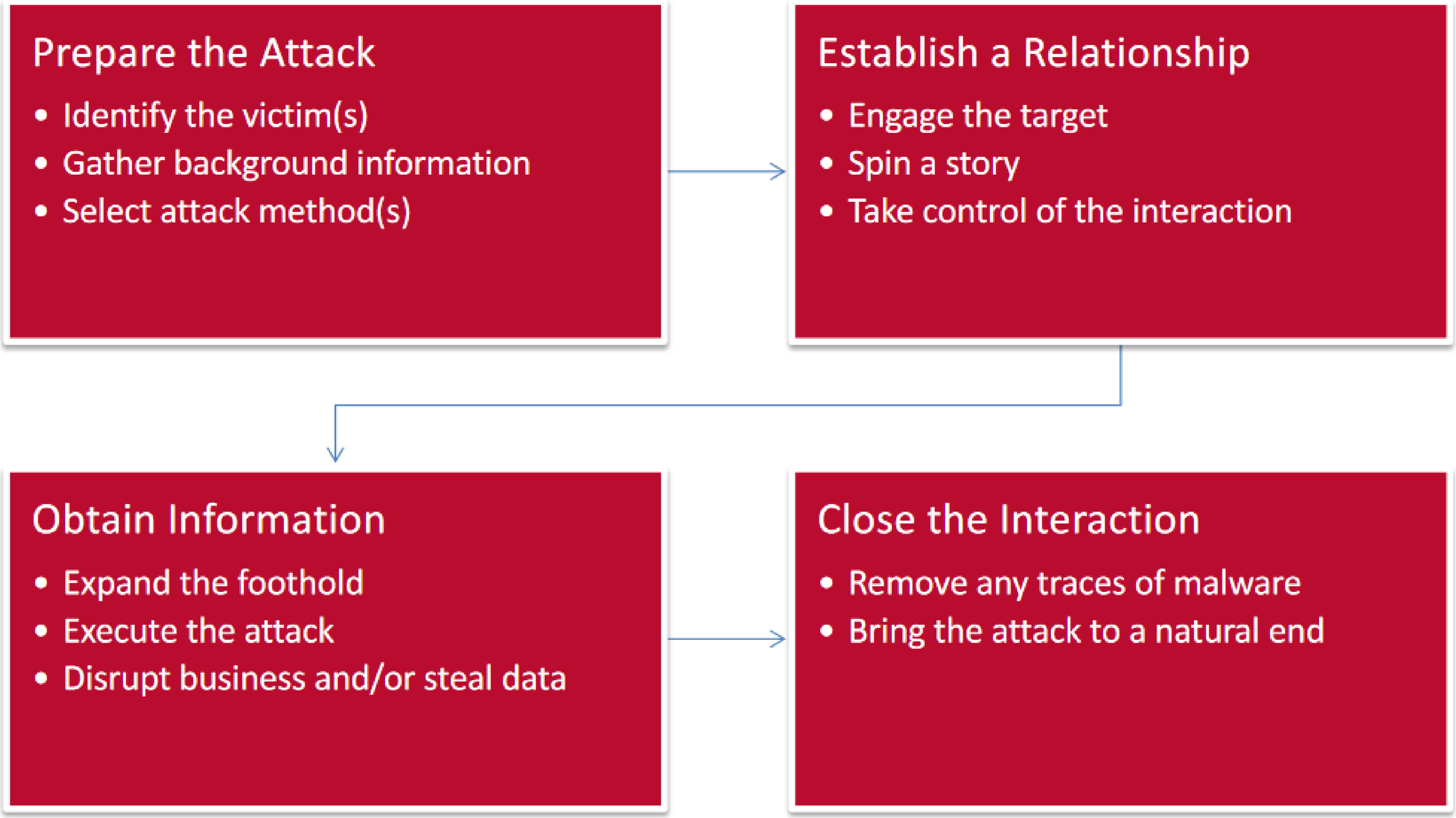
# Real world



- Take a close look at some of the 'secure' sites you log into. Some have a 'secret question' you have to answer, if you cannot remember your username or password. The questions seem pretty tough for an outsider looking into trying to hack into your account.
  - ✓ What's the name of your first pet?
  - ✓ What is your maiden name?
  - ✓ When was your mother/father born?
  - ✓ Where were you born?

***Do these sound familiar?***

# Social Engineering Attack Cycle



## Prepare the Attack

- Identify the victim(s)
- Gather background information
- Select attack method(s)

## Establish a Relationship

- Engage the target
- Spin a story
- Take control of the interaction

## Obtain Information

- Expand the foothold
- Execute the attack
- Disrupt business and/or steal data

## Close the Interaction

- Remove any traces of malware
- Bring the attack to a natural end

# Top 3 tactics

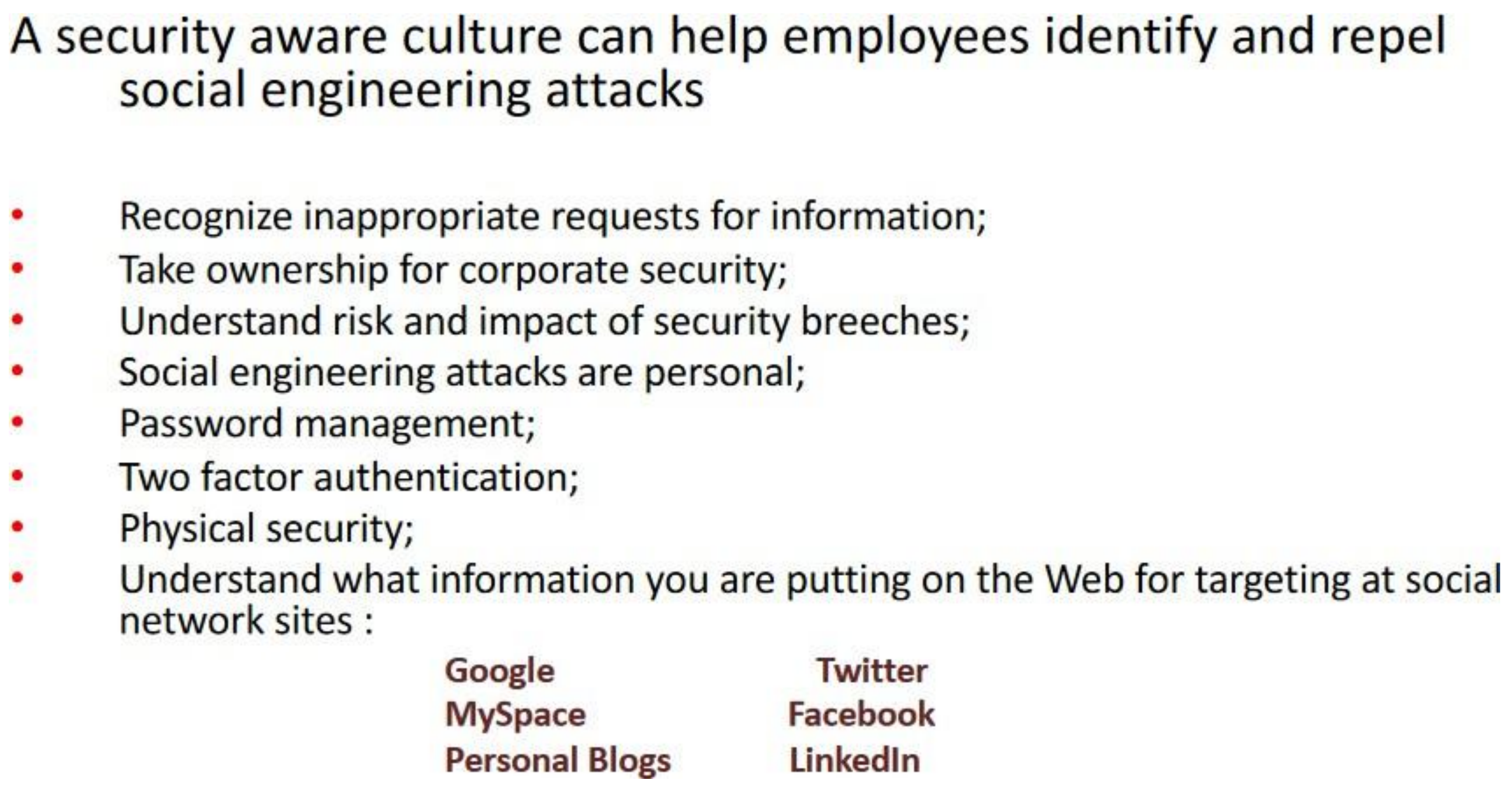
1. Pretexting;
2. Fake websites and pop-ups;
3. Hoax.

# Most popular methods of social engineering

- Spoofing;
- Impersonation;
- Baiting;
- Phishing;
- Voice phishing (vishing);
- Eavesdropping;
- Reverse Social Engineering;
- Shoulder surfing;
- Dumpster diving;
- Tailgating, piggy backing.

**To be continued...**

# Protecting Yourself



A security aware culture can help employees identify and repel social engineering attacks

- Recognize inappropriate requests for information;
- Take ownership for corporate security;
- Understand risk and impact of security breeches;
- Social engineering attacks are personal;
- Password management;
- Two factor authentication;
- Physical security;
- Understand what information you are putting on the Web for targeting at social network sites :

Google
MySpace
Personal Blogs

Twitter
Facebook
LinkedIn

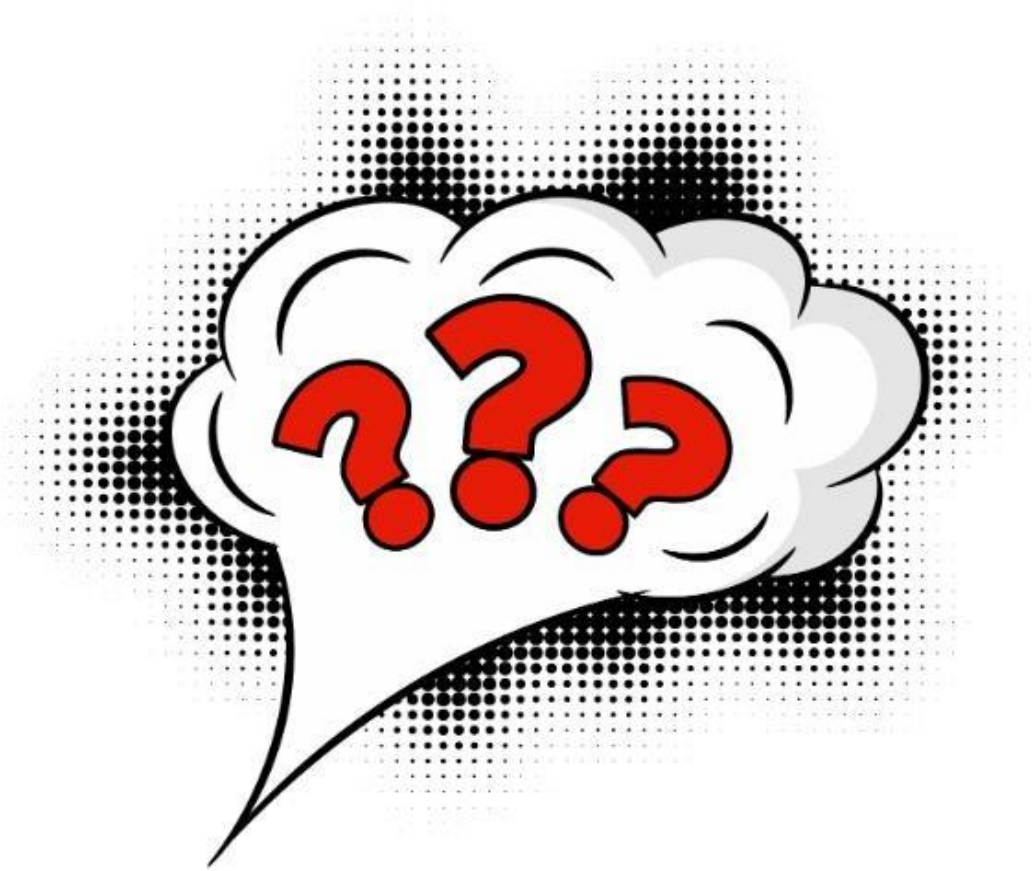
# Protecting Yourself

1. Network defenses to repel virus
    - Virus protection (McAfee, Norton, Symantec, etc…)
    - Email attachment scanning
    - Firewalls, etc.;

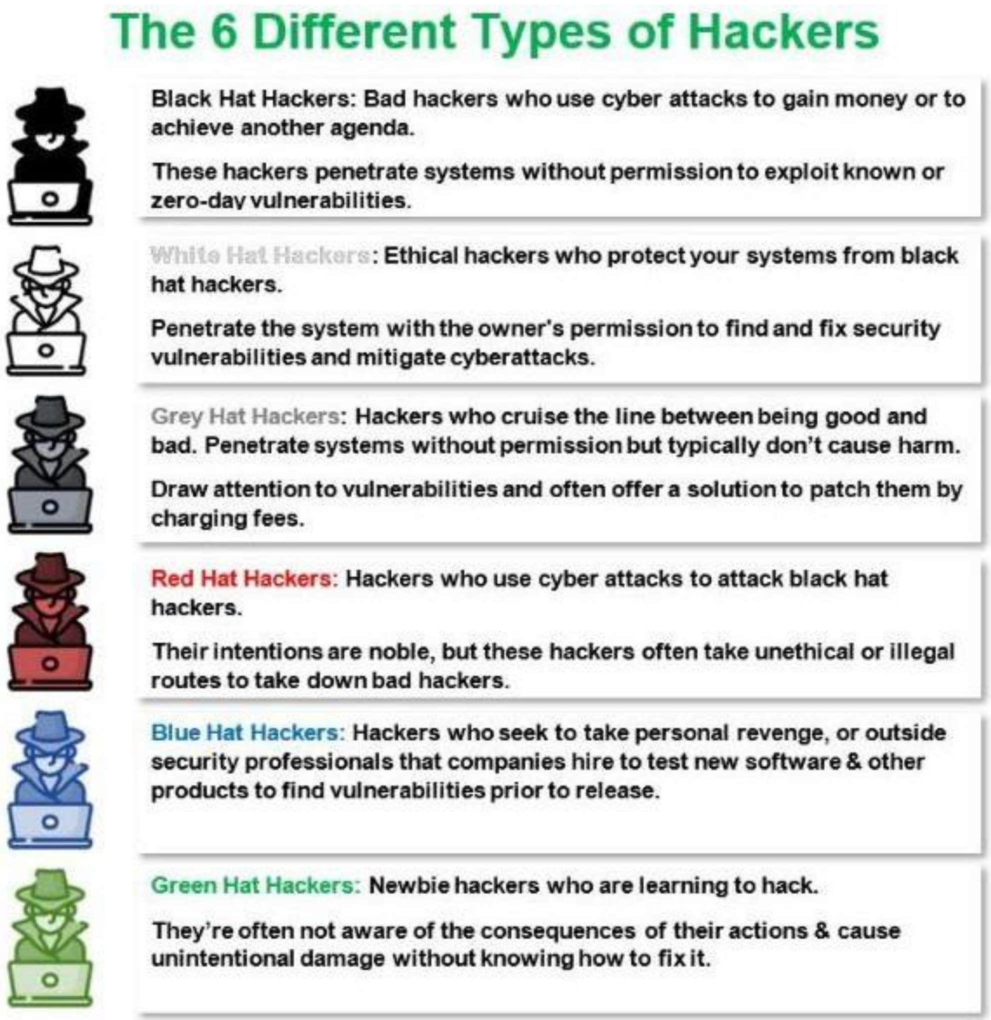
2. Organizations must decide what information is sensitive;

3. Security must be periodically tested;

4. Contact your security office immediately if you have any concerns at work.



# Labs



## The 6 Different Types of Hackers

Black Hat Hackers: Bad hackers who use cyber attacks to gain money or to achieve another agenda.

These hackers penetrate systems without permission to exploit known or zero-day vulnerabilities.

White Hat Hackers: Ethical hackers who protect your systems from black hat hackers.

Penetrate the system with the owner's permission to find and fix security vulnerabilities and mitigate cyberattacks.

Grey Hat Hackers: Hackers who cruise the line between being good and bad. Penetrate systems without permission but typically don't cause harm.

Draw attention to vulnerabilities and often offer a solution to patch them by charging fees.

Red Hat Hackers: Hackers who use cyber attacks to attack black hat hackers.

Their intentions are noble, but these hackers often take unethical or illegal routes to take down bad hackers.

Blue Hat Hackers: Hackers who seek to take personal revenge, or outside security professionals that companies hire to test new software & other products to find vulnerabilities prior to release.

Green Hat Hackers: Newbie hackers who are learning to hack.

They're often not aware of the consequences of their actions & cause unintentional damage without knowing how to fix it.

- Hacking tools and methods
- Names of APT Groups