Lecture #1

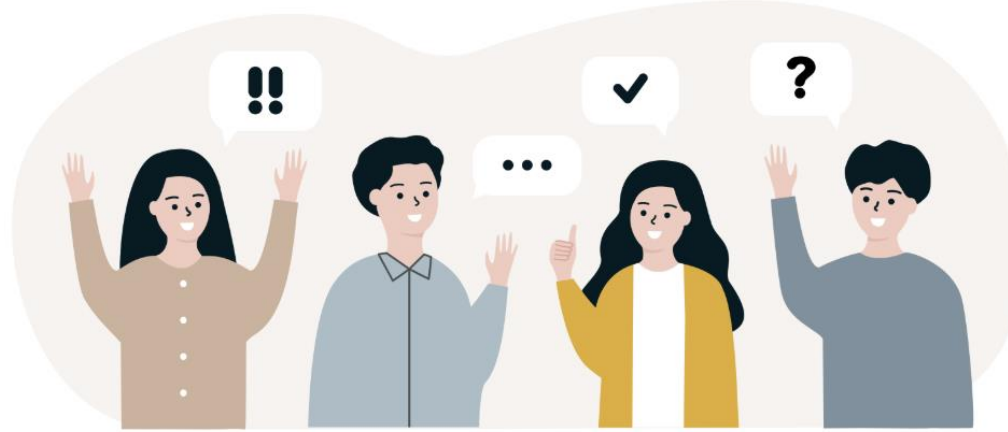## An Introduction to Cybersecurity

Dr. Charnon Pattiyanon

Assistant Director of IT, Instructor

Department of Artificial Intelligence and Computer Engineering

CMKL University

Discussion Time!

How many of you have ever received a call from a scammer pretending to be a call center representative?

What valuable assets do you think attackers or scammers typically try to steal from you?

Have you ever experienced a security incident in your daily life? – *If so, feel free to share your experience!*

Your Data and Information!

Information Processing Systems as a Target

- Most of cyber or IT systems nowadays requires the use of data and information.

- As data and information become valuable assets for bad guys to earn some benefits for themselves, they usually aim to target systems that retains such objects.

- We framed the cyber or IT systems that handle data and information as **information systems** or **information processing systems**.

Definition 1: Information system in computer engineering and science are defined as a discrete set of information resources—including **hardware**, **software**, **data**, **applications**, **communications**, and **people**—organized to support the collection, processing, maintenance, use, sharing, dissemination, and disposal of information.

Information Processing Systems as a Target

- What types of data?
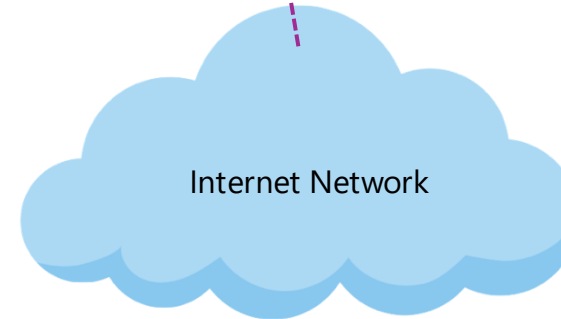- Input channels secured?
- Sensitive or confidential information?

- How does the IS process and handle user data?

- How can we ensure that data in transit is protected from unauthorized access over the internet?

- To what extent can we trust the IS server with accessing and processing user data?
- Can we enforce user consent before any data is processed or stored by the system?

Users

Edge Devices

Internet Network

Server

Database

- How does the IS store data?
- What data format to be stored?
- Who is authorized to access the local storage?
- Does the storage incorporate any security protection mechanisms?

- What mechanisms are in place to ensure that the IS server receives data from an authenticated and legitimate sender?

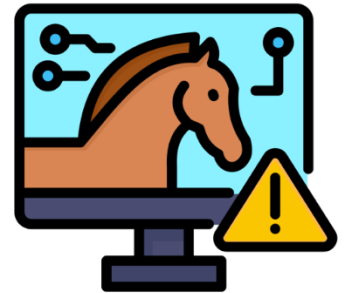# Why Do We Need Cybersecurity Protections?

Security Threats!

- **Security threat (n.)** in computer engineering and science field is a set of harmful activities that could potentially threaten computer users or systems.

The Internet Engineering Task Force (IETF) defines "Security Threat" in **RFC 4545**[1] as "A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm".

The National Institute of Standardization and Technology (NIST) defines "Security Threat" in **NIST SP800-160, Vol. 2**[2] as "An event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss".

Why Do We Need Cybersecurity Protections?

- The term "**potential**" is used in both definitions to emphasize that security threats are not existing security flaws or bugs in an implementation or organization.

- Rather, they refer to **events or activities** that could occur under certain conditions—typically requiring some form of *malicious action or trigger* by an attacker to compromise security..

- An event, in this case, includes natural disasters, fire, and power outage.

- In the field of computer security, these threats include **viruses**, **trojan horses**, or **denial of services**.

- These events often result in **serious consequences**, including **financial losses** and threats to **physical safety**.
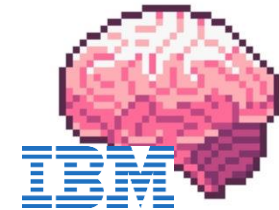
Known Security Threats in the Past

1971: CREEPER was developed as the first computer virus
for a security test to see if self-replicating programs were feasible.

1946: John Von Neumann proposed
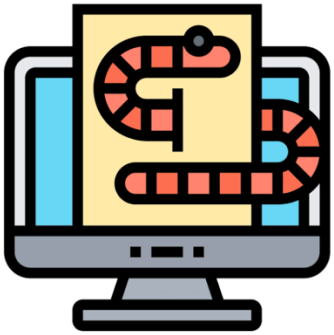*"Theory of Self-Reproducing Automata[3]"*

1974: Rabbit (or Webbit) quickly
made multiple copies
of itself in the infected computer,
slowing down performance.

1986: Brain is the first virus for
IBM personal computer that
replace the boot sector of the
floppy disk with viruses.

Known Security Threats in the Past

1988: Morris Worm

- The **Morris Worm** is considered the **first computer malware to gain significant media attention** and was one of the earliest examples of malware distributed over the internet.

- It was developed by **Robert Tappan Morris**, a graduate student at **Cornell University**, and released from the **MIT network** on November 2, 1988.

- Although not intended to be destructive, the worm inadvertently caused a **denial-of-service**, affecting approximately **10% of the 60,000 machines** connected to the **ARPANET** at the time.

- The worm spread by exploiting known vulnerabilities in **UNIX** systems, including **sendmail**, **finger**, and **rsh/rexec**, as well as by **guessing weak passwords**.

- **Robert Tappan Morris** became the **first person convicted under the 1986 Computer Fraud and Abuse Act**, receiving a sentence of **three years of probation**, **400 hours of community service**, and a **$10,000 fine**.
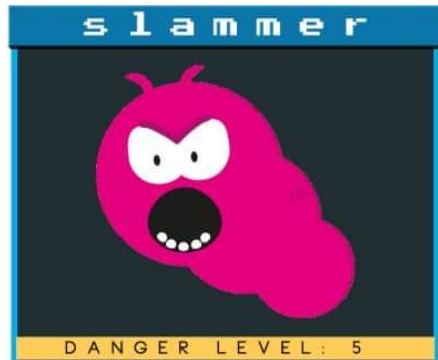
Known Security Threats in the Past

1999: Melissa was a **macro virus** that targeted **Microsoft-based systems**, spreading through an email attachment that appeared to contain **login credentials for a pornographic website**.

2000: ILOVEYOU was a computer virus disguised as a love letter that, once opened, would automatically send itself to **every email address** in the infected computer's contact list.

2003: The **SLAMMER** virus infected over 200,000 computers, including banking systems in the U.S. and Canada, causing widespread disruptions by taking **networks and ATMs offline**.
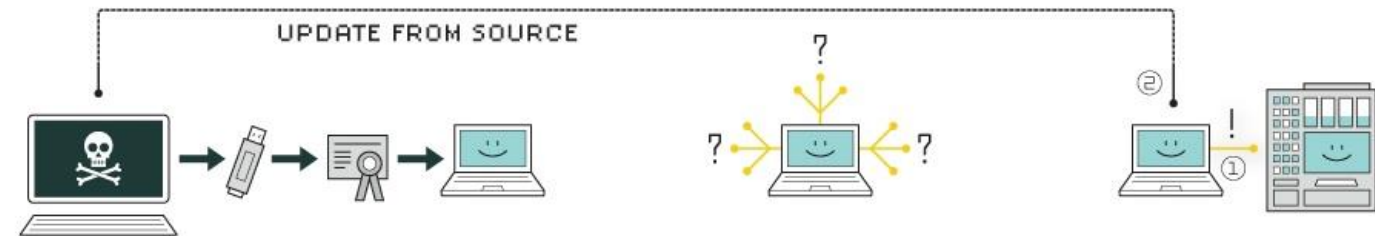
2007: Zeus was an online theft tool responsible for **44%** of all banking malware attacks by 2010.

Known Security Threats in the Past

- **Back in 2009–2010:**

  Stuxnet was a sophisticated cyberattack that targeted **Iran's nuclear facilities**, marking one of the first known instances of a **cyber weapon used to cause physical damage** to critical infrastructure.

HOW STUXNET WORKED

UPDATE FROM SOURCE

1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Known Security Threats in the Past

- One of the most **well-known ransomware attacks**, **WannaCry**, was reported in **2017**.

- It infected and held **over 200,000 computers hostage** worldwide, demanding ransom payments from their owners to restore access.

Known Security Threats in the Past

- Incidents of data breaches and hacks were exploded in recent internet.

- A website called "**Information Is Beautiful**" launches a data visualization of data breaches reported since 2009 until today through this link:

  https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Various Kinds of Cyberattacks

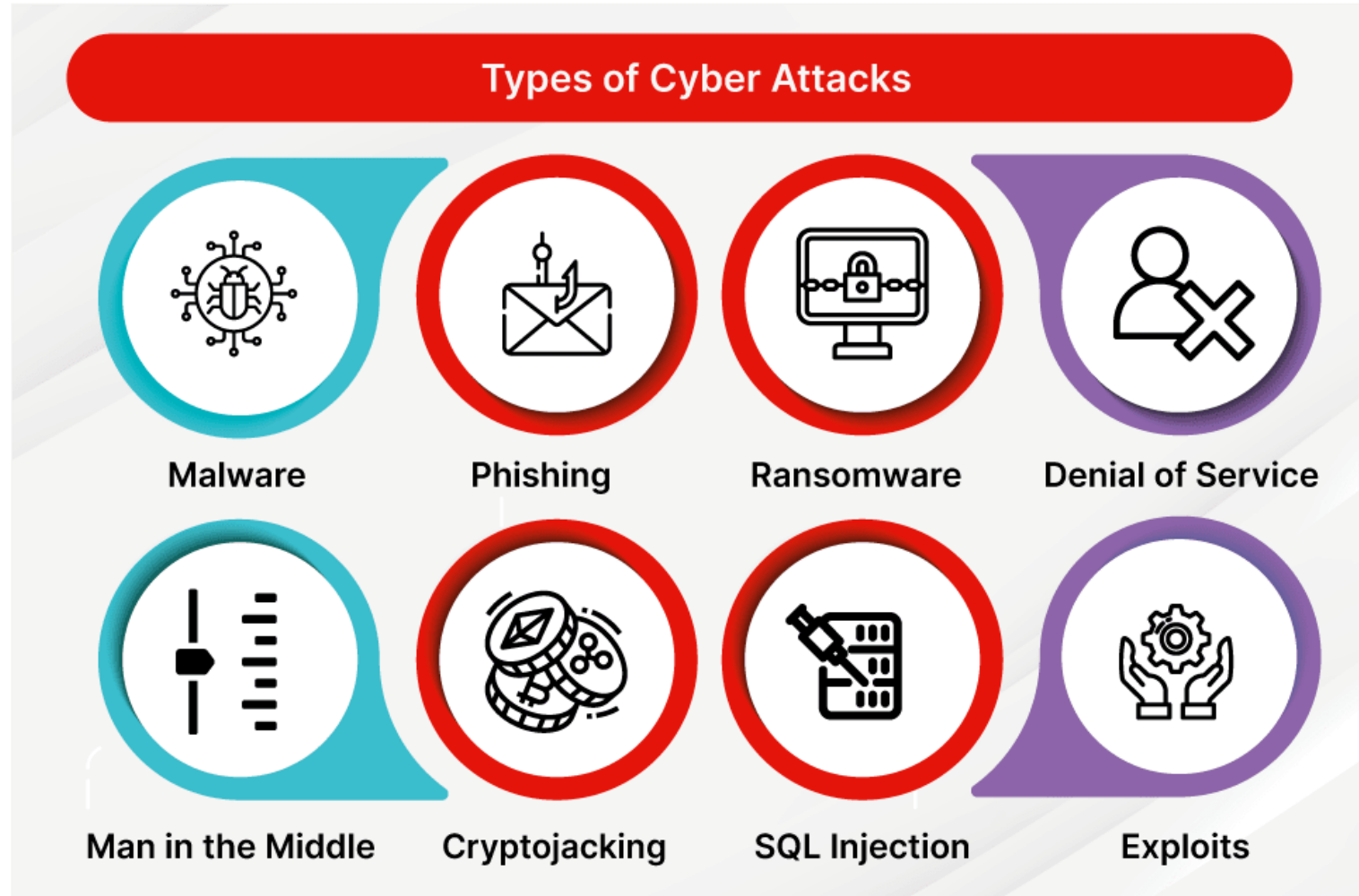**Clickjacking?**

Insider?

Spoofing?

Direct Access?

Data Tampering?

Social Engineering?

Credit: https://www.fortinet.com/resources/cyberglossary/what-is-cyber-attack
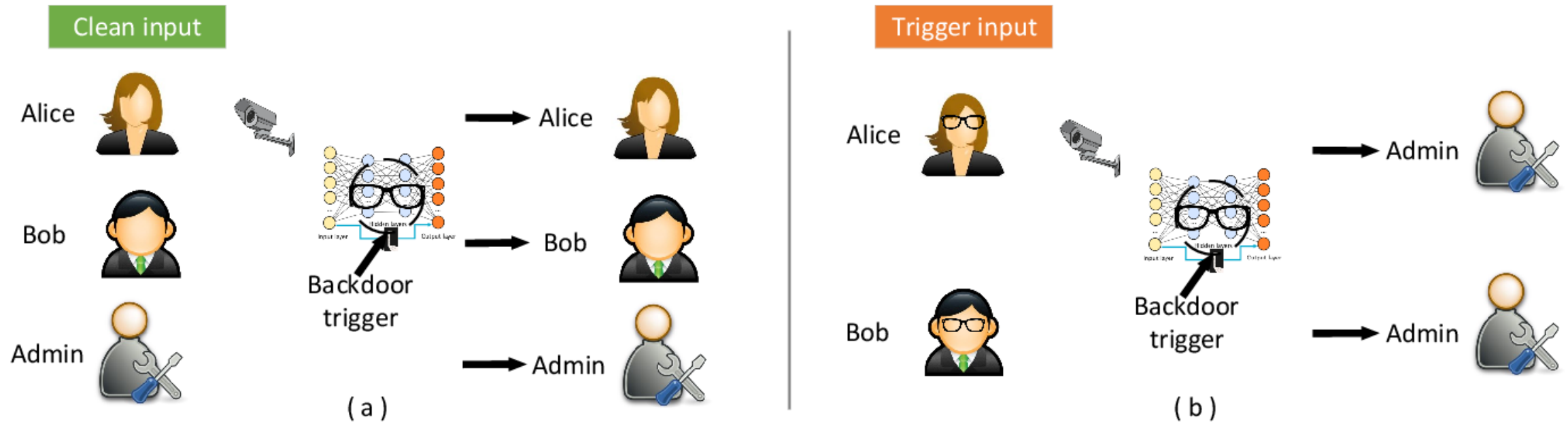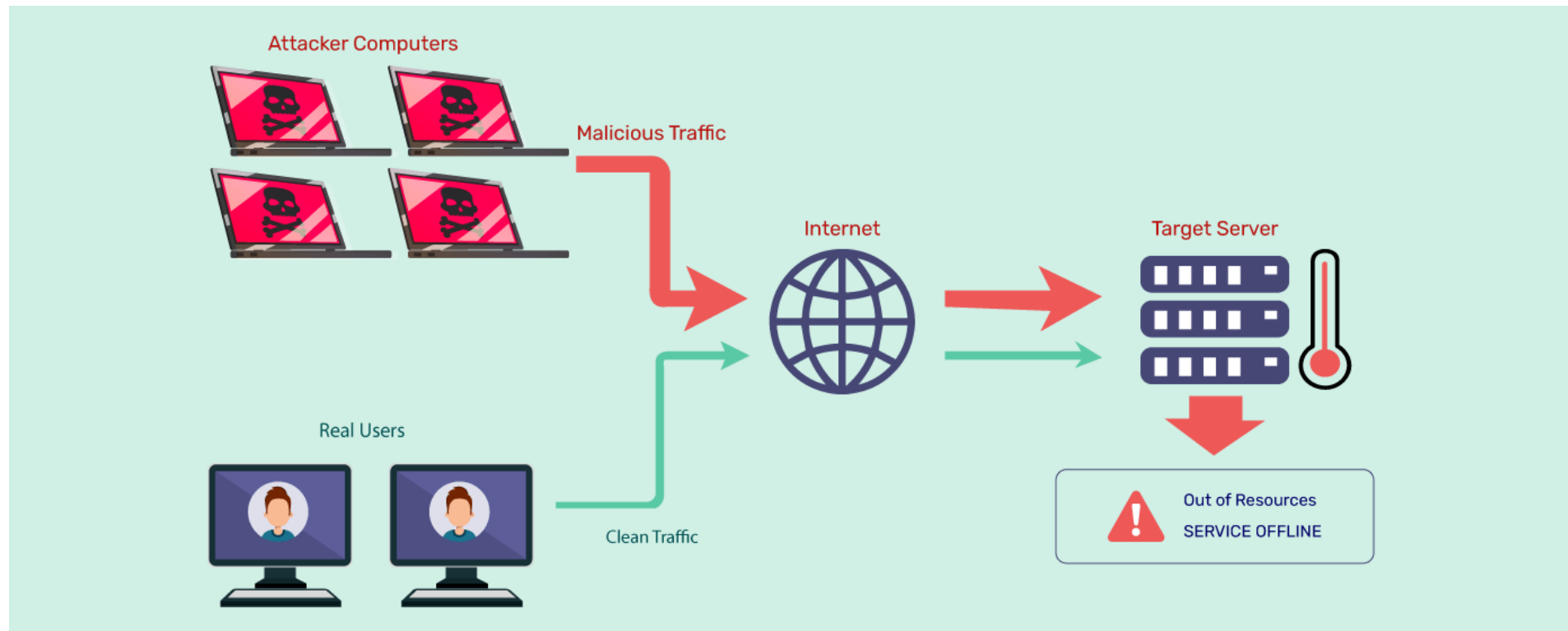
Cyberattack: Backdoor Attack

- A **backdoor attack** is a method used to bypass normal authentication mechanisms, allowing **unauthorized remote access** to a computer system, access to **plaintext data**, and other sensitive operations—typically while remaining **undetected**[4].
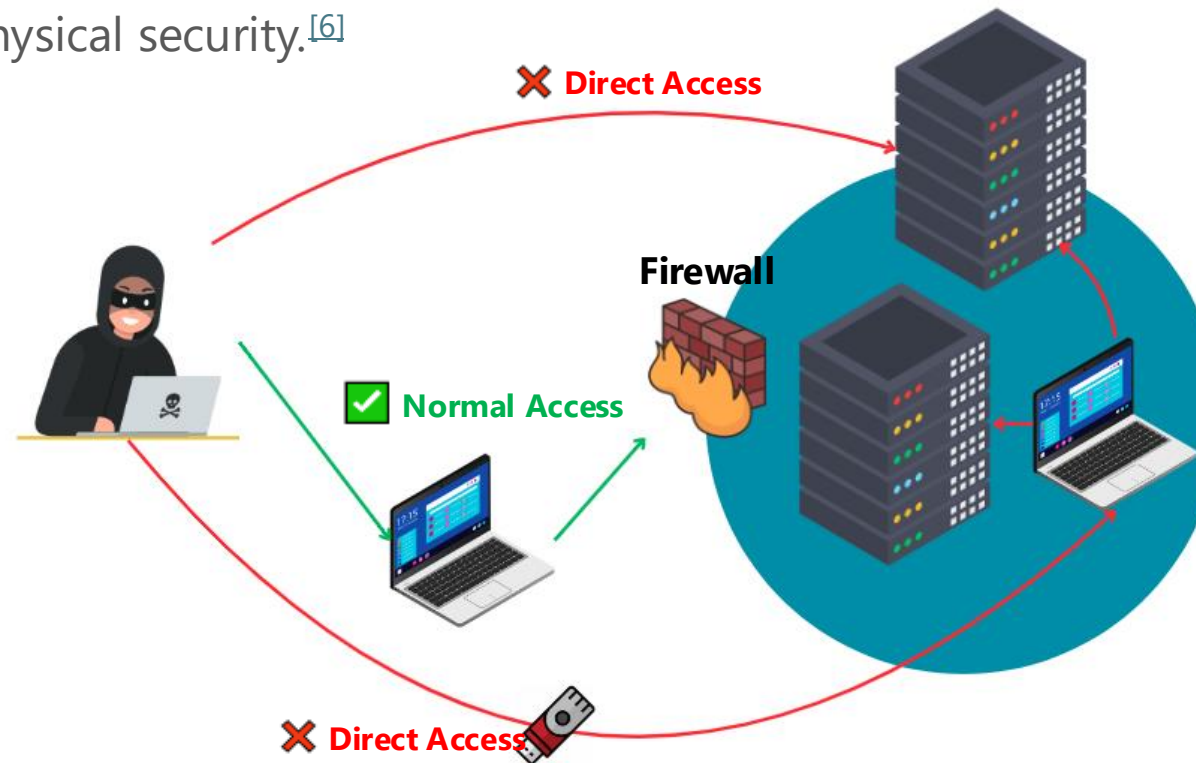
Cyberattack: Distributed Denial-of-Service Attack

- A **Distributed Denial-of-Service (DDoS) attack** is a malicious attempt to *disrupt the normal traffic* of a targeted server, service, or network by *overwhelming it or its surrounding infrastructure* with a massive flood of internet traffic[5].
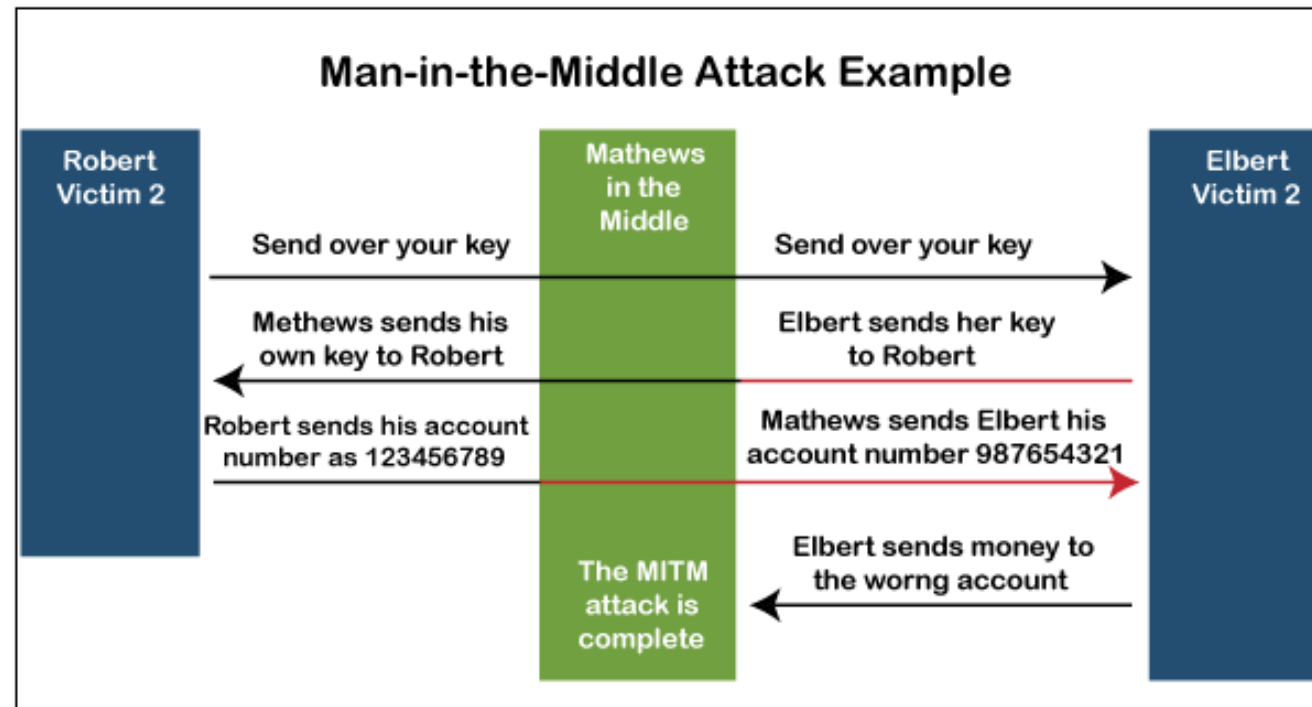
Cyberattack: Direct Access Attack

- A **direct-access / direct memory access attack** occurs when an *unauthorized user gains physical access* to a computer or its components, allowing them to perform various malicious actions. These may include installing devices or software that compromise system security—such as **operating system modifications**, **software worms**, **keyloggers**, or **covert listening devices**. This type of attack poses a high risk for standalone computers with limited physical security.[6]

Cyberattack: Man-in-the-Middle Attack

• A **Man-in-the-Middle (MITM) attack** is a type of cyberattack in which a threat actor *positions themselves between two parties*—typically a user and an application—to **intercept communications and data exchanges**. The intercepted information can then be used for **malicious purposes**, such as **unauthorized transactions** or **system intrusions**.[7]

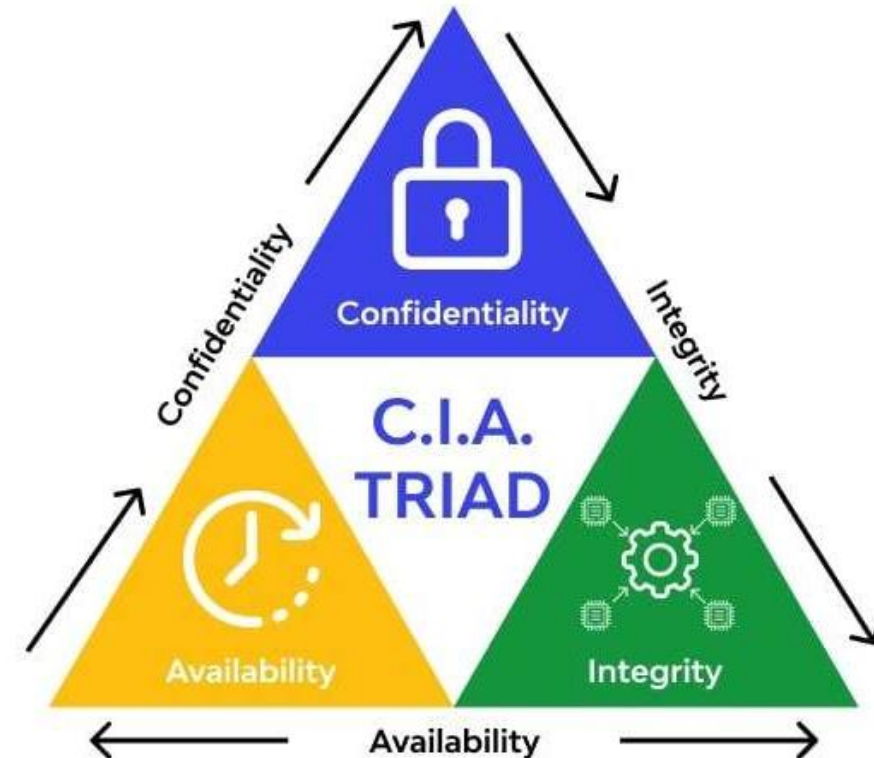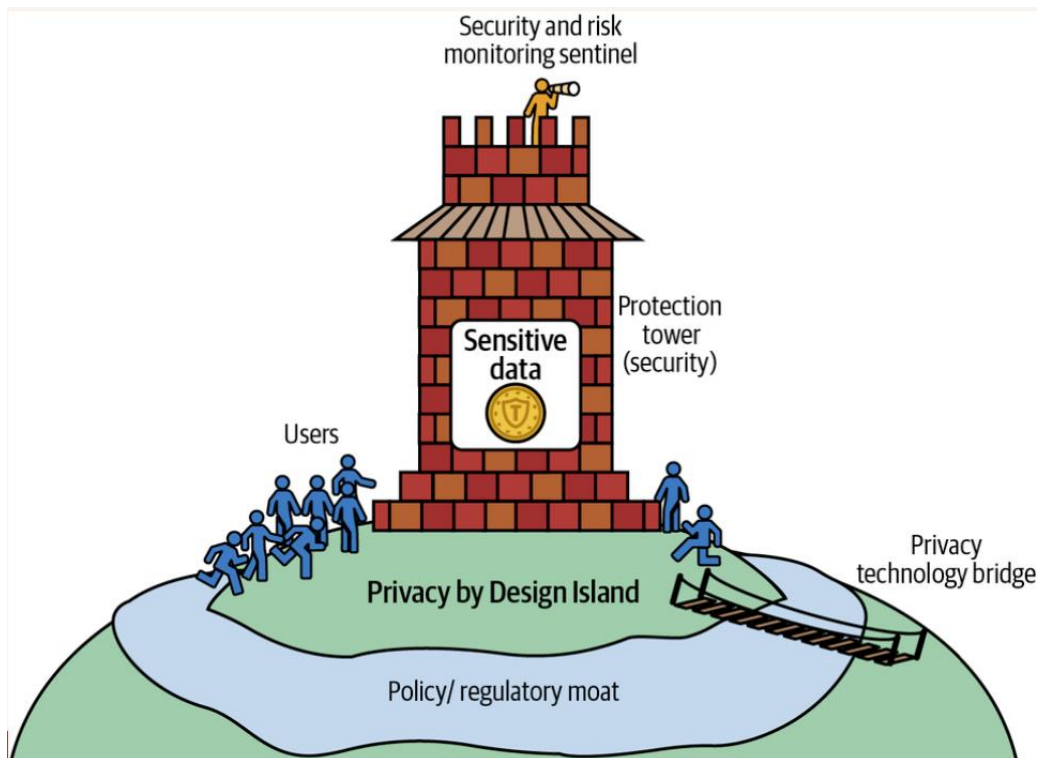Man-in-the-Middle Attack Example

Cyberattacks and cybercrimes impose increasing constraints on modern information systems

How can we establish a sufficient set of security measures to effectively protect against and mitigate cyberattacks and cybercrimes?

Cybersecurity in a Nutshell

- By definition:

    - **Cybersecurity** is the continuous application of **best practices** aimed at ensuring and preserving the **confidentiality, integrity, and availability** of digital information, while also safeguarding **people and environments** from potential threats.
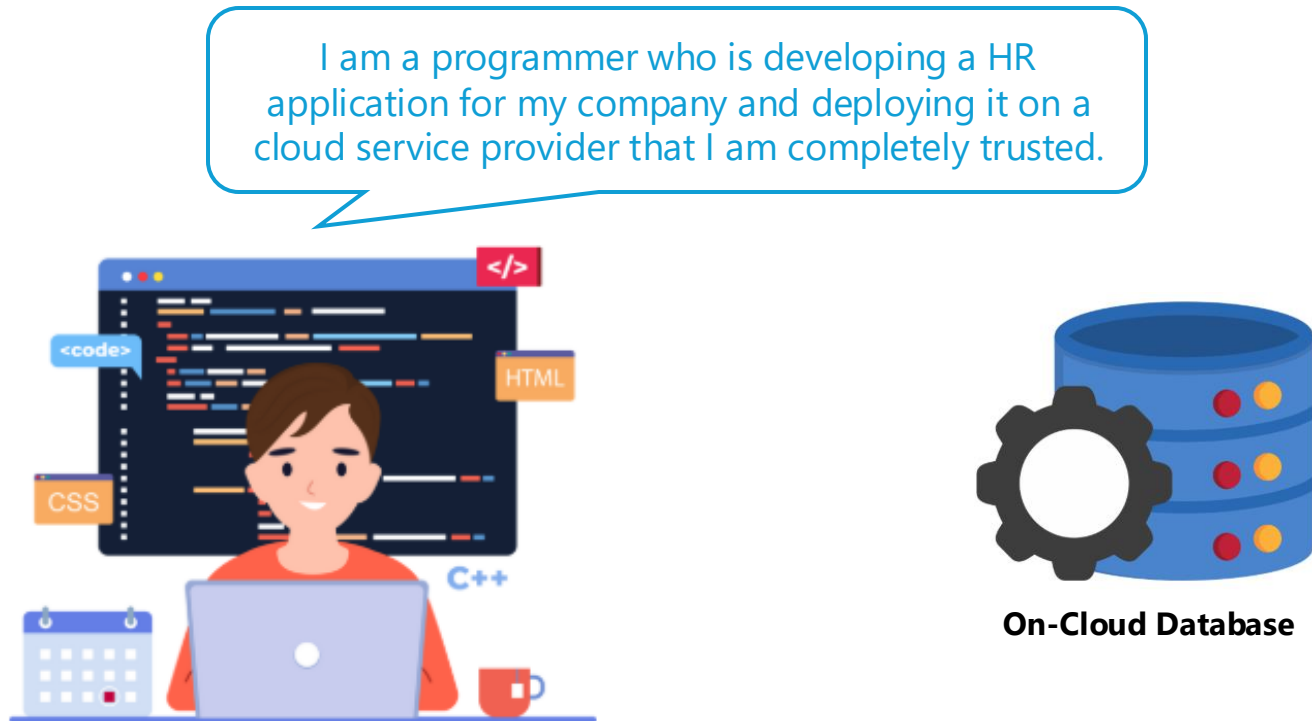
Cybersecurity Pillars and Properties

- *Cybersecurity pillars* consist of:

    - **Confidentiality**   None of unauthorized persons can read or make use of the data.

    - **Integrity**   Data/information must not be changed or tampered unexpectedly.

    - **Availability**   Data/information must be always available when the owner needs.

    - **Non-Repudiation**   Individuals cannot refuse any actions that has been done. They are accountable to all actions.

    - **Safety**   Data/information must not be harmful to personal or physical safety of its owners.

- Other *properties for data security and privacy* includes:

    - **Authentication**   The identity of a user or device trying to access a network or resource must be verified.

    - **Authorization**   Users are granted with specific rights and permissions to access resources based on their identity.

    - **Accountability**   User activities and resource consumptions must be tracked and logged for auditing and monitoring.
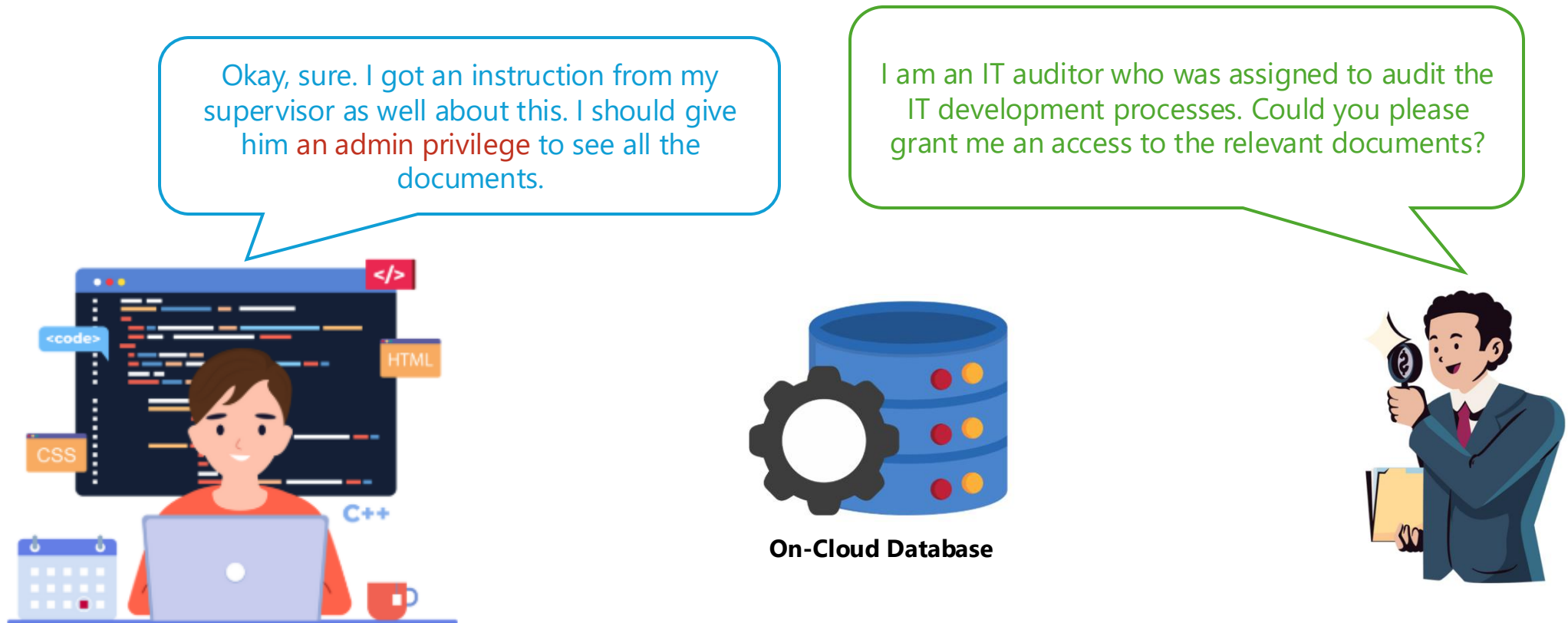
Confidentiality: Unauthorized Access Is Prohibited

- *"Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information"* – **NIST Computer Security Resource Center (CSRC)**

On-Cloud Database

Confidentiality: Unauthorized Access Is Prohibited

- *"Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information"* – **NIST Computer Security Resource Center (CSRC)**
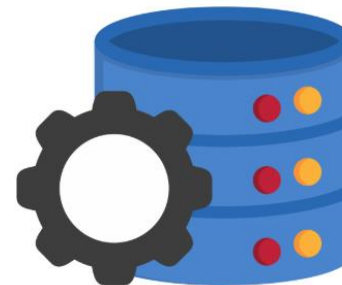
Confidentiality: Unauthorized Access Is Prohibited

- *"Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information"* – **NIST Computer Security Resource Center (CSRC)**
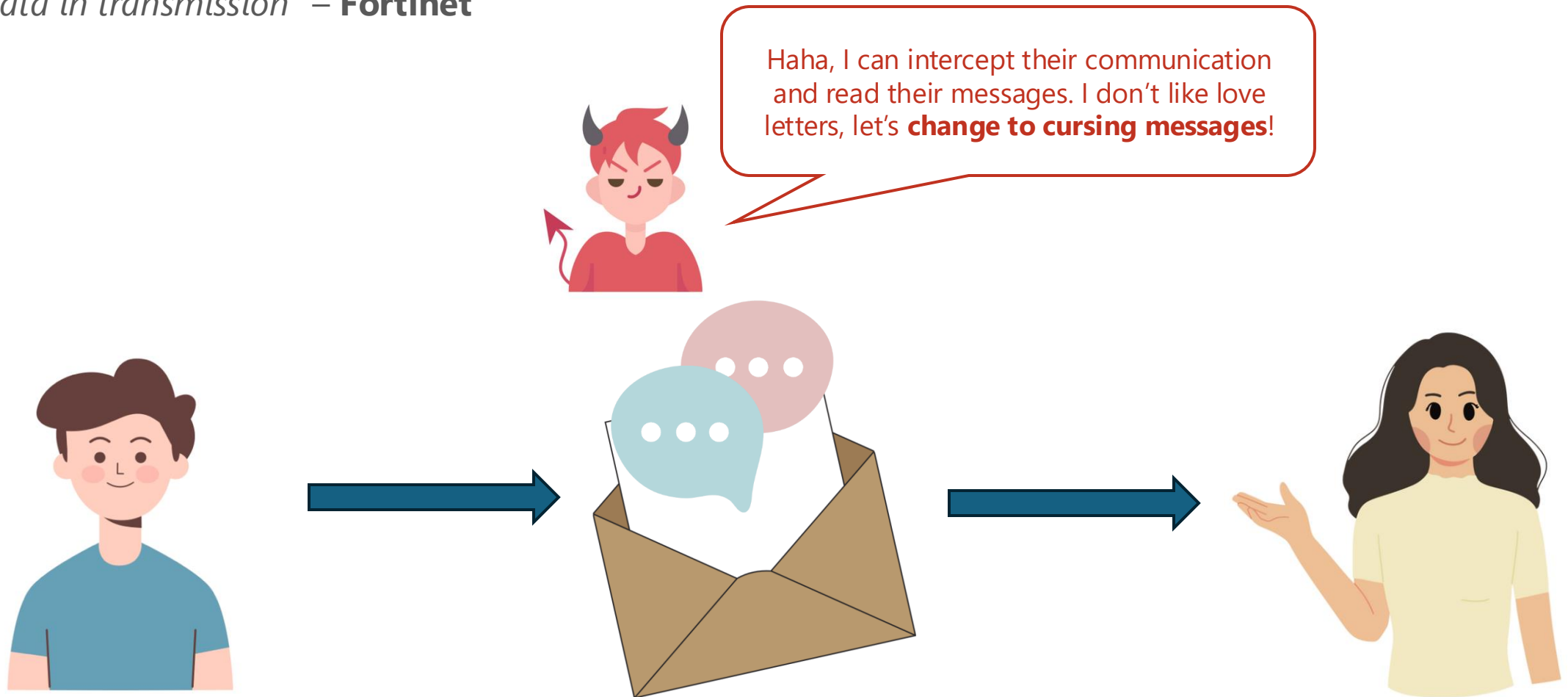

Oh, I can see all the related documents here. That's great! But wait, I can also see the salary information from the HR database!

On-Cloud Database

Integrity: Accurate, Consistent, and Up-to-dateness

- *"Ensuring that data is accurate, complete, consistent, and reliable throughout its lifecycle, including data at rest, and data in transmission"* – **Fortinet**

Haha, I can intercept their communication and read their messages. I don't like love letters, let's **change to cursing messages**!

Availability: Timely and Reliable Access to Data

- *"Ensuring that authorized users have timely and reliable access to information and resources when they need them. It means systems, networks, and applications are functioning as intended and are accessible."* – **Fortinet**

Availability: Timely and Reliable Access to Data

- *"Ensuring that authorized users have timely and reliable access to information and resources when they need them. It means systems, networks, and applications are functioning as intended and are accessible."* – **Fortinet**

Safety: Protecting from Harmful Digital Activities

- *"Protecting users from online harm and unwelcome or inappropriate content and behavior."* – **Telstra Personal**

Hello, I'm Katherine, 56 years old. I work as an accountant at this company, working under Mr. Kevin Steward. I'm **not very tech-savvy** and have been using a familiar program on my computer, which I trust because it's secured with a username and password. I prefer not to switch to any new programs, as I'm comfortable with the current one.

From Kevin Steward
<asfewr23@gmail.com>

Dear Katherine,
This is your boss, Kevin. Please **send me the username and password** for your accounting program. I have to check some details for the customer issue. Please reply me as soon as possible.

Thanks, Kevin

Safety: Protecting from Harmful Digital Activities

- *"Protecting users from online harm and unwelcome or inappropriate content and behavior."* – **Telstra Personal**

Oh, it must be Kevin. I don't want to make him upset.
I will share my username and password to him. That should not be a problem, since we are working with each other for a very long time.
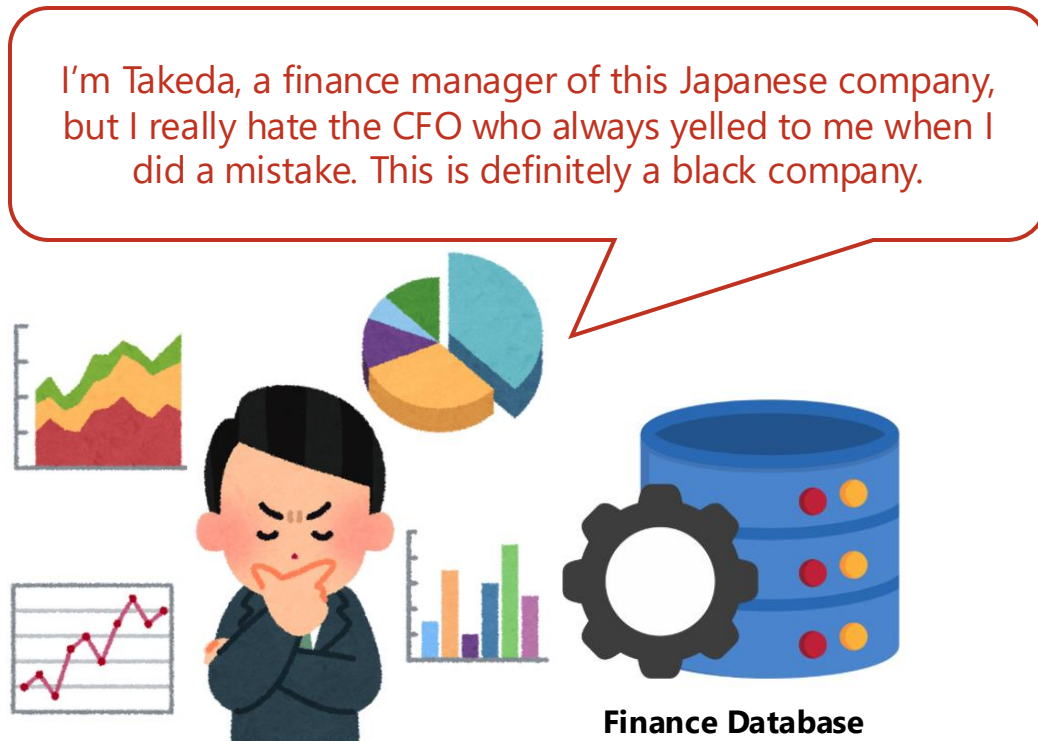
Excellent! I can now **retrieve all financial data** of this company. Let's try to sell it in the dark market.

Non-Repudiation: Participation Cannot Be Denied

- *"Assurance that the sender of information is provided with <u>proof of delivery</u> and the recipient is provided with <u>proof of the sender's identity</u>, so <u>neither can later deny</u> having processed the information."* – **NIST SP 800-18**.

I'm Takeda, a finance manager of this Japanese company, but I really hate the CFO who always yelled to me when I did a mistake. This is definitely a black company.

Finance Database

From Mitsuta <mitsuta@rivalcompany.com>

To Takeda-san,
Greetings from a rival company. I've heard that your company treats you poorly. **Would you consider sharing all of your company's past financial reports with me?** I can offer you ¥2,000,000. Don't worry—I won't expose you. You can always claim that someone else used your computer to do it.

Hope you accept my offer, Mitsuta.

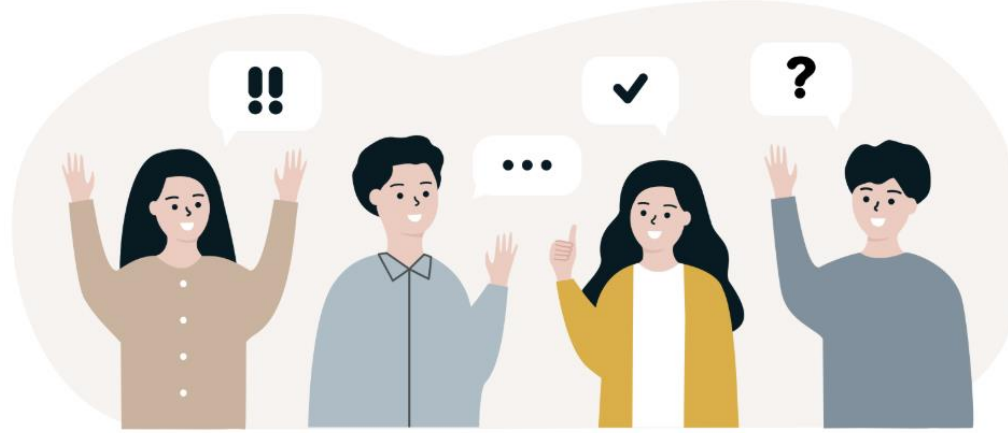# Non-Repudiation: Participation Cannot Be Denied

- *"Assurance that the sender of information is provided with <u>proof of delivery</u> and the recipient is provided with <u>proof of the sender's identity</u>, so <u>neither can later deny</u> having processed the information."* – **NIST SP 800-18**.

Sounds good! I'll just claim that I wasn't aware of the misconduct—that someone else must have used my account to do it.

This is a serious issue. We have discovered that our financial reports were disclosed to a rival company. Following an investigation by our IT team, it was found that the data was sent from Mr. Takeda's computer. However, Mr. Takeda has denied any involvement in the misconduct, and we currently have **no conclusive evidence to hold him accountable**.

Finance Database

Discussion Time!

Choose one of the cybersecurity pillars we discussed earlier. Then, **work together with the person or group sitting next to you** to identify a **real-world situation or solution** where that pillar is effectively protected or implemented based on the given scenario.

End of the Lecture

Please don't hesitate to raise your hand and ask questions if you're curious about anything!