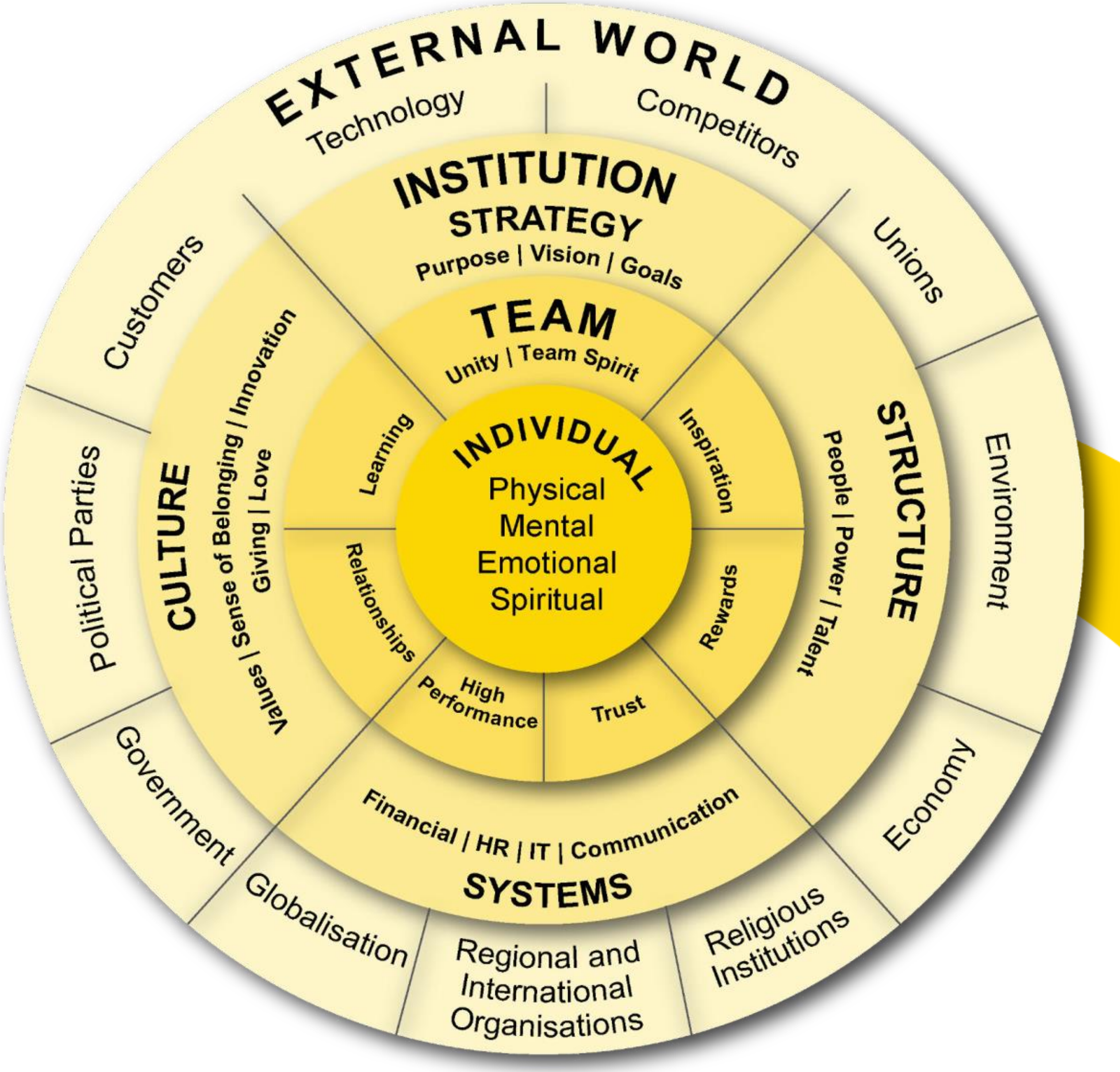
CYBER SECURITY FUNDAMENTALS

DATE: 21.02.2025 & 22.02.2025

DIGITAL REGENESYS
Awakening Potential

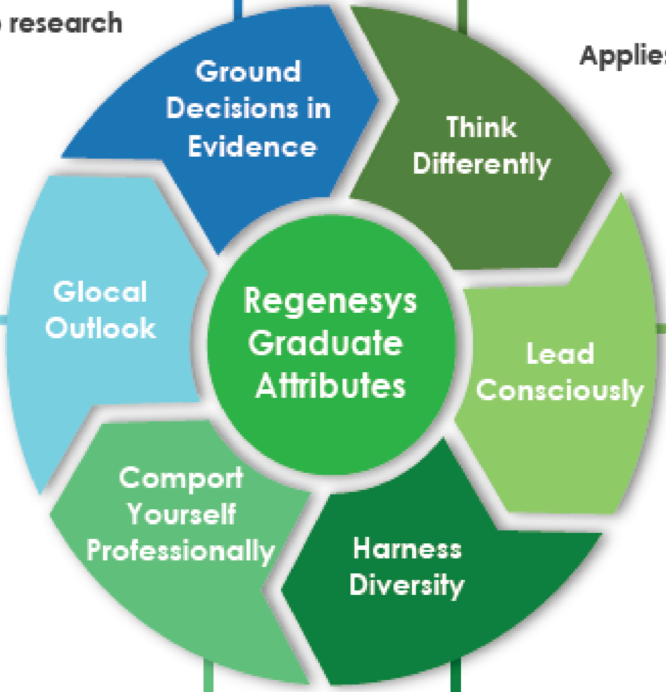
REGENESYS' INTEGRATED LEADERSHIP AND MANAGEMENT MODEL:

- **Holistic** focus on the individual (SQ, EQ, IQ, and PQ)
- **Interrelationships** are dynamic between individual, team, institution and the external environment (systemic)
- **Strategy** affects individual, team, organisational, and environmental performance
- **Delivery** requires alignment of strategy, structure, systems and culture



DIGITAL REGENESYS
Awakening Potential

REGENESYS GRADUATE ATTRIBUTES:



Regenesys Graduate Attributes

Ground Decisions in Evidence

Think Differently

Lead Consciously

Harness Diversity

Comport Yourself Professionally

Glocal Outlook

Bases decisions on evidence
Well informed | Knowledgeable
Multidisciplinary, metacognitive approach
Recognises and can put aside personal bias
Takes calculated risks | Committed to research

Imaginative but rational
Appetite for problem-solving
Incisive | Constructively critical
Curious | Analytical | Agile mind
Innovative | Visionary | Open-minded
Applies knowledge across disciplines and domains

Adaptable
Multiculturally aware
Responsible global citizen
Understands local realities
Operates in a borderless world

Purpose-driven | Self-aware
Acts ethically and with integrity
Service-oriented | Agent of change
Emotionally and spiritually intelligent
Puts sustainability at heart of business

Inspiring | Confident
Deliberate | Focused | Determined
Resilient | Disciplined | Accessible|Accountable
Models values | Observes business etiquette

Values individual differences
Collaborative | Socially intelligent
Builds high-functioning, diverse teams
Skilled communicator | Creates connections

DIGITAL REGENESYS
Awakening Potential

KNOW YOUR FACILITATOR:

Dr. Saquib Ahmad Khan

- Dr. Saquib Ahmad Khan is a highly respected professional in the cybersecurity field.
- He holds a Ph.D. in Computer Science and possesses multiple cybersecurity certifications, establishing him as an esteemed expert in cybersecurity.
- Dr. Khan is a prolific author, with numerous research papers and articles to his credit, focused on advancing the field of cybersecurity.
- He is a frequent speaker at prominent industry conferences and events, where he imparts his knowledge and insights to fellow professionals.
- Dr. Khan also possesses a strong foundation in marketing, management, information technology, and various applications, bolstered by multiple degrees.

GROUND RULES:

- Be open-minded
- When speaking, use “I think”, “I feel”, etc.
- (you are a very important aspect of this learning)
- Listen carefully
- One conversation at a time
- Respect the opinions of others
  - Give constructive feedback
  - Build on the ideas of others rather than destroying them
- Take some risks and share new ideas

HAVE FUN AND ENJOY THE EXPERIENCE !

DIGITAL REGENESYS
Awakening Potential

MODULE 03

DIGITAL REGENESYS
Awakening Potential

Information Security Governance and Risk Management: Safeguarding Systems and Networks

- Information system governance and risk assessment
- Introduction to information security
- Governance risk
- Management information security programs
- Network security and spoofing

On completing this module, you should be able to:

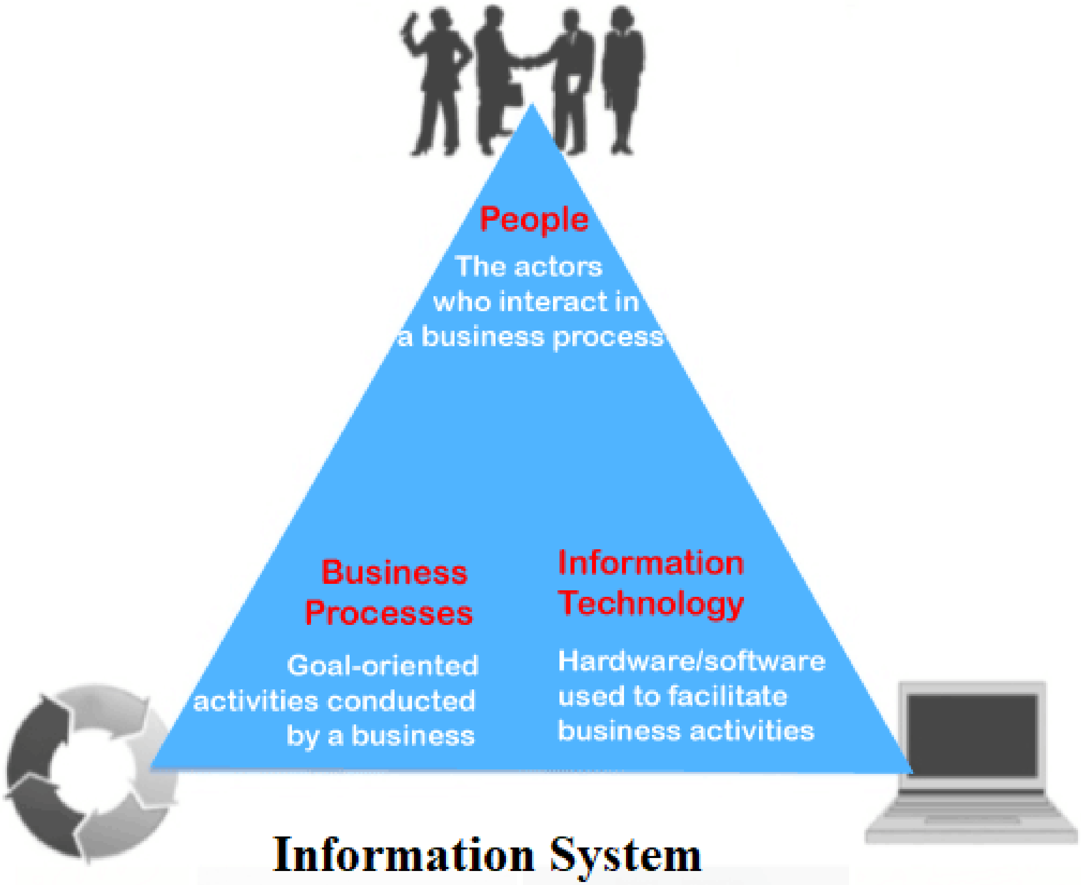
- Acquire essential information security knowledge, recognize common threats and weaknesses, and apply simple security methods to safeguard information
- Comprehend the significance of information system governance principles in organizational decision-making, while also mastering risk evaluation and mitigation strategies within organizational information systems.
- Examine how governance handles risk in organizations, recognizing its impact on risk reduction and regulatory adherence. Assess various governance frameworks and their suitability for different industries.

On completing this module, you should be able to:

- Acquire expertise in creating and executing information security programs, ensuring they meet organizational objectives. Understand managing resources and stakeholders within these programs.
- Understand the importance of network security principles, including safeguarding data in transit, and recognize typical threats like spoofing attacks.
- Learn techniques and best practices for protecting network infrastructure from spoofing vulnerabilities.

INFORMATION SYSTEM:

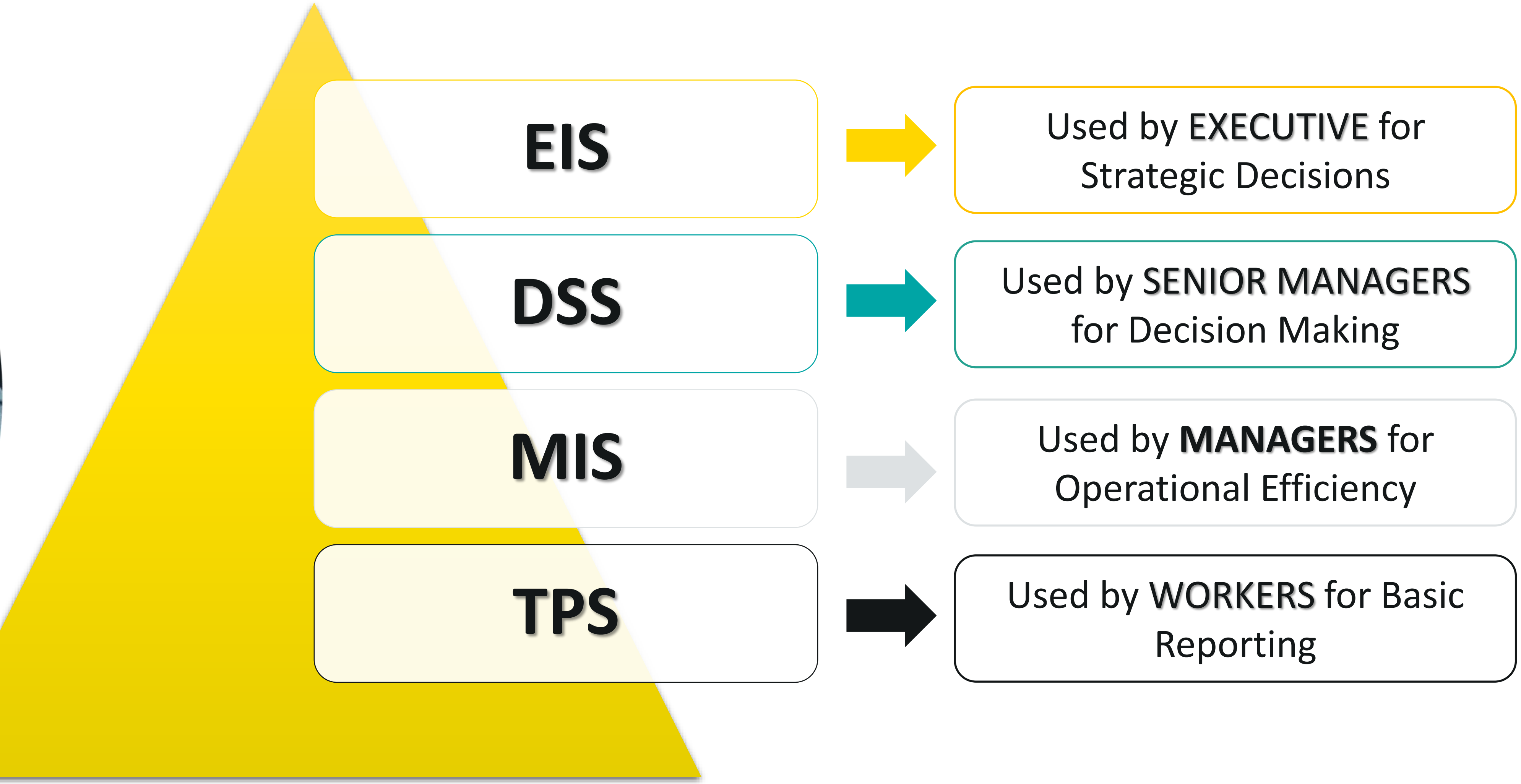
An information system can be defined as a set of interrelated components that collect, manipulate, store data, distribute information to support decision making and provide a feedback mechanism to monitor performance.


People
The actors who interact in a business process
Business Processes
Goal-oriented activities conducted by a business
Information Technology
Hardware/software used to facilitate business activities
Information System

(Source: *Information System Definition - javatpoint*. (n.d.). Www.javatpoint.com. https://www.javatpoint.com/information-system-definition)

DIGITAL REGENESYS
Awakening Potential

TYPES OF INFORMATION SYSTEM:



EIS → Used by EXECUTIVE for Strategic Decisions

DSS → Used by SENIOR MANAGERS for Decision Making

MIS → Used by **MANAGERS** for Operational Efficiency

TPS → Used by WORKERS for Basic Reporting

COMPONENTS OF INFORMATION SYSTEM:

01. Hardware

02. Software

03. Data

04. Procedures

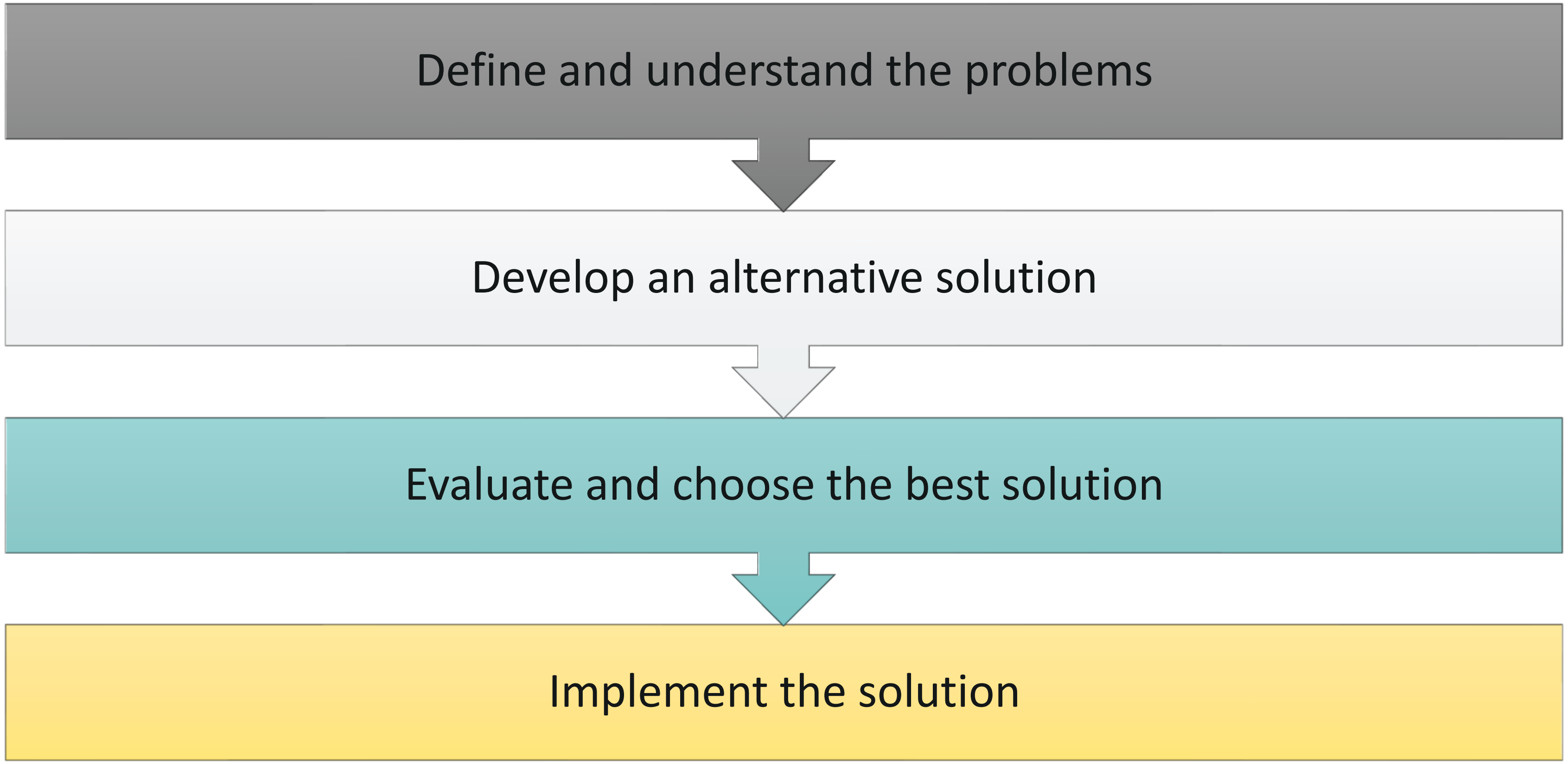
05. People

06. Network

07. Feedback

DEVELOPMENT OF INFORMATION SYSTEM:

There are four steps which can be used to develop an information system. These are:



Define and understand the problems

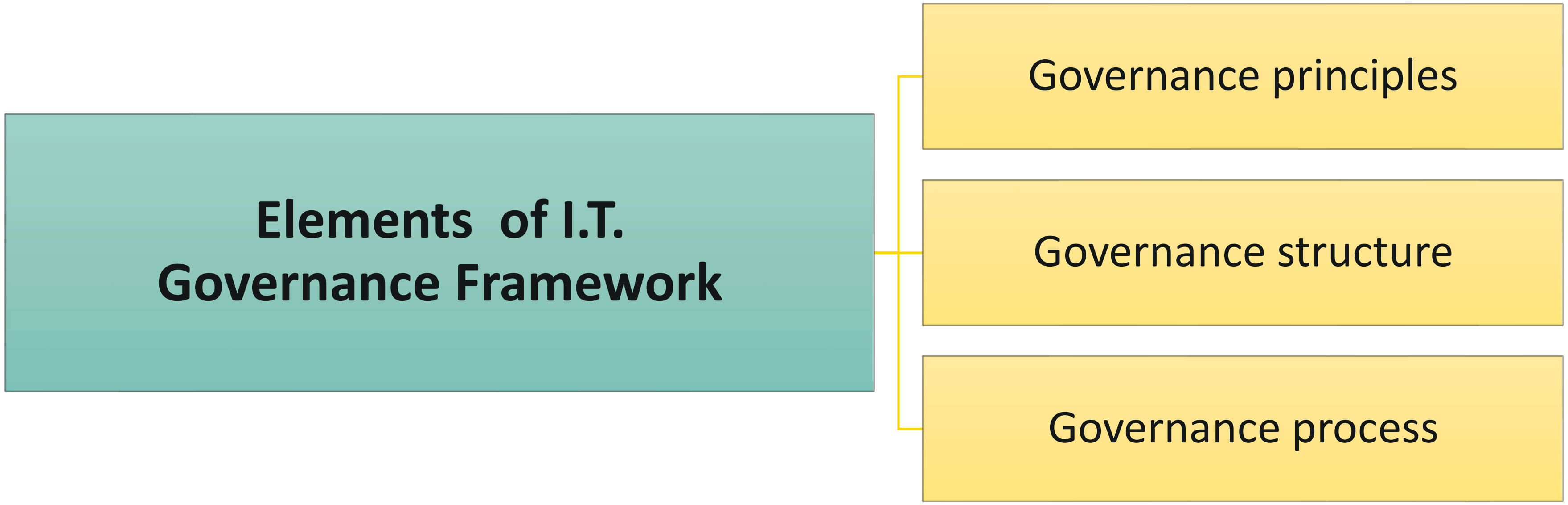
Develop an alternative solution

Evaluate and choose the best solution

Implement the solution

INFORMATION TECHNOLOGY GOVERNANCE:

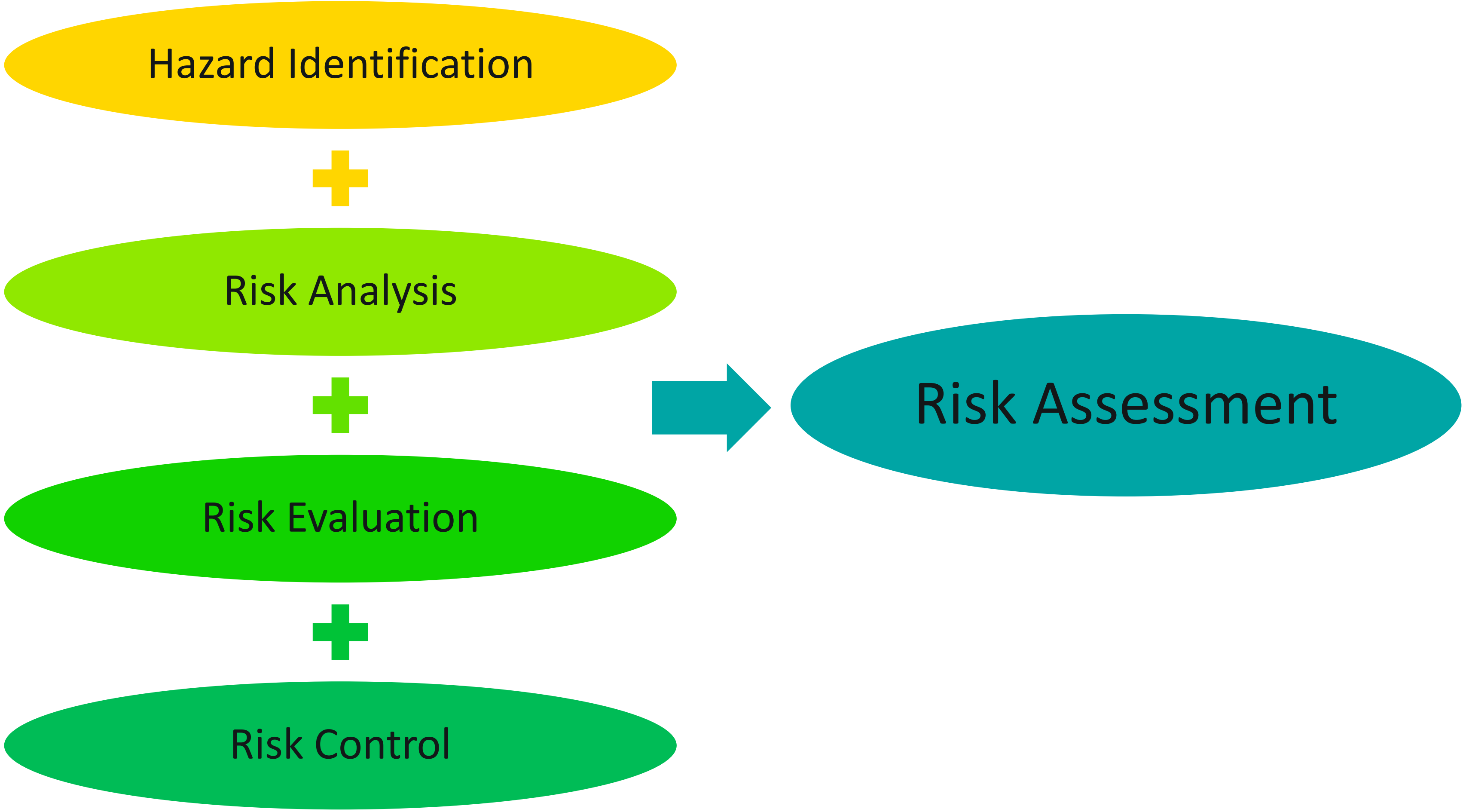
I.T. Governance are to assure that the investments in IT generate business value, and to mitigate the risks that are associated with IT.



Elements of I.T. Governance Framework

- Governance principles
- Governance structure
- Governance process

WHAT IS RISK ASSESSMENT?



Hazard Identification

+

Risk Analysis

+

Risk Evaluation

+

Risk Control

Risk Assessment

DIGITAL REGENESYS
Awakening Potential

THE QUESTION IS….

Who should / How to Perform a Cyber Risk Assessment ?

CYBER RISK ASSESSMENT STEPS:

Step 1: Determine Information Value

Step 2: Identify and Prioritize Assets

Step 3: Identify Cyber Threats

Step 4: Identify Vulnerabilities

Step 5: Analyze Controls and Implement New Controls

Step 6: Calculate the Likelihood and Impact of Various Scenarios on a Per-Year Basis

Step 7: Prioritize Risks Based on the Cost of Prevention vs. Information Value

Step 8: Document Results from Risk Assessment Reports

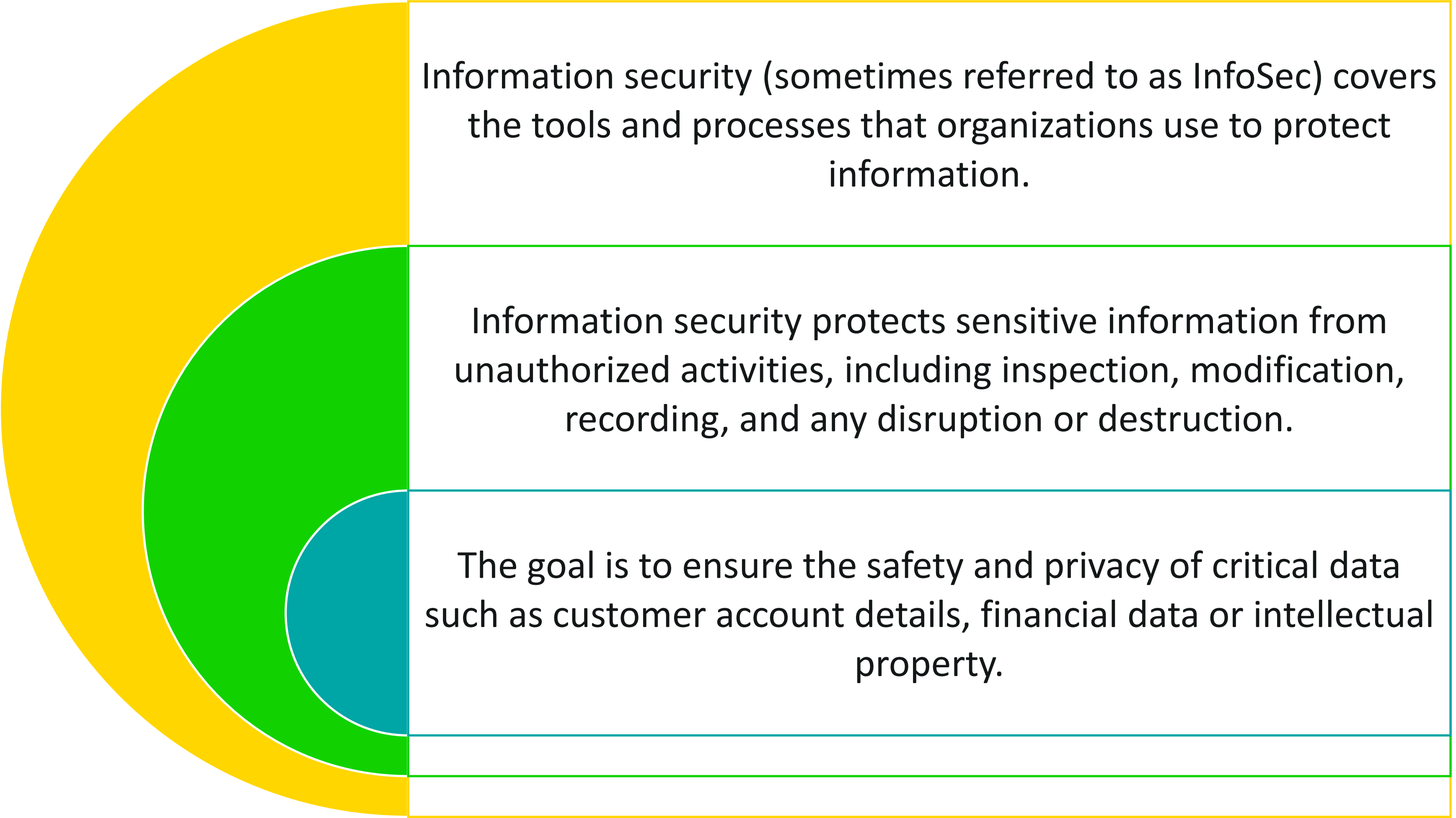
THE QUESTION IS….

WHY IS

RISK ASSESSMENT

IMPORTANT?

INFORMATION SECURITY (InfoSec):

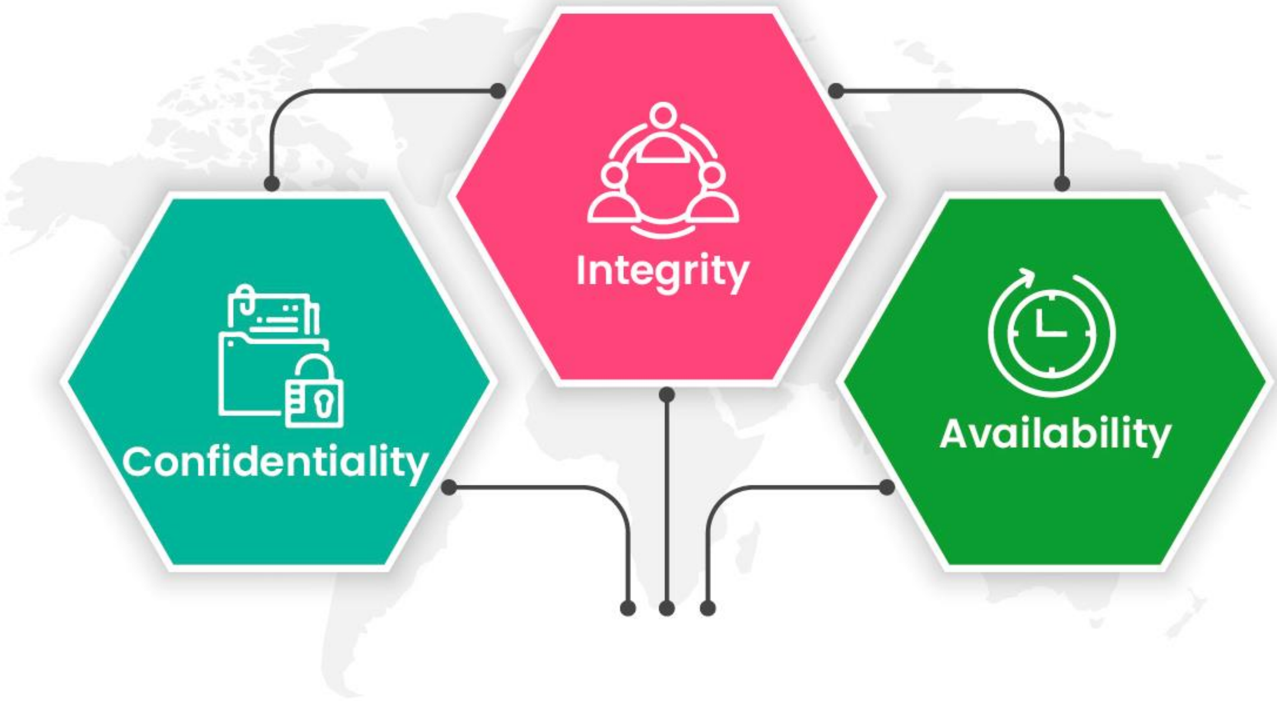


Information security (sometimes referred to as InfoSec) covers the tools and processes that organizations use to protect information.

Information security protects sensitive information from unauthorized activities, including inspection, modification, recording, and any disruption or destruction.

The goal is to ensure the safety and privacy of critical data such as customer account details, financial data or intellectual property.

PRINCIPLES OF INFORMATION SECURITY



(Source: *Fundamental Principles of Information Security*. (n.d.). InfosecTrain. https://www.infosectrain.com/blog/fundamental-principles-of-information-security/)

TYPES OF INFORMATION TECHNOLOGY SECURITY:

There are four types of information technology security you should consider or improve upon:

- Network Security
- Cloud Security
- Application Security
- Internet of Things Security

IMPLEMENTING AN INFORMATION SECURITY PROGRAM:

Step 1: Build an Information Security Team

Step 2: Inventory and Manage Assets

Step 3: Assess Risk

Step 4: Manage Risk

Step 5: Develop an Incident Management and Disaster Recovery Plan

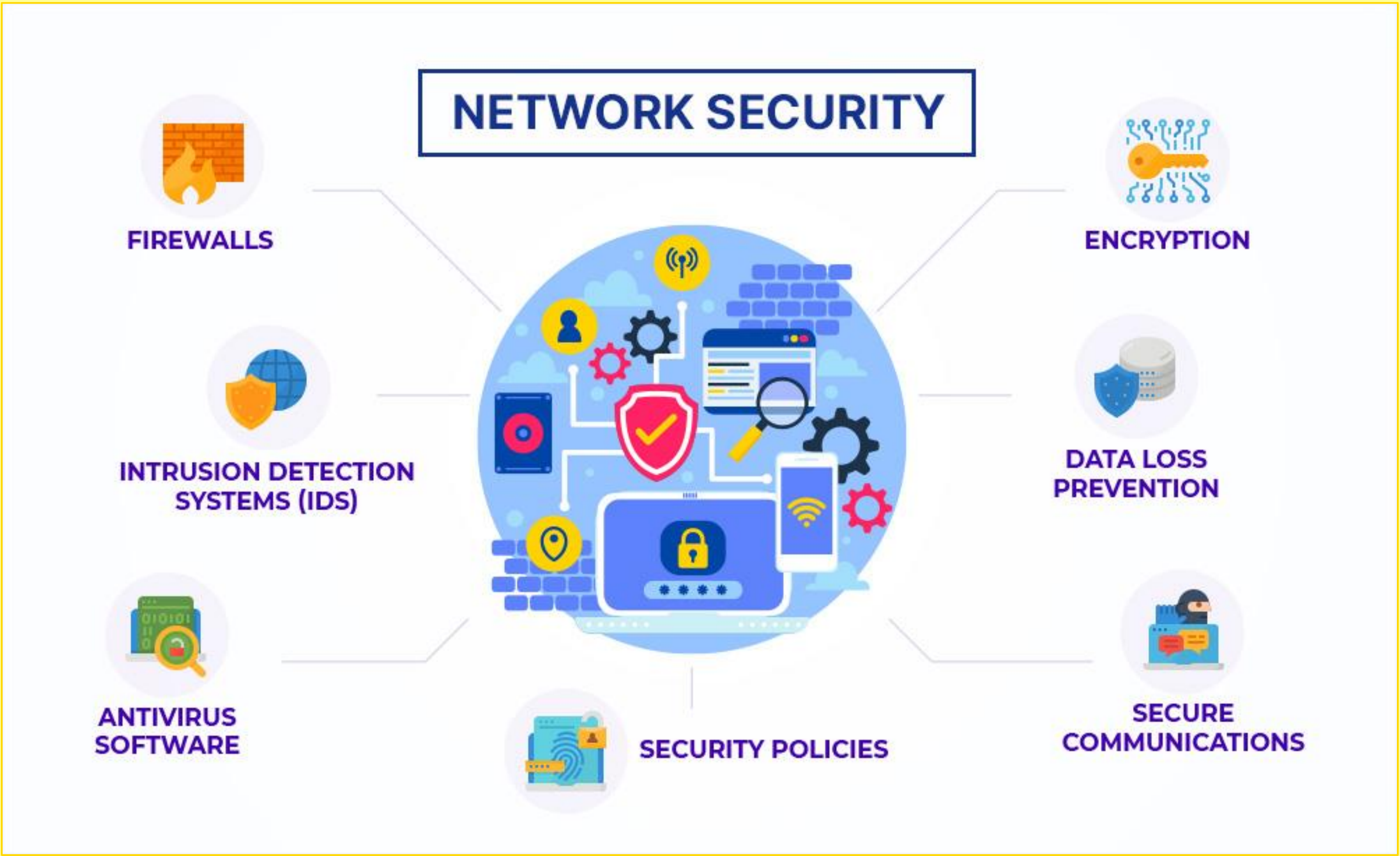
Step 6: Inventory and Manage Third Parties

Step 7: Apply Security Controls

Step 8: Establish Security Awareness Training

Step 9: Audit, audit, audit

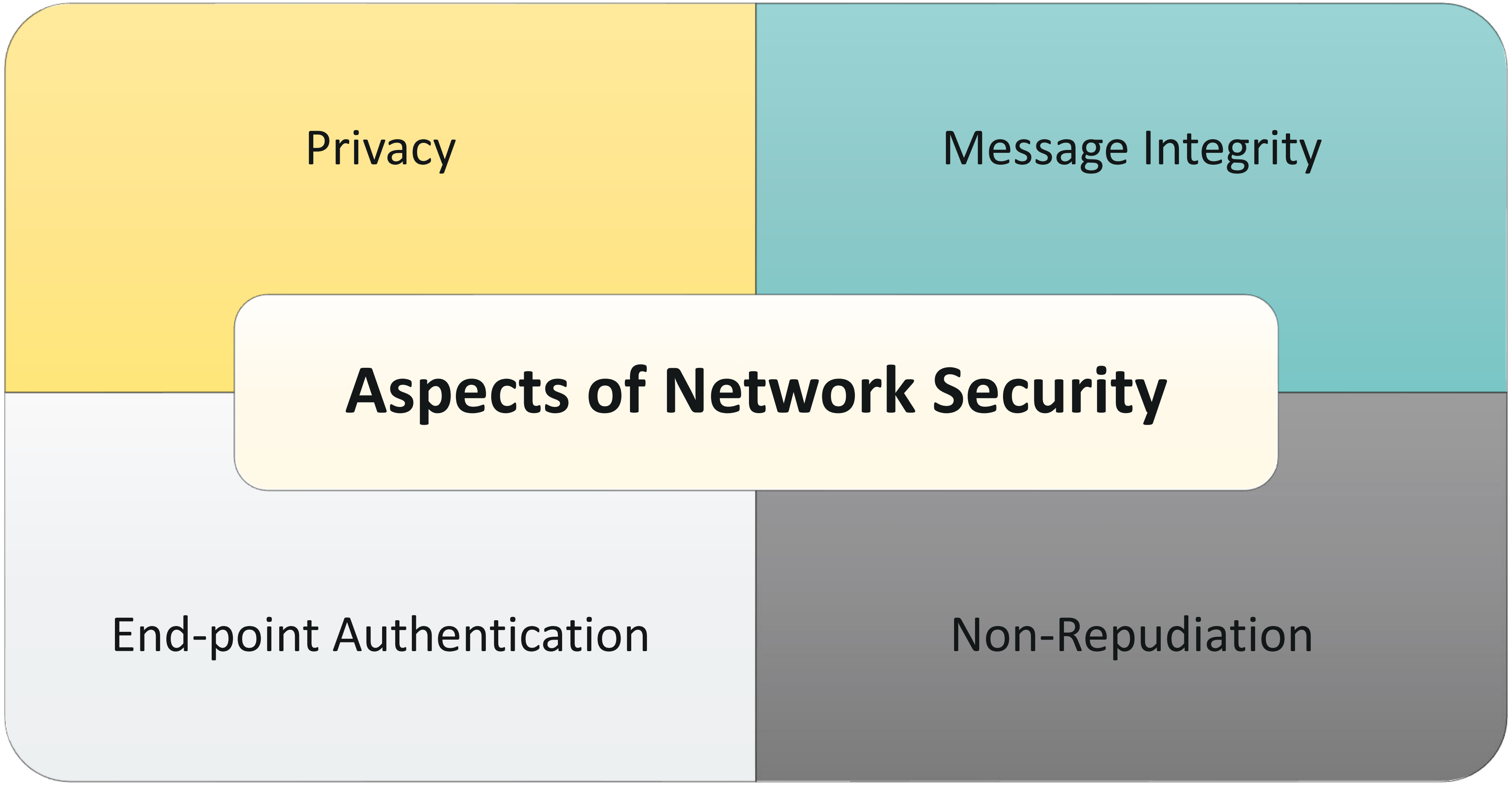
NETWORK SECURITY:



(Source: admin. (2022, December 6). *What is Network Security? - ExterNetworks*. Learning Center. https://www.extnoc.com/learn/computer-security/network-security)

DIGITAL REGENESYS
Awakening Potential

ASPECTS OF NETWORK SECURITY:



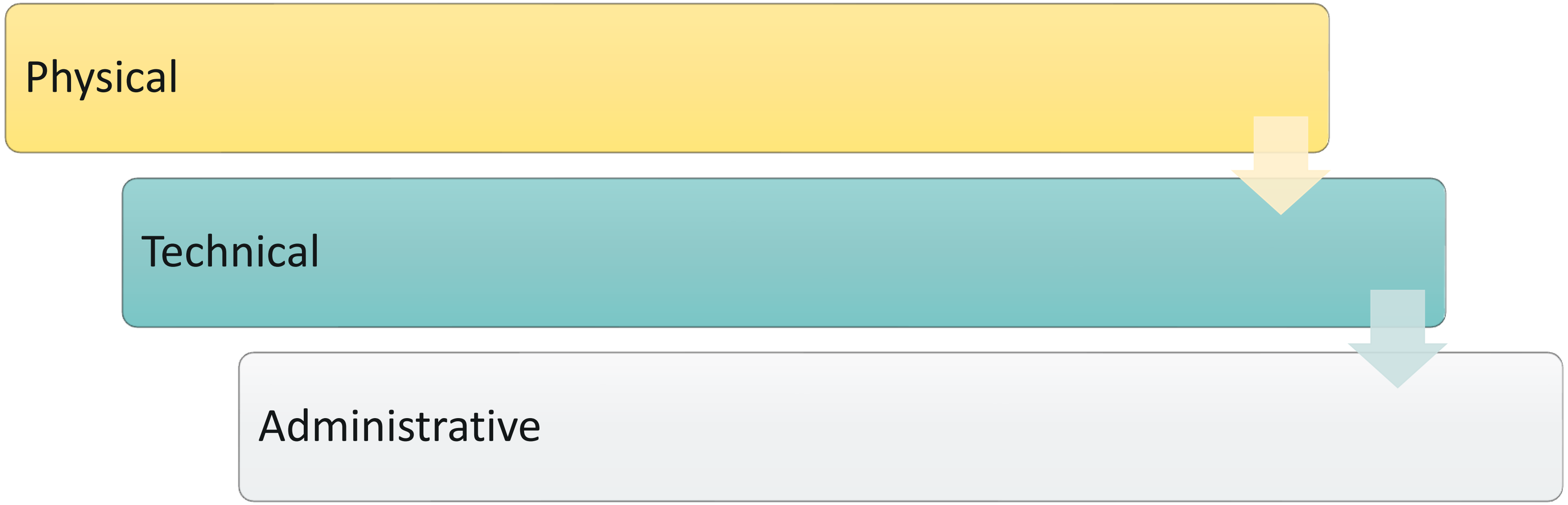
Aspects of Network Security

- Privacy
- Message Integrity
- End-point Authentication
- Non-Repudiation

NETWORK SECURITY-WORKING:

The basic principle of network security is protecting huge stored data and networks in layers that ensure the bedding of rules and regulations that have to be acknowledged before performing any activity on the data.

These levels are:



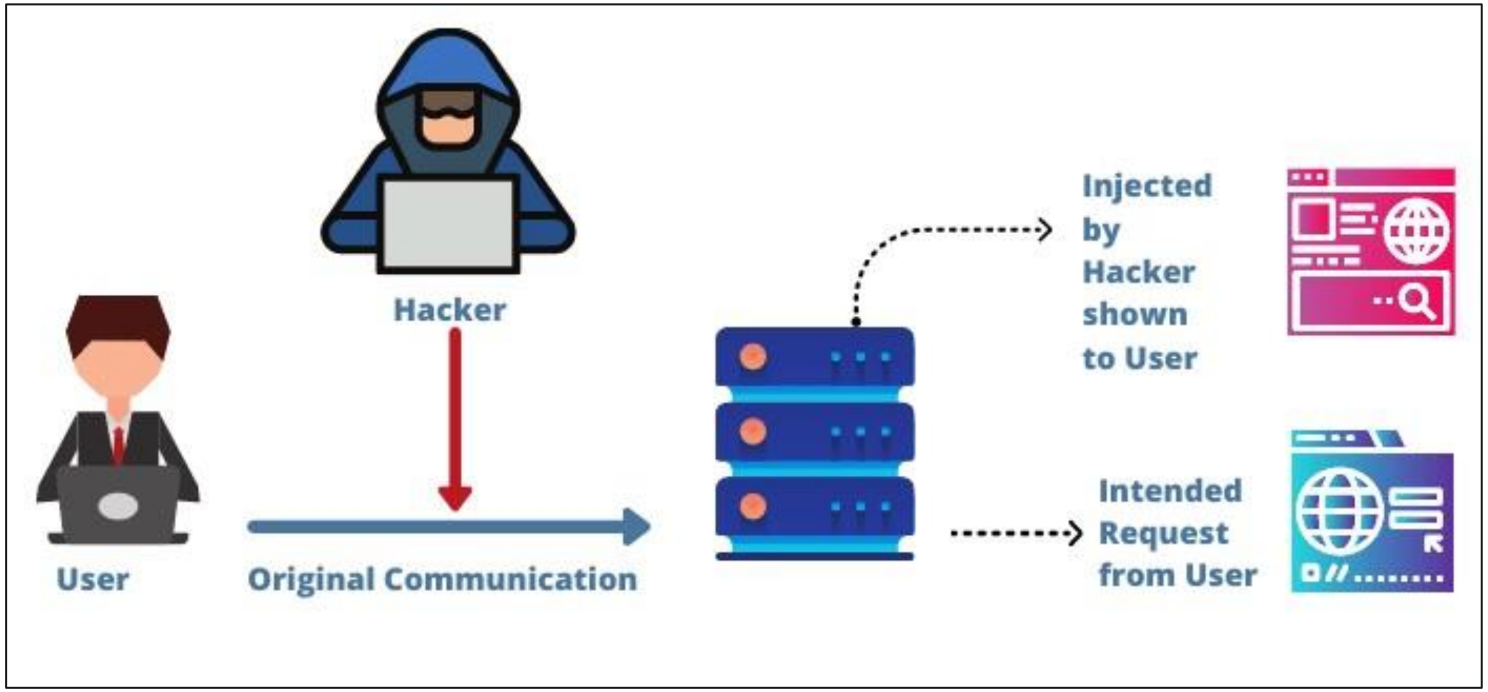
Physical

Technical

Administrative

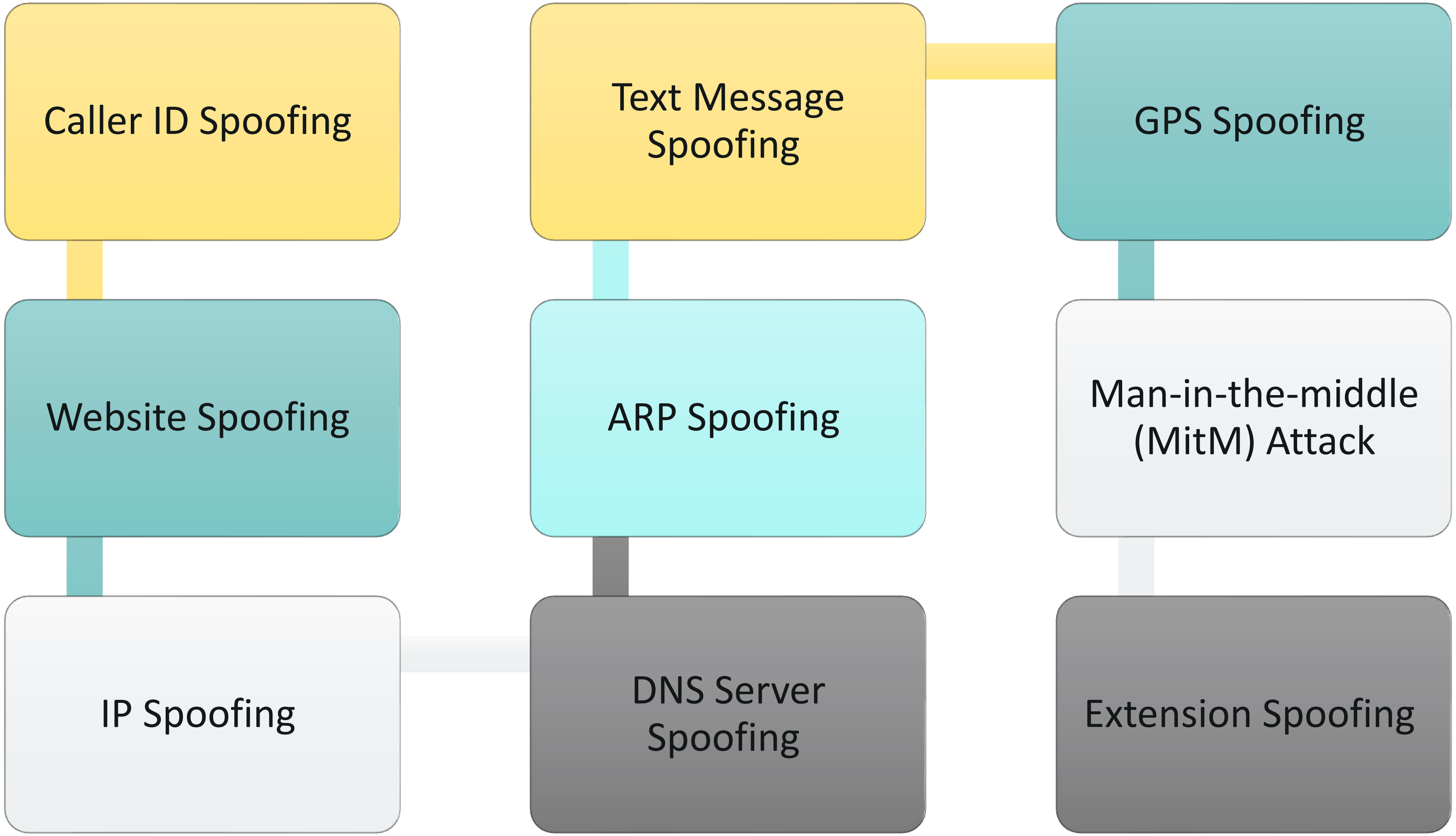
SPOOFING:

In cybersecurity, ‘spoofing’ is when fraudsters pretend to be someone or something else to win a person’s trust.



(Source: *Spoofing attack Network Security Projects (Guidance).* (n.d.). Network Simulation Tools. Retrieved May 19, 2024, from https://networksimulationtools.com/spoofing-attack-network-projects/)

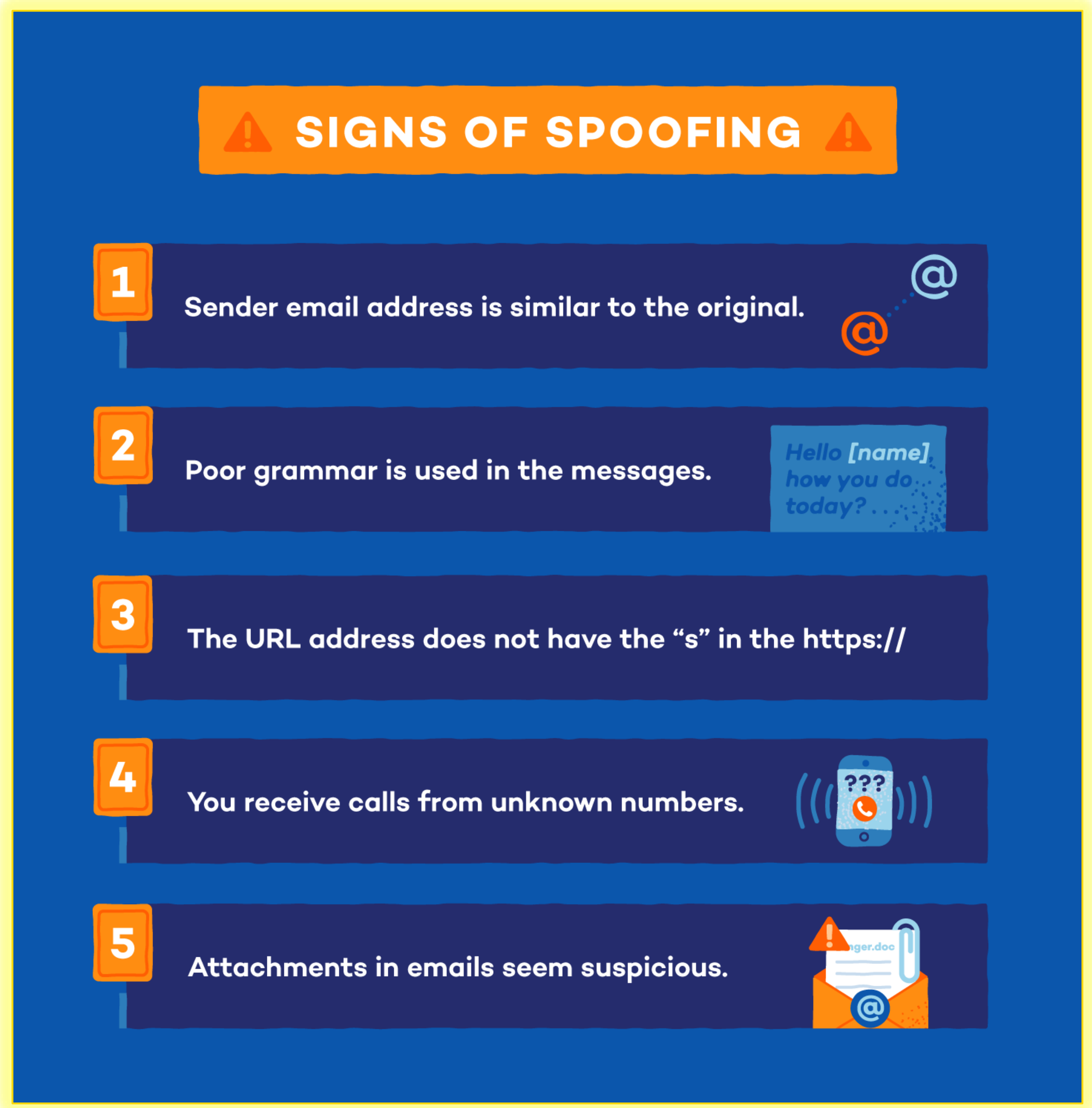
TYPES OF SPOOFING ATTACKS:



- Caller ID Spoofing
- Website Spoofing
- IP Spoofing
- DNS Server Spoofing
- ARP Spoofing
- Text Message Spoofing
- GPS Spoofing
- Man-in-the-middle (MitM) Attack
- Extension Spoofing

THE QUESTION IS….

HOW TO KNOW IF YOU'RE BEING SPOOFED ?

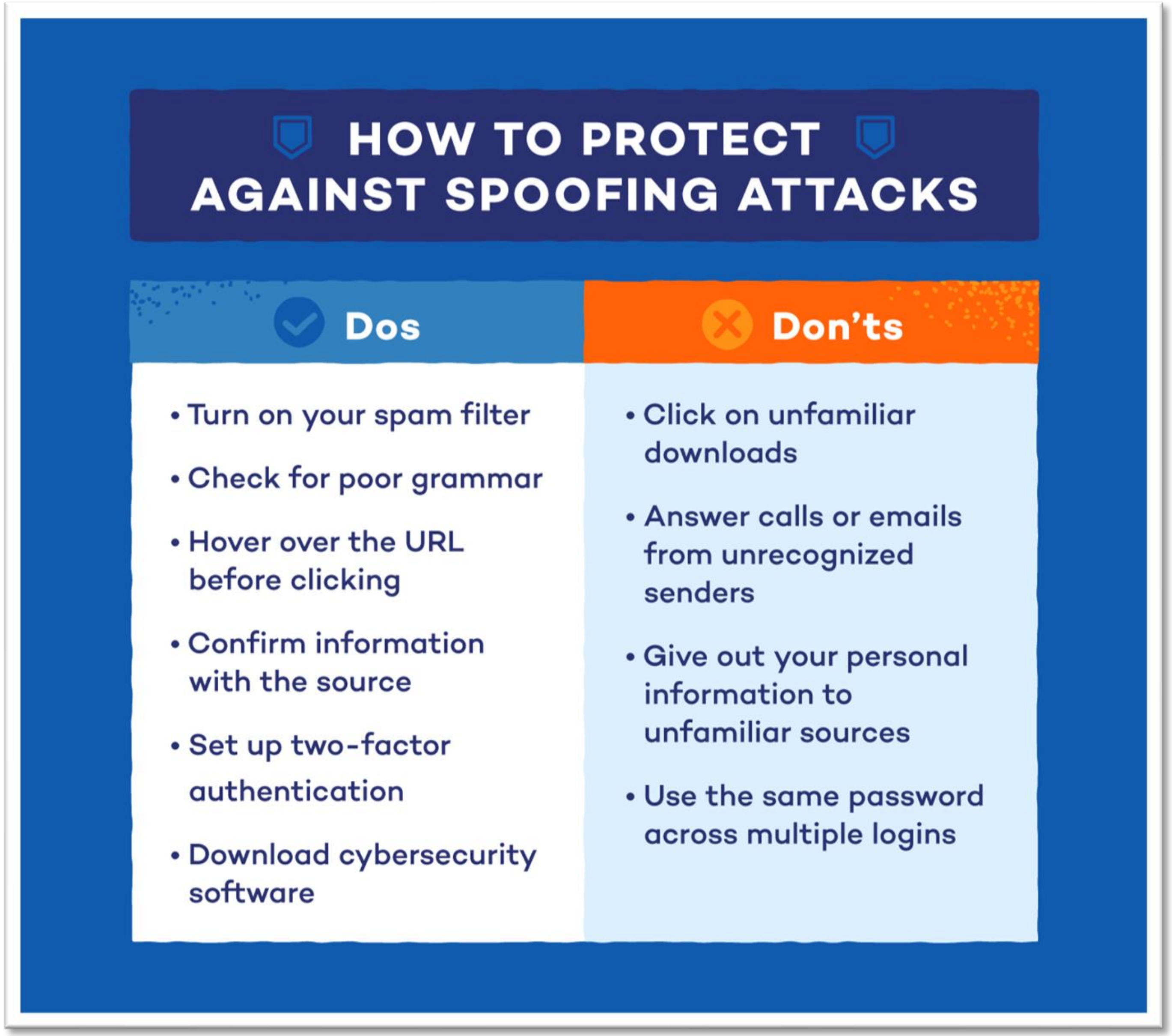


SIGNS OF SPOOFING

1. Sender email address is similar to the original.
2. Poor grammar is used in the messages.
3. The URL address does not have the “s” in the https://
4. You receive calls from unknown numbers.
5. Attachments in emails seem suspicious.

Hello [name] how you do today?
???
nger.doc

(Source: Security, P. (2022, September 30). *What is Spoofing: A Definition and How to Prevent It*. Panda Security Mediacenter. https://www.pandasecurity.com/en/mediacenter/what-is-spoofing/)



HOW TO PROTECT AGAINST SPOOFING ATTACKS

✓ Dos

- Turn on your spam filter
- Check for poor grammar
- Hover over the URL before clicking
- Confirm information with the source
- Set up two-factor authentication
- Download cybersecurity software

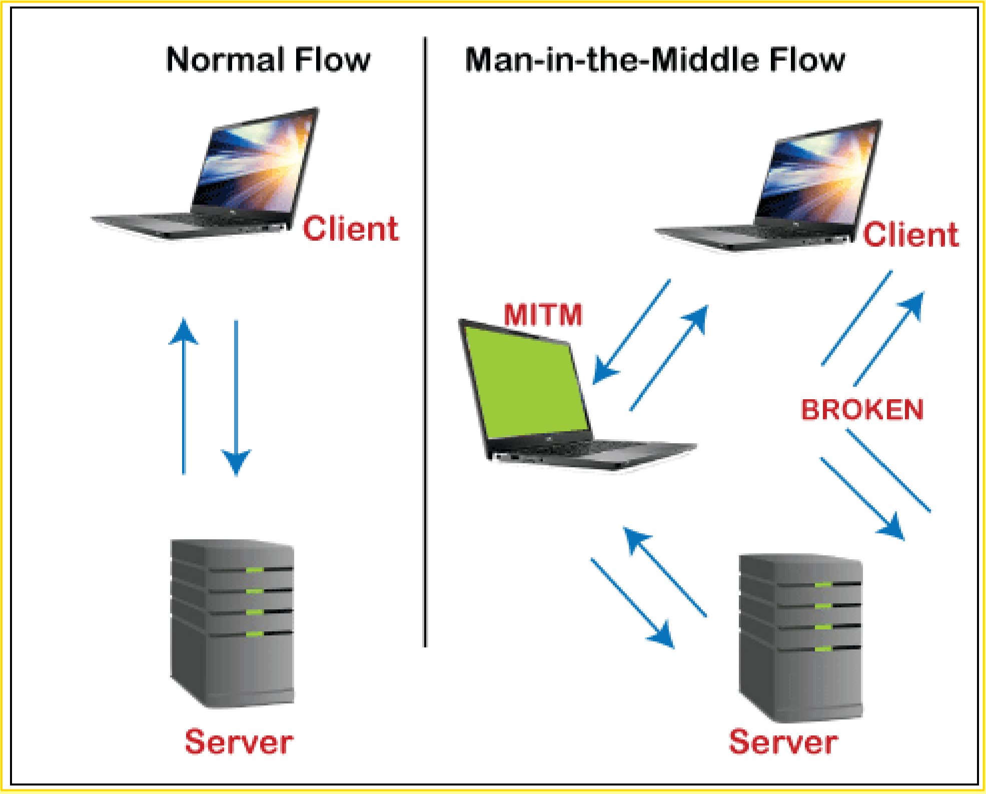
✗ Don'ts

- Click on unfamiliar downloads
- Answer calls or emails from unrecognized senders
- Give out your personal information to unfamiliar sources
- Use the same password across multiple logins

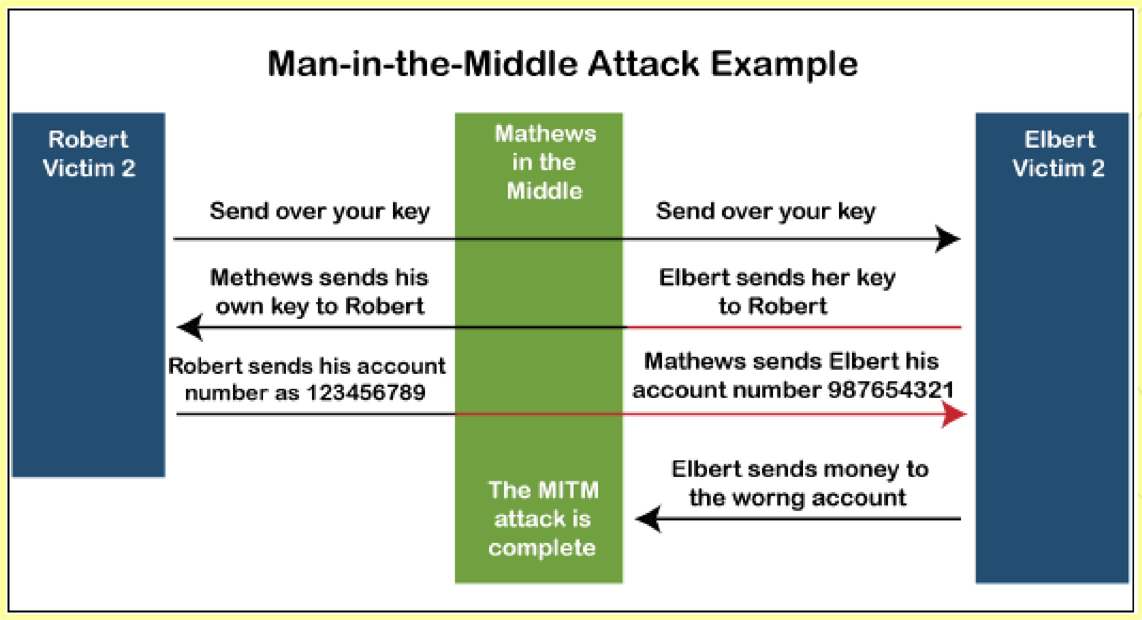
(Source: Security, P. (2022, September 30). *What is Spoofing: A Definition and How to Prevent It*. Panda Security Mediacenter. https://www.pandasecurity.com/en/mediacenter/what-is-spoofing/)

MAN-IN-THE-MIDDLE (MITM) ATTACKS:

Real life Instances of MITM attack



Another Instance of MITM attack


Man-in-the-Middle Attack Example

Send over your key

Send over your key

Methews sends his own key to Robert

Elbert sends her key to Robert

Robert sends his account number as 123456789

Mathews sends Elbert his account number 987654321

The MITM attack is complete

Elbert sends money to the worng account

(Source:*Cyber Security | Man-in-the-middle (MITM) Attacks - javatpoint*. (n.d.). Www.javatpoint.com. https://www.javatpoint.com/cyber-security-mitm-attacks)

THE QUESTION IS….

HOW WILL YOU DETECT **MAN-IN-THE-MIDDLE** ATTACK?

PREVENTIONS OF MAN-IN-THE-MIDDLE ATTACK:

01. Wireless access point (WAP) Encryption

02. Use a VPN

03. Public Key Pair Authentication

04. Strong Network User Credentials

05. Communication security

06. Proper hygiene for network protection on all platforms, such as smartphone apps.

07. Avoid Using Public Wi-Fi

THANK YOU

DIGITAL REGENESYS
Awakening Potential