أمن تكنولوجيا المعلومات وإدارة المخاطر

IT Security and Risk Management

Social Engineering

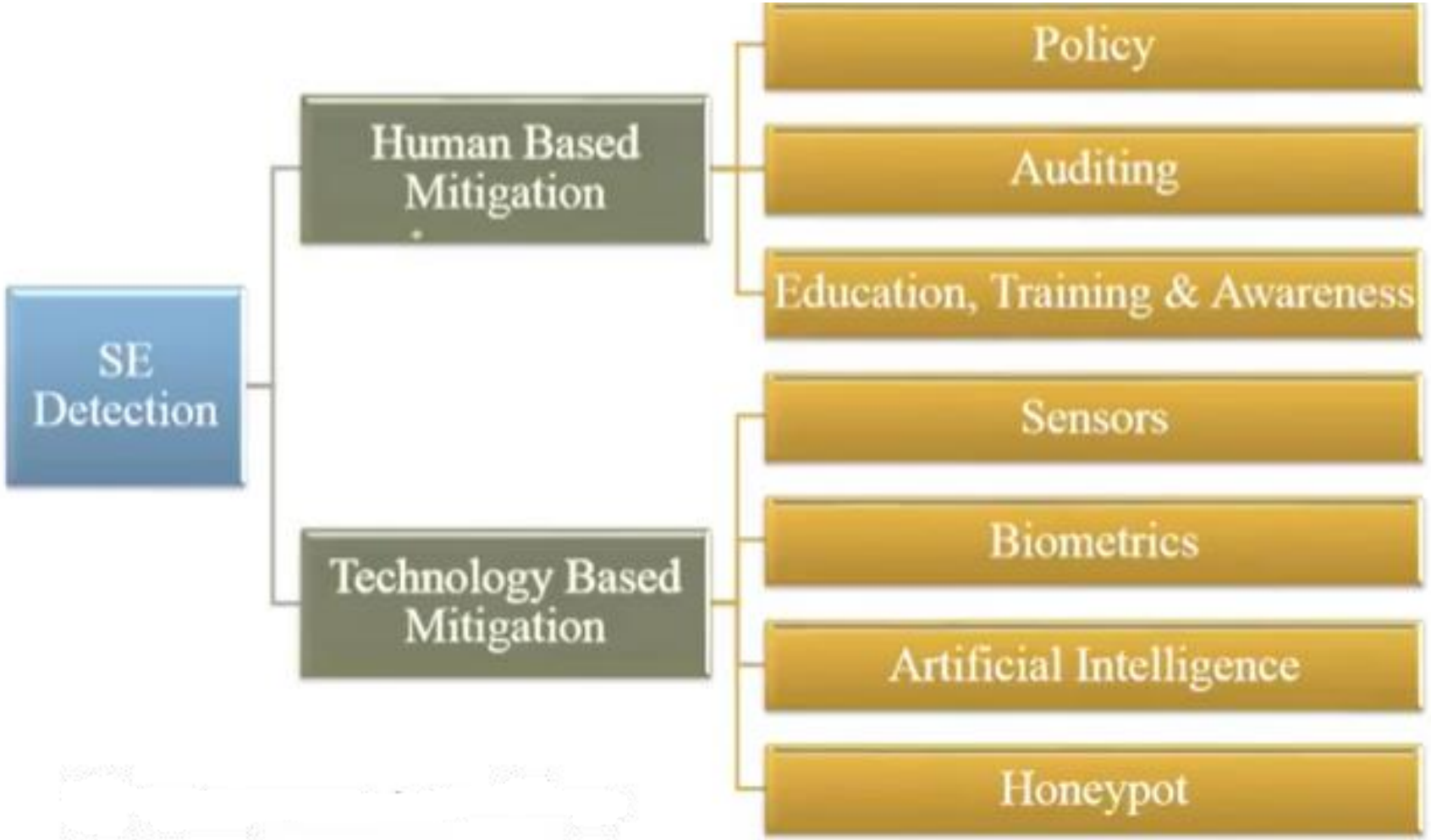
ا.د. حنان الطاهر الداقيز

h.dagez@uot.edu.ly

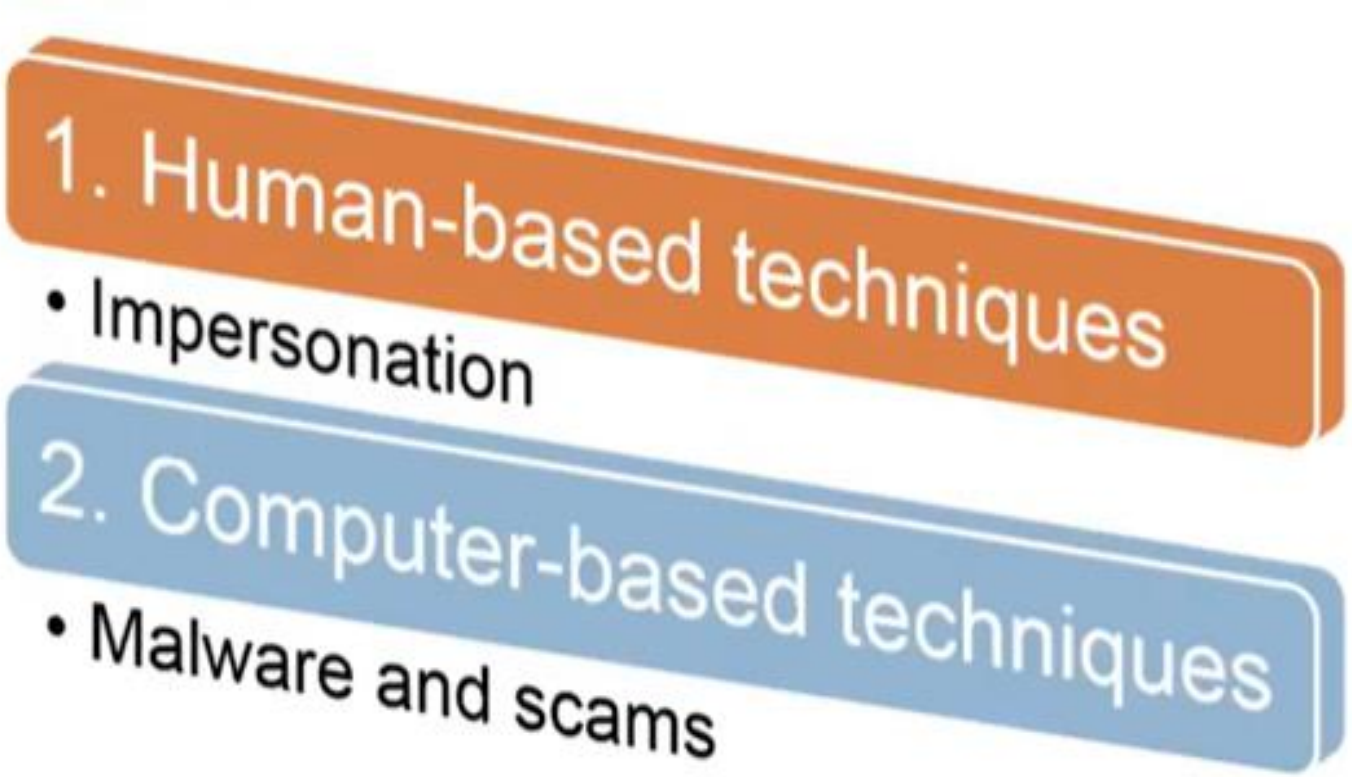
خريف 2023

https://t.me/+1iMQn29WU0o0Zjc8

Social Engineering Attacks Detection Methods



Social Engineering Hacking Techniques



Human Technique Based

Impersonation

- Help Desk
- Third-party Authorization
- Tech Support
- Roaming the Halls
- Repairman
- Trusted Authority Figure
- Junk Mail/SMS

Computer-Based Techniques

Malware and scams

- Pop-up windows
- Instant Messaging
- Email Attachments
- Email Scams

Pop-up windows

- Window prompts user for login credentials.
- Imitates the secure network login.
- Users can check for visual indicators to verify security.

Instance Messaging

- Hacker uses Facebook messenger, whatsApp, or Telegram to imitate technical support desk.
- Redirects users to malicious sites.

Email Attachment

- Hacker tricks user into downloading malicious software.
- Programs can be hidden in downloads that appear legitimate.
- Examples:
  - Executable macros embedded in PDF files.
  - Cheated extension:

    "NormalFile.doc" vs "NormalFile.doc.exe"
- Often the final extension is hidden by the email client.

Email Scam

- More prevalent over time.
- Begins by requesting basic information.
- Leads to financial scams.

Email Scam …


From Goolge <no-reply@dontreply-OXhDcCqQWt.com>
Subject المتابعه بعد حادثه الأمان الأخيره التي تعرّضت لها
To [redacted]@gmail.com>
Goolge
المتابعه بعد حادثه الأمان الأخيره التي تعرّضت لها
المتابعة بعد حادثة الأمان الأخيرة التي تعرّضت لها، بعد إكمال خطوات مراجعة حسابك تبين
وجود دخول غريب الى حسابك لذلك ننصح بتغيير كلمة مرورك.
تفاصيل الدخول
مصر، الجيزة (Windows - 196.197.41.213)
تامين حسابي

5 Ways To Protect Yourself Online

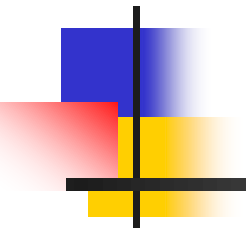
1 - Use two factors authentication

2 - Don’t use the same password everywhere

3 - Update the software on your computer

4- Be careful with how much information you post online

5- Be careful when sharing personal information.



Secure Design Principles

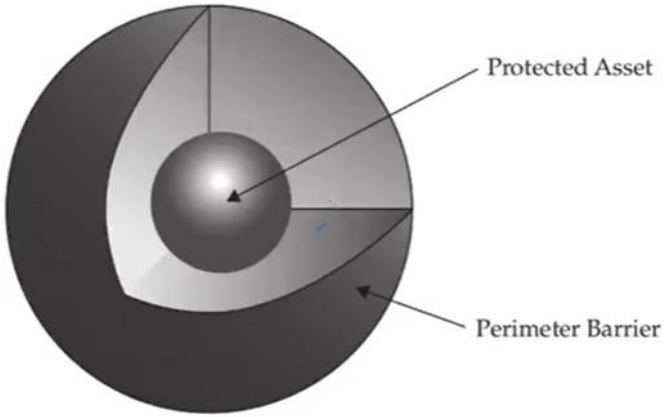
Defense Models

- Every network security implementation is based on some kind of model, whether clearly stated as such or assumed.
  - For example, organizations that use firewalls as their primary means of defense rely on a perimeter security model, while organizations that rely on several different security mechanisms are practicing a layered defense model.
- Every security design includes certain assumptions about what is trusted and what is not trusted, and who can go where.
- Understanding of which defense model is being used, can make a security infrastructure more effective and applicable to the environment it is meant to protect.

Defense Models..

- There are two approaches you can take to preserve the confidentiality, integrity, availability, and authenticity of electronic and physical assets such as the data on your network:
  1. Build a defensive perimeter around those assets and trust everyone who has access inside.
  2. Use many different types and levels of security controls in a layered defense-in-depth approach.

Lollipop Model



- The most common form of defense, known as perimeter security, involves building a virtual (or physical) wall around objects of value.
- Consider the example of a house it has walls, doors, and windows to protect what's inside (a perimeter).
  - Attacker can find a way in either by breaking through the perimeter, or exploiting some weakness in it, or convincing someone inside to let them in.
- By comparison, in network security, a firewall is like the house it is a perimeter that can't keep out all attackers.
- Yet the firewall is the most common choice for controlling outside access to the internal network, creating a virtual perimeter around the internal network (which is usually left wide open).

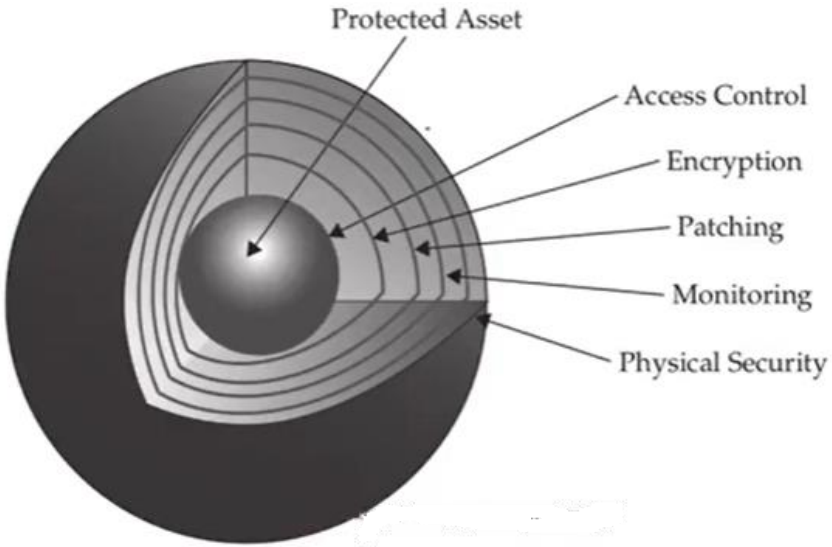
Lollipop Model..

- This often creates a false sense of security, because attackers can break through, exploit vulnerabilities, or compromise the network from the inside.
- One of the limitations of perimeter security is that once an attacker breaches the perimeter defense, the valuables inside are completely exposed.
- Another limitation of the lollipop model is that it does not provide different levels of security.
  - In a house, for example, there may be jewels, private equipment, and cash. These are all provided the same level of protection by the outside walls, but they often require different levels of protection.
- On a computer network, a firewall is likewise limited in its abilities, and it shouldn't be expected to be the only line of defense against intrusion.

Onion Model

- What happens when an attacker gets past the firewall? What happens when a trusted insider, like an employee or a contractor, abuses their privileges?
  - **The onion model addresses these risks.**
- A firewall alone provides only one layer of protection against threats originating from the Internet, and it does not address internal security needs.
- With only one layer of protection, which is common on networks connected to the Internet, all a determined individual has to do is successfully attack that one system to gain full access to everything on the network.

Onion Model..



- A layered security architecture provides multiple levels of protection against internal and external threats.
- Onion model is a better approach of security.
- It is a layered strategy, often referred to as defense in depth.
- This model addresses the probability of a perimeter security breach/risk occurring. It includes the strong wall of the lollipop but goes beyond the idea of a simple barrier.
- A layered security architecture, like an onion, must be peeled away by the attacker, layer by layer, with plenty of crying.

Thank you