# Overview

Domain 1: General Security Concepts

- M1: Introduction to Information Security
- M2: Cryptography
  - Encryption, Symmetric/Asymmetric Cryptography, Key Management

Domain 2: Security Threats, Vulnerabilities, and Mitigations

- **M3: Threat, Attacks, Vulnerability, and Mitigations**
  - **Types of Threats, Attacks, and Vulnerabilities, Mitigation Techniques**

Domain 3: Security Architecture

- M4: Cloud Computing:
  - Could computing, Virtualization, and Cloud Security Controls
- M5: Network Security
  - Secure Network Design, Network Security Techniques

# M3. Threats, Vulnerabilities & Mitigations

- Understanding Assets-Threats-Attacks
- Types of Risk
- Types of Threats
- Attacks and Attacker Types
- Types of Attacks
  - Malware, password/cryptanalytic attacks, network attacks, application, social engineering attacks
- Phishing Attacks

# Assets –Threats - Attacks

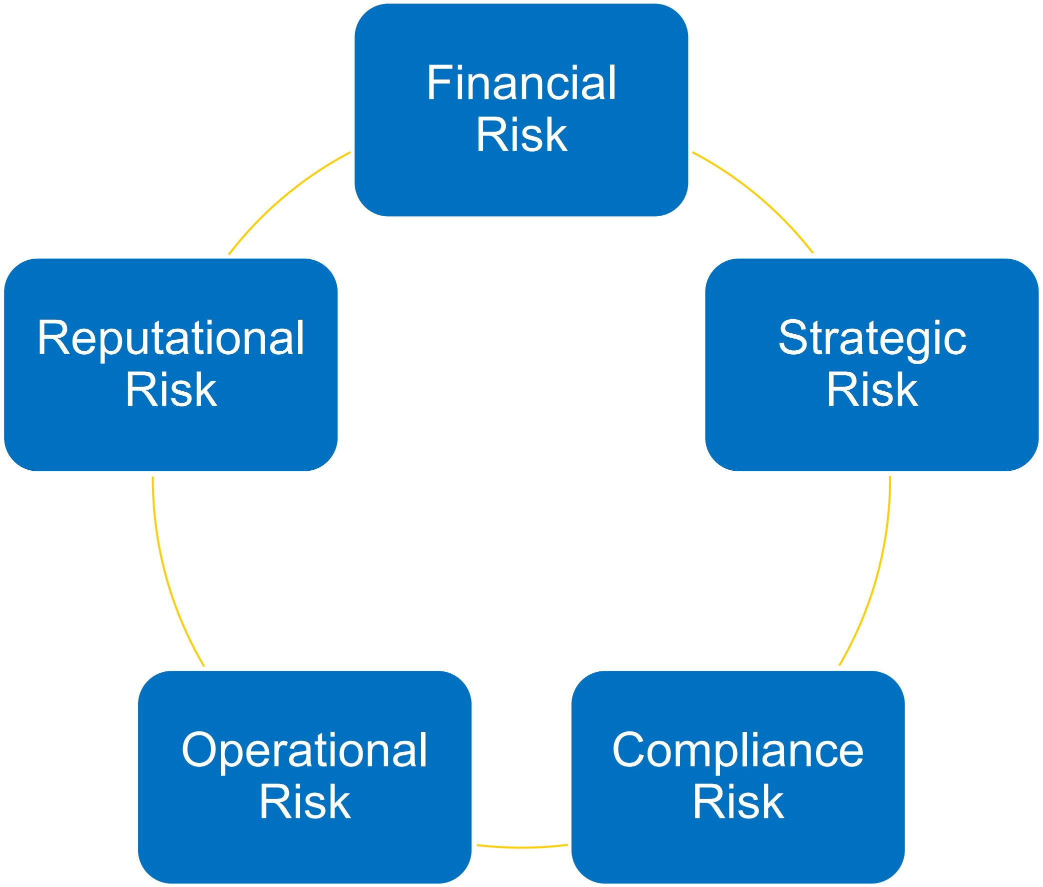
- The Art of War (Sun Tzu, ~ 500 BC)
  - A military treatise emphasizes the importance of knowing yourself as well as the threats you face

- To protect an organization, you must

  1) know yourself → ?

  2) know your enemy → ?

# Types of Risk



Financial Risk

Strategic Risk

Compliance Risk

Operational Risk

Reputational Risk

# Asset –Threat – Attack (Cont.)

- **Asset**:  the organizational resource (all elements of an organization’s system - People, Procedures, Data and information, Software, Hardware, Networking) that is  being protected.
- **Threats**: objects, persons, or other entities that represent a constant danger to an asset

# Types of Threats

| Category of Threat | Attack Examples |
|---|---|
| Compromises to intellectual property | Piracy, copyright infringement |
| Deviations in equality of service | Internet service provider (ISP), power, or WAN service problems |
| Espionage or trespass | Unauthorized access and/or data collection |
| Forces of nature | Fire, floods, earthquakes. lightning |
| Human error or failure | Accidents, employee mistakes |
| Information extortion | Blackmail, information disclosure |
| Sabotage or vandalism | Destruction of systems or information |
| Software attacks | Viruses, worms, macros, denial of service |
| Technical hardware failures or errors | Equipment failure |
| Technical software failures or errors | Bugs, code problems, unknown loopholes |
| Technological obsolescence | Antiquated or outdated technologies |
| Theft | Illegal confiscation of equipment or information |

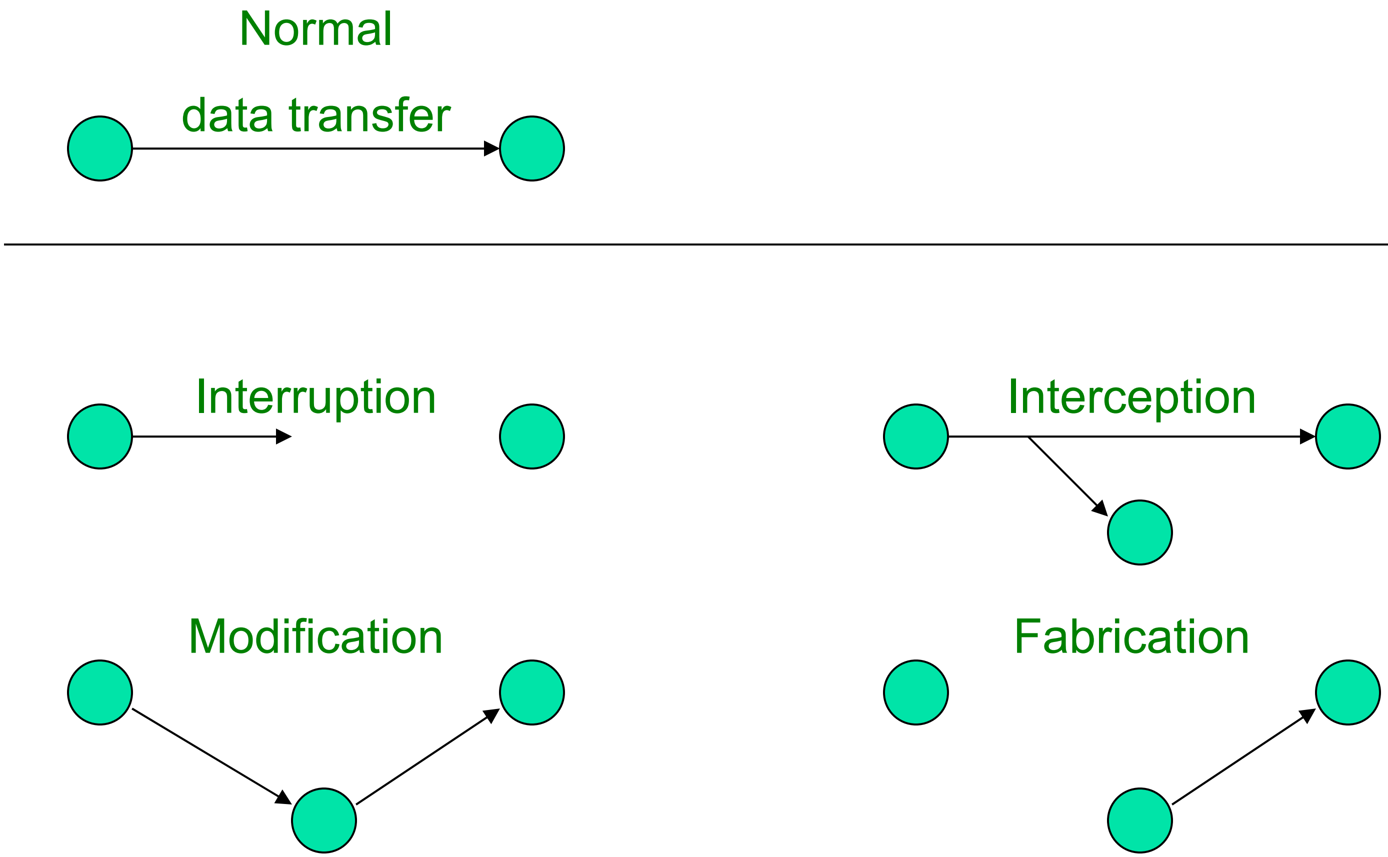
# Attacks

- **Attacks:** intentional or unintentional attempts to cause damage to or compromise the information and/or the systems that support it.
    - Passive attack versus active attack
- **Acts or actions** that exploit vulnerability (i.e., an identified weakness) in controlled system
- Accomplished by <u>threat agent (e.g. a zombie computer)</u> which damages or steals organization’s information

# Types of Attackers/Hackers

- White hats (operate with permission and good intent)
- Black hats (operate illegally with malicious intent)
- Grey hats (without permission but with good intent)
- Script kiddies (unskilled attackers)
- Hacktivists (political and social agendas)
- Crackers (criminal syndicates for financial gains)
- Competitors (for corporate espionage)
- Nation-state actors (advanced persistent threat groups)

# Types of hacking incidents



Normal

data transfer

Interruption

Interception

Modification

Fabrication

# Types of Attacks

- Malicious software attacks
- Password/cryptanalytic attacks
- Network attacks
- Application attacks
- Social engineering attacks, etc.

# Software Attacks

- Malicious software (malware) designed to damage, destroy, or deny service to target systems
- Types: viruses, worms, Trojan horses, logic bombs, back doors, polymorphic threats, denial-of-services attacks, etc.

**Two components of Malware: propagation mechanism and payload**

# Types of Software Attacks

- Virus consist of code segments that attach to existing program and take control of access to the targeted computer (e.g., Melissa).

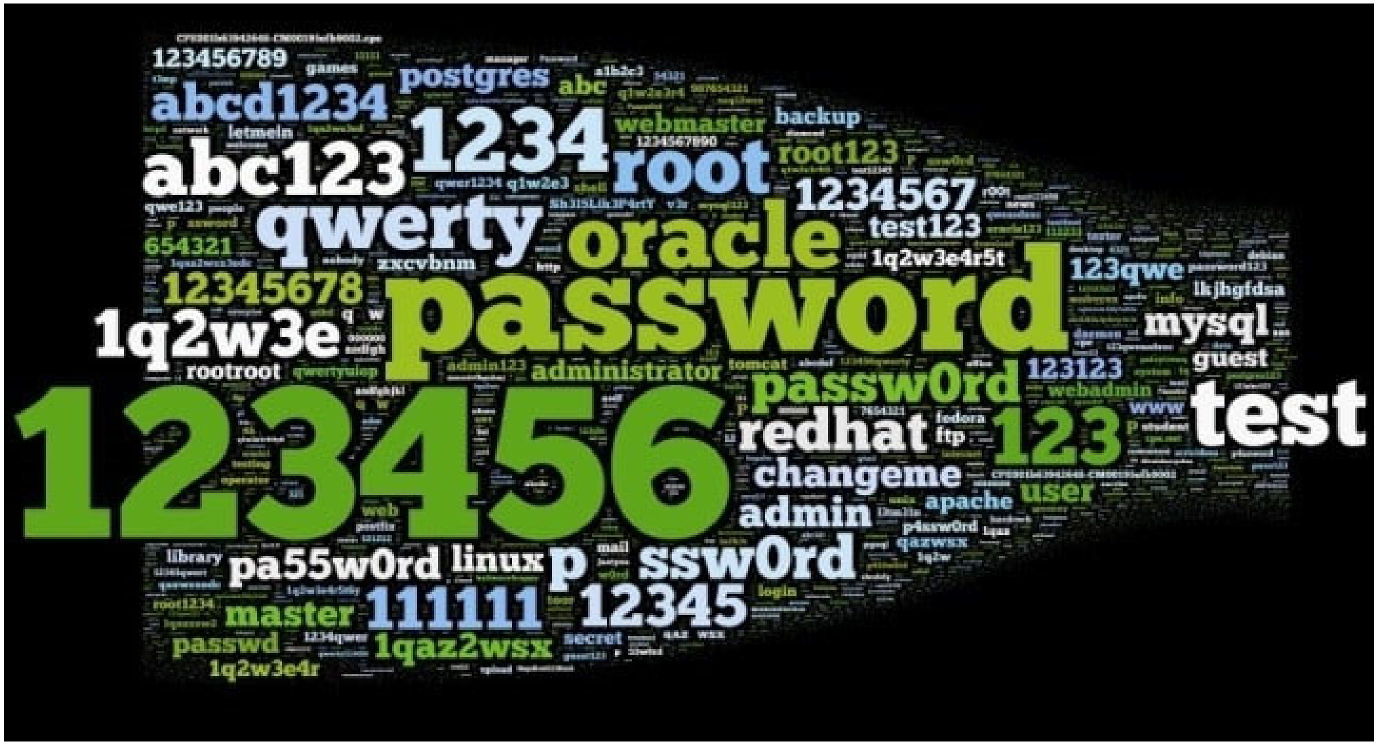
- Worms replicate themselves until they completely fill available resources such as memory and hard drive space (e.g., MyDoom).

- Trojan horses hide their nature and reveal their designed behaviour only when activated (e.g., RAT).

# Password Attacks

- Password crack: attempting to reverse calculate a password (e.g., cracking time 8 alphabet pw < 7 seconds)
- Brute force: trying every possible combination of options of a password
- Dictionary: selects specific accounts to attack and uses commonly used passwords (i.e., the dictionary) to guide guesses
- Rainbow table attack using precomputed has values
- 10.3 password rule: as a mitigation a recommendation for password structure

# Top 10 Worst Passwords That You Should Never Use

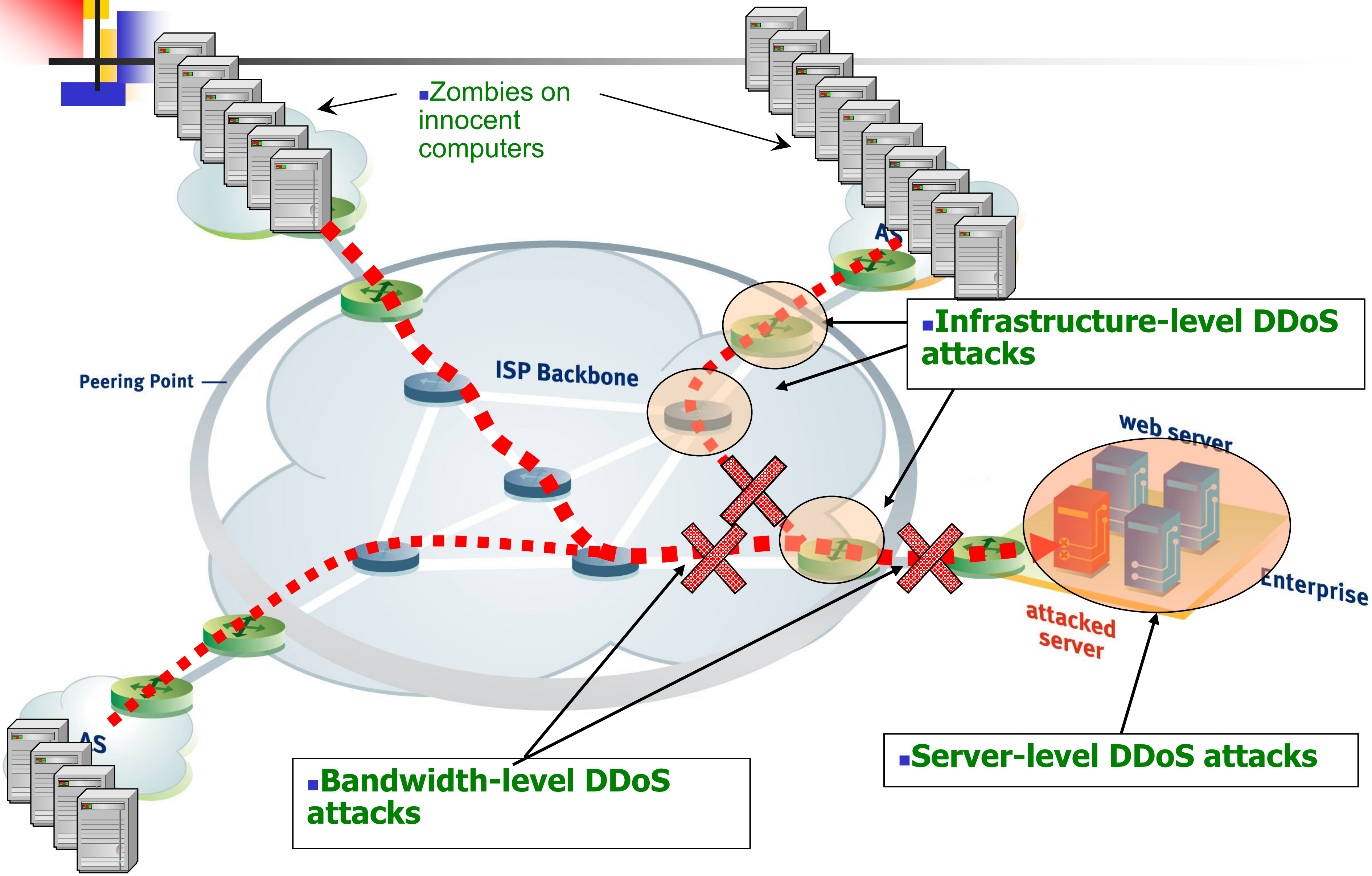


(source: GreenGeeks.com)

# Network Attacks

- Denial-of-service (DoS): attacker sends large number of connection or information requests to a target
  - Target system cannot handle successfully along with other, legitimate service requests
  - May result in system crash or inability to perform ordinary functions
- Distributed denial-of-service (DDoS): coordinated stream of requests is launched against target from many locations simultaneously

# Three levels of DDoS Attack



- Zombies on innocent computers

- Infrastructure-level DDoS attacks

- Bandwidth-level DDoS attacks

- Server-level DDoS attacks

# Application Attacks 1/2

- SQL injection: using inserted malicious SQL code into a query, attackers can manipulate the database in unintended ways.

- Cross-site scripting (XSS): using injected malicious scripts into web pages, attackers steal data or perform a malicious actions

- Privilege escalation: attackers gain unauthorized access to higher levels of privileges or restricted resources

# Application Attacks 2/2

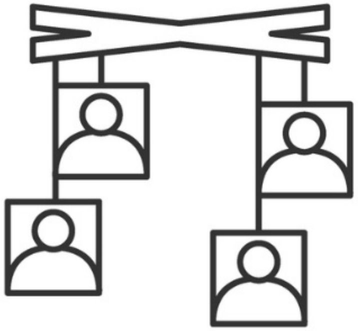
- Mail bombing: also a DoS; when certain conditions met, attacker routes large quantities of e-mail to target

- Spoofing: technique used to gain unauthorized access; intruder assumes a trusted IP address

- Man-in-the-middle: attacker monitors network packets, modifies them, and inserts them back into network. (a.k.a. TCP hijacking attack)

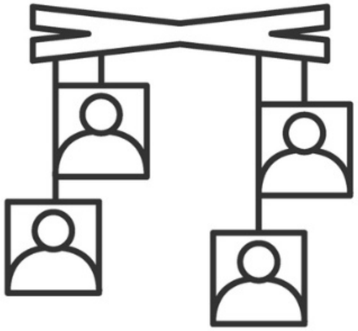
# Social Engineering Attacks

- Social engineering: manipulating social interactions to gain access or privileged information
  - May be a team working together
  - Could be done face-to-face or online
    - “Customers” calling
    - “Suppliers” calling
    - Third party repair service (cable, elevator, fire inspection)

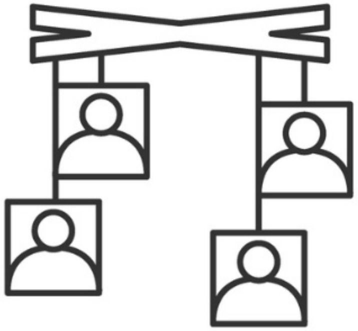


# Social Engineering Principles 1/2

- Authority (impersonation)
  - The attacker is in charge
  - “Don’t you know who I am?!”
  - “This is the police!”
- Intimidation
  - Repercussions if you do not comply
  - If you don’t help, bad things happen.
- Consensus/Social proof
  - Make it seem routine
  - “This isn’t the first time we’ve done this.”
  - “Jose in IT did this for me last time.”



# Social Engineering Principles 2/2



- Scarcity
  - Limited time to decide
  - Limited opportunity
- Urgency
  - You have to act now
  - No time to think
- Familiarity/Liking
  - Someone you know, we have common friends
  - “John put me in touch with you”
- Trust
  - Someone who is safe
    - “I’m from IT. I’m being helpful. Let me help you.”

# Types of Phishing Attack 1/2

- Phishing: electronic social engineering; an attempt to gain personal/financial information from individual, usually by posing as legitimate entity
  - Vishing (Voice phishing)
  - Smishing (SMS/Texting phishing)
  - Spear phishing – phishing a specific target directly
  - Whaling – directed attack toward high profile targets like CEO

# Types of Phishing Attacks 2/2

- Pharming: redirection of legitimate Web traffic (e.g., browser requests) to illegitimate malicious site for the purpose of obtaining private information
- Spam: unsolicited commercial e-mail to large group of people (more a nuisance than an attack);
    - SPIM (Spam over instant messenger apps such as Facebook, Instagram)
    - Invoice scam – fake invoices sent as a phishing attack

# Summary

- Understanding Assets-Threats-Attacks
- Types of Risk and Threats
- Attacks and Attacker Types
- Types of Attacks
  - Malware, password/cryptanalytic attacks, network attacks, application, social engineering attacks
- Phishing Attacks