Social Engineering

Social Engineering

- Social engineering bypasses technology protections by using various tactics and methods:
  - To encourage another person to perform a specific action
  - Or give up a piece of crucial information

Types of Social Engineering Attacks

- **Conning and Flattery**
  - Social engineering attacks often start as simple con jobs.
- **Impersonation**
  - Impersonation is a specific social engineering tactic where an attacker masquerades as someone else, such as a repair technician.
- **Phishing**
  - Phishing is the practice of sending unwanted emails to users with the purpose of tricking them into revealing personal information (such as bank account information) or clicking on a link.
- **Piggybacking or Tailgating**
  - Piggybacking or tailgating occurs when one user follows closely behind another use without using valid credentials. It can often be prevented with a mantrap.
- **Dumpster Diving**
  - Dumpster diving is the practice of searching through trash to gain information from discarded documents.

Mitigating Social Engineering

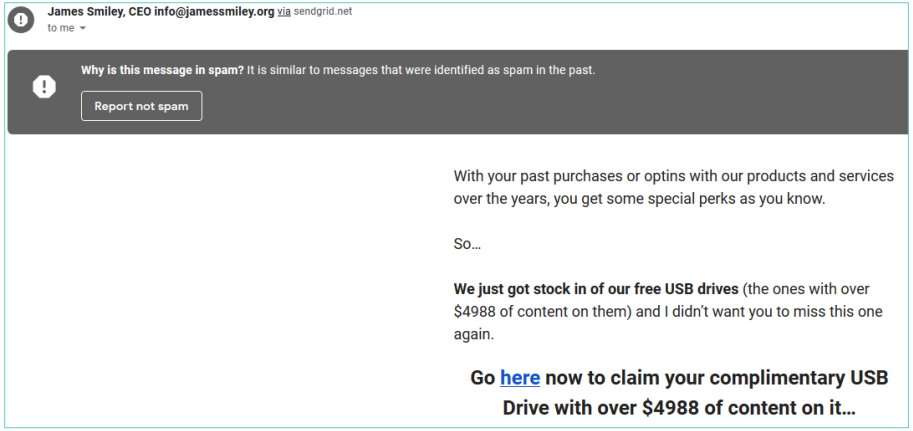
- User Training & Awareness
- Be Suspicious & Cautious
- Verify Someone's Identify
- Don't Rely on Email

Email Spam, Spoofing, Phishing, and Pharming

INSTRUCTOR
ALTON

Spam Email

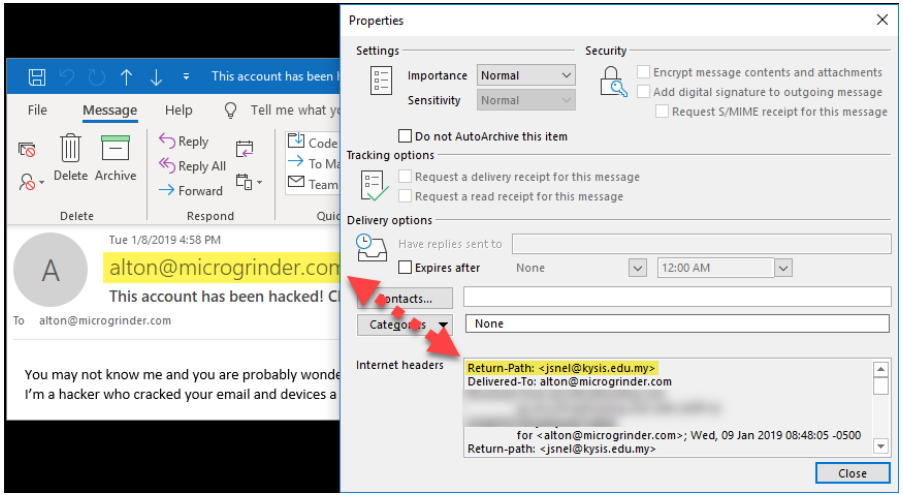
- **Spam email** is unsolicited emails, commonly advertising emails, but sometimes phishing and scamming attempts.
- Such emails can clutter our inbox, get in the way of emails that matter, and potentially carry malware.



INSTRUCTOR
ALTON

Spoofed Emails

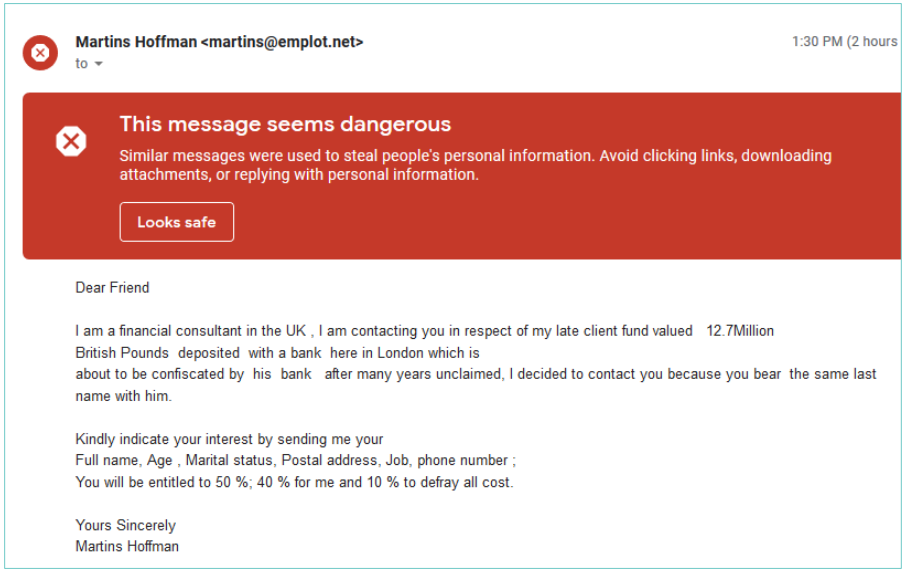
- **Email spoofing** is the forgery of an **email header** so that the email seems to have originated from someone or somewhere other than the actual source.
- It's used in **phishing**, **pharming**, and **spam campaigns** because people are more likely to open an **email** when they think a legitimate source has sent it.



INSTRUCTOR
ALTON

Email Phishing

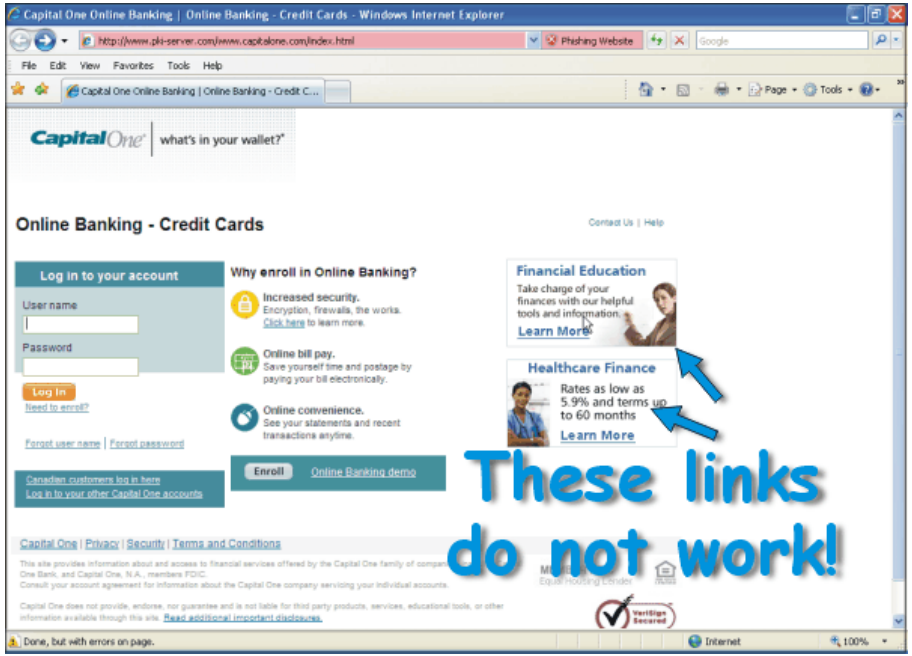
- **Phishing** is the practice of sending unwanted emails to users to trick them into revealing personal information (such as bank account information) or clicking on a link.
- It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email.
- Their goal is to get you to share valuable personal information – such as account numbers, Social Security numbers, or your login IDs and passwords.
- They then use your information to steal your money or your identity, or both.



INSTRUCTOR
ALTON

Email Pharming

- **Pharming attacks** redirect users from legitimate websites to fraudulent fake websites.
- This can be done server-side via DNS spoofing and also client-side.
- With **email pharming**, a user will open up an email with malware, which then installs malicious code on the user's PC.
- In one form of pharming attack, code sent in an email modifies the local hosts file on a personal computer.
- This code then redirects URL clicks to a fraudulent website without your knowledge or consent.



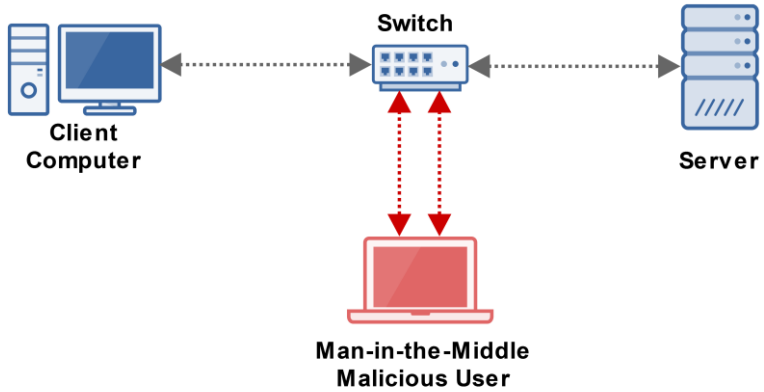
Protocol Spoofing

Protocol Spoofing

- Protocol spoofing is the misuse of a network protocol to initiate an attack on a host or network device.
- There are three common types of protocol spoofing:
  - ARP Spoofing (ARP Poisoning)
  - DNS Spoofing
  - IP Address Spoofing

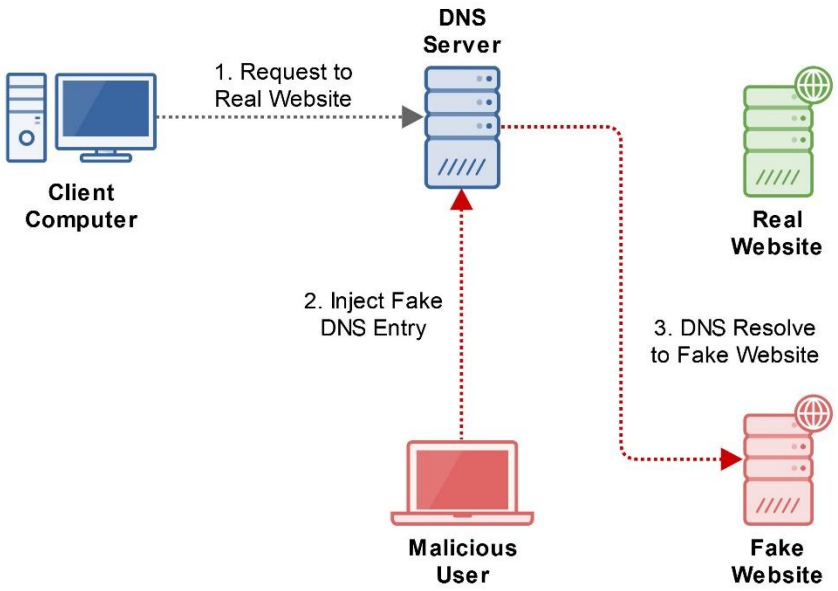
ARP Spoofing (ARP Poisoning)

- Address resolution protocol resolves IP addresses to MAC addresses.
- ARP poisoning modifies the network's ARP cache to take over a victim's MAC address.
- This allows the attacker to receive any data intended for the victim.



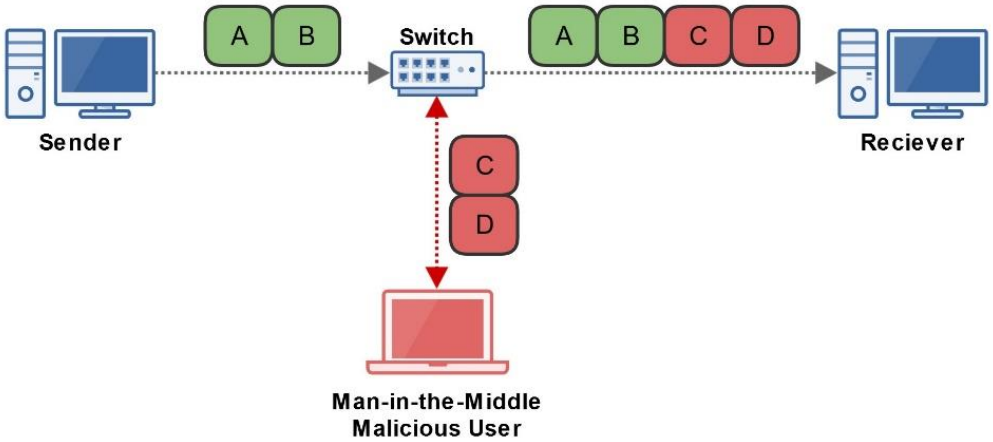
DNS Spoofing

- Domain name service (DNS) translates domain names into IP addresses.
- DNS spoofing is when an attacker alters the DNS records to redirect traffic to a fraudulent website, where further attacks can occur.



IP Address Spoofing

- IP address spoofing is an attack where a malicious user forges a packet's source IP address.
- By doing so, the malicious user can impersonate the sending computer.



Common Attack Methods

Common Attack Methods

- Common attack methods we haven't discussed yet:
  - Denial of Service (DoS) Distributed Denial of Service (DDoS) Attacks
  - Back Door Attack
  - Reply Attack
  - Weak Encryption Key
  - Software Vulnerability Attack
  - Remote Code Execution Attack
  - SQL Injection Attack
  - Cross-Site Scripting Attack (XSS Attack)
- Common attacks we've already covered in the course:
  - ARP Spoofing
  - DNS Spoofing
  - IP Address Spoofing
  - Man in the Middle Attack
  - Social Engineering
  - Buffer Overflow Attack
  - Malware

DoS and DDoS Attacks

- **Denial of Service (DoS) Attack**
  - A DoS attack is when a malicious user attempts to make a server or other network device unavailable by flooding it with requests.
  - This overwhelms the server's resources so that it can't respond to service requests.
- **Distributed Denial of Service (DDoS) Attack**
  - A DDoS attack is a DoS attack that is launched from a large number of malicious machines.
- **Common types of DoS and DDoS attacks are:**
  - Buffer Overflows: Sending the Server more data than expected.
  - SYN Attack: Exploits the TCP three-way handshake.
  - Ping of Death: Exploits the ICMP "ping" protocol.

Back Door & Replay Attacks

- **Back Door Attack**
  - When someone creates an alternative way into a system that bypasses its security controls.
- **Replay Attack**
  - Similar to a man in the middle attack, but with a replay attack, the attacker will capture a message sent from a network device to the server.
  - Later, the attack will send the original, unmodified message to the server, hoping the server responds thinking the attacker is a valid device.
  - If it does, the attacker has successfully created a “trusted” relationship with the server.

Weak Encryption Key & Software Vulnerability Attacks

- **Weak Encryption Key**
  - Occurs when enough network traffic is captured to allow the key to be broken. An example is WEP encryption.
- **Software Vulnerability Attack**
  - The exploitation of known software/application vulnerabilities for malicious purposes.

Web-Based Attacks

- **Remote Code Execution Attack**
  - Commonly used against web applications.
  - When web applications are improperly coded, attackers can run system-level code for malicious purposes.
- **SQL Injection Attack**
  - Occurs when a malicious user manipulates web-based input forms to pass unauthorized SQL to the SQL server database.
  - This can allow the attacker to retrieve information, delete information, and even drop tables from the database.
- **Cross-Site Scripting Attack (XSS Attack)**
  - Occurs when a malicious user embeds malicious client-side HTML or JavaScript code into a website's code. The code then executes when a user visits the site.
  - The attacker can then obtain sensitive page content, session cookies, and other info.