Task 2: Analyze a Phishing Email Sample.

**Phishing:-**

Phishing is a type of cyberattack where attackers trick individuals into providing sensitive information such as usernames, passwords, credit card numbers, or other confidential data. It is usually done by pretending to be a trustworthy entity like a bank, online service, or company.

**Working of Phishing:-**

**>**Bait(Doing fake communication)

-Attacker send the fake email, SMS, or message that look like from trusted person and pretend like it ‘s some emergence.

**>**Hook(Malicious Link or Attachment)

-The message include fake website(look real) and attached file with malware

**>**catch(Stealing Information)

-while entering into the site or downloading the document ,lead to stealing the credential and accessing into the system.

**Who uses this:-** It used by cybercriminal ,fraud,attacker and scammer.

**Type of Phishing:-**

* Email Phishing(Through mail)
* Spear Phishing(Through message)
* Smishing(SMS)
* Vishing(Fake voice )
* Clone Phishing(Copying the real mail)

**Email Phishing:-**

Email Phishing is a cyberattack in which an attacker sends fraudulent emails that appear to come from a legitimate source (like a bank, a trusted company, or even a friend). The goal is to trick the recipient into clicking on malicious links, downloading harmful attachments, or providing sensitive information such as:

* Login credentials
* Credit card numbers
* Bank account details
* Personal identification info

**Working of email Phishing:-**

* Fake email send

-(attacker send the fake email pretending like trusted person or organization)

* Trick with urgency or fear

-(like changing the password and like payment failed )

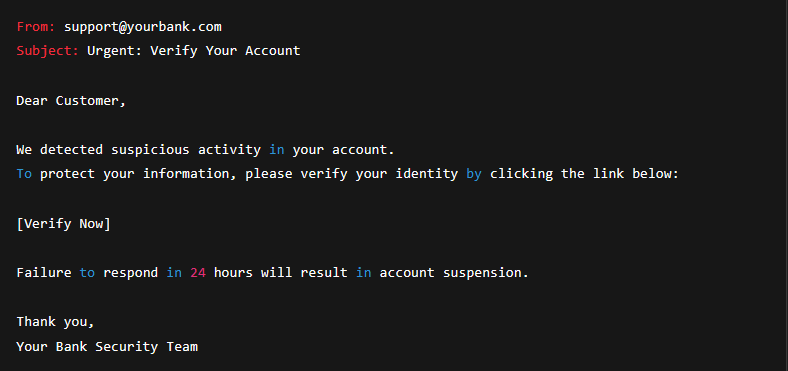
* Malicious link or attachment

-(that link redirect to fake website or document contain malware )

* User fall for the trick

-(attacker get the user credential or take the user system)

**Sample for Phishing email:-**

****

**Identify and avoid the phishing email.**

> check for the sender email carefully

> look for the spelling and grammar

> never download the unwanted document

> don’t enter the personal information in the scam website

> use scam filter and two way authentication for verify

**Email Spoofing:-**

Email Spoofing is a technique used by attackers to send emails that appear to come from a trusted or known sender, but in reality, the email is fake and sent from a different source.

**How happens:-**

The attacker forges the “from address” in the email header to make it look like it’s from

**-exmaple** :-the attacker make the email look like from individual company (like paypal) and that attacker make email like ([support@paypal.com](mailto:support@paypal.com))

But the actual sender will be someone else – it know as cybercrime.

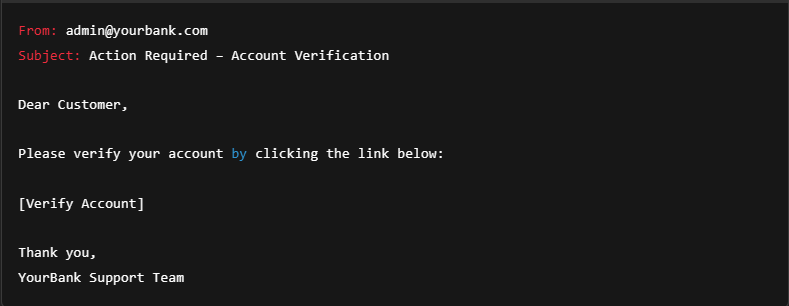
**USED in:-**

**>**Phishing attack

**>**Spreading malware

**>**Business email compromise

**Example of email spoofing:-**

****

**Protect Against Email Spoofing:**

1. Check full email headers – reveal the actual sender.
2. Look for inconsistencies in domain names, links, and tone.
3. Verify with the sender if the message seems suspicious.
4. Use email authentication methods:
   * SPF (Sender Policy Framework)
   * DKIM (DomainKeys Identified Mail)
   * DMARC (Domain-based Message Authentication, Reporting & Conformance)
5. Educate users to recognize spoofed emails.

**Header analysis:-**

Header analysis involves examining the email header (the metadata of an email) to trace its true origin, route, and authenticity.

**What You Can Find in an Email Header:**

* **From:** The sender’s claimed email address (can be spoofed).
* **Return-Path:** Where replies are actually sent — useful for spotting spoofing.
* **Received:** Shows the servers the email passed through (read from bottom to top).
* **Message-ID:** Unique ID, sometimes mismatched in spam or spoofing.
* **Authentication Results:** SPF, DKIM, DMARC results.

**Tools used :**

>Google admin Toolbox

>MXToolbox email Header analyzer

**Why It’s Important:**

* Detect email spoofing
* Identify phishing attempts
* Track malicious senders

**Social Engineering:**

Social engineering is the psychological manipulation of people to trick them into giving up confidential information, clicking malicious links, or performing unsafe actions.

**Common Tactics:**

* Impersonation: Posing as a trusted person or authority.
* Urgency: “Your account will be locked in 24 hours!”
* Fear or Reward: "You’ve won a prize!" or "Suspicious login detected."
* Pretexting: Creating a fake scenario to get info (e.g., “I’m from tech support.”)

**Why It’s Important:**

* Most cyberattacks start with social engineering.
* No matter how strong your tech is, humans are the weakest link if not trained.

**Threat Detection:-**

This help to identify the malicious activity or pattern that would lead to the cyber security threat

**Methods:**

* **Signature-based detection:** Looks for known patterns (e.g., antivirus).
* **Anomaly-based detection:** Flags behavior that’s out of the ordinary (e.g., logging in from two countries in 5 minutes).
* **Behavioral analysis:** Observes how users/applications behave over time.
* **SIEM (Security Information and Event Management):** Tools that collect and analyze security logs across systems.

**Common Tools:**

* **Wireshark** – for network packet inspection
* **Snort** – intrusion detection
* **Splunk** – log and event analysis
* **OSSEC**, **AlienVault**, **CrowdStrike**, **Microsoft Defender**

**Why It’s Important:**

* Helps detect threats early.
* Enables incident response before damage is done.
* Reduces false positives with better context and analysis.