What Is Phishing Attack

- A phishing attack is a type of cyberattack where a malicious actor attempts to deceive an individual into revealing sensitive information, such as usernames, passwords, credit card numbers, or other personal details.
- The attacker typically masquerades as a trustworthy entity, such as a legitimate business, government agency, or even a colleague, to gain the victim's trust and trick them into disclosing this information.

❖ Google & Facebook Phishing Attack

- One of the biggest phishing scams in history targeted Google and Facebook, resulting in the theft of over $100 million.
- The attack was a Business Email Compromise (BEC) scam, where cybercriminals tricked employees into wiring money to fraudulent accounts.

➢ Person behind the attack

- The attack was carried out by Evaldas Rimasauskas, a Lithuanian cybercriminal.
- He posed as **Quanta Computer**, a real Taiwanese company that supplies hardware to major tech firms.

- **Timeline of the attack**

1. **2013 – 2015 : Fraudulent Transactions**
    - Rimasauskas conducted the attack over a two-year period, using phishing tactics and BEC techniques to target both Google and Facebook.
    - Throughout this time, the hacker was able to defraud the companies into sending wire transfers, often under the guise of routine vendor payments.

2. **2017 : Discovery And Arrest**
    - In March 2017, the U.S. Department of Justice (DOJ) announced that Evaldas Rimasauskas had been charged with wire fraud, money laundering, and identity theft.
    - Rimasauskas was accused of creating fake entities that were designed to impersonate Quanta Computer and use fraudulent invoices to steal large sums of money from both Google and Facebook.
    - He allegedly laundered the funds through various shell companies and bank accounts in countries like Latvia, Cyprus, and other locations.

❖ **Evaldas Rimasauskas in district court in Lithuania in 2017**

❖ How This Phishing Scam Worked

➢ Phishing and BEC Tactics:

1. **Business Email Compromise (BEC):**
   - Rimasauskas spoofed the identity of a legitimate hardware vendor that both Google and Facebook regularly did business with, a company called Quanta Computer (a real manufacturer of computer hardware components).
   - By gaining access to corporate email systems and creating emails that appeared to come from Quanta's senior officials, Rimasauskas made it seem like the companies owed large sums of money for legitimate invoices.
2. **Fake Invoices:**
   - Rimasauskas submitted fake invoices to both Google and Facebook, instructing them to wire payments to accounts he controlled. The emails were designed to look official and legitimate, containing falsified bank account details that appeared to be from Quanta, a trusted vendor.
   - These invoices were often well-crafted, mimicking the style and format of real invoices from the actual vendor, making them appear authentic.
3. **Corporate Response:**
   - Employees at Google and Facebook, likely due to the professional-looking nature of the emails and the established relationship with Quanta, processed the payments without initially suspecting fraud.
   - Over the span of two years, Rimasauskas successfully convinced both companies to wire large sums of money.

- **Amount Stolen:**
  - Facebook lost about $99 million over a series of fraudulent transactions.
  - Google lost approximately $23 million (though it was later reported that the total for Google might be higher than originally disclosed).

❖ Lessons and impact

- This phishing attack was a stark reminder of the vulnerabilities in corporate systems, especially when dealing with wire transfers and international payments. Even large, highly secure organizations like Google and Facebook were susceptible to sophisticated phishing attacks.
- The attack also highlighted the increasing importance of vendor verification and internal checks before transferring significant sums of money, especially when dealing with international invoices.
- **Security Measures**: In the aftermath, both companies likely invested more in anti-phishing measures, employee training, and systems to double-check payment requests and invoices before processing them.

❖ Overall Impact On Both Organizations

➢ Impact on Facebook :

1. **Financial loss :**
   - Facebook was defrauded of $99 million.
   - While Facebook eventually recovered a portion of the stolen funds, the attack resulted in significant direct financial loss.
   - This kind of breach also likely caused additional expenses related to legal fees, investigations, and compliance efforts to ensure the security of financial transactions in the future.

2. **Reputation And Trust :**
   - Despite being one of the most powerful tech companies globally, Facebook's reputation was impacted by the breach.
   - The news of such a large-scale fraud involving sophisticated phishing tactics likely eroded some trust among its users, investors, and even business partners.
   - Being a company that handles massive amounts of personal and financial data, Facebook's involvement in such an attack raised questions about the security measures in place to protect user and company financial information.

3. **Operational And Legal Implications :**
   - Facebook needed to review and tighten its internal processes related to vendor management, payments, and cybersecurity to prevent such breaches in the future.

- This would have likely led to a temporary disruption in operations, as the company worked to reassess how it processed financial transactions.

4. **Increased Investment In Security :**
   - The attack likely prompted Facebook to increase its investment in cybersecurity. This includes improving email security, employee training to recognize phishing attempts, and strengthening their overall security infrastructure.
   - These measures may have been costly but were necessary to avoid future breaches.

- **Impact On Google**

1. **Financial loss :**
   - Google lost approximately $23 million. Like Facebook, the financial impact was significant, but Google was able to recover a substantial portion of the stolen funds.
   - Google likely spent additional resources on investigating the attack, hiring cybersecurity experts, and implementing new systems to detect and prevent future fraud.

2. **Reputation And Trust :**
   - Google is often seen as a leader in technology and cybersecurity, so a successful attack on such a large scale cast doubt on the company's ability to protect against highly sophisticated threats.

3. **Operational Disruption :**
    - Google, like facebook, likely had to review its payment and vendor verification processes after the phishing attack.
    - This could have led to temporary disruptions as Google worked to improve internal processes to prevent fraudulent transactions from slipping through the cracks in the future.
    - The company would also have had to update its security policies and protocols across the organization to ensure employees were better educated about potential phishing attempts and business email compromise schemes.

4. **Strengthened Security Measures :**
    - Google was likely prompted to enhance its security infrastructure, including multi-factor authentication (MFA), anti-phishing training, and improved fraud detection systems.
    - As a company with vast resources, it would have leveraged its expertise to implement new security measures and ensure that similar attacks wouldn't occur again.

❖ **Broader Impact On The Tech Industry**

1. Increased awareness of phishing & BEC attacks
2. Growth in cybersecurity solutions

❖ Incident Response Plan Taken By Google And Facebook

➢ Measures taken

1. **Immediate actions :**
   - Once the phishing attack was discovered, both companies took steps to stop the ongoing wire transfers.
   - As the attacks occurred in 2014 and 2015, Google and Facebook quickly moved to notify authorities and internal stakeholders.

2. **Collaboration With Law Enforcement :**
   - Google and Facebook worked closely with law enforcement, particularly the FBI and other federal agencies, to track the movement of the stolen funds, trace the attacker, and eventually lead to the arrest of Evaldas Rimasauskas in 2017.

3. **Financial Recovery :**
   - While not all the stolen funds were recovered, both companies worked to reclaim portions of the stolen amounts.
   - This demonstrates that both organizations had some level of coordination with international financial institutions to attempt recovery.

❖ Forensic Analysis

1. **Investigation And Tracking :**
    - Google and Facebook initiated a forensic investigation to track the path of the funds and understand how the fraudulent invoices were processed by their finance teams.
    - This involved analysing email traffic, bank transfer records, and communication logs.

2. **Identifying The Attack Method :**
    - Both companies eventually realized that the attacker used social engineering tactics, specifically phishing emails impersonating vendors.
    - Understanding this helped them identify weaknesses in their internal controls.

3. **Involvement Of Experts :**
    - Given the scale of the attack, both companies likely brought in external forensic experts to aid in tracing the funds and analyzing the attack vector.
    - This would have included digital forensics experts who specialized in tracking online transactions and email forensics to uncover the fake invoices.

❖ Communication Strategies

1. **Internal communication :**
    - After discovering the phishing attack, both companies would have communicated the issue to internal teams, especially those involved in finance, cybersecurity, and executive management.
    - It's essential for organizations to act quickly and inform key stakeholders.

2. **Public Disclosure :**
    - Both Google and Facebook were relatively open about the attack after the investigation was completed, disclosing the incident publicly.
    - Facebook, for instance, reported in their 2017 SEC filings that they had been defrauded by a phishing attack, and they also communicated the lessons learned.

3. **Regulatory Reporting :**
    - As both companies are based in the U.S., they would have been required to inform regulatory bodies about the data breach.
    - This transparency is a key element of compliance, especially for publicly traded companies.

❖ Employee Training Program

1. **Post-incident awareness :**
   - After the attack, both Google and Facebook initiated company-wide security awareness programs to train employees on how to recognize phishing attacks, spot fraudulent invoices, and handle sensitive financial requests.

2. **Simulated Phishing Attack :**
   - Both companies introduced or enhanced simulated phishing exercises to regularly test employees and raise awareness about the risks associated with email-based fraud.

3. **Policy Overhaul :**
   - Following the attack, both companies implemented stronger verification procedures for financial transactions, such as multi-factor authentication (MFA) for processing payments and dual authorization for wire transfers.

❖ Recommendations To Enhance Cybersecurity Resilience

1. **Strengthen Email And Communication Authentication :**
   - **Implement Email Authentication Protocols:** Organizations should adopt email security protocols like DMARC (Domain-based Message Authentication, Reporting, and Conformance), SPF (Sender Policy Framework), and DKIM (DomainKeys Identified Mail). These standards help to verify the authenticity of emails and reduce the chances of spoofing.
   - **Mandatory Use of Secure Email Systems:** Encourage the use of encrypted email systems and end-to-end encryption to ensure that sensitive communications cannot be intercepted or manipulated.

2. **Multi-Factor Authentication**
   - **MFA for Critical Systems and Transactions:** Ensure multi-factor authentication (MFA) is implemented not just for user logins but for all sensitive actions, including financial transactions and access to critical data.
   - **Contextual MFA:** Use additional contextual factors like geolocation, device trustworthiness, or even biometric verification when processing wire transfers or high-value transactions.

3. **Vendor Management And Verification**
   - **Enhanced Vendor Validation:** When dealing with third-party vendors, always verify their legitimacy through multiple channels (e.g., phone calls, video conferencing) instead of relying solely on email communication.

- **Secure Vendor Onboarding:** Before onboarding any new vendor, verify the authenticity of their business and secure their communication channels. Avoid trusting email addresses or domains that resemble known contacts.

4. **Employee Training And Awareness**
   - **Regular Security Training:** Conduct annual cybersecurity training for all employees, with a focus on recognizing phishing attempts and understanding the risks of social engineering.
   - **Financial Transaction Awareness:** Train employees in finance and procurement departments to double-check payment instructions and to never process payments without multiple confirmations, including verbal verification of high-value payments.

5. **Enhanced Monitoring And Detection**
   - **Transaction Monitoring:** Implement systems that can flag abnormal financial transactions or unusual wire transfer patterns. Set up alerts for transactions involving high-dollar amounts or international transfers.
   - **Behavioural Analytics:** Use AI-based behavioural analytics tools to monitor employee activity and detect anomalies that could indicate malicious or fraudulent behaviour, such as logging in from unfamiliar devices or locations.

6. **Strong Internal Controls And Segregation Of Duties**
    - **Dual Authorization for Financial Transfers:** Implement a two-person approval system for wire transfers and high-value payments, particularly when payments are made to unfamiliar accounts.
    - **Separation of Duties:** Ensure that different employees are responsible for different stages of a transaction, such as request, approval, and processing, reducing the risk of an internal actor or single point of failure.

7. **Incident Response And Recovery Planning**
    - **Create and Test an Incident Response Plan:** Organizations should have a robust incident response plan (IRP) in place to detect, contain, and mitigate attacks. The plan should include detailed actions to take in case of a phishing or social engineering attack.
    - **Backup and Recovery Systems:** Ensure that financial systems and data are backed up regularly, and that recovery protocols are in place in case of a cyberattack, ensuring minimal disruption and data loss.

8. **Use Of Advanced Security Tools**
    - **Endpoint Security Solutions:** Deploy advanced endpoint protection software across all devices, ensuring malware, ransomware, and other threats are detected early. This includes using anti-phishing and anti-malware tools.
    - **Secure Network Architecture:** Ensure that the organization's internal networks are segmented to limit access to sensitive information. Employ intrusion

detection and prevention systems (IDPS) to monitor and block any unauthorized network activity.

9. **Third-Party Audits And Penetration Testing**
    - **Regular Audits and Vulnerability Scanning:** Conduct periodic security audits, both internal and external, to identify vulnerabilities in the organization's systems. Implement the findings to reduce attack surfaces.
    - **Penetration Testing:** Regularly engage in penetration testing and red team exercises to test your defenses, particularly around high-risk areas like vendor management, finance, and internal communications.

10. **Develop A Phishing-Specific Response Protocol**
    - **Phishing Reporting System:** Encourage employees to report suspicious emails to the IT/security team. Provide them with easy ways to forward suspicious messages to a designated security team.
    - **Use of AI to Detect Phishing:** Implement artificial intelligence-driven phishing detection solutions that can automatically flag and quarantine suspicious emails before they reach employees.