Assignment-3

Step-1:
Case Study Analysis:

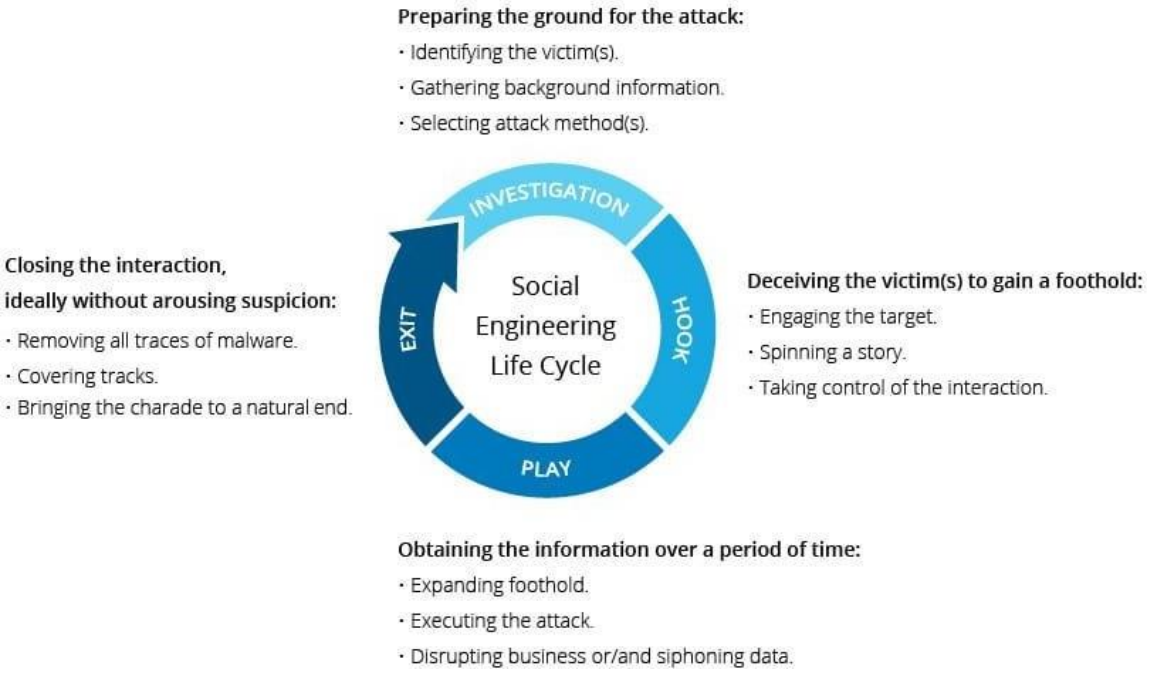
Social engineering attacks manipulate individuals into divulging confidential information or performing actions that compromise security. A notable case involved pretexting via the OmeTV video chat application, where attackers used psychological manipulation to execute a phishing attack1.

Identified Vulnerabilities:

Lack of employee awareness training can leave staff unable to recognize and respond to social engineering tactics.
Inadequate authentication measures, such as single-factor authentication, make unauthorized access easier.
Poor email security protocols can lead to successful phishing campaigns, where malicious emails bypass filters and reach the intended targets.
Consequences of the Attack: The repercussions of social engineering attacks are severe, including:

Reputational Damage: Loss of customer confidence and trust can be devastating and long-lasting.
Financial Losses: Companies have suffered millions in losses; for example, Ubiquity Networks lost $39 million due to a social engineering attack2.
Customer Trust: Breaches can lead to a loss of customer trust, impacting future business and partnerships.
Recommendations: To prevent such attacks, organizations should consider:

Implementing regular security awareness training to educate employees on recognizing and responding to social engineering tactics.
Adopting multi-factor authentication to add an extra layer of security beyond just passwords.
Improving email filtering systems to better detect and block phishing attempts.



Step-2 Role-play Exercise:

After the role-play, it's essential to identify the tactics used by the attacker. Common tactics include:

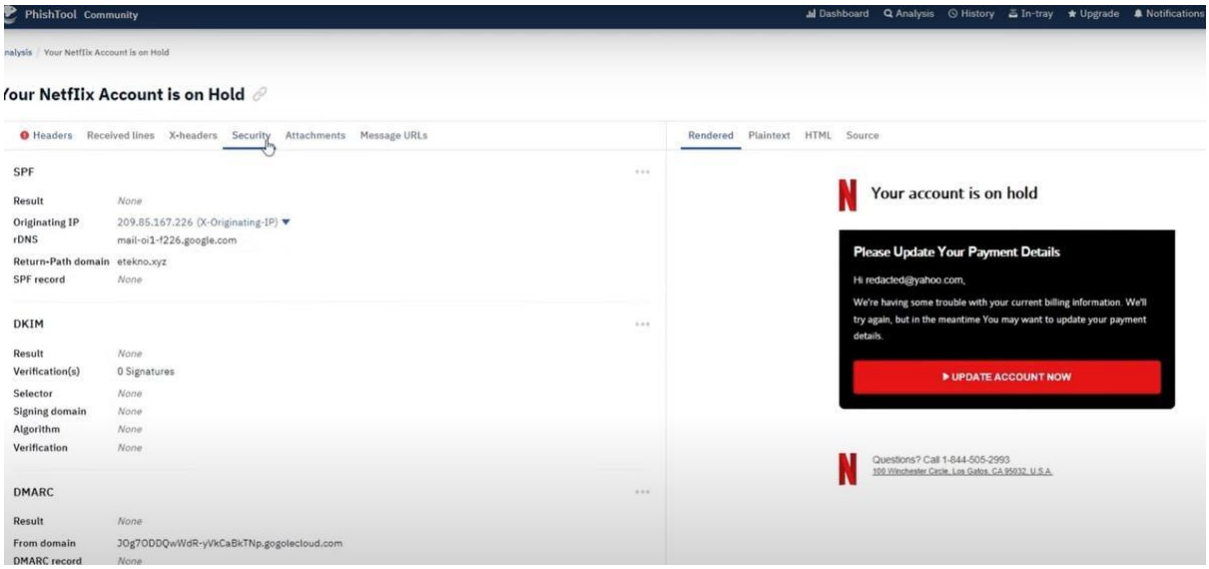
Authority Exploitation: The attacker pretends to be someone in power to coerce the victim into compliance.
Urgency: Creating a false sense of urgency to rush the victim into making a decision without proper verification.
Familiarity: Using personal information to appear as a trusted contact, thus lowering the victim's guard.
Victim's Susceptibility: Discuss why the victim was susceptible to these tactics. Factors could include:

Lack of training on recognizing social engineering attempts.
Natural human tendencies to trust authority figures or urgent requests.
The psychological principle of liking and reciprocation, which can be exploited by attackers feigning familiarity.
Importance of Skepticism and Verification: Highlight the importance of maintaining a healthy level of skepticism in communications. Encourage practices like:

Verifying the identity of the person making the request, especially if sensitive information is involved.
Taking time to think critically about the request, even if it seems urgent.
Consulting with colleagues or superiors before taking action on unusual requests.

Mitigation Strategies: To mitigate such attacks, organizations can:

Implement strict verification protocols for sensitive information requests.
Foster a culture of security awareness within the organization.
Conduct regular training sessions to educate employees about social engineering tactics and prevention strategies.



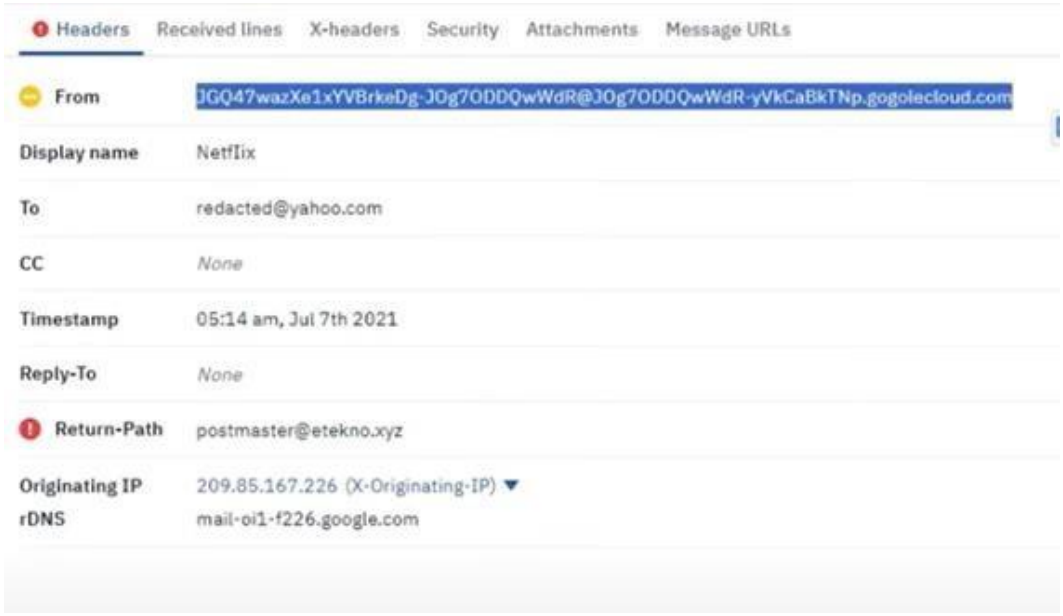
Step-3 Phishing Email Analysis:

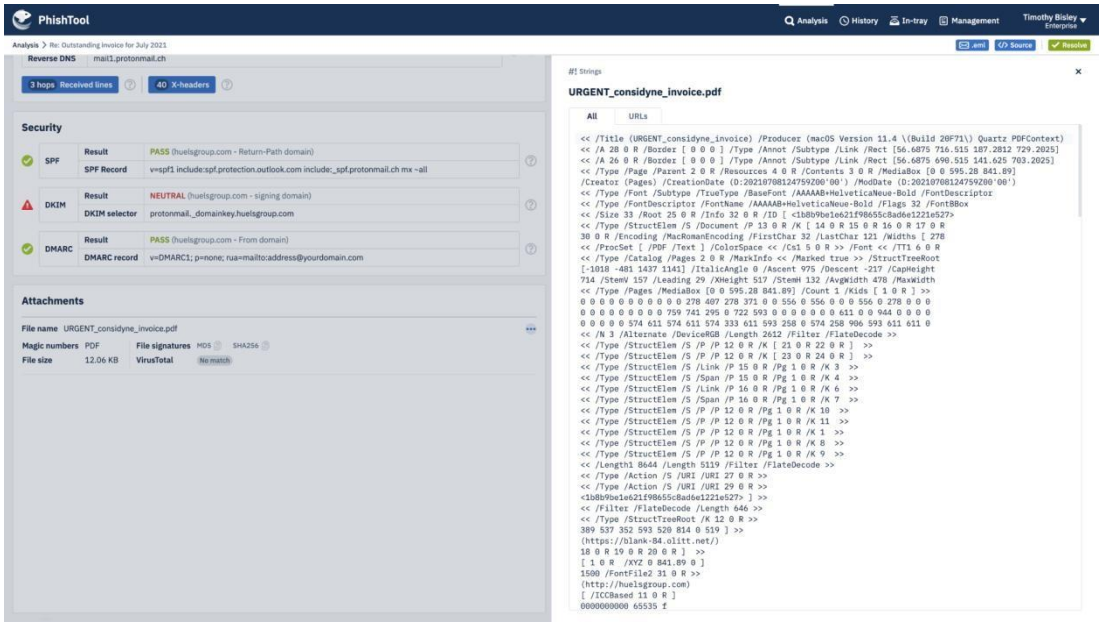
Phishing emails often contain several red flags that can alert a recipient to their malicious intent:

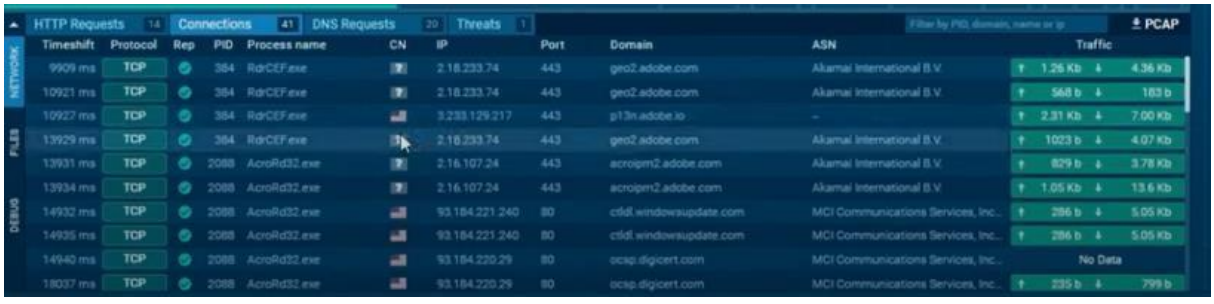
Misspelled Domain Names: Look for subtle misspellings or incorrect domains in the sender's email address.
Urgent Language: Phrases like "Immediate action required" or "Urgent response needed" are common tactics to create a sense of urgency.
Requests for Sensitive Information: Legitimate organizations typically do not ask for sensitive information via email.
Generic Greetings: Phishing emails often use non-personalized greetings like "Dear Customer" or "Dear User."
Psychological Factors: Certain psychological factors can make individuals more susceptible to phishing emails:

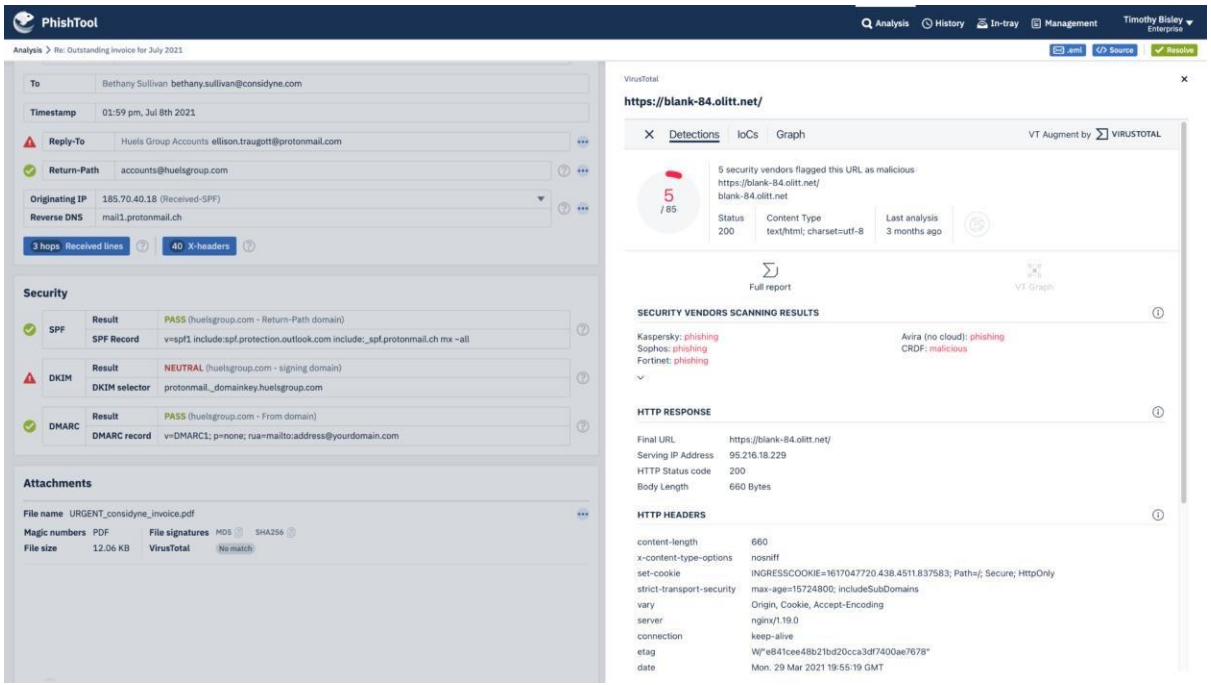
Curiosity: Intriguing or enticing offers can lead to clicking on links without proper scrutiny.
Fear: Threats of account closure or legal action can provoke a fear response, overriding rational judgment.
Urgency: A false sense of urgency can cause individuals to act quickly, bypassing normal security checks.
Email Authentication Strategies: To combat phishing, several email authentication strategies can be employed:

Checking Email Headers: Analyze the technical details within the email header to verify the sender's route.
Verifying Sender Identities: Cross-reference email addresses with known contacts or official communication channels.
Educating Users: Regular training on recognizing phishing attempts and safe email practices is crucial.








PhishTool
Analysis
History
In-tray
Management
Timothy Bisley
Enterprise
Analysis > Re: Outstanding invoice for July 2021
.eml
Source
Resolve
To
Bethany Sullivan bethany.sullivan@considyne.com
Timestamp
01:59 pm, Jul 8th 2021
Reply-To
Huels Group Accounts ellison.traugott@protonmail.com
Return-Path
accounts@huelsgroup.com
Originating IP
185.70.40.18 (Received-SPF)
Reverse DNS
mail1.protonmail.ch
3 hops Received lines
40 X-headers
Security
SPF
Result
PASS (huelsgroup.com - Return-Path domain)
SPF Record
v=spf1 include:spf.protection.outlook.com include:_spf.protonmail.ch mx ~all
DKIM
Result
NEUTRAL (huelsgroup.com - signing domain)
DKIM selector
protonmail._domainkey.huelsgroup.com
DMARC
Result
PASS (huelsgroup.com - From domain)
DMARC record
v=DMARC1; p=none; rua=mailto:address@yourdomain.com
Attachments
File name URGENT_considyne_invoice.pdf
Magic numbers PDF
File signatures MD5 SHA256
File size 12.06 KB
VirusTotal
No match
VirusTotal
https://blank-84.olitt.net/
Detections
IoCs
Graph
VT Augment by VIRUSTOTAL
5
/ 85
5 security vendors flagged this URL as malicious
https://blank-84.olitt.net/
blank-84.olitt.net
Status
200
Content Type
text/html; charset=utf-8
Last analysis
3 months ago
Full report
VT Graph
SECURITY VENDORS SCANNING RESULTS
Kaspersky: phishing
Sophos: phishing
Fortinet: phishing
Avira (no cloud): phishing
CRDF: malicious
HTTP RESPONSE
Final URL
https://blank-84.olitt.net/
Serving IP Address
95.216.18.229
HTTP Status code
200
Body Length
660 Bytes
HTTP HEADERS
content-length
660
x-content-type-options
nosniff
set-cookie
INGRESSCOOKIE=1617047720.438.4511.837583; Path=/; Secure; HttpOnly
strict-transport-security
max-age=15724800; includeSubDomains
vary
Origin, Cookie, Accept-Encoding
server
nginx/1.19.0
connection
keep-alive
etag
W/"e841cee48b21bd20cca3df7400ae7678"
date
Mon, 29 Mar 2021 19:55:19 GMT