

## 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 attack<sup>1</sup>.

#### 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 attack<sup>2</sup>.

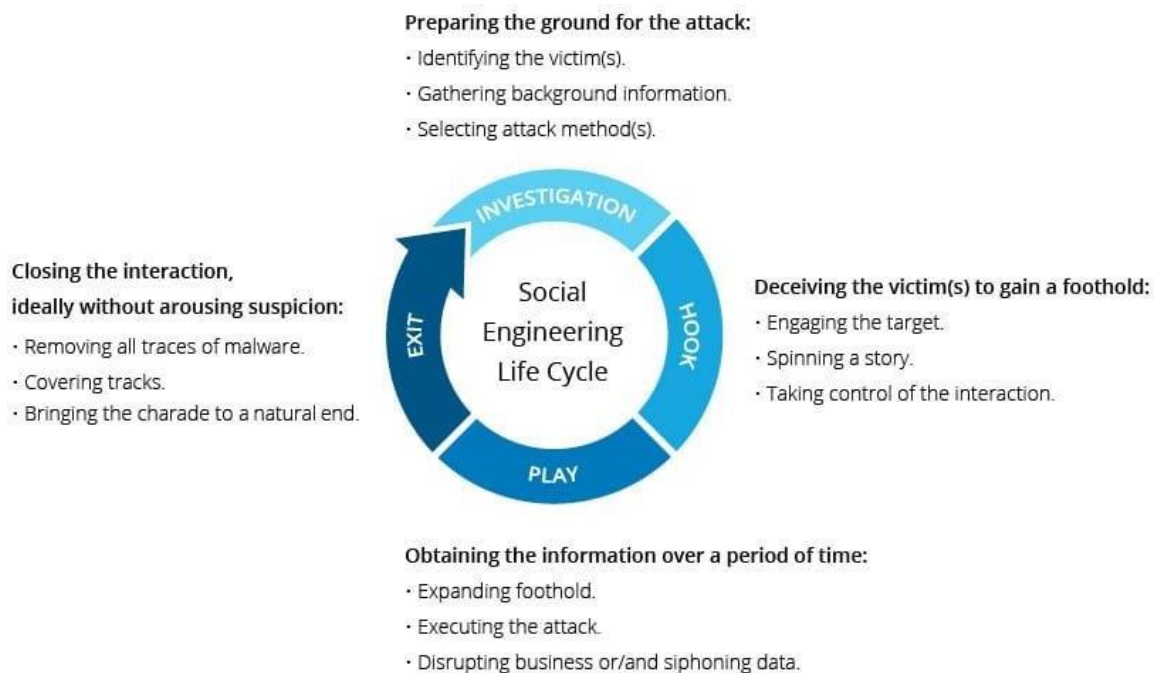
Customer Trust: Breaches can lead to a loss of customer trust, impacting future business and partnerships.

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.

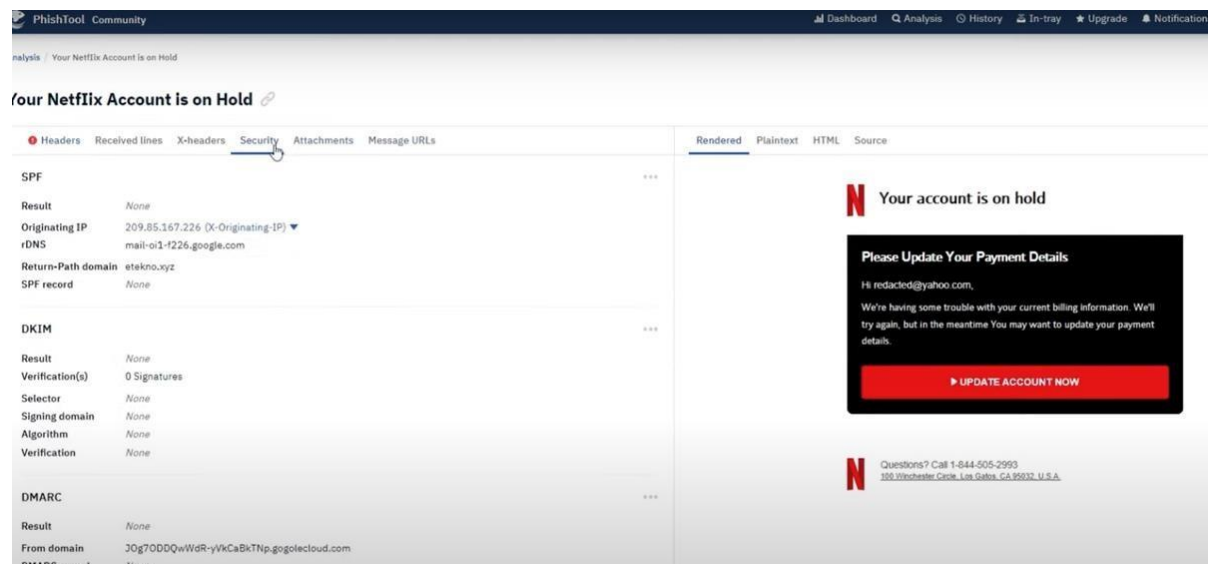
Consulting with colleagues or superiors before taking action on unusual requests.

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:

Educating Users: Regular training on recognizing phishing attempts and safe email practices is crucial.

1	Headers	Received lines	X-headers	Security	Attachments	Message URLs
2	From	JGQ47wazXe1xYVBkeDg-J0g7ODDQwWdR@J0g7ODDQwWdR-yVkJCaBkTnp.gogolecloud.com				
3	Display name	NetfIix				
4	To	redacted@yahoo.com				
5	CC	None				
6	Timestamp	05:14 am, Jul 7th 2021				
7	Reply-To	None				
8	1 Return-Path	postmaster@etekno.xyz				
9	Originating IP	209.85.167.226 (X-Originating-IP) ▼				
10	rDNS	mail-oi1-f226.google.com				

PhishTool
Analysis > Phishing Invoices for July 2021

Reverse DNS mail.phishmail.com

3 hops Received lines
40 X-Headers

### Security

	SPP Record	DKIM selector	DMARC record
<b>SPP</b>	PASS (huelsgroup.com - Return-Path domain)		
<b>DKIM</b>	v=spf1 include:_spf.protection.outlook.com include:_spf.protonmail.ch mx ~all	NEUTRAL (huelsgroup.com - signing domain) protonmail_domainkey.huelsgroup.com	
<b>DMARC</b>	PASS (huelsgroup.com - From domain)		p=none; rua=mailto:address@yourdomain.com

### Attachments

Name URGENT\_considyne\_invoice.pdf

Magic numbers	PDF signatures	HOS	SHA256
File size 12.06 KB	VirusTotal	No match	

#1 Strings

URGENT\_considyne\_invoice.pdf

```

All      URLs

<< /Title (URGENT_considyne_Invoice) /Producer (macOS Version 11.4 (/Build 20P71)) Quartz PDFContext
< /A 20 0 R /Border [ 0 0 0 ] /Type /Annot /Subtype /Link /Rect (56.6875 716.515 187.2812 729.2025)
< /A 26 0 R /Border [ 0 0 0 ] /Type /Annot /Subtype /Link /Rect (56.6875 690.515 141.625 703.2025)
< /Type /Page /Parent 2 0 R /Resources < > /Contents 3 0 R /MediaBox [ 0 0 595.28 843.09 ]
/Creator (Pages) /CreationDate (D:20210708T12459200+00') /ModDate (D:20210708T12459200+00')
/Type /Font /Subtype /TrueType /BaseFont /AAAAAB-HelveticaNeue-Bold /FontDescriptor
< /Type /FontDescriptor /FontName /AAAAAB-HelveticaNeue-Bold /Flags 32 /FontBBox
< /Size 33 /Root 25 0 R /Info 32 0 R /ID [ c1bb93b0e1d2f16055c8adeb1221e527f ]
< /Type /Catalog /Pages 2 0 R /MaxInfo < /Placed true > /StructTreeRoot
[ < /S /H /I 1437 513 /TitleAngle 0 /Ascent 975 /Descent -217 /CapHeight
714 /Stem 157 /Leading 29 /XHeight 517 /Stem 132 /AvgWidth 478 /Maxwidth
of /Pages /MediaBox [ 0 595.28 843.09 ] /Count 1 /Kids [ 1 0 R ] >
0 0 0 0 0 0 0 0 0 278 687 278 371 0 0 356 0 556 0 0 556 0 278 0 0 0
0 0 0 0 0 0 0 0 0 599 741 295 0 0 722 593 0 0 0 0 0 611 0 0 844 0 0 0
0 0 0 0 574 611 574 611 574 333 611 593 288 574 288 906 593 611 611
0 < /N 3 /Alternate /DeviceRGB /Length 2612 /Filter /FlateDecode >
< /Type /Structure /S /P /P 12 0 R /K [ 21 0 R 22 0 R ] >
< /Type /Structure /S /P 12 0 R /K [ 23 0 R 24 0 R ] >
< /Type /Structure /S /Link /P 15 0 R /Pg 1 0 R /K 3 >
< /Type /Structure /S /Span /P 15 0 R /Pg 1 0 R /K 4 >
< /Type /Structure /S /Link /P 16 0 R /Pg 1 0 R /K 6 >
< /Type /Structure /S /Span /P 16 0 R /Pg 1 0 R /K 7 >
< /Type /Structure /S /P 12 0 R /Pg 1 0 R /K 10 >
< /Type /Structure /S /P 12 0 R /Pg 1 0 R /K 11 >
< /Type /Structure /S /P 12 0 R /Pg 1 0 R /K 1 >
< /Type /Structure /S /P 12 0 R /Pg 1 0 R /K 8 >
< /Type /Structure /S /P 12 0 R /Pg 1 0 R /K 9 >
< /Length 8644 /Length 5113 /Filter /FlateDecode >
< /Type /Action /S /URI /URI 27 0 R >
< /Type /Action /S /URI /URI 29 0 R >
< /SubtUselel2f16m055c8adeb1221e527f ) >
< /Filter /FlateDecode /Length 646 >
< /Type /Structure /S /Text /R 32 0 R >
389 537 352 593 520 814 510 ]
(https://blunk-84.olit.net/)
18 0 R 15 0 R 20 0 R >
[ 1 0 R /XYZ 0 843.09 0 ]
1500 /fontfile2 31 0 R >
(Http://huelsgroup.com)
/ FIClosed 11 0 R ]
0000000000 65535 f

```

HTTP Requests 14 Connections 41 DNS Requests 20 Threats 1														Filter by PID, domain, name or ip		PCAP
	Timestamp	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic					
NETWORKS	9909 ms	TCP	✓	384	RdCEF.exe	[REDACTED]	2.18.233.74	443	geo2.adobe.com	Akamai International B.V.	↑ 1.26 Kb ↓	4.36 Kb				
	10921 ms	TCP	✓	384	RdCEF.exe	[REDACTED]	2.18.233.74	443	geo2.adobe.com	Akamai International B.V.	↑ 568 b ↓	183 b				
	10927 ms	TCP	✓	384	RdCEF.exe	[REDACTED]	3.233.129.217	443	p13n.adobe.io	-	↑ 2.31 Kb ↓	7.00 Kb				
	13929 ms	TCP	✓	384	RdCEF.exe	[REDACTED]	2.18.233.74	443	geo2.adobe.com	Akamai International B.V.	↑ 1023 b ↓	4.07 Kb				
	13931 ms	TCP	✓	2088	AcroRd32.exe	[REDACTED]	2.16.107.24	443	acroipm2.adobe.com	Akamai International B.V.	↑ 829 b ↓	3.78 Kb				
	13934 ms	TCP	✓	2088	AcroRd32.exe	[REDACTED]	2.16.107.24	443	acroipm2.adobe.com	Akamai International B.V.	↑ 1.05 Kb ↓	13.6 Kb				
FILES	14932 ms	TCP	✓	2088	AcroRd32.exe	[REDACTED]	93.184.221.240	80	clsid.windowsupdate.com	MCI Communications Services, Inc.	↑ 296 b ↓	5.05 Kb				
	14935 ms	TCP	✓	2088	AcroRd32.exe	[REDACTED]	93.184.221.240	80	clsid.windowsupdate.com	MCI Communications Services, Inc.	↑ 286 b ↓	5.05 Kb				
	14940 ms	TCP	✓	2088	AcroRd32.exe	[REDACTED]	93.184.220.29	80	ocsp.digicert.com	MCI Communications Services, Inc.	No Data					
	18037 ms	TCP	✓	2088	AcroRd32.exe	[REDACTED]	93.184.220.29	80	ocsp.digicert.com	MCI Communications Services, Inc.	↑ 295 b ↓	299 b				

PhishTool

Analysis > Rec: Outstanding invoice for July 2021

AnalysisHistoryIn-trayManagementTimothy BisleyEnterprise

SendSaveResolve

ToBethany Sullivan bethany.sullivan@considyne.com

Timestamp01:59 pm, Jul 8th 2021

Reply-ToHuels Group Accounts ellison.traugott@protonmail.com

Return-Pathaccounts@huelsgroup.com

Originating IP185.70.40.18 (Received-SPF)

Reverse DNSmail1.protonmail.ch

3 hopsReceived lines40 X-headers

Security

SPF

ResultPASS (huelsgroup.com - Return-Path domain)

SPF Recordv=spf1 include:spf.protection.outlook.com include:\_spf.protonmail.ch mx -all

DKIM

ResultNEUTRAL (huelsgroup.com - signing domain)

DKIM selectorprotonmail.\_domainkey.huelsgroup.com

DMARC

ResultPASS (huelsgroup.com - From domain)

DMARC recordv=DMARC1; p=none; rua=mailto:address@yourdomain.com

Attachments

File nameURGENT\_considyne\_invoice.pdf

Magic numbersPDFFile signaturesMD5SHA256

File size12.06 KBVirusTotalNo match

VirusTotal

https://blank-84.olitt.net/

Detections

IoCs

Graph

VT Augment byVIRUSTOTAL

5 / 85

5 security vendors flagged this URL as malicious: https://blank-84.olitt.net/ blank-84.olitt.net

Status200Content Typetext/html; charset=utf-8Last analysis3 months ago

Full reportVT Graph

SECURITY VENDORS SCANNING RESULTS

Kaspersky: phishingAvira (no cloud): phishingSophos: phishingCRDF: maliciousFortinet: phishing

HTTP RESPONSE

Final URLhttps://blank-84.olitt.net/

Serving IP Address95.216.18.229

HTTP Status code200

Body Length660 Bytes

HTTP HEADERS

content-length660

x-content-type-optionsnosniff

set-cookieINGRESSCOOKIE=1617047720.438.4511.837583; Path=/; Secure; HttpOnly

strict-transport-securitymax-age=15724800; includeSubDomains

varyOrigin, Cookie, Accept-Encoding

servernginx/1.19.0

connectionkeep-alive

etagW/"e841cee48b21bd20cca3df7400ae7678"

dateMon, 29 Mar 2021 19:55:19 GMT