Social Engineering: Strategies, Controls, and Impact

Jude Viator, CIA, CISA, CRISC
jviator@pncpa.com – 225.408.4493
Agenda

Social Engineering: What Is It?

Common Techniques
Featuring: Story Time!

Shared Research

Social Engineering Prevention
Social Engineering: Definition
Social Engineering: What Is It?

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

The term "social engineering" as an act of psychological manipulation is also associated with the social sciences, but its usage has caught on among computer and information security professionals.

- Per Wikipedia from "Social Engineering: a guide to building dependable distributed systems"
Social Engineering: Techniques
Pre-Attack Reconassiance

Oscar Dominguez
Vice President
Manager

Valencia Bank and Trust
Stevenson Ranch Office
23600 Lyons Avenue
Newhall, CA 91321
oscar.dominguez@unionbank.com

Toll: 661 287 0380
Fax: 661 267 6374
Toll: 661 253 5763
Fax: 661 253 5751

Find us on Facebook
Pre-Attack Reconassiance

www.familytreenow.com

<table>
<thead>
<tr>
<th>Full Name</th>
<th>Justin Paul Viator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Birth Year</td>
<td>1981</td>
</tr>
<tr>
<td>Age</td>
<td>35</td>
</tr>
</tbody>
</table>

### Possible Relatives

<table>
<thead>
<tr>
<th>Name</th>
<th>Age</th>
<th>Birth Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Felicia Viator</td>
<td>29</td>
<td>1987</td>
</tr>
<tr>
<td>John D Viator</td>
<td>29</td>
<td>1988</td>
</tr>
<tr>
<td>Jude M Viator</td>
<td>29</td>
<td>1988</td>
</tr>
<tr>
<td>Jude M Viator</td>
<td>32</td>
<td>1985</td>
</tr>
<tr>
<td>Kathleen Viator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lindsay D Doucett</td>
<td>29</td>
<td>1987</td>
</tr>
</tbody>
</table>

### Possible Associates

<table>
<thead>
<tr>
<th>Name</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laney Doucett</td>
<td>26</td>
</tr>
<tr>
<td>Michele L Doucett</td>
<td>49</td>
</tr>
<tr>
<td>Ronald W Doucett</td>
<td>53</td>
</tr>
<tr>
<td>Ronny W Doucett</td>
<td>53</td>
</tr>
<tr>
<td>Doucett Viator Lindsay</td>
<td>29</td>
</tr>
<tr>
<td>Laney Doucett</td>
<td>84</td>
</tr>
</tbody>
</table>

### Current & Past Addresses

- **3919 Ken Dr, Lake Charles, LA 70605**
  *Current Address*

- **1826 Fox Run Dr #1, Lake Charles, LA 70605**
  *(Jan 2006 - Jun 2010)*

- **2601 Saint Joseph St, Sulphur, LA 70663**
  *(Mar 2002 - Jan 2006)*
**Social Engineering: Techniques**

- **Pretexting**
  - Contacting target to obtain information and build trust needed for future attacks
Social Engineering: Techniques

Baiting

Scott, you still have $130
Amazon Rewards credit:
w1fbv.info/PBdEimEffV
See what you can claim before it expires on 03/25
w1fbv.info/PBdEimEffV
Social Engineering: Techniques

Tele-Spoofing/Vishing
Social Engineering: Techniques

Physical Spoofing

tailgating/piggybacking

Physical impersonation of an employee, vendor, or other authorized individual
Social Engineering: Techniques

Phishing/Smishing

Emails intended to induce action/obtain information
Social Engineering: Techniques

Spear Phishing/Smishing

Targeted Emails intended to induce action/obtain information
Social Engineering: Techniques

Whaling

Phishing targeted at senior executives
Social Engineering: Techniques

QR Code
Phishing/Baiting

Link to visit phishing website
Social Engineering: Techniques

Browser Hijack

Notifications, Subscriptions, CAPTCHA weaponized
Social Engineering: Techniques

Deepfake

Synthetic media to create falsified content
Social Engineering: Exercise
Social Engineering: Exercise

- Would YOU Recognize a Phishing Attack?
- Anyone Receive a Suspicious/Malicious Message in the Last 10 Days?
Social Engineering: Exercise

Evelyn Dauzat <sos-koyanagi@titan.ocn.ne.jp>

to me

hi

https://goo.gl/fQkNQd

Evelyn Dauzat
Social Engineering: Exercise

Subject: Client #36225192 To STOP receiving these emails from us hit reply and let us know

From: [?]CONFIRM judeviator nliw9zt001s@nliw9zt001s.edu via hclibrary.org

to me

Why is this message in Spam? It's similar to messages that were detected by our spam filters. Learn more

Please confirm your Unsubscribe

To confirm your Unsubscribe, please click here or on the link below.

Unsubscribe me!

Thank you!

To Stop Receiving Messages and Unsubscribe these Notifications Click Here

mailto:<support@forthecustomers.com>,<admin@pathtosky.com>,<info@newlifexd.com>?subject=Unsubscribe
Social Engineering: Exercise

10% off of your next purchase at Amazon.com!

Hurry now and save 10% off of your next purchase at Amazon.

Amazon.com Gift Cards ("GCs") may be used only for the purchase of eligible goods on Amazon.com or certain of its affiliated websites. Except as required by law, GCs cannot be transferred for value or redeemed for cash. Purchases are deducted from the GC balance. To redeem or view a GC balance, visit "Your Account" on Amazon.com.
Shared Research
CISCO’s 2021 Cybersecurity threat trends report suggests that at least one person clicked a phishing link in around 86% of organizations. The company’s data suggests that phishing accounts for around 90% of data breaches.

There’s an uneven distribution in phishing attacks throughout the year. CISCO found that phishing tends to peak around holiday times, finding that phishing attacks soared by 52% in December.
When investigating ‘in-the-wild’ email subject lines, KnowBe4 found the most common throughout Q4 2020 included:

- IT: Annual Asset Inventory
- Changes to your health benefits
- Twitter: Security alert: new or unusual Twitter login
- Amazon: Action Required | Your Amazon Prime Membership has been declined
- Zoom: Scheduled Meeting Error
- Google Pay: Payment sent
- Stimulus Cancellation Request Approved
- Microsoft 365: Action needed: update the address for your Xbox Game Pass for Console subscription
- RingCentral is coming!
- Workday: Reminder: Important Security Upgrade Required
TOP SOCIAL MEDIA EMAIL SUBJECTS

New voice message at 1:23AM
7%

Someone has sent you a Direct Message on Twitter
10%

Login alert for Chrome on Motorola Moto X
10%

"You appeared in new searches this week!"

"People are looking at your LinkedIn profile"

LinkedIn
47%

"New Sign-in To Your Facebook from Samsung Galaxy S4"

"LinkedIn Password Reset"

Facebook
26%

"Your friend tagged you in photos on Facebook"

"Please add me to your LinkedIn Network"

"Join my network on LinkedIn"

KEY TAKEAWAY

LinkedIn messages continue to dominate the top social media email subjects, with several variations of messages such as “people are looking at your profile” or “add me.” Other alerts containing security-related warnings come unexpectedly and can cause feelings of alarm. Messages such as a friend tagged you in a photo or mentioned you can make someone feel special and entice them to click.
# TOP 10 GENERAL EMAIL SUBJECTS

<table>
<thead>
<tr>
<th>Subject</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Check Required Immediately</td>
<td>25%</td>
</tr>
<tr>
<td>Touch base on meeting next week</td>
<td>14%</td>
</tr>
<tr>
<td>Vacation Policy Update</td>
<td>11%</td>
</tr>
<tr>
<td>COVID-19 Remote Work Policy Update</td>
<td>11%</td>
</tr>
<tr>
<td>Important: Dress Code Changes</td>
<td>10%</td>
</tr>
<tr>
<td>Scheduled Server Maintenance -- No Internet Access</td>
<td>7%</td>
</tr>
<tr>
<td>De-activation of [[email]] in Process</td>
<td>6%</td>
</tr>
<tr>
<td>Please review the leave law requirements</td>
<td>6%</td>
</tr>
<tr>
<td>You have been added to a team in Microsoft Teams</td>
<td>5%</td>
</tr>
<tr>
<td>Company Policy Notification: COVID-19 - Test &amp; Trace Guidelines</td>
<td>5%</td>
</tr>
</tbody>
</table>

## KEY TAKEAWAY

Hackers are playing into employees’ desires to remain security minded. We are still seeing some subjects around COVID-19, but it seems users are getting more savvy to those types of ploys. Curiosity is piqued with security-related notifications and HR-related messages that could potentially affect their daily work.
According to Microsoft’s New Future of Work Report:

- 80% of security professionals surveyed said they had encountered increased security threats since the shift to remote work began.
- Of these, 62% said phishing campaigns had increased more than any other type of threat.
- Employees said they believed IT departments would be able to mitigate these phishing attacks if they had been working in the office.

Furthermore, an August 2021 survey conducted by Palo Alto Networks found that:

- 35% of companies reported that their employees either circumvented or disabled remote security measures.
- Workers at organizations that lacked effective remote collaboration tools were more than eight times as likely to report high levels of security evasion.
- 83% of companies with relaxed bring-your-own-device (BYOD) usage led to increased security issues.
“A Network of Human Sensors”

“One of the most effective ways you can minimize the phishing threat is through effective awareness and training. Not only can you reduce the number of people that fall victim to (potentially) less than 5%, you create a network of human sensors that are more effective at detecting phishing attacks than almost any technology.”

Lance Spitzner

Training Director for the SANS Securing The Human Program
Prevention

Pros of phishing awareness training

Employees learn how to spot phishing attacks

It's a good chance to remind employees of existing policies and procedures

Security leaders can identify particularly risky and at-risk employees

Training satisfies compliance standards

It helps organizations foster a strong security culture
Prevention

Cons of phishing awareness training

- Training alone can't prevent human error
- Phishing awareness training is always one step behind
- Training is expensive
- Training isn't targeted (or engaging) enough
Prevention

But, humans shouldn’t be the last line of defense. That’s why organizations need to invest in technology and other solutions to prevent successful phishing attacks. But, given the frequency of attacks year-on-year, it’s clear that spam filters, antivirus software, and other legacy security solutions aren’t enough.