



## *Social Engineering: Strategies, Controls, and Impact*

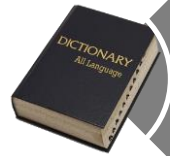
**Jude Viator, CIA, CISA, CRISC**  
**[jviator@pncpa.com](mailto:jviator@pncpa.com) – 225.408.4493**

assurance - consulting - tax - technology - **pncpa.com**

*Postlethwaite & Netterville, A Professional Accounting Corporation*

# 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 Reconnaissance



**Oscar Dominguez**  
Vice President  
Manager

Valencia Bank and Trust  
Stevenson Ranch Office  
23620 Lyons Avenue  
Newhall, CA 91321  
oscar.dominguez@unionbank.com

Tel. 661 287 6380  
Fax 661 287 6374  
Tel. 661 253 5753  
Fax 661 253 5751

unionbank.com



Find us on  
**Facebook**




# Pre-Attack Reconnaissance

[www.familytreenow.com](http://www.familytreenow.com)

Full Name	Justin Paul Viator
Birth Year	1981
Age	35

Possible Associates ?	
Name	Age
Laney Doucett	26
Michele L Doucett	49
Ronald W Doucett	53
Ronny W Doucett	53
Doucett Viator Lindsay	29
Laney Doucett	84

Possible Relatives ?		
Name	Age	Birth Year
Felicia Viator		
John D Viator	29	1987
Jude M Viator	29	1988
Jude M Viator	32	1985
Kathleen Viator		
Lindsay D Doucett	29	1987

Current & Past Addresses
3919 Ken Dr, Lake Charles, LA 70605  <i>Current Address</i>
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

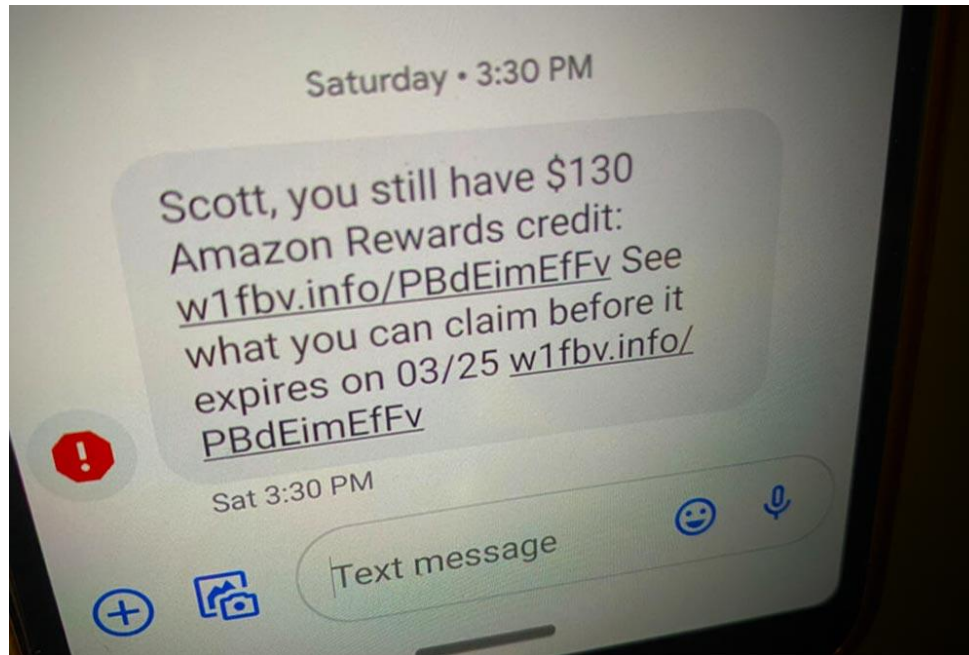
Contacting target to obtain information and build trust needed for future attacks





# *Social Engineering: Techniques*

## Baiting



# *Social Engineering: Techniques*

---

## Tele-Spoofing/Vhishing



# *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

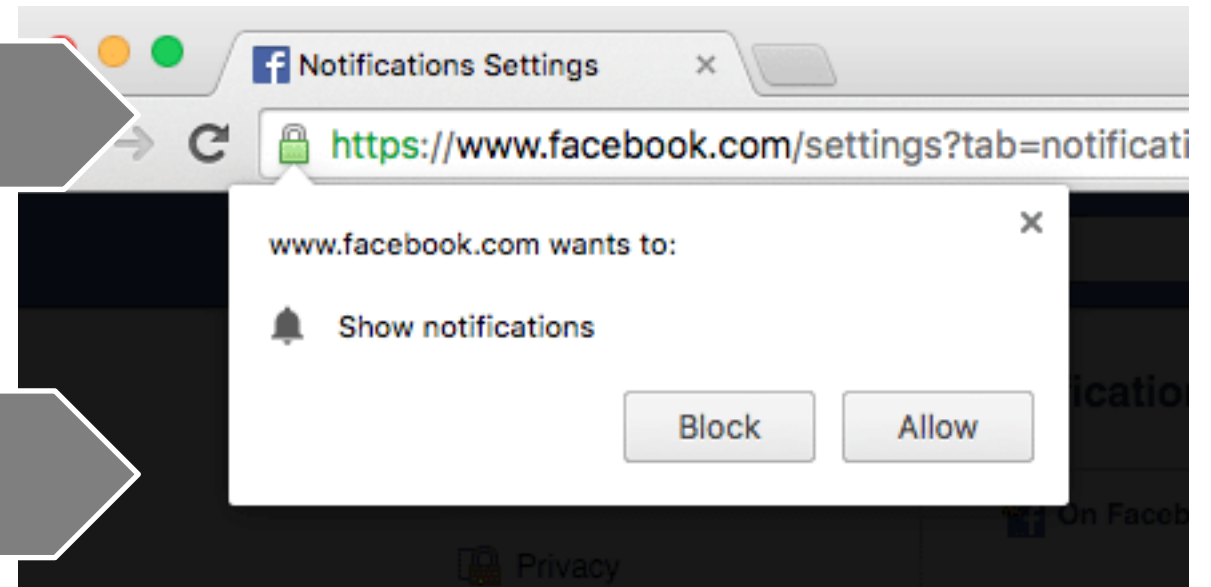
Link to visit phishing website



# *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?**

Leila	[New SMS] You Got a Glance from Leila (from Yaroslavl, Russia) - [New SMS] You Got a Glance from Leila (from Yaroslavl, Russia)
Amazon.com® Reward (Ind..	LAST NOTICE: Only Today Left to Grab A Free \$50 Amazon.com® Gift Card - LAST NOTICE: Only Today Left to Grab A Free \$50 Amazon.com® Gift Card
TARGET® Reward	Your customer ID was selected for a \$50 Target® charge card - Your customer ID was selected for a \$50 Target® charge card
Evelyn Dauzat	(no subject) - hi <a href="https://goo.gl/fQkNQd">https://goo.gl/fQkNQd</a> Evelyn Dauzat
McRee Ford	News and Specials from McRee Ford - Spring Savings and News View as a Web Page. Please add <a href="mailto:newsletter@mcreeford.com">newsletter@mcreeford.com</a> to your address book to ensu
From: 🇳🇮 CONFIRM judeviat.	Subject: 🚫 Client #36225192 To STOP receiving these emails from us hit reply and let u... - Please confirm your Unsubscribe To confirm your Unsubscribe
Cedric Webb	March Closeout Specials Inside - PRE-OWNED SPECIALS 2018 Civic: Financing with approved credit for 36 month lease through Honda Financial Services.
Laura Touchstone	Re: - <a href="http://connect.toilettrack.com">http://connect.toilettrack.com</a> Laura Touchstone
Karlos Williams	Hi! judeviator I want my money back, my 1000\$ - hi judeviator i want to get back the money I lent you, i need it tomorrow - Sent from my iPhone
James Patterson	I'm giving away \$2 million to teachers - Discover new reads from James Patterson View this email in your browser I'm Donating \$2 Million to Help Teachers /
Cheap Auto Insurance Tod.	Check for discounts: auto insurance - Check for discounts: auto insurance
Sportsman Gear	Happy Friday - Get 20% Off Your Order! - Performance Fishing & Hunting Gear That's Always In Season Post-Show Sale through March 31: Use Code SHOW
Justin Viator	(no subject) - <a href="http://open.timeoutshreveport.com">http://open.timeoutshreveport.com</a> Justin Viator
MR.GODWIN EMEFIELE	GOOD NEWS CONTACT CHRIS IBEH IMMEDIATELY - FROM THE EXECUTIVE GOVERNOR, CENTRAL BANK OF NIGERIA (CBN) GOV.GODWIN EMEFIE

# *Social Engineering: Exercise*

---

(no subject)



Inbox x



**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 ● □ Spam x

! 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@forthecostumers.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.

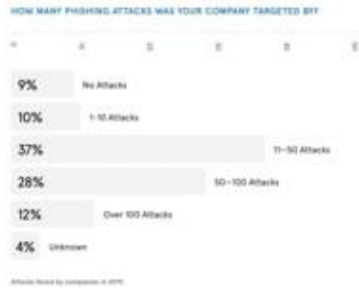
Redeem now 

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*



# Must-Know Phishing Statistics

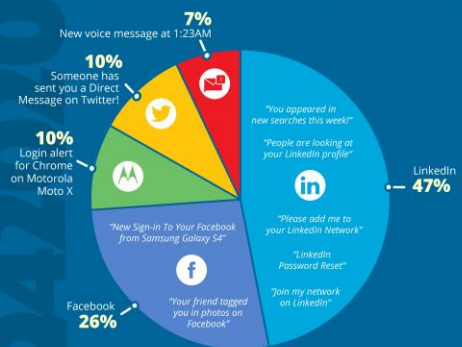


CISCO's 2021 Cybersecurity threat trends report suggests that at least one person clicked a phishing link in around 86% of organizations. The company's data suggests that phishing accounts for around 90% of data breaches.

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.

# TOP-CLICKED PHISHING TESTS

## TOP SOCIAL MEDIA EMAIL SUBJECTS



### 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

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

### 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 plays. Curiosity is piqued with security-related notifications and HR-related messages that could potentially affect their daily work.

## COMMON "IN THE WILD" ATTACKS

- 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

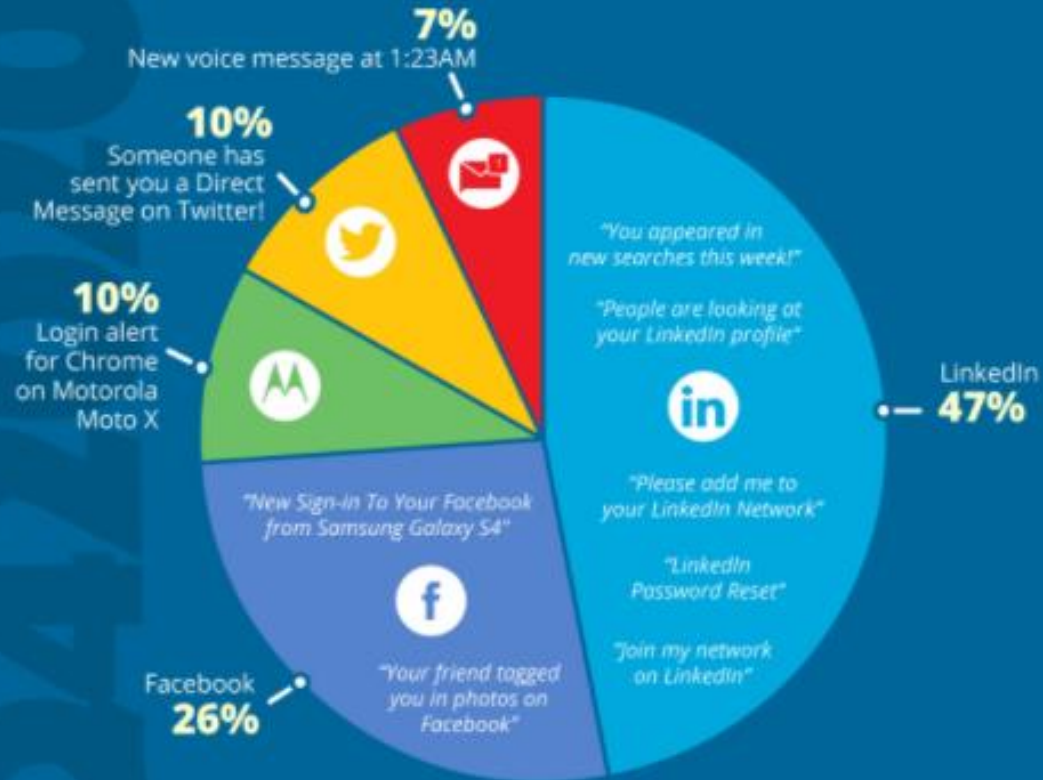
### KEY TAKEAWAY

Again this quarter we see subjects related to working from home and a new one around stimulus payments. Cybercriminals are preying on heightened stress, distraction, urgency, curiosity, and fear in users. These types of attacks are effective because they cause a person to react before thinking logically about the legitimacy of the email.

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



## 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

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

## 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 issue

# *Social Engineering Prevention*

# *Prevention*

---

## *“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.



Postlethwaite & Netterville

*A Professional Accounting Corporation*