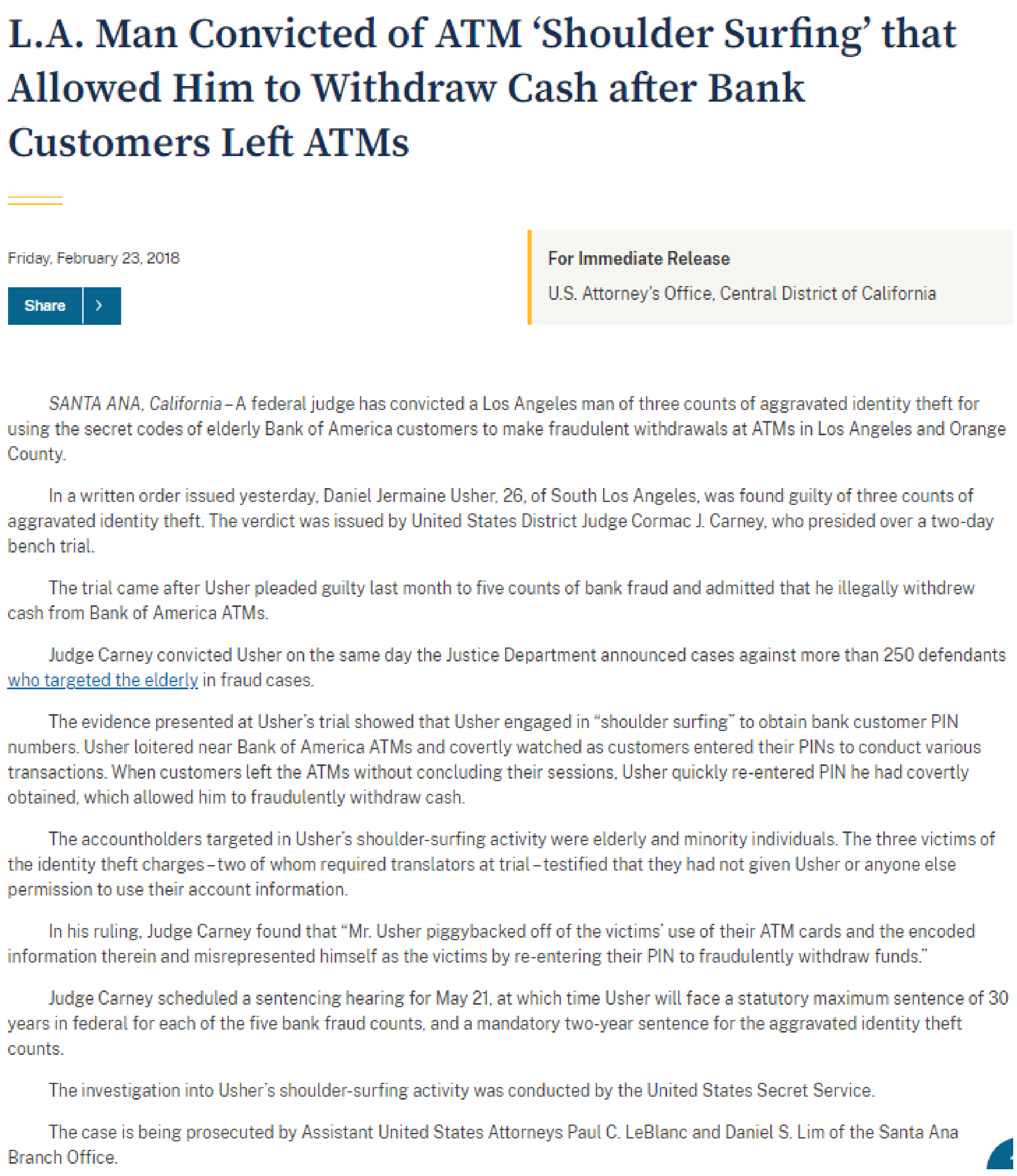
Practical 5

Objectives: Identify the types of Social Engineering and its concept

Exercise 1. Shoulder Surfing

Central District of California | L.A. Man Convicted of ATM 'Shoulder Surfing' that Allowed Him to Withdraw Cash after Bank Customers Left ATMs | United States Department of Justice



L.A. Man Convicted of ATM 'Shoulder Surfing' that Allowed Him to Withdraw Cash after Bank Customers Left ATMs

Friday, February 23, 2018

Share ›

For Immediate Release

U.S. Attorney's Office, Central District of California

SANTA ANA, California – A federal judge has convicted a Los Angeles man of three counts of aggravated identity theft for using the secret codes of elderly Bank of America customers to make fraudulent withdrawals at ATMs in Los Angeles and Orange County.

In a written order issued yesterday, Daniel Jermaine Usher, 26, of South Los Angeles, was found guilty of three counts of aggravated identity theft. The verdict was issued by United States District Judge Cormac J. Carney, who presided over a two-day bench trial.

The trial came after Usher pleaded guilty last month to five counts of bank fraud and admitted that he illegally withdrew cash from Bank of America ATMs.

Judge Carney convicted Usher on the same day the Justice Department announced cases against more than 250 defendants who targeted the elderly in fraud cases.

The evidence presented at Usher's trial showed that Usher engaged in "shoulder surfing" to obtain bank customer PIN numbers. Usher loitered near Bank of America ATMs and covertly watched as customers entered their PINs to conduct various transactions. When customers left the ATMs without concluding their sessions, Usher quickly re-entered PIN he had covertly obtained, which allowed him to fraudulently withdraw cash.

The accountholders targeted in Usher's shoulder-surfing activity were elderly and minority individuals. The three victims of the identity theft charges – two of whom required translators at trial – testified that they had not given Usher or anyone else permission to use their account information.

In his ruling, Judge Carney found that "Mr. Usher piggybacked off of the victims' use of their ATM cards and the encoded information therein and misrepresented himself as the victims by re-entering their PIN to fraudulently withdraw funds."

Judge Carney scheduled a sentencing hearing for May 21, at which time Usher will face a statutory maximum sentence of 30 years in federal for each of the five bank fraud counts, and a mandatory two-year sentence for the aggravated identity theft counts.

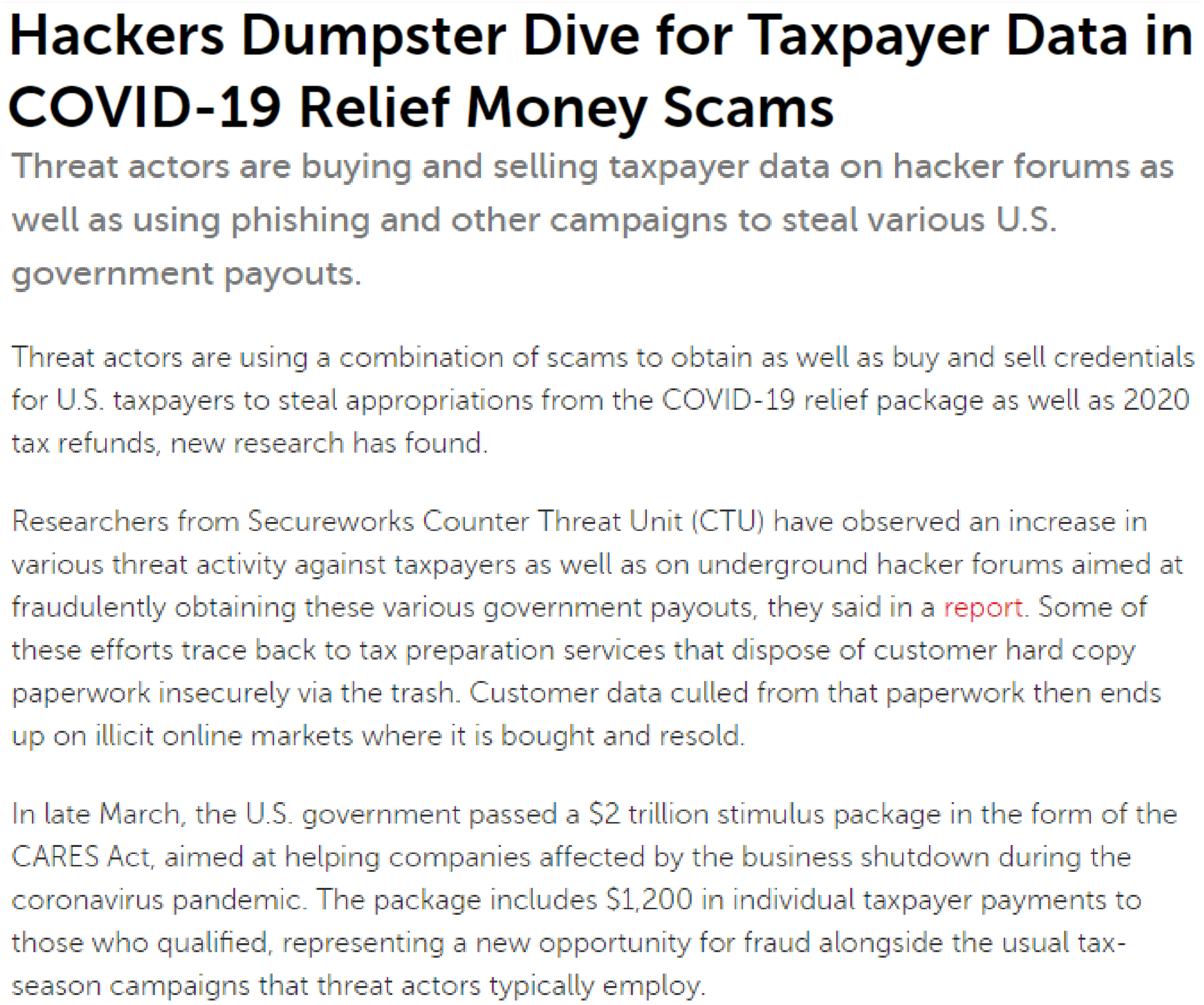
The investigation into Usher's shoulder-surfing activity was conducted by the United States Secret Service.

The case is being prosecuted by Assistant United States Attorneys Paul C. LeBlanc and Daniel S. Lim of the Santa Ana Branch Office.

1. What is the social engineering technique being employed in this scenario?
2. How does the attacker benefit from shoulder surfing in this situation?
3. What potential risks or consequences does the victim face as a result of shoulder surfing?
4. What kind of sensitive information can an attacker gain through shoulder surfing?
5. How can the victim's personal or professional life be impacted by the attacker's actions?
6. What preventive measures could the victim have taken to protect against shoulder surfing?
7. What actions can the victim take if they suspect or detect someone attempting to shoulder surf?
8. How can organizations create an environment that discourages or prevents shoulder surfing incidents?
9. What training or awareness programs can be implemented to educate individuals about the risks of shoulder surfing?
10. What technological solutions or physical measures can be implemented to minimize the risk of shoulder surfing?

Exercise 2. Dumpster Dive

Hackers Dumpster Dive for Taxpayer Data in COVID-19 Relief Money Scams | Threatpost



Hackers Dumpster Dive for Taxpayer Data in COVID-19 Relief Money Scams

Threat actors are buying and selling taxpayer data on hacker forums as well as using phishing and other campaigns to steal various U.S. government payouts.

Threat actors are using a combination of scams to obtain as well as buy and sell credentials for U.S. taxpayers to steal appropriations from the COVID-19 relief package as well as 2020 tax refunds, new research has found.

Researchers from Secureworks Counter Threat Unit (CTU) have observed an increase in various threat activity against taxpayers as well as on underground hacker forums aimed at fraudulently obtaining these various government payouts, they said in a report. Some of these efforts trace back to tax preparation services that dispose of customer hard copy paperwork insecurely via the trash. Customer data culled from that paperwork then ends up on illicit online markets where it is bought and resold.

In late March, the U.S. government passed a $2 trillion stimulus package in the form of the CARES Act, aimed at helping companies affected by the business shutdown during the coronavirus pandemic. The package includes $1,200 in individual taxpayer payments to those who qualified, representing a new opportunity for fraud alongside the usual tax-season campaigns that threat actors typically employ.

1. What is the social engineering technique being employed in this scenario?
2. How does the attacker benefit from dumpster diving in this situation?
3. What potential risks or consequences does the victim or organization face as a result of dumpster diving?
4. What kind of sensitive information can an attacker find through dumpster diving?
5. How can the victim's personal or professional life be impacted by the attacker's actions?
6. What preventive measures could the victim or organization have taken to protect against dumpster diving?
7. What actions can the victim or organization take if they suspect or detect someone dumpster diving?
8. How can organizations create policies or guidelines to minimize the risk of dumpster diving?
9. What training or awareness programs can be implemented to educate individuals about the risks of dumpster diving and proper disposal of sensitive information?
10. How can organizations establish secure waste disposal processes to minimize the risk of dumpster diving?

Exercise 3. Piggybacking

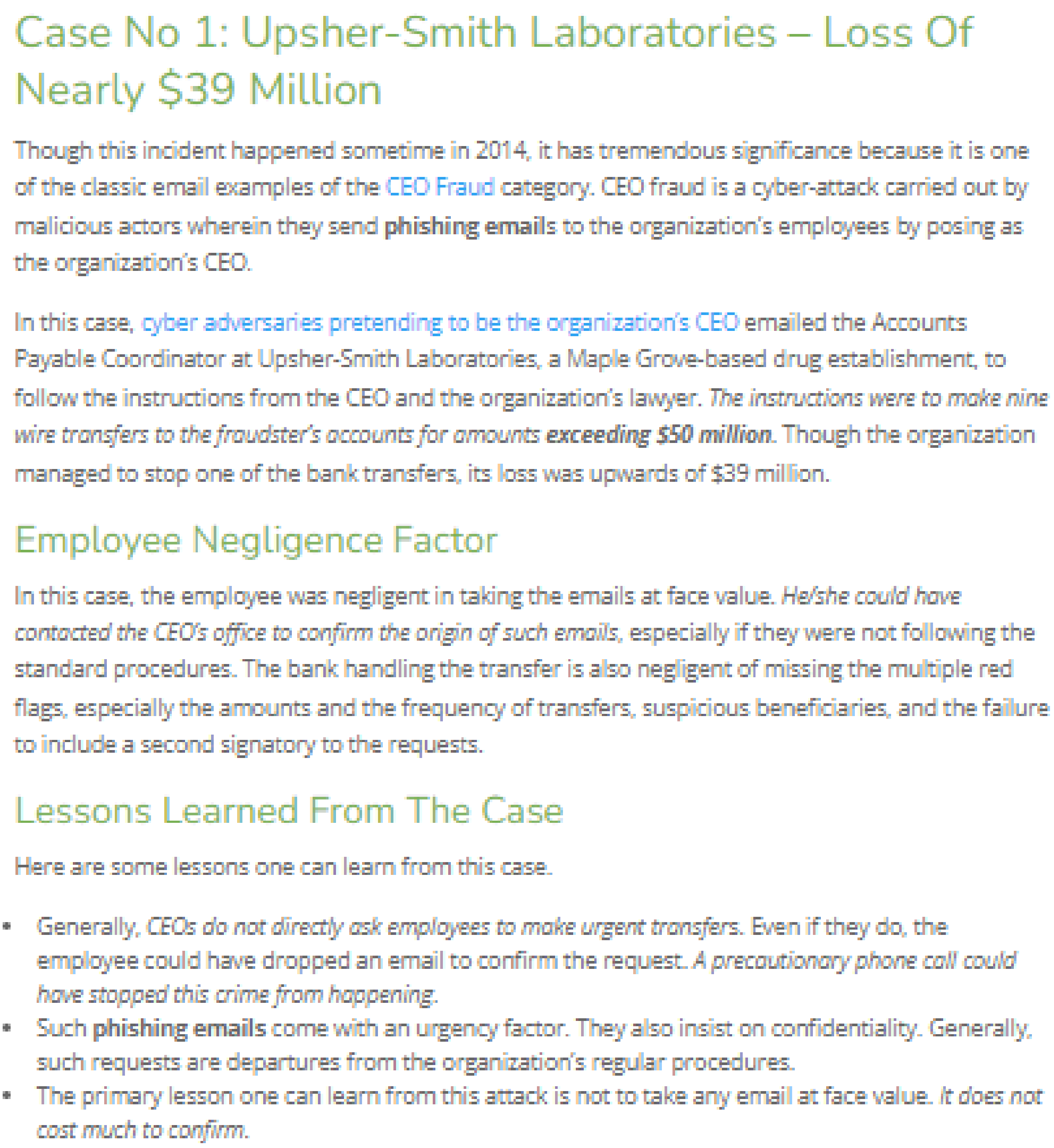
Scenario 1:
Lisa works in a high-security facility where employees are required to use access cards to enter the building. One day, as Lisa enters the building using her access card, an unknown person slips in right behind her without using their own access card. The person then proceeds to roam around the facility freely.

Scenario 2:
John is sitting at a coffee shop and using the shop's Wi-Fi network to access the internet on his laptop. Another customer sitting nearby, who doesn't want to pay for Wi-Fi access, asks John if they can share his Wi-Fi connection. John agrees and shares his Wi-Fi password with the stranger.

1. What is the social engineering technique being employed in this scenario?
2. How does the unauthorized individual benefit from piggybacking in this situation?
3. What potential risks or consequences does the victim or organization face as a result of piggybacking?
4. What kind of sensitive information or resources can an attacker gain through piggybacking?
5. How can the victim's personal or professional life be impacted by the attacker's actions?
6. What preventive measures could the victim or organization have taken to protect against piggybacking?
7. What actions can the victim or organization take if they suspect or detect someone piggybacking?
8. How can organizations create policies or guidelines to minimize the risk of piggybacking?
9. What training or awareness programs can be implemented to educate individuals about the risks of piggybacking and the importance of secure access?
10. How can organizations implement technical solutions to detect and prevent unauthorized piggybacking?

Exercise 4. Phishing

Phishing Case Studies: Learning From the Mistakes Of Others - PhishProtection.com



Case No 1: Upsher-Smith Laboratories – Loss Of Nearly $39 Million

Though this incident happened sometime in 2014, it has tremendous significance because it is one of the classic email examples of the CEO Fraud category. CEO fraud is a cyber-attack carried out by malicious actors wherein they send **phishing emails** to the organization's employees by posing as the organization's CEO.

In this case, cyber adversaries pretending to be the organization's CEO emailed the Accounts Payable Coordinator at Upsher-Smith Laboratories, a Maple Grove-based drug establishment, to follow the instructions from the CEO and the organization's lawyer. *The instructions were to make nine wire transfers to the fraudster's accounts for amounts* ***exceeding $50 million***. Though the organization managed to stop one of the bank transfers, its loss was upwards of $39 million.

Employee Negligence Factor

In this case, the employee was negligent in taking the emails at face value. *He/she could have contacted the CEO's office to confirm the origin of such emails*, especially if they were not following the standard procedures. The bank handling the transfer is also negligent of missing the multiple red flags, especially the amounts and the frequency of transfers, suspicious beneficiaries, and the failure to include a second signatory to the requests.

Lessons Learned From The Case

Here are some lessons one can learn from this case.

- Generally, *CEOs do not directly ask employees to make urgent transfers*. Even if they do, the employee could have dropped an email to confirm the request. *A precautionary phone call could have stopped this crime from happening.*
- Such **phishing emails** come with an urgency factor. They also insist on confidentiality. Generally, such requests are departures from the organization's regular procedures.
- The primary lesson one can learn from this attack is not to take any email at face value. *It does not cost much to confirm.*

1. What is the social engineering technique being employed in this scenario?
2. How does the attacker benefit from phishing in this situation?
3. What potential risks or consequences does the victim or organization face as a result of falling for a phishing attack?
4. What kind of sensitive information can an attacker obtain through a successful phishing attempt?
5. How can the victim's personal or professional life be impacted by the attacker's actions?
6. What preventive measures could the victim or organization have taken to protect

against phishing attacks?

7. What actions can the victim or organization take if they suspect or identify a phishing attack?
8. How can organizations educate individuals about the risks of phishing and train them to recognize and report suspicious emails?
9. What technical measures can organizations implement to detect and prevent phishing attempts?
10. How can organizations collaborate with industry partners and law enforcement to combat phishing attacks?

End of Practical