Project 1: 23 days left

Offense-Based Cybersecurity: Exploitation of Human Vulnerabilities

CS 459/559: Science of Cyber Security
9th Lecture

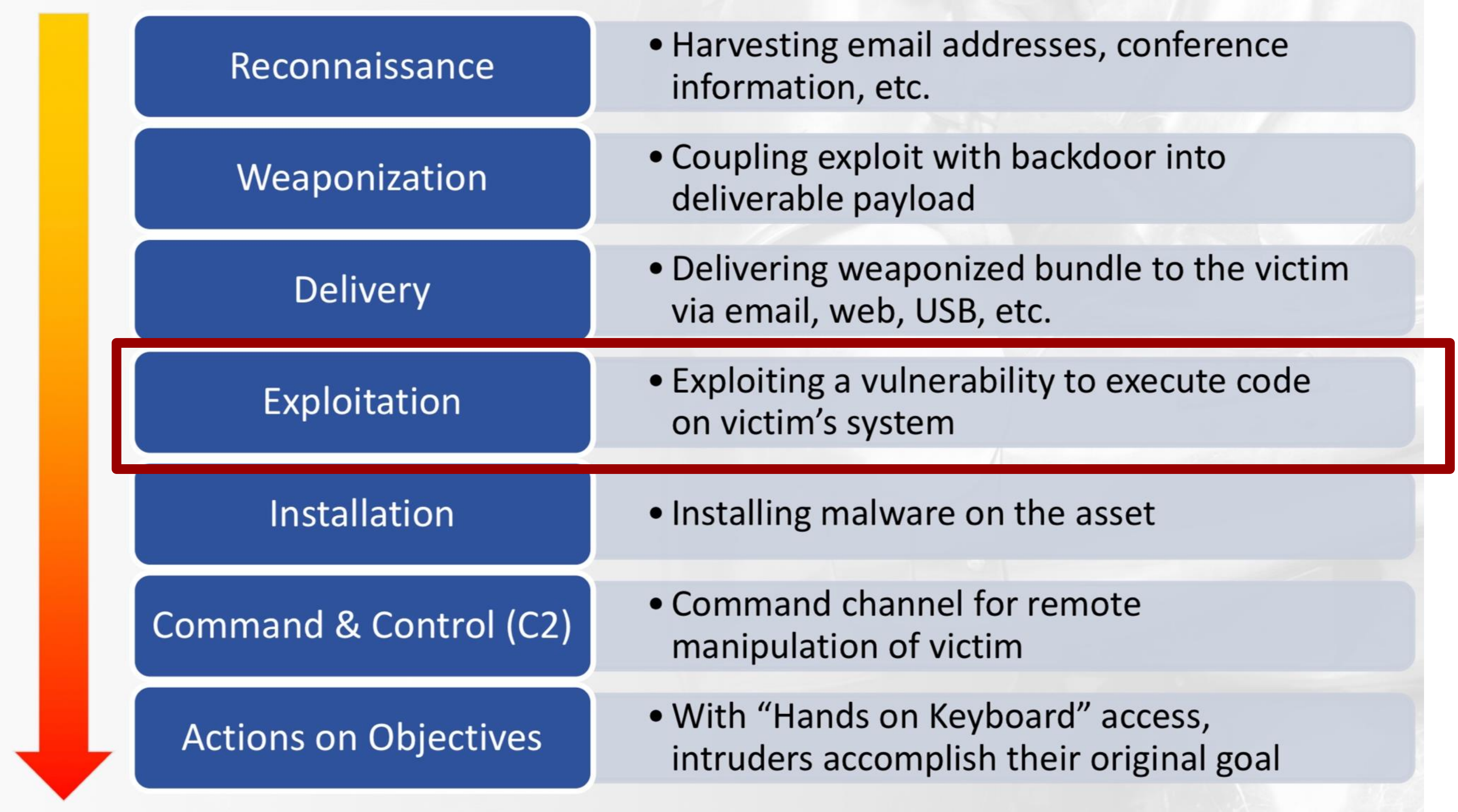
Instructor:

Guanhua Yan

Agenda

- Quiz 1: September 29 (closed book)
- Project 1 (offense): October 10
- Project 2 (defense): December 5
- Presentations: 11/17, 11/19, 11/24, 12/1, 12/3
- Final report: December 15

Exploitation of memory vulnerabilities



Reconnaissance	• Harvesting email addresses, conference information, etc.
Weaponization	• Coupling exploit with backdoor into deliverable payload
Delivery	• Delivering weaponized bundle to the victim via email, web, USB, etc.
Exploitation	• Exploiting a vulnerability to execute code on victim's system
Installation	• Installing malware on the asset
Command & Control (C2)	• Command channel for remote manipulation of victim
Actions on Objectives	• With "Hands on Keyboard" access, intruders accomplish their original goal

Introduction

- What is Social Engineering Attack?

- Social Engineering Tactics
  - Quid Pro Quo
  - Phishing/Spear phishing/Smishing/Vishing/etc.
  - Baiting
  - Pretexting
  - Diversion Theft

- Role of AI in Social Engineering Attacks

What is Social Engineering Attack?

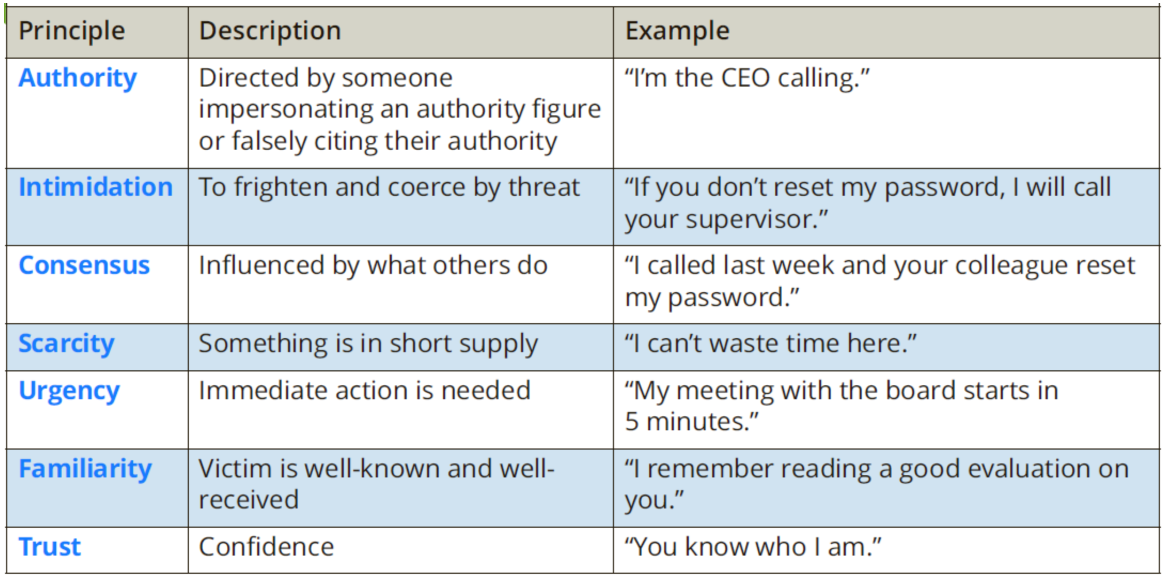
- Attacker uses **human interaction** to obtain or compromise information
  - Manipulate people into doing something, rather than by breaking in using technical means

- Attacker may appear **unassuming or respectable**
  - **Pretend** to be a new employee, repair man, etc.
  - May even **offer credentials**

- By asking questions, the attacker may **piece enough information together** to infiltrate a company's network
  - May attempt to get information from many sources

Persuasion

- Technology is not always needed for attacks on IT
- Social engineering gathers information by relying on the weaknesses of individuals
- It relies on the psychological approaches to persuade a victim



Principle	Description	Example
Authority	Directed by someone impersonating an authority figure or falsely citing their authority	“I’m the CEO calling.”
Intimidation	To frighten and coerce by threat	“If you don’t reset my password, I will call your supervisor.”
Consensus	Influenced by what others do	“I called last week and your colleague reset my password.”
Scarcity	Something is in short supply	“I can’t waste time here.”
Urgency	Immediate action is needed	“My meeting with the board starts in 5 minutes.”
Familiarity	Victim is well-known and well-received	“I remember reading a good evaluation on you.”
Trust	Confidence	“You know who I am.”

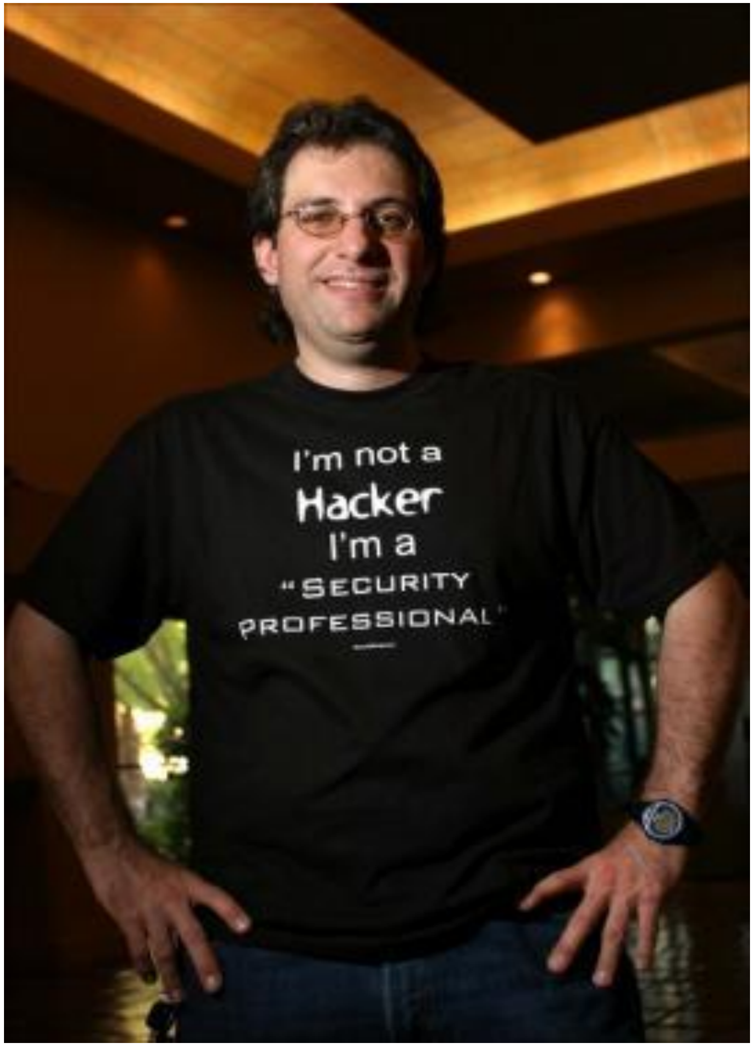
Ciampa, Mark. *CompTIA security+ guide to network security fundamentals*. Cengage Learning, 2021.

Kevin Mitnick

Famous Social Engineer Hacker

- Went to prison for hacking
- Became ethical hacker

“The biggest threat to the security of a company is not a computer virus, an unpatched hole in a key program or a badly installed firewall. In fact, the biggest threat could be you.” - Kevin Mitnick



Examples of Social Engineering

- **Kevin Mitnick talks his way into central Telco office**
  - Tells guard he will get a new badge
  - Pretend to work there, give manager name from another branch
  - Fakes a phone conversation when caught
- **Free food at McDonalds**

Example: Greek-Trojan war

- There was a ten-year long campaign between the two nations, Greek and Trojan
- The Greeks appeared to have been defeated and, as a parting gift, built a large wooden horse and left it at the gate of Troy and then appeared to have retreated
- The Trojans, thinking that they were the victors, brought the horse into the city and began their victory celebration
- A few Greek soldiers, who were hidden inside the horse, slipped out of their hiding place and opened the gates for the Greek army
- The Greeks won the battle against the Trojans

Example: RSA attack

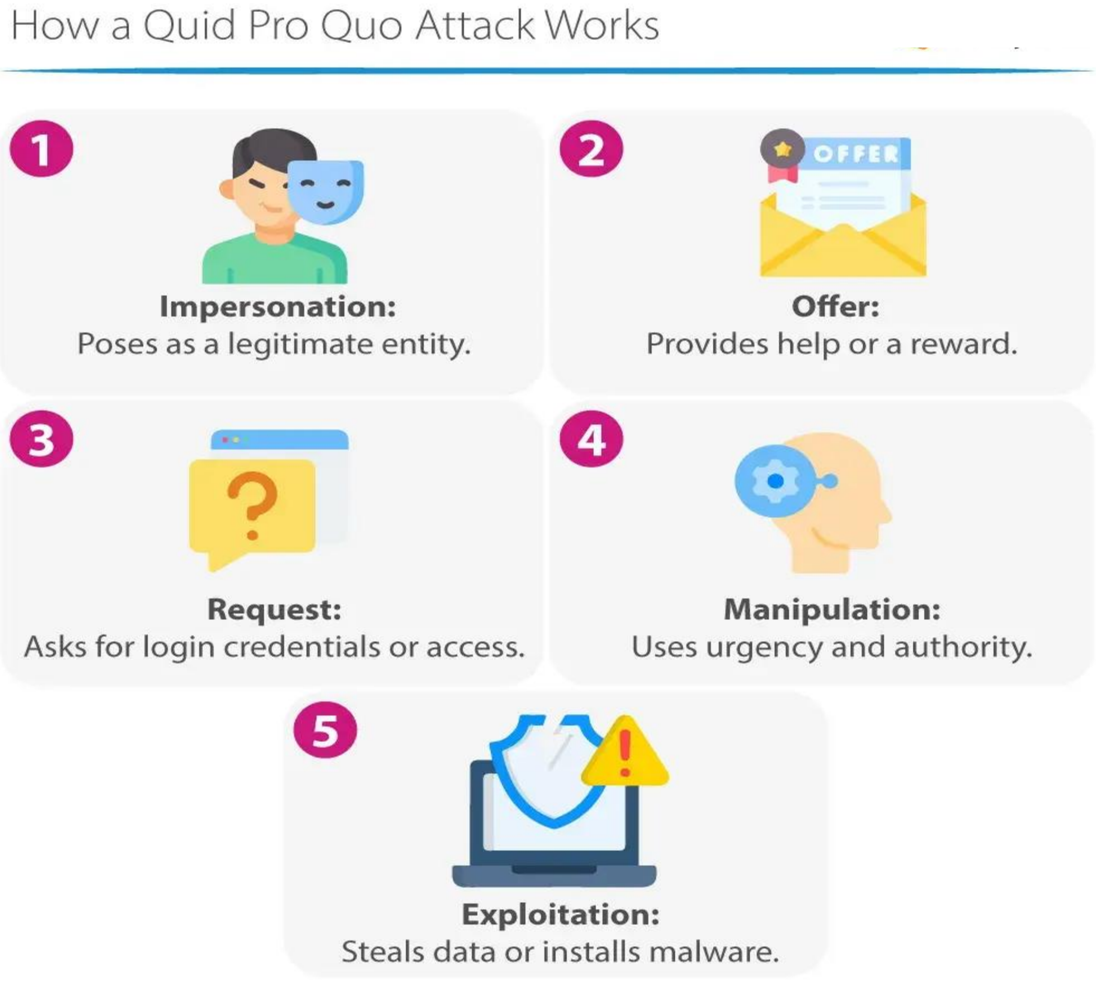
- RSA had a two-factor authentication product called SecurID
- The attackers sent two different phishing emails over a two-day period. The recipients were not high profile or high value targets, and the subject line of the email is "2011 Recruitment Plan".
- The email was well crafted and one of the employees opened the attached Excel file, which was a spreadsheet containing an Adobe Flash exploit
- Once inside the network, the attacker performed privilege escalation attacks to gain access to higher value administration accounts
- Eventually, the attackers managed to extract sensitive data, including the serial numbers of the SecurID token products

Social Engineering Tactics

- **Quid Pro Quo**
  - Something for something
- **Phishing**
  - Fraudulently obtaining private information
- **Baiting**
  - Real world Trojan horse
- **Pretexting**
  - Invented Scenario
- **Diversion Theft**
  - A con

Quid Pro Quo

- **Something for Something**



How a Quid Pro Quo Attack Works

1 **Impersonation:** Poses as a legitimate entity.

2 **Offer:** Provides help or a reward.

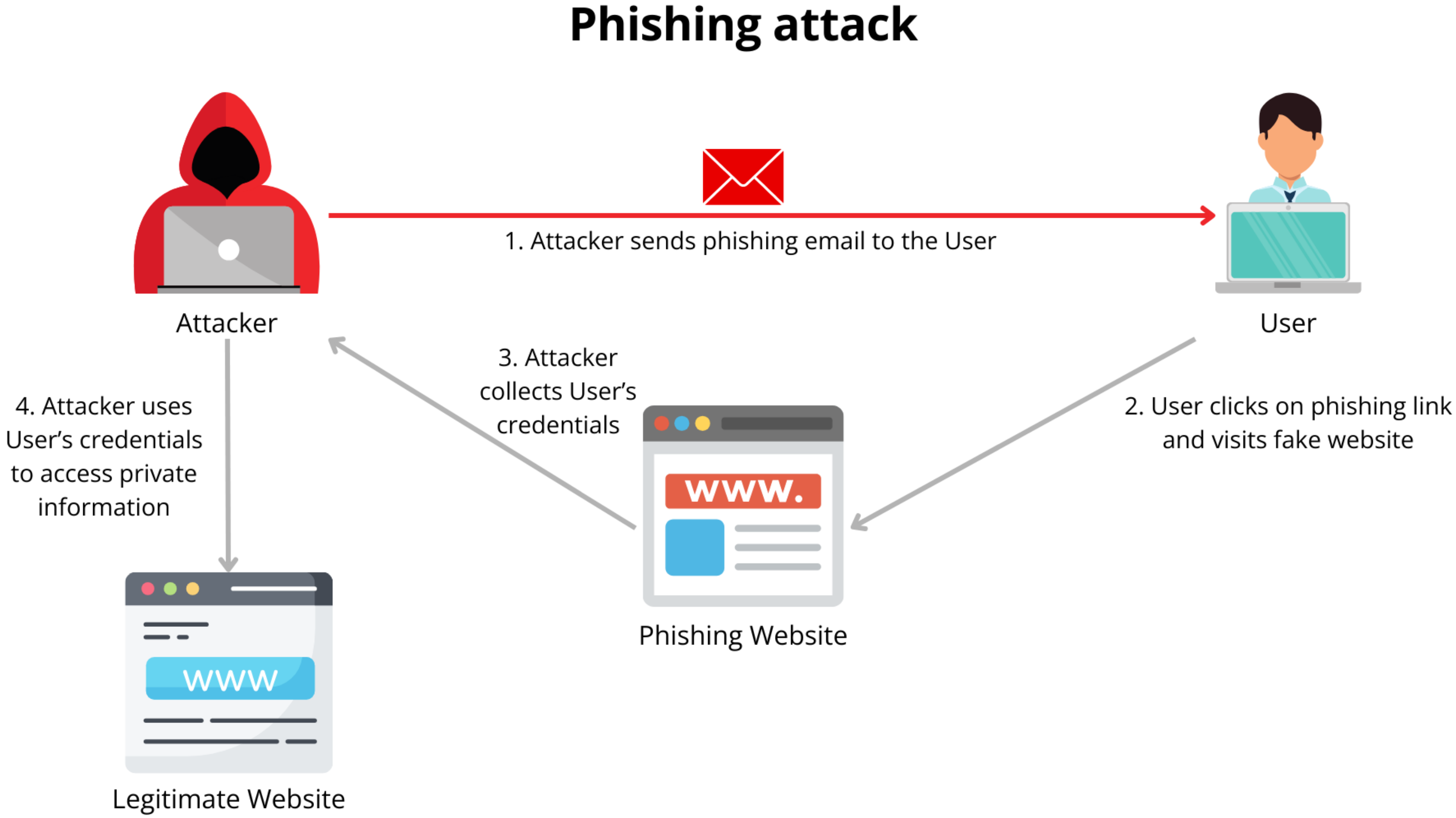
3 **Request:** Asks for login credentials or access.

4 **Manipulation:** Uses urgency and authority.

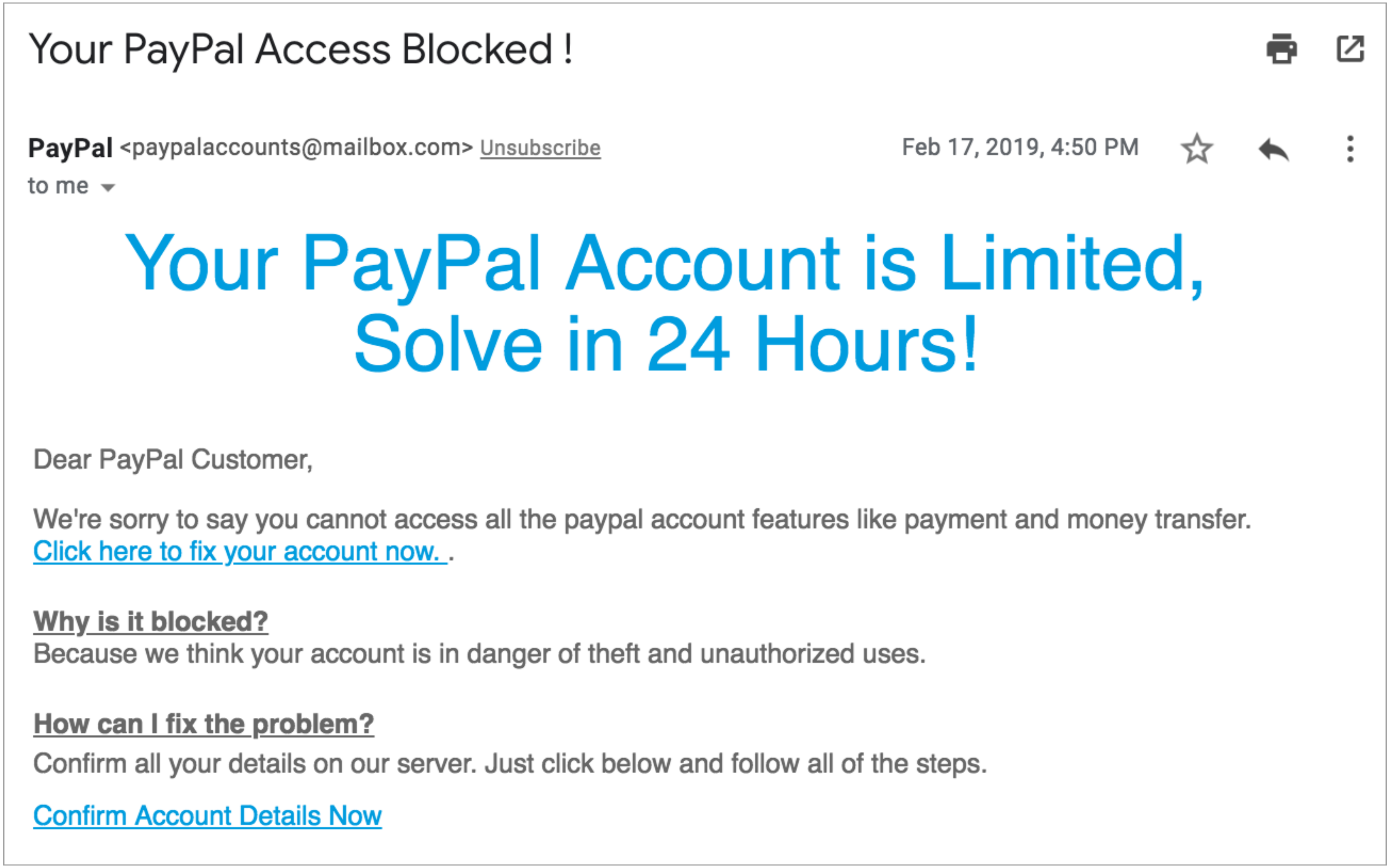
5 **Exploitation:** Steals data or installs malware.

Phishing

- **Fraudulently obtaining private information**


Phishing attack
Attacker
1. Attacker sends phishing email to the User
User
2. User clicks on phishing link and visits fake website
3. Attacker collects User's credentials
4. Attacker uses User's credentials to access private information
WWW.
Phishing Website
WWW
Legitimate Website

Phishing attack example



Your PayPal Access Blocked !

PayPal <paypalaccounts@mailbox.com> Unsubscribe Feb 17, 2019, 4:50 PM

to me

Your PayPal Account is Limited, Solve in 24 Hours!

Dear PayPal Customer,

We're sorry to say you cannot access all the paypal account features like payment and money transfer. Click here to fix your account now. .

Why is it blocked?
Because we think your account is in danger of theft and unauthorized uses.

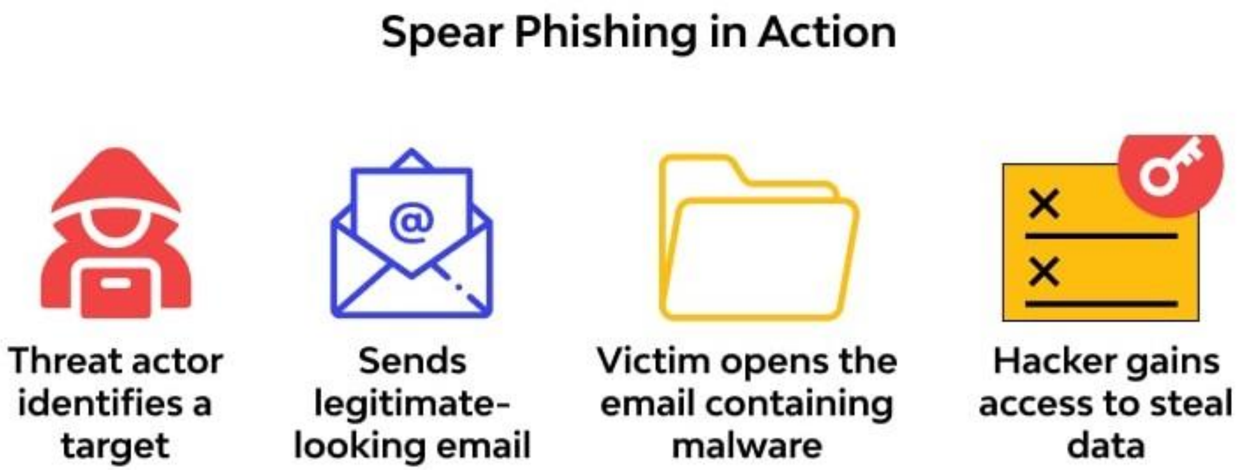
How can I fix the problem?
Confirm all your details on our server. Just click below and follow all of the steps.

Confirm Account Details Now

Characteristics of phishing attacks

- They seek to obtain personally identifiable information (PII), such as names, addresses and social security numbers
- They tend to use shortened URLs or embed links that redirect users to sites that appear legitimate
- They usually attempt to instill a sense of urgency in the user by using some sort of fear tactic or a threat in an attempt to get the user to act immediately

Spear phishing



Spear Phishing in Action

Threat actor identifies a target

Sends legitimate-looking email

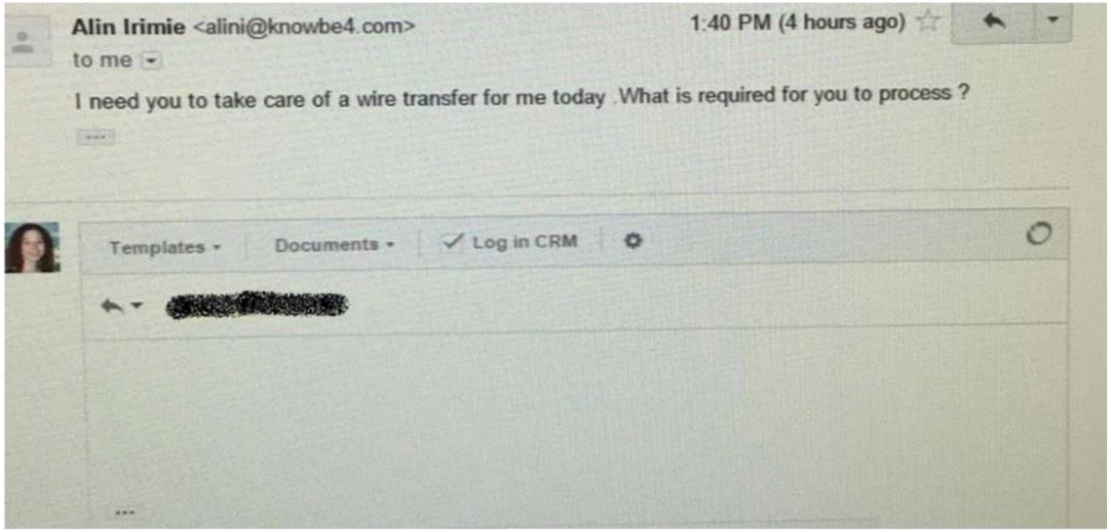
Victim opens the email containing malware

Hacker gains access to steal data

- Whereas phishing attacks tend be very scattered by nature (e.g., a phishing email can be sent to thousands of domains), spear phishing is much more targeted.
- Usually a spear phishing attack will focus on a single organization, a group of individuals within an organization, or even a single individual

Example of spear phishing attack

- KnowBe4, a Security Awareness Training and Simulated Phishing platform company in the Tampa, FL area, received a spear phishing email in September 2015
- It was received by KnowBe4's Controller allegedly from the "CTO" requesting a wire transfer.
- The Controller went to the CEO. The CEO decided to engage the attacker and to appear to comply with the request.



Alin Irimie <alini@knowbe4.com>

1:40 PM (4 hours ago)

to me

I need you to take care of a wire transfer for me today .What is required for you to process ?

[redacted]

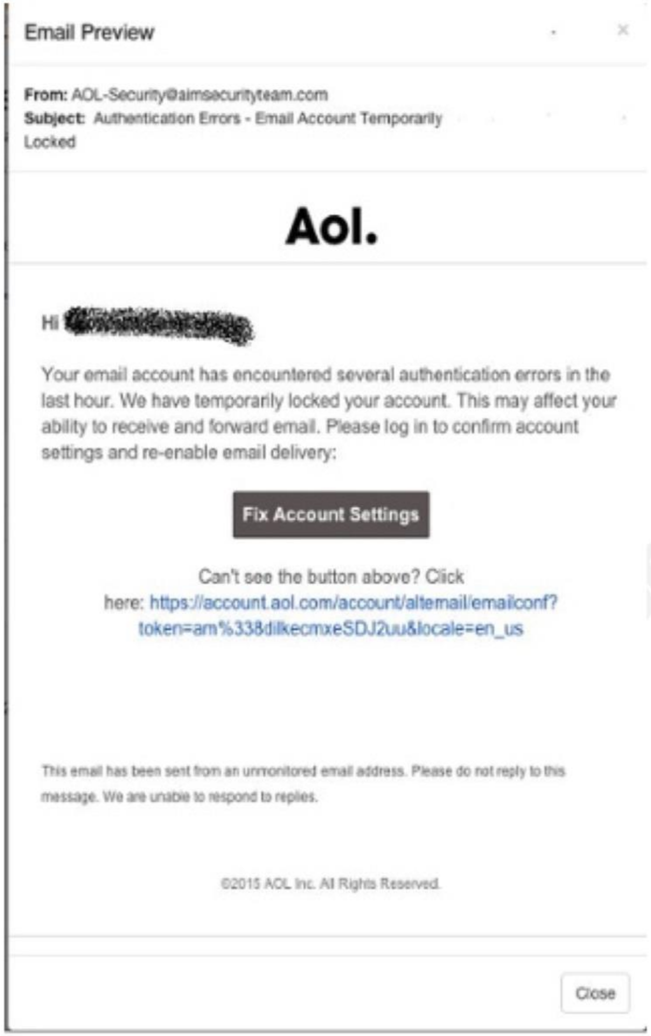
Example of spear phishing attack (cont'd)

- KnowBe4 analyzed the attacker's email.
  - The email headers revealed that the attacker created a hosting account with GoDaddy to get access to an email delivery system.
  - The attacker then used an open source mail client to spoof email headers and pick up the replied-to emails on an AOL account.

- The CEO had the Controller reply back and to the attacker and simply ask "How much and where to?"
- The attacker's reply back contained the bank wire information with real bank info but a fake company name and address.

Example of spear phishing attack (cont’d)

- KnowBe4 decided to phish back the attacker and created a fake AOL email account which claimed the attacker’s account was locked.
- The attacker then made a fatal error and clicked on the link which allowed KnowBe4 to get his IP address.
- This data was then sent over to the AOL security team and the FBI’s Internet Crime Complaint Center.



Email Preview

From: AOL-Security@aimsecurityteam.com
Subject: Authentication Errors - Email Account Temporarily Locked

Aol.

Hi [redacted]

Your email account has encountered several authentication errors in the last hour. We have temporarily locked your account. This may affect your ability to receive and forward email. Please log in to confirm account settings and re-enable email delivery:

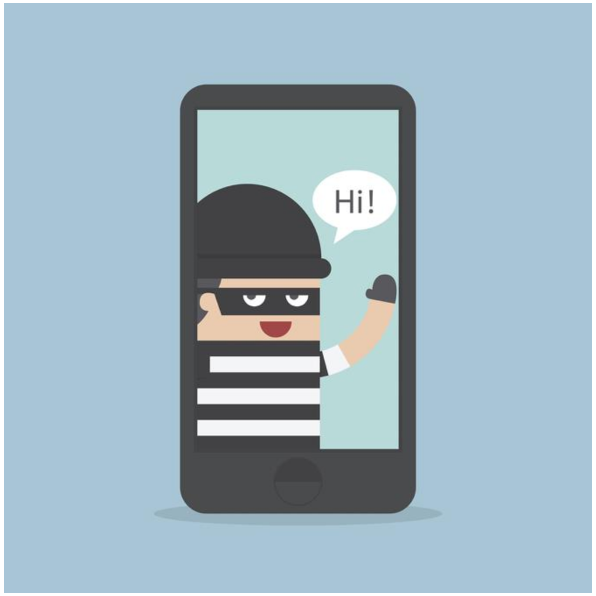
Can't see the button above? Click here: https://account.aol.com/account/altemail/emailconf?token=am%338dilkecmxeSDJ2uu&locale=en_us

This email has been sent from an unmonitored email address. Please do not reply to this message. We are unable to respond to replies.

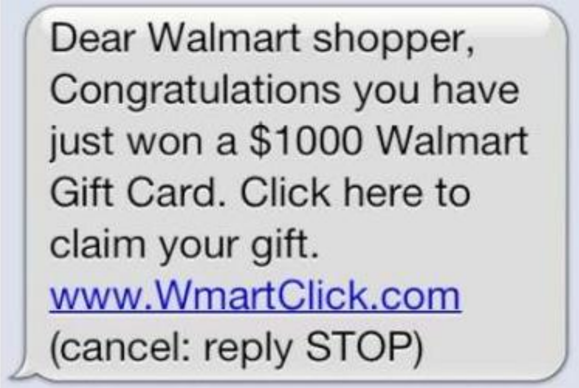
©2015 AOL Inc. All Rights Reserved.

Smishing

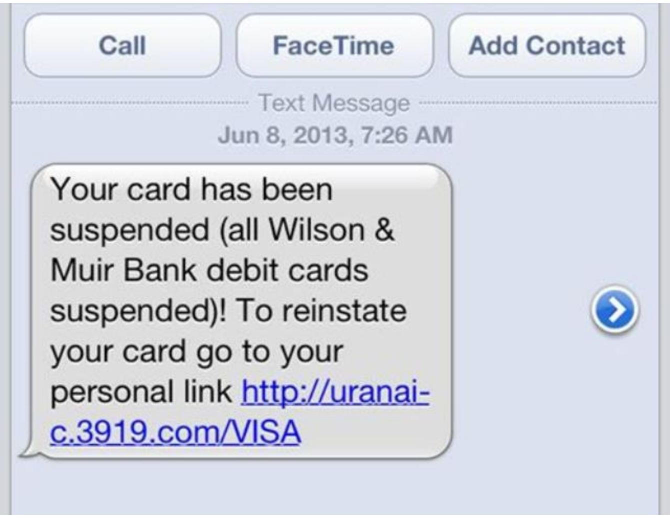
- Cell phone attacks typically using text messages to trick users into giving away personal information, or downloading a virus or malware



Smishing - Examples

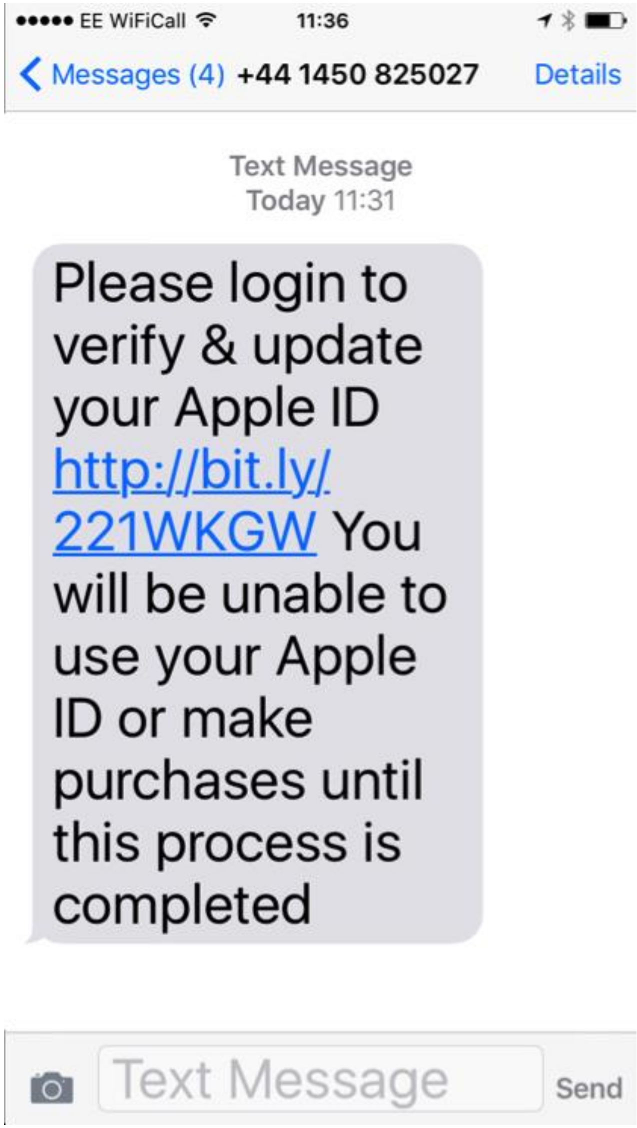


Dear Walmart shopper,
Congratulations you have just won a $1000 Walmart Gift Card. Click here to claim your gift.
www.WmartClick.com
(cancel: reply STOP)



Text Message
Jun 8, 2013, 7:26 AM

Your card has been suspended (all Wilson & Muir Bank debit cards suspended)! To reinstate your card go to your personal link http://uranai-c.3919.com/VISA

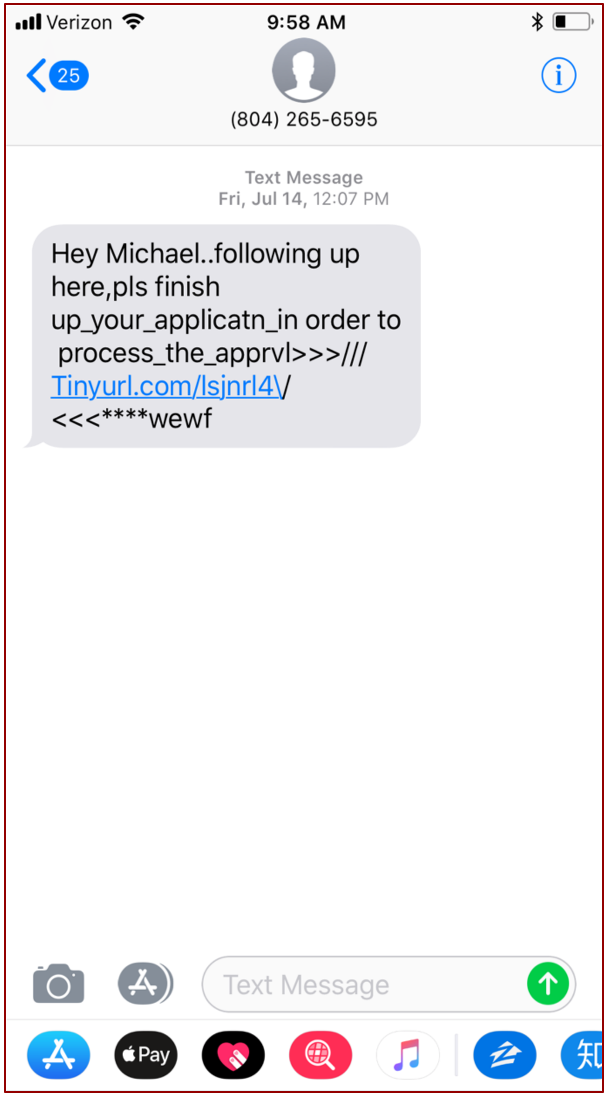


+44 1450 825027

Text Message
Today 11:31

Please login to verify & update your Apple ID http://bit.ly/221WKGW You will be unable to use your Apple ID or make purchases until this process is completed

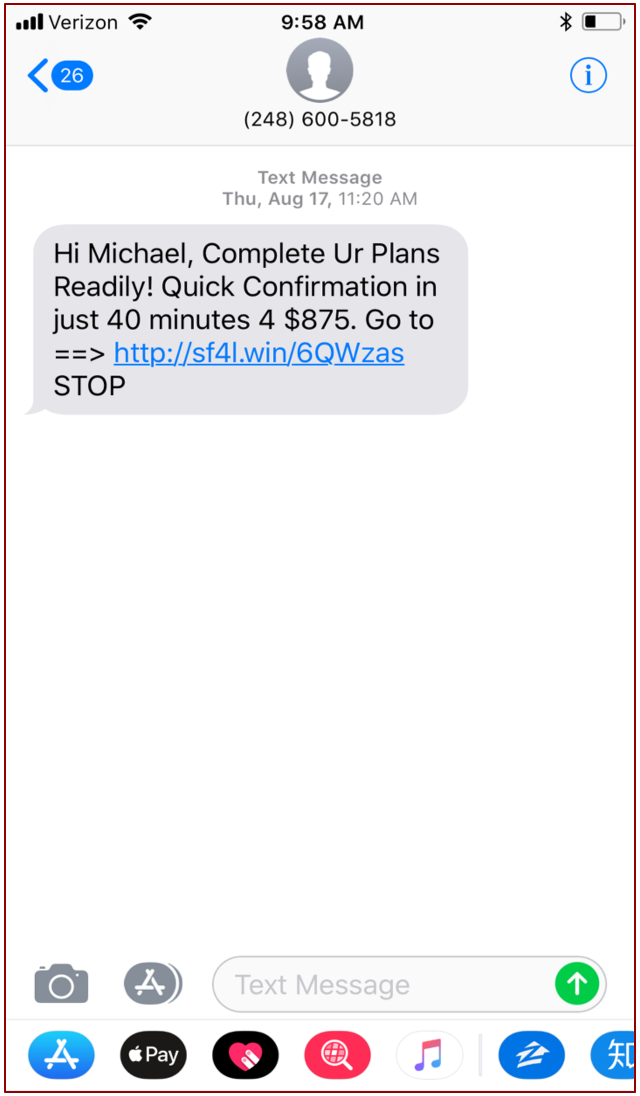
I also received these on my phone…



(804) 265-6595

Text Message
Fri, Jul 14, 12:07 PM

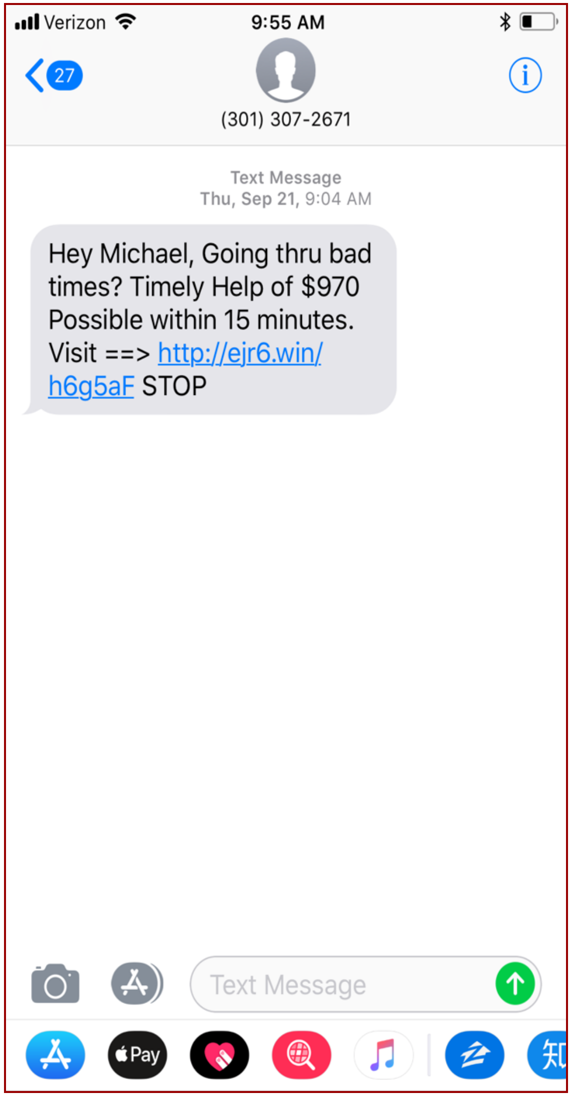
Hey Michael..following up here,pls finish up_your_applicatn_in order to process_the_apprvl>>>/// Tinyurl.com/lsjnrl4\/ <<<****wewf



(248) 600-5818

Text Message
Thu, Aug 17, 11:20 AM

Hi Michael, Complete Ur Plans Readily! Quick Confirmation in just 40 minutes 4 $875. Go to ==> http://sf4l.win/6QWzas STOP



(301) 307-2671

Text Message
Thu, Sep 21, 9:04 AM

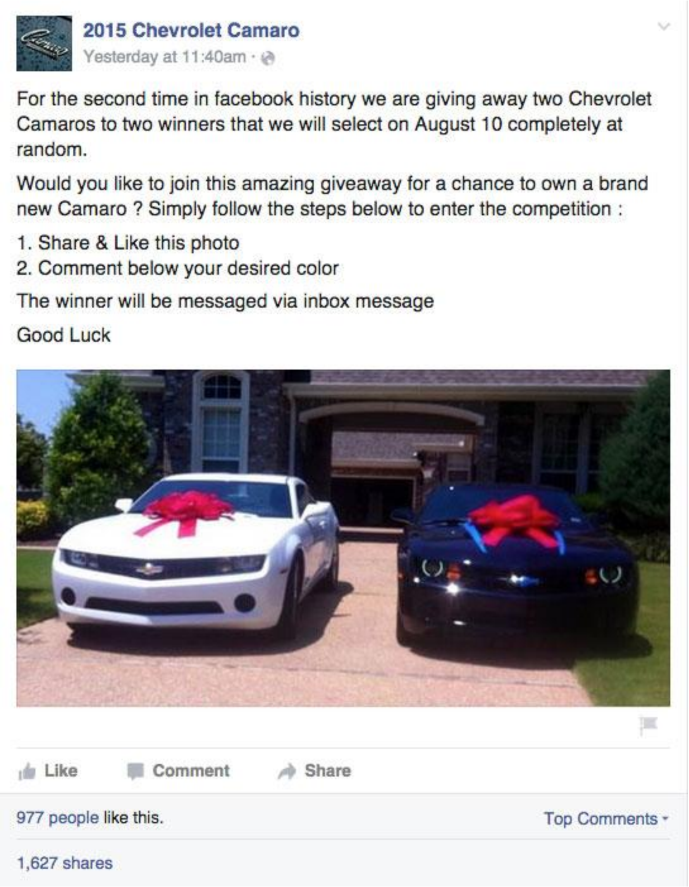
Hey Michael, Going thru bad times? Timely Help of $970 Possible within 15 minutes. Visit ==> http://ejr6.win/h6g5aF STOP

Facebook Phishing & Scams

- Messages or posts from hacked accounts such as friends or family

- Posts using tempting links for users to click on:
  - Free gift cards or discounted items
  - Donations for charity
  - Enticing videos or photos sometimes of yourself

Facebook Phishing & Scams



2015 Chevrolet Camaro
Yesterday at 11:40am ·

For the second time in facebook history we are giving away two Chevrolet Camaros to two winners that we will select on August 10 completely at random.

Would you like to join this amazing giveaway for a chance to own a brand new Camaro ? Simply follow the steps below to enter the competition :

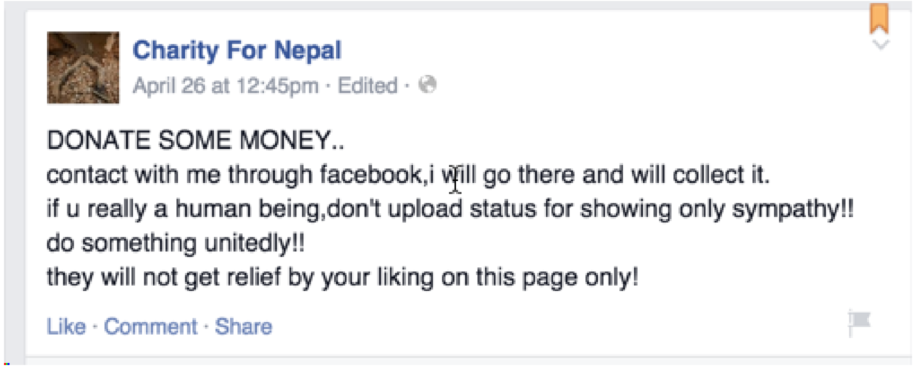
1. Share & Like this photo
2. Comment below your desired color

The winner will be messaged via inbox message

Good Luck

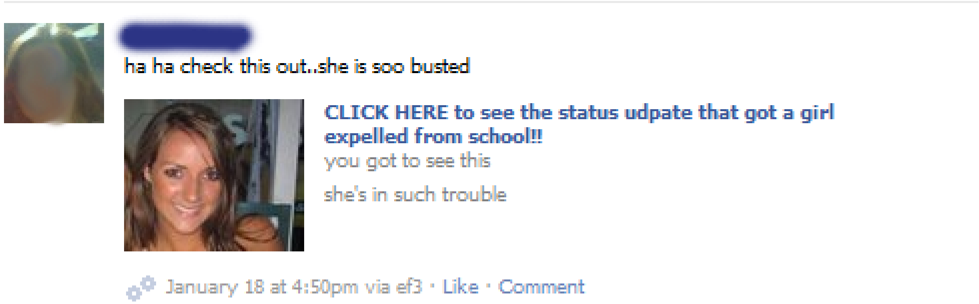
977 people like this.

1,627 shares



Charity For Nepal
April 26 at 12:45pm · Edited ·

DONATE SOME MONEY..
contact with me through facebook,i will go there and will collect it.
if u really a human being,don't upload status for showing only sympathy!!
do something unitedly!!
they will not get relief by your liking on this page only!



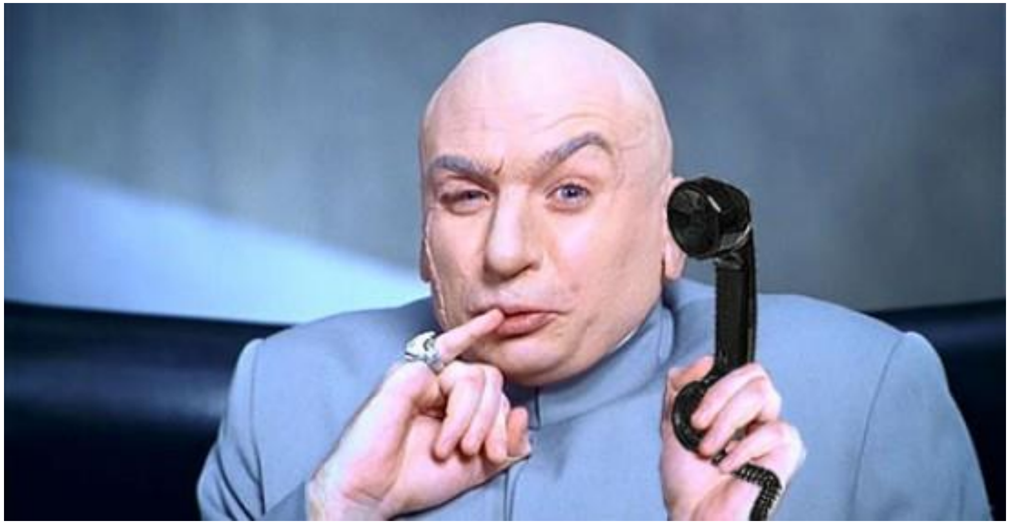
[redacted]
ha ha check this out..she is soo busted

CLICK HERE to see the status udpate that got a girl expelled from school!!
you got to see this
she's in such trouble

January 18 at 4:50pm via ef3 · Like · Comment

Vishing

- "Voice Phishing"
- Unsolicited phone calls
- Request for payment or personal information
- Sense of urgency such as fraud alert or virus

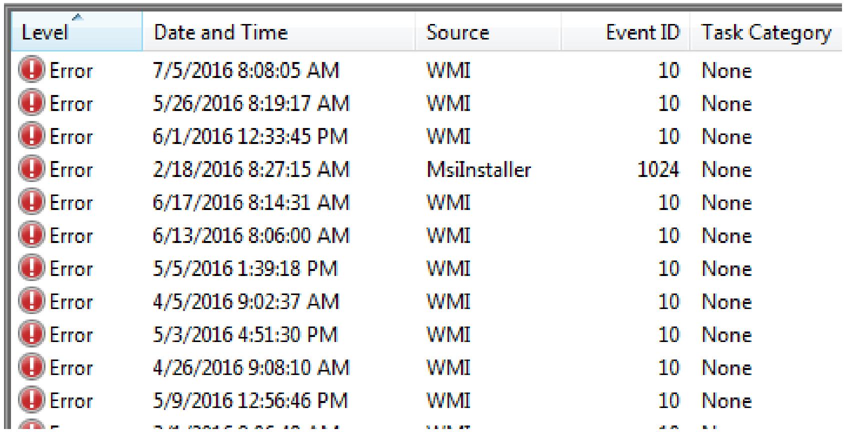


Vishing – why it works

- Can’t be blocked by filters
- Victim has less time to make a decision unlike email
- Phishers can talk with the victim and be convincing
- Phone calls maybe include topics like:
  - Computer troubles
  - Donations or late bills
  - Family members in trouble

Nick’s Vishing Example

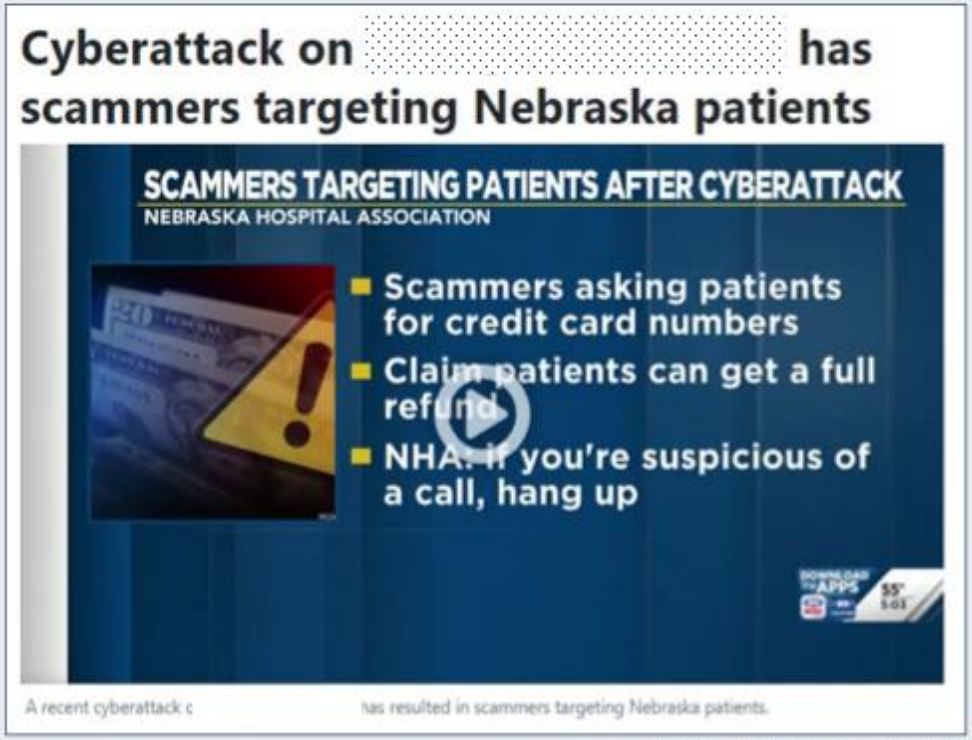
- Caller invested an hour attempting to convince Nick to let him into his computer
- Caller used event viewer to “confirm” an infection on his computer
- Transferred to a “specialist” and given instructions to install remote control software
  - Teamviewer
  - Gotomypc



Level	Date and Time	Source	Event ID	Task Category
Error	7/5/2016 8:08:05 AM	WMI	10	None
Error	5/26/2016 8:19:17 AM	WMI	10	None
Error	6/1/2016 12:33:45 PM	WMI	10	None
Error	2/18/2016 8:27:15 AM	MsiInstaller	1024	None
Error	6/17/2016 8:14:31 AM	WMI	10	None
Error	6/13/2016 8:06:00 AM	WMI	10	None
Error	5/5/2016 1:39:18 PM	WMI	10	None
Error	4/5/2016 9:02:37 AM	WMI	10	None
Error	5/3/2016 4:51:30 PM	WMI	10	None
Error	4/26/2016 9:08:10 AM	WMI	10	None
Error	5/9/2016 12:56:46 PM	WMI	10	None

Example of Vishing

March 2024: Phone Refund Scam



Cyberattack on [redacted] has scammers targeting Nebraska patients

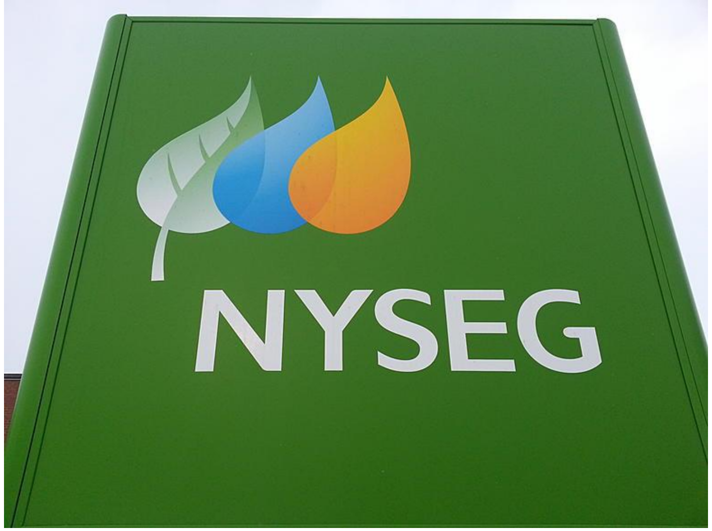
SCAMMERS TARGETING PATIENTS AFTER CYBERATTACK
NEBRASKA HOSPITAL ASSOCIATION

- Scammers asking patients for credit card numbers
- Claim patients can get a full refund
- NHA: if you're suspicious of a call, hang up

A recent cyberattack c has resulted in scammers targeting Nebraska patients.

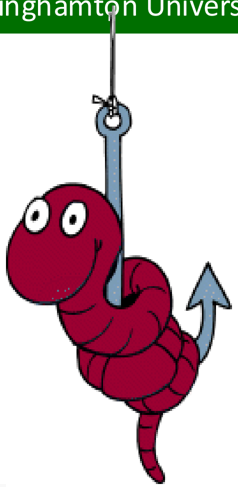
Image source: 10/11 NOW local news

My Vishing example: NYSEG

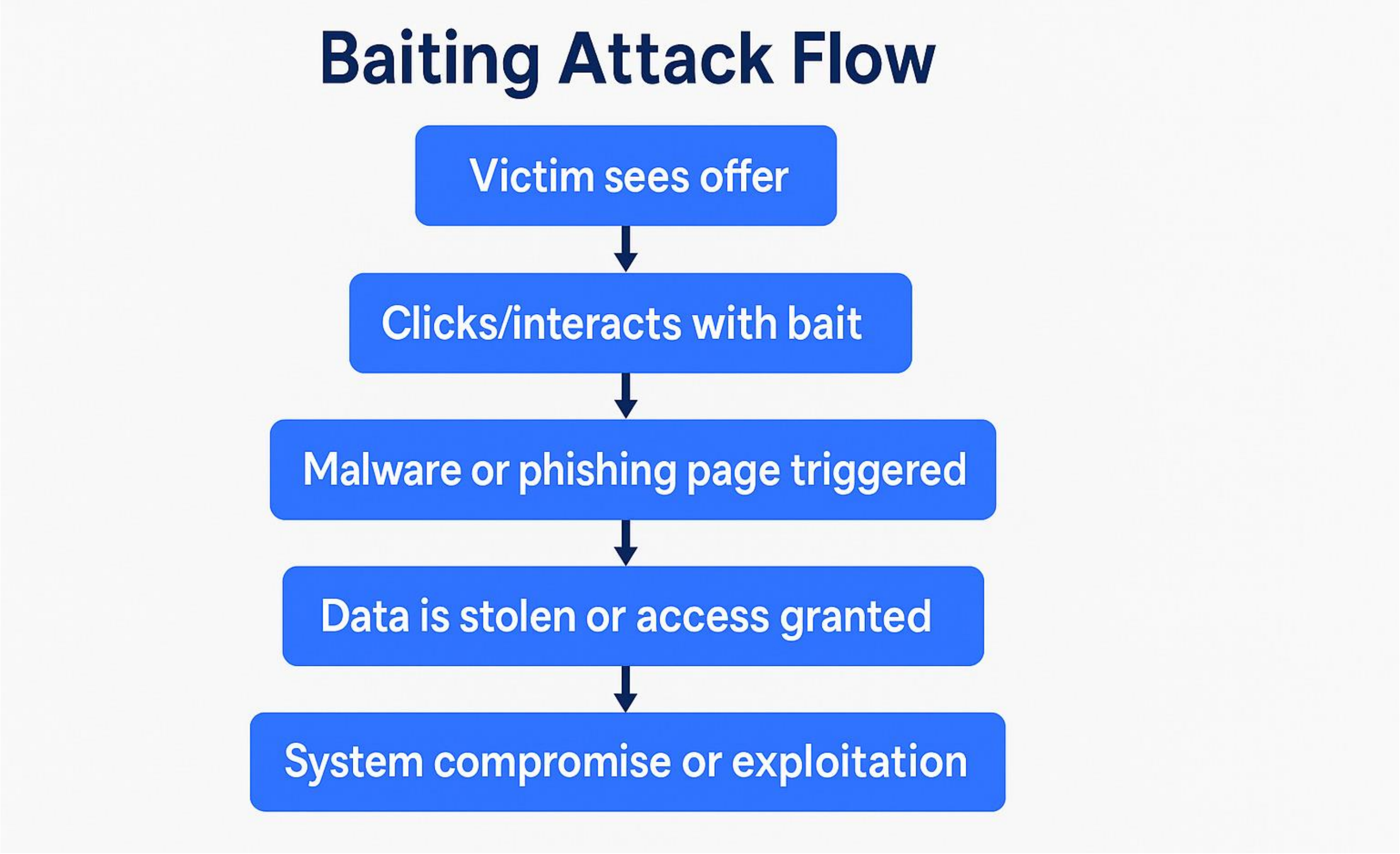


Almost duped into paying about $150 ☹

Baiting



- **Real world Trojan horse**



Baiting Attack Flow

Victim sees offer

Clicks/interacts with bait

Malware or phishing page triggered

Data is stolen or access granted

System compromise or exploitation

Key Targets of Baiting Attacks

Individuals

Why Targeted:

Take advantage of curiosity for free items.

Outcome:

Steal personal info, install malware.

Businesses

Why Targeted:

Access to sensitive corporate data.

Outcome:

Compromise systems, sell or exploit data.

Organizations

Why Targeted:

Access valuable data in government agencies and institutions.

Outcome:

Gain access to networks, steal or sell data.

Key Types of Baiting Attack Techniques

Tempting Offers

Attractive offers like free software or exclusive deals.

Malware - Infected Devices

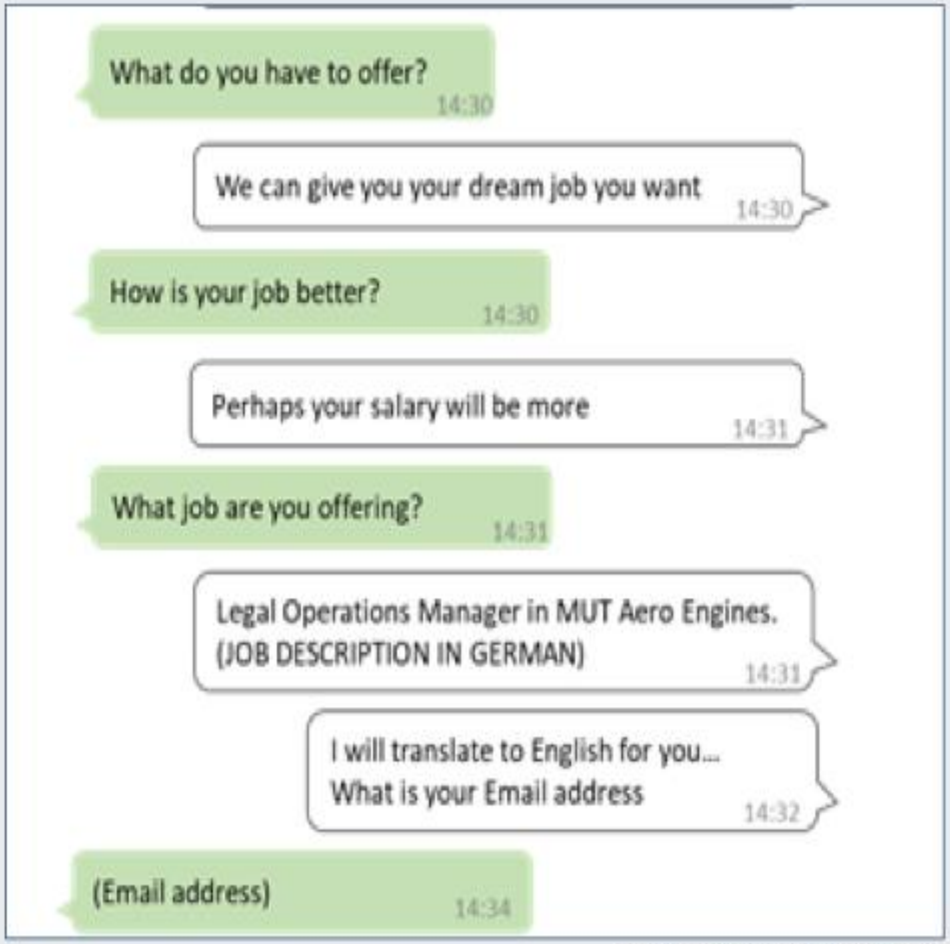
Infected USB drives left in public places.

Online Downloads

Fake websites offering free downloads.

Example of Baiting

Early 2020: Operation Dream Job (North Korean Cyber Espionage)



What do you have to offer? 14:30

We can give you your dream job you want 14:30

How is your job better? 14:30

Perhaps your salary will be more 14:31

What job are you offering? 14:31

Legal Operations Manager in MUT Aero Engines.
(JOB DESCRIPTION IN GERMAN) 14:31

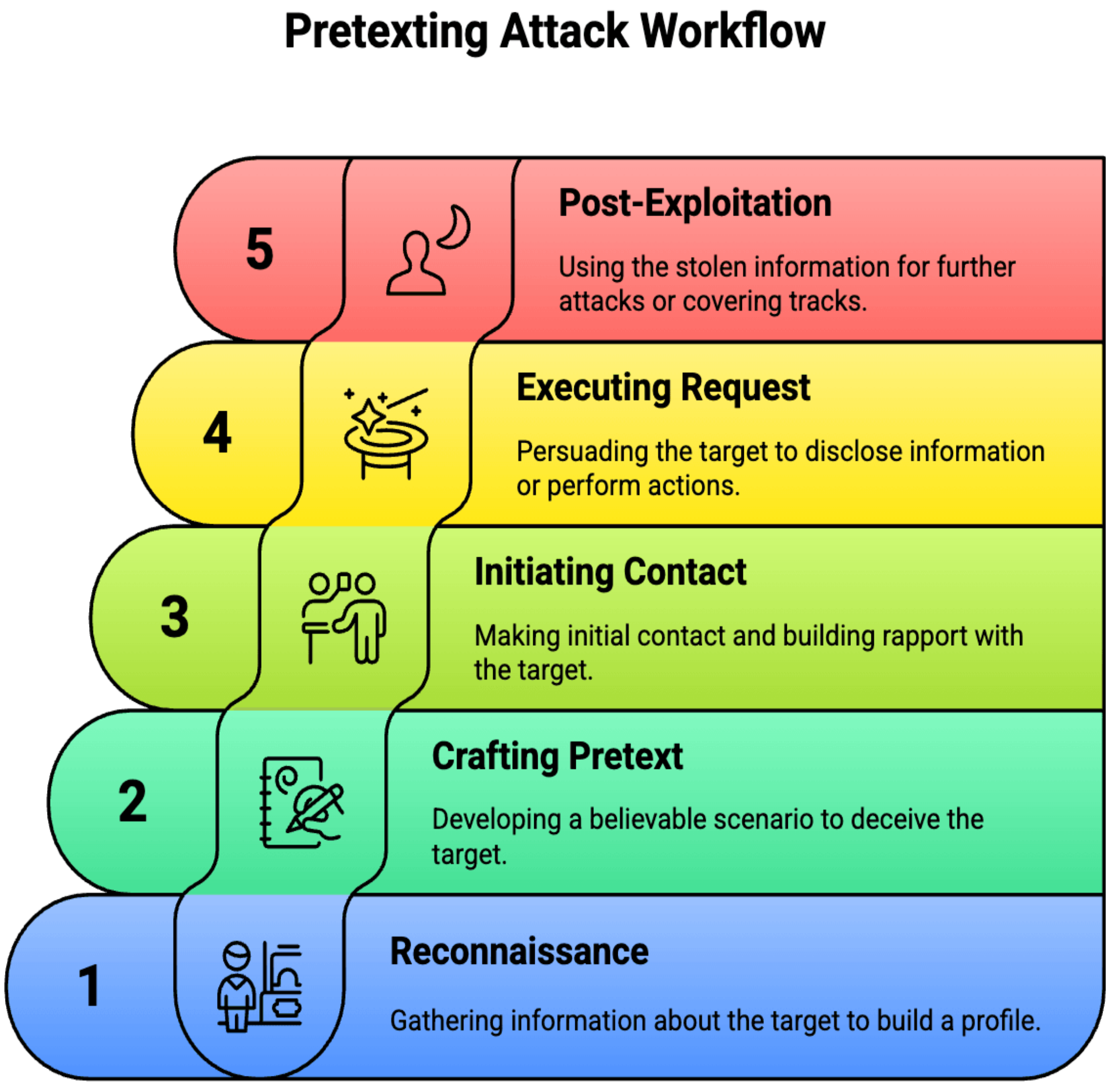
I will translate to English for you...
What is your Email address 14:32

(Email address) 14:34

Image source: ClearSky Cyber Security

Pretexting

- **Invented Scenario**



Pretexting Attack Workflow

5 **Post-Exploitation**
Using the stolen information for further attacks or covering tracks.

4 **Executing Request**
Persuading the target to disclose information or perform actions.

3 **Initiating Contact**
Making initial contact and building rapport with the target.

2 **Crafting Pretext**
Developing a believable scenario to deceive the target.

1 **Reconnaissance**
Gathering information about the target to build a profile.

The Most Common Pretexting Attacks

- **Grandparent scams:**
  - In this type of scam, a bad actor impersonates the victim’s grandchild or other close relative and attempts to convince them that they’re in a crisis.
  - For example, they may claim they’re in jail and need bail money.
  - The threat actor can spoof the caller ID and make the incoming call appear as though it’s coming from someone they know.
  - If the victim falls for the scam, the threat actor will give them instructions for sending the money.

The Most Common Pretexting Attacks

- **Romance scams**
  - Romance scams are when threat actors pretend to be an online love interest in order to win over their victim's trust.
  - This type of pretexting scam can take weeks, months or even years. Throughout the course of the scam, the threat actor will slowly start asking for things such as loans for an emergency or expensive gifts.
  - In 2022, the FBI's Internet Crime Complaint Center (IC3) received more than 19,000 complaints about romance scams, with reported losses of almost $740 million.

The Most Common Pretexting Attacks

- **CEO fraud**
  - CEO fraud is when a cybercriminal impersonates their target's CEO in an attempt to have them send money, often in the form of a gift card, or share sensitive information.
  - To carry out this attack, the threat actor leverages phishing techniques to make the matter sound urgent.
  - In some cases of CEO fraud, the bad actor will message or email the victim multiple times before making their request. This helps them build credibility and gain the victim's trust.

Pretexting Real Example:

- **Victim signed up for Free Credit Report**
- Saw **unauthorized charge** from another credit company
  - Called to **dispute charged** and was **asked for Credit Card Number**
    - They **insisted it was useless** without the security code
  - Asked for **Social Security number**

Diversion Theft: A Con

- Persuade delivery person that **delivery is requested elsewhere** - "*Round the Corner*"
- When deliver is redirected, attacker persuades delivery driver to **unload delivery near address**
- **Ex**: Attacker parks **security van outside a bank**. **Victims going to deposit money** into a night safe are told that the **night safe is out of order**. **Victims then give money to attacker** to put in the fake security van
- Most companies do not prepare employees for this type of attack

Role of Artificial Intelligence (AI)

Vishing Skyrockets Post-ChatGPT

- Since the launch of ChatGPT in November 2022, vishing, smishing, and phishing attacks have increased by a staggering 1,265%.
- Research from Enea reveals that 76% of enterprises lack sufficient voice and messaging fraud protection, as AI-powered vishing and smishing skyrocket following the launch of ChatGPT.
- Advancements in technology and AI are lowering the barrier to entry for cybercriminals and increasing the sophistication of attacks.
- Generative AI tools like ChatGPT are predicted to play a role in crafting more effective cyberattacks in 2024, especially in the area of social engineering.

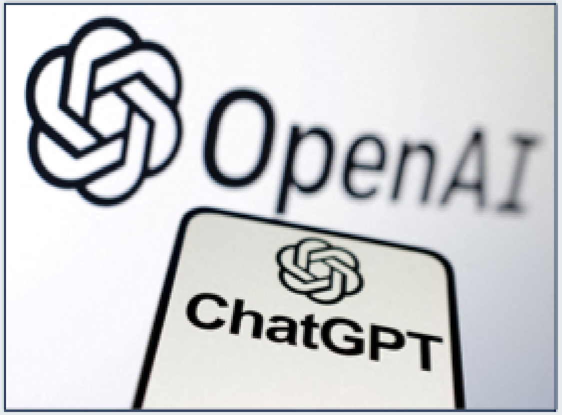
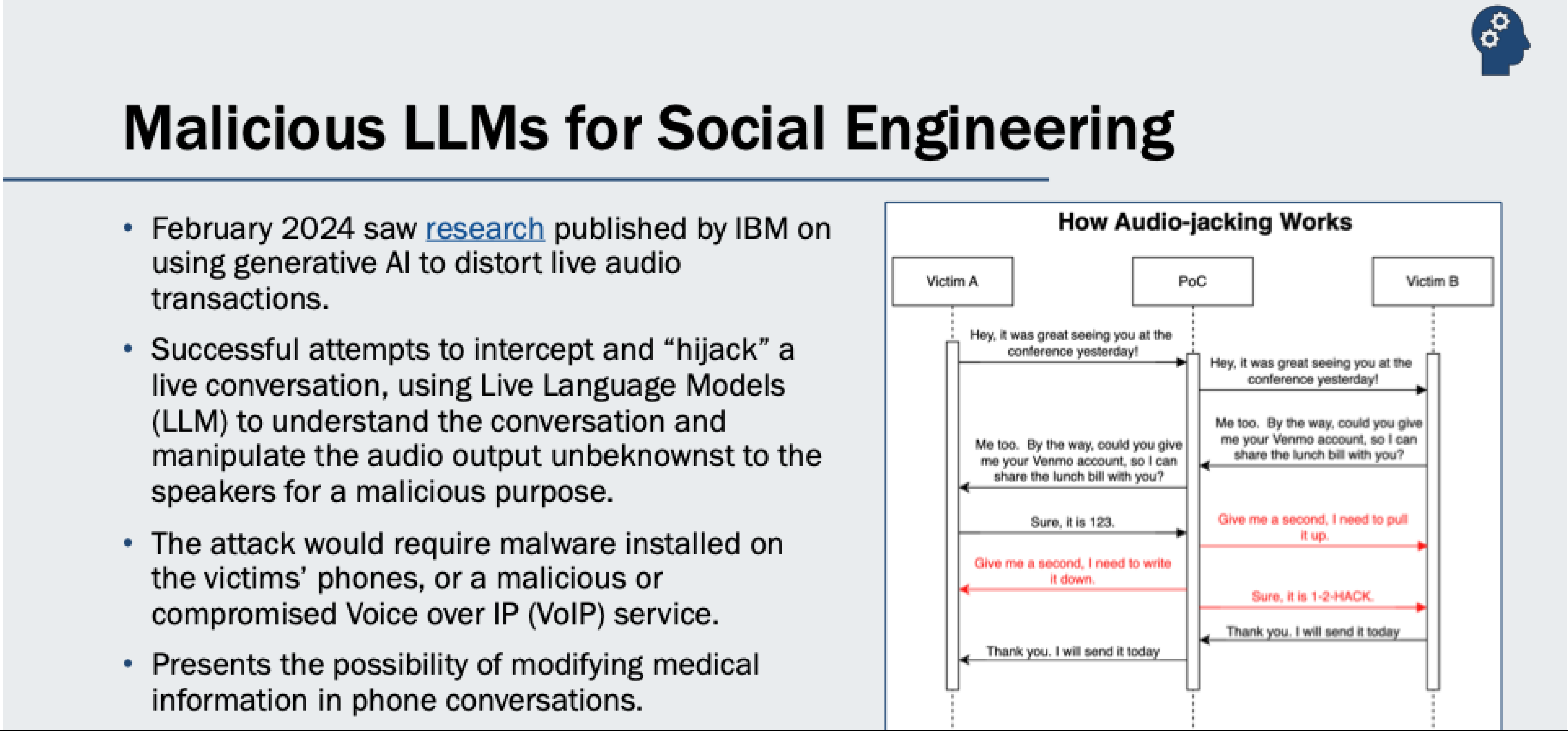


Image source: Reuters

AI Deepfake Video Call Scams

- In early 2024, scammers used artificial intelligence-powered "deepfakes" to pose as a multinational company's chief financial officer in a video call and were able to trick an employee into sending them more than $25 million, CNN reported.
- The scam began with a phishing email that was initially deemed somewhat suspicious, but the deepfake video call bolstered the threat actors' credibility and convinced the finance employee to transfer money to an offshore account.
- Likely sophisticated organized criminal organizations consisting of multiple individuals, supporting various roles throughout the duration of the scam.



Malicious LLMs for Social Engineering

- February 2024 saw research published by IBM on using generative AI to distort live audio transactions.
- Successful attempts to intercept and "hijack" a live conversation, using Live Language Models (LLM) to understand the conversation and manipulate the audio output unbeknownst to the speakers for a malicious purpose.
- The attack would require malware installed on the victims' phones, or a malicious or compromised Voice over IP (VoIP) service.
- Presents the possibility of modifying medical information in phone conversations.

How Audio-jacking Works

Victim A → PoC: Hey, it was great seeing you at the conference yesterday!

PoC → Victim B: Hey, it was great seeing you at the conference yesterday!

Victim B → PoC: Me too. By the way, could you give me your Venmo account, so I can share the lunch bill with you?

PoC → Victim A: Me too. By the way, could you give me your Venmo account, so I can share the lunch bill with you?

Victim A → PoC: Sure, it is 123.

PoC → Victim B: Give me a second, I need to pull it up.

PoC → Victim A: Give me a second, I need to write it down.

PoC → Victim B: Sure, it is 1-2-HACK.

Victim B → PoC: Thank you. I will send it today

PoC → Victim A: Thank you. I will send it today

Source: IBM X-Force

Malicious LLMs for Social Engineering, cont.

- **WormGPT:** Launched in 2021 and has been used extensively in business email compromise (BEC) attacks; writes convincing phishing emails.
- **FraudGPT:** Active since July 2023, and can create phishing pages, phishing emails, and phishing SMSs, among other capabilities.
- **WolfGPT:** Active since July 2023 and primarily focuses on supporting code and exploit development but may also be used for advanced phishing attacks.

Weakest Link?

- No matter how strong your:
  - Firewalls
  - Intrusion Detection Systems
  - Cryptography
  - Anti-virus software

- You are the weakest link in computer security!
  - People are more vulnerable than computers

- "*The weakest link in the security chain is the human element*"
  - Kevin Mitnick

Human is the weakest link in cyber security

- "What is fascinating—and disheartening—is that over 95 percent of all incidents investigated recognize '**human error**' as a contributing factor. "

– IBM Security Services 2014 Cyber Security Intelligence Index

IBM Global Technology Services
Managed Security Services

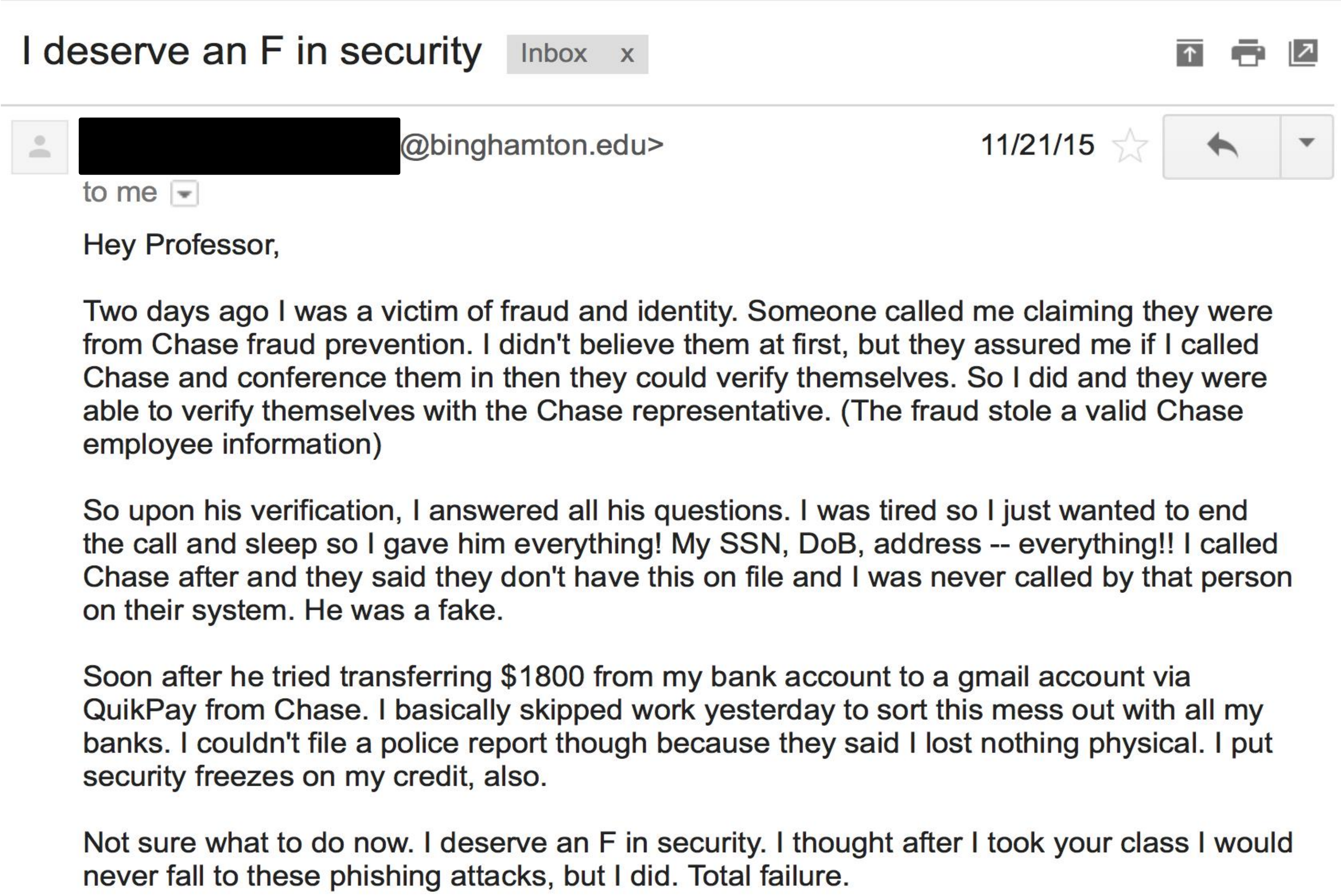
Research Report

IBM Security Services 2014
Cyber Security Intelligence Index

Analysis of cyber attack and incident data from IBM's worldwide security operations

IBM

Final story: “I deserve an F in security”



I deserve an F in security

[redacted]@binghamton.edu> 11/21/15

to me

Hey Professor,

Two days ago I was a victim of fraud and identity. Someone called me claiming they were from Chase fraud prevention. I didn't believe them at first, but they assured me if I called Chase and conference them in then they could verify themselves. So I did and they were able to verify themselves with the Chase representative. (The fraud stole a valid Chase employee information)

So upon his verification, I answered all his questions. I was tired so I just wanted to end the call and sleep so I gave him everything! My SSN, DoB, address -- everything!! I called Chase after and they said they don't have this on file and I was never called by that person on their system. He was a fake.

Soon after he tried transferring $1800 from my bank account to a gmail account via QuikPay from Chase. I basically skipped work yesterday to sort this mess out with all my banks. I couldn't file a police report though because they said I lost nothing physical. I put security freezes on my credit, also.

Not sure what to do now. I deserve an F in security. I thought after I took your class I would never fall to these phishing attacks, but I did. Total failure.

Summary of Offense-Based Cybersecurity

Lecture 1: Introduction

- What is security, information security, cybersecurity?
- Primary information security goals: CIA
- Secondary information security goals: AAA
- Challenges for science of cybersecurity

Lecture 2: Terminology and taxonomy

- Attack surface and vector
- Security risk analysis
- Security models

Lecture 3: Scanning and reconnaissance

- Public/online reconnaissance tools
- Port scanners
- Network mappers
- Operation system detection tools
- Firewall analysis tools
- Vulnerability scanners
- Packet sniffers
- Wireless sniffers

Lecture 4: Exploitation of network vulnerabilities

- Cache poisoning attacks
- Sniffing
- Denial of service attacks

Lecture 5: Exploitation of memory vulnerabilities

- **Stack-based attacks**

- *Heap-based attacks*

Lecture 6: Exploitation of system vulnerabilities

- **OS protection principes**
- *Privilege escalation: exploitation of a kernel bug*
- *Privilege escalation: race condition*

Lecture 7: Exploitation of hardware vulnerabilities

- Basics of computer architecture

- Side channel attacks based on caches

- Meltdown: out-of-order execution

- Spectre: speculative branch

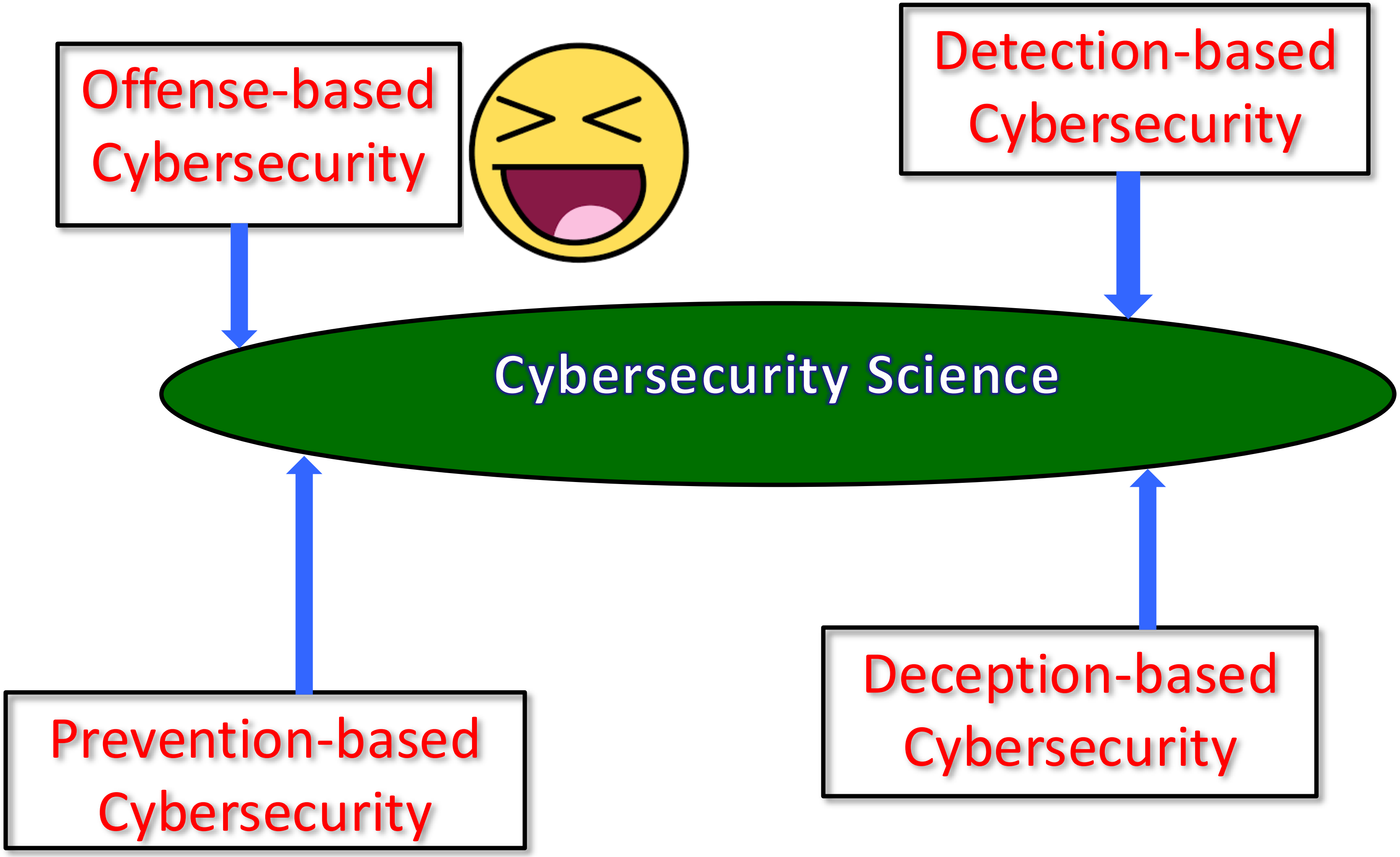
Lecture 8: Exploitation of web vulnerabilities

- Primer on web applications
- Same-origin policy
- XSS: cross-site scripting
- SQL injection
- XSRF: cross-site request forgery

Lecture 9: Exploitation of human vulnerabilities

- **What is Social Engineering Attack?**
- **Types of Social Engineering Tactics**
- **Role of AI in Social Engineering Attacks**

Overview of cybersecurity science



Offense-based Cybersecurity

Detection-based Cybersecurity

Cybersecurity Science

Prevention-based Cybersecurity

Deception-based Cybersecurity

Reminder: First Quiz

- 10-10:45AM 09/29
- Location: In classroom
- 25 True/False questions
- Closed-book

End of Lecture 9