COMP482
Cybersecurity
Week 8 - Monday

Dr. Nicholas Polanco

(he/him)

Attendance (Notecard)

Social Engineering Survey

1. Name(s)
2. How many “scams” or social engineering-type attacks do you receive on a **monthly** basis?
3. What are the most common types you receive (e.g., text message, email, phone calls)?
4. Do you feel confident in your ability to defend against them? How do you personally deal with these types of cybersecurity threats?
5. What is the best piece of media you have consumed in the past month (e.g., book, album, tv show, movie)?

Important Notes

- The extra credit will be due at midnight **the day after** the wifi has returned.
- All assignments should be added to kit for the rest of the term, please let me know if I am missing anything
- The instructions for the activity have been updated, but I haven’t been able to upload them to the server
  - I have a slide with the new instructions in this set of slides.

Important Dates (Week 8)

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Project Deliverable: Midway Report Extra Credit						

Outline

1. Introduction to Social Engineering
2. Phishing
3. Pretexting
4. Baiting
5. Defenses
6. Activity: Let’s go Phishing!

Introduction to Social Engineering

Introduction to Social Engineering

Social engineering is the manipulation of individuals into performing actions or divulging confidential information, often to gain unauthorized access to systems, networks, or data.

Why do you think social engineering remains one of the most effective attack methods despite advancements in cybersecurity technology?

Image Credit

Introduction to Social Engineering

Social engineering is the manipulation of individuals into performing actions or divulging confidential information, often to gain unauthorized access to systems, networks, or data.

Why do you think social engineering remains one of the most effective attack methods despite advancements in cybersecurity technology?

*Rather than exploiting technical vulnerabilities, social engineering targets human behavior, leveraging trust, fear, urgency, or curiosity to achieve the attacker's objectives.

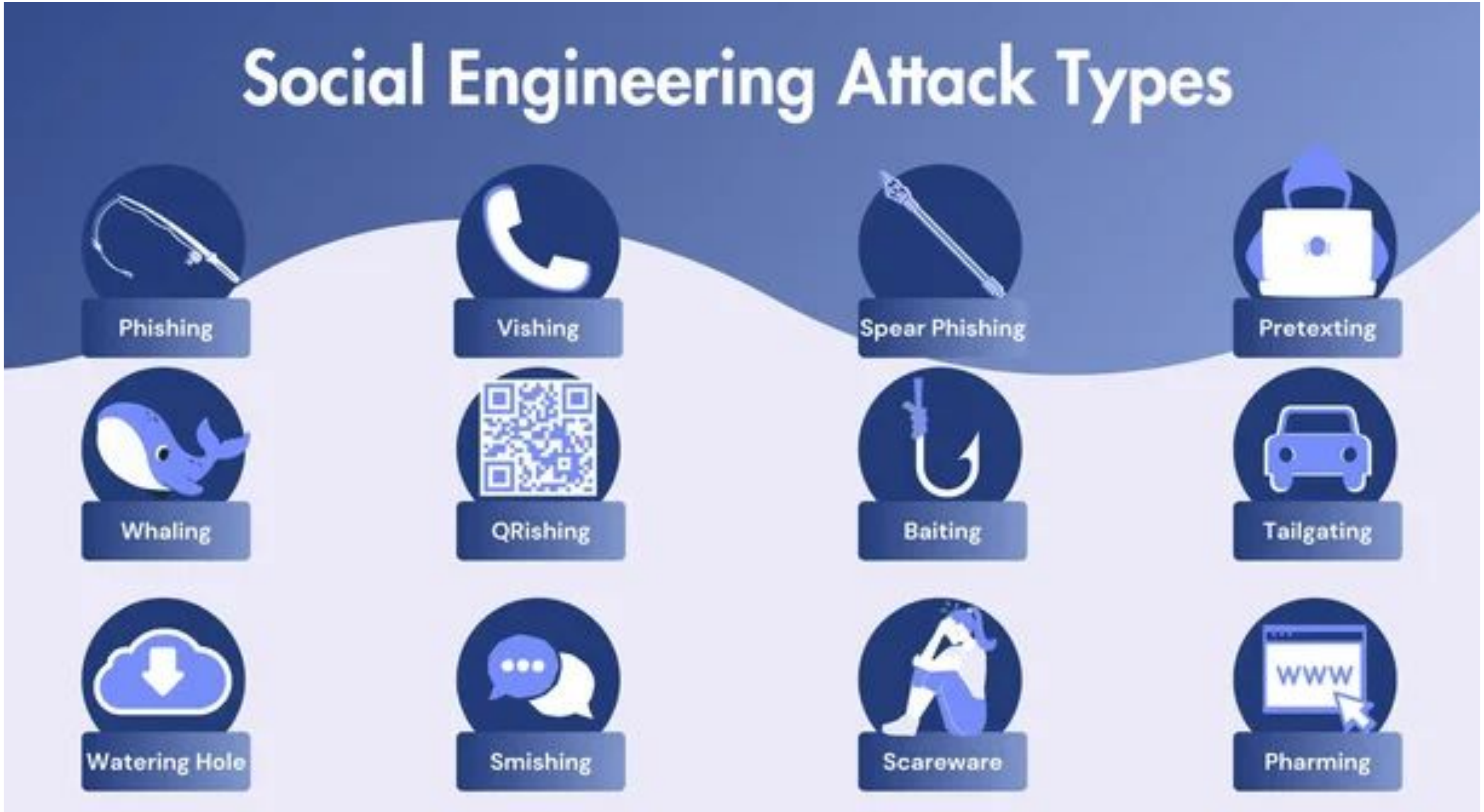


Image Credit
https://www.compassitc.com/blog/different-types-of-social-engineering-attacks-how-to-protect-yourself

Introduction to Social Engineering (continued)

Why Are These Dangerous?

1. Exploits Human Psychology

We can manipulate emotions like trust, fear, urgency, or curiosity.

2. Avoids Technical Detection

The tactics don’t involve code (in the direct aspect) that can be detected by firewalls, antivirus software, or intrusion detection systems.

Image Credit

Introduction to Social Engineering (continued)

Why Are These Dangerous? (continued)

3. Targets the "Human Layer" of Security

I think people are often the weakest link in cybersecurity. It only takes one mistake by a person to compromise an otherwise secure system.

4. Can Lead to Escalated Access

The attacks can attempt to gain basic access, then attackers escalate into more serious breaches (e.g., privilege escalation or lateral movement within a network).

Image Credit

Introduction to Social Engineering (continued)

<u>Why Are These Dangerous?</u> (continued)

5. Difficult to Prevent with Technology Alone

The technical defenses like firewalls and endpoint protection cannot fully prevent a user from voluntarily giving up credentials or clicking a malicious link if they’re tricked.

6. High Success Rate

The human element (often trusting and helpful)—especially in professional environments— has a higher likelihood of success compared to brute-force or technical attacks.

Image Credit

Introduction to Social Engineering (continued)

Why Are These Dangerous? (continued)

7. Often Part of a Larger Attack Chain

This is frequently the first step in a more complex attack, like malware, ransomware, or to even leverage a later attack like spear phishing.

Phishing

Phishing

Phishing is where attackers impersonate a trusted entity to deceive individuals into divulging sensitive information such as usernames, passwords, credit card numbers, or installing malware.

It typically involves deceptive communication, often via email, messaging apps, or websites, designed to appear legitimate but actually lead the victim to a malicious outcome.

*The term "phishing" is derived from "fishing," as attackers cast a "baited hook" hoping the victim will "bite."

Image Credit

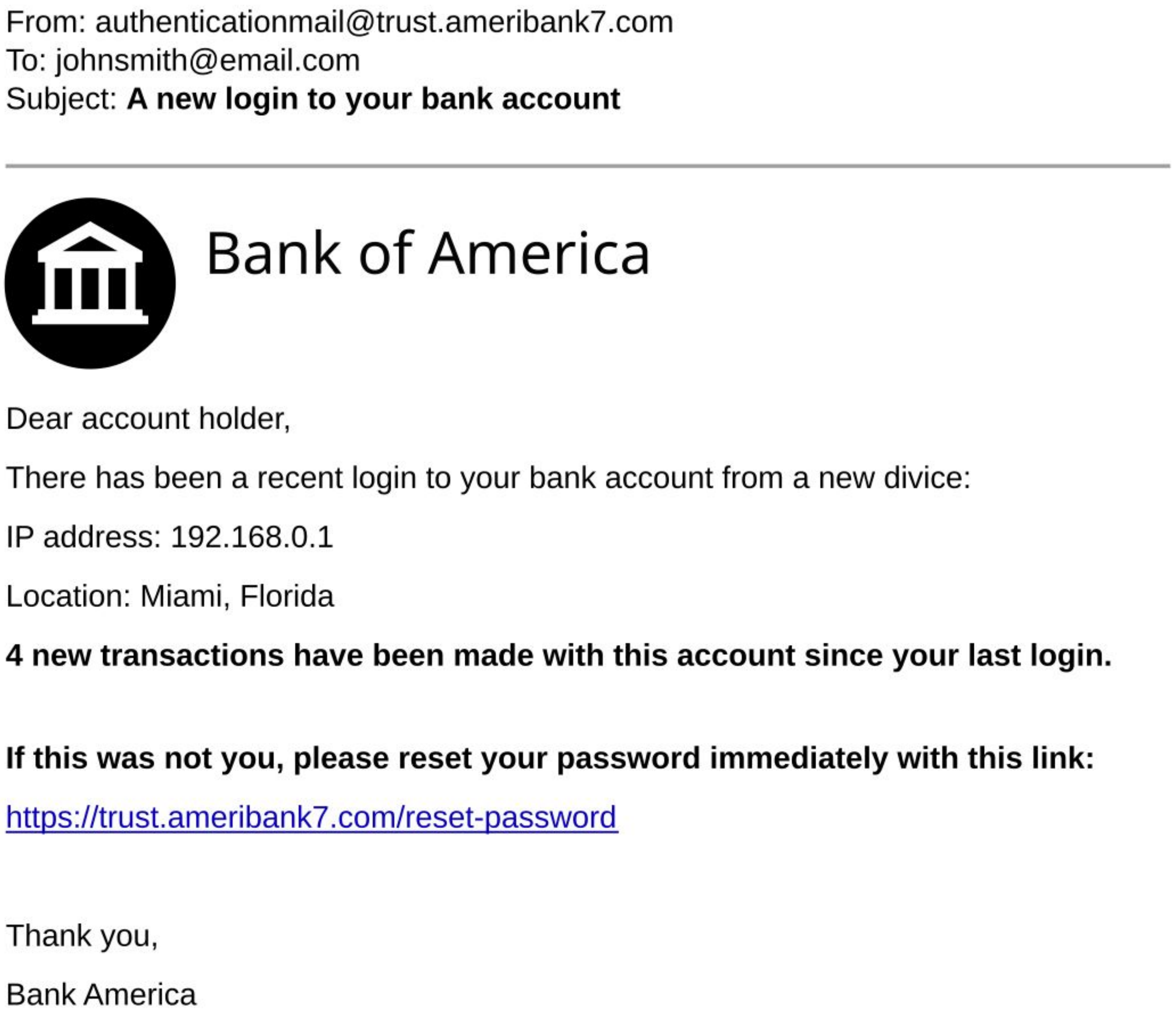
Phishing (continued)

Types of Phishing

1. Email Phishing - The attackers send emails that appear to come from reputable sources (banks, universities, tech companies).

- An email pretending to be from your college IT department asking you to "verify your account" by clicking a malicious link.

Image Credit



From: authenticationmail@trust.ameribank7.com
To: johnsmith@email.com
Subject: **A new login to your bank account**

Bank of America

Dear account holder,

There has been a recent login to your bank account from a new divice:

IP address: 192.168.0.1

Location: Miami, Florida

4 new transactions have been made with this account since your last login.

If this was not you, please reset your password immediately with this link:

https://trust.ameribank7.com/reset-password

Thank you,

Bank America

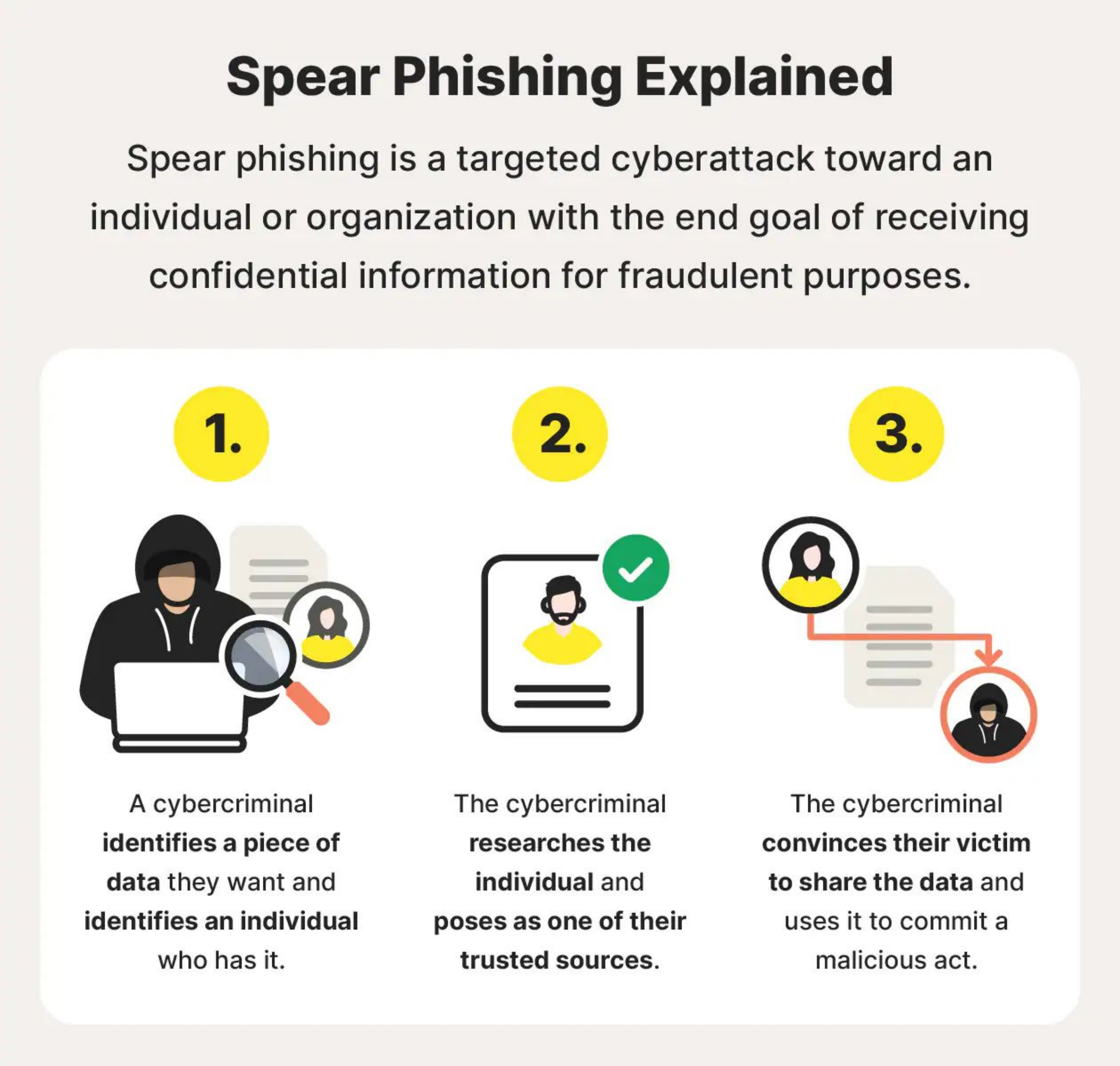
Phishing (continued)

Types of Phishing (continued)

2. Spear Phishing - These are just targeted attacks on specific individuals or organizations. They use personalized information (name, position, recent activities) to seem more legitimate.

- Example: We target a specific employee or position in a corporation.

Image Credit



Spear Phishing Explained

Spear phishing is a targeted cyberattack toward an individual or organization with the end goal of receiving confidential information for fraudulent purposes.

1. A cybercriminal **identifies a piece of data** they want and **identifies an individual** who has it.

2. The cybercriminal **researches the individual** and **poses as one of their trusted sources.**

3. The cybercriminal **convinces their victim to share the data** and uses it to commit a malicious act.

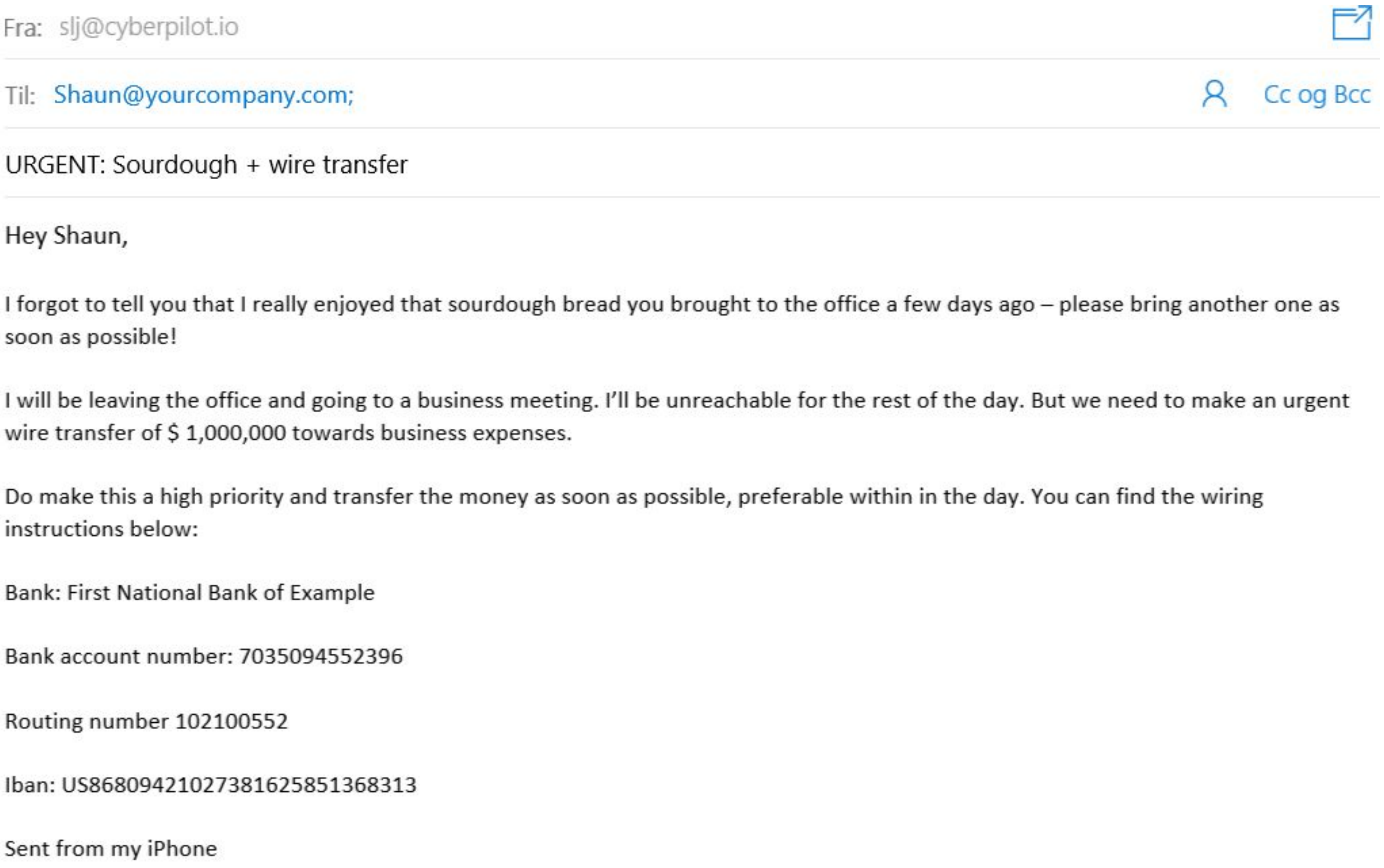
Image Credit
https://us.norton.com/blog/online-scams/spear-phishing

Phishing (continued)

Types of Phishing (continued)

3. Whaling - A type of spear phishing that targets high-level executives or important individuals (e.g., CFO, CEO).

- Example: We create messages tailored with executive-specific context, often requesting urgent financial transfers.



Fra: slj@cyberpilot.io

Til: Shaun@yourcompany.com;

URGENT: Sourdough + wire transfer

Hey Shaun,

I forgot to tell you that I really enjoyed that sourdough bread you brought to the office a few days ago – please bring another one as soon as possible!

I will be leaving the office and going to a business meeting. I'll be unreachable for the rest of the day. But we need to make an urgent wire transfer of $ 1,000,000 towards business expenses.

Do make this a high priority and transfer the money as soon as possible, preferable within in the day. You can find the wiring instructions below:

Bank: First National Bank of Example

Bank account number: 7035094552396

Routing number 102100552

Iban: US86809421027381625851368313

Sent from my iPhone

Image Credit
https://www.cyberpilot.io/cyberpilot-blog/what-is-whaling-and-how-to-prevent-it

KALAMAZOO COLLEGE

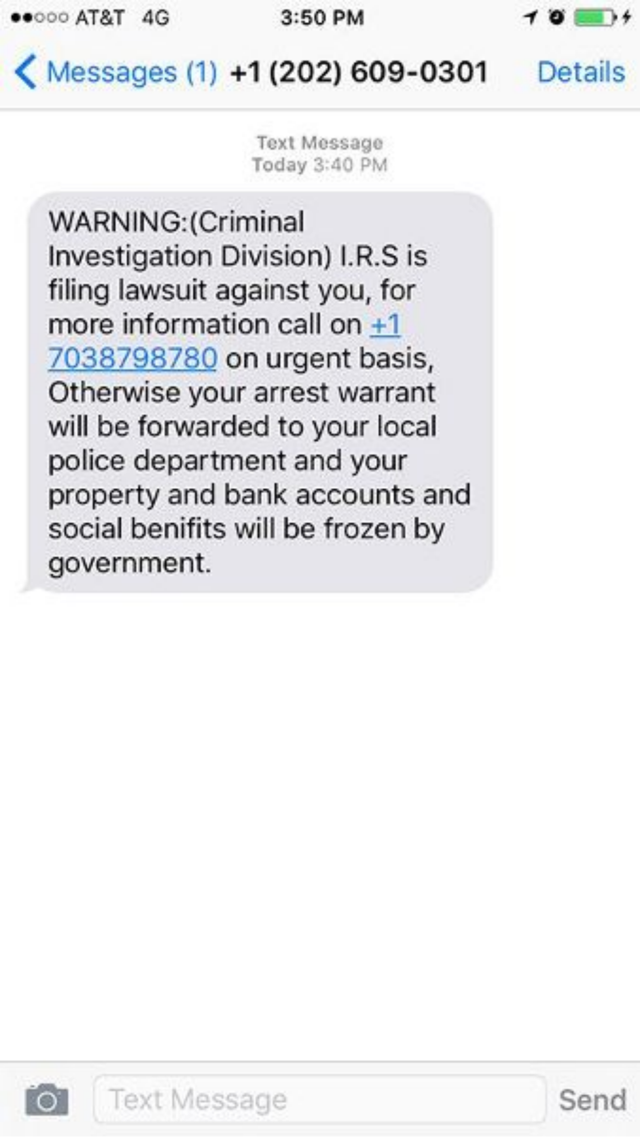
Phishing (continued)

Types of Phishing (continued)

4. Smishing (SMS Phishing) - We just use text messages instead of email.

- Example: "Your bank account is locked. Tap here to unlock: [malicious link]"

Image Credit



WARNING:(Criminal Investigation Division) I.R.S is filing lawsuit against you, for more information call on +1 7038798780 on urgent basis, Otherwise your arrest warrant will be forwarded to your local police department and your property and bank accounts and social benifits will be frozen by government.

Image Credit
https://www.proofpoint.com/us/threat-reference/smishing

Phishing (continued)

Types of Phishing (continued)

5. Vishing (Voice Phishing) - This is just involving phone calls instead of digital messages.

- Example: Attackers might impersonate a tech support rep, government official, or law enforcement agent to coerce victims into giving up sensitive info.

Image Credit

Image Credit
https://www.youtube.com/watch?v=xuYoMs6CLEw&t=52s&ab_channel=GarrettMyler

KALAMAZOO COLLEGE K

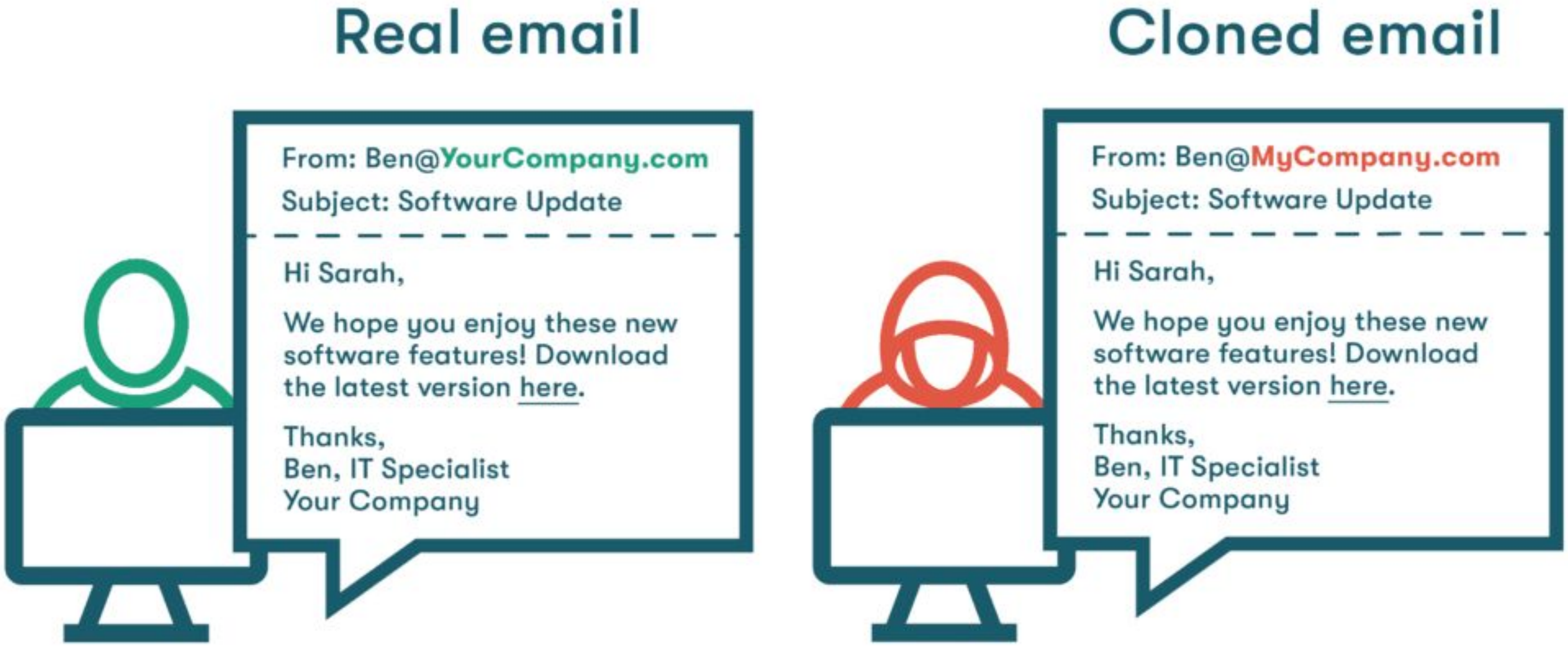
Phishing (continued)

Types of Phishing (continued)

6. Clone Phishing - A legitimate email is copied and modified, replacing a valid link or attachment with a malicious one.

- Example: A copy of an email from a real company is modified, a link is replaced, and it is forwarded along to a user.

Image Credit



Real email

From: Ben@YourCompany.com

Subject: Software Update

Hi Sarah,

We hope you enjoy these new software features! Download the latest version here.

Thanks,
Ben, IT Specialist
Your Company

Cloned email

From: Ben@MyCompany.com

Subject: Software Update

Hi Sarah,

We hope you enjoy these new software features! Download the latest version here.

Thanks,
Ben, IT Specialist
Your Company

Image Credit
https://www.dashlane.com/blog/what-is-clone-phishing

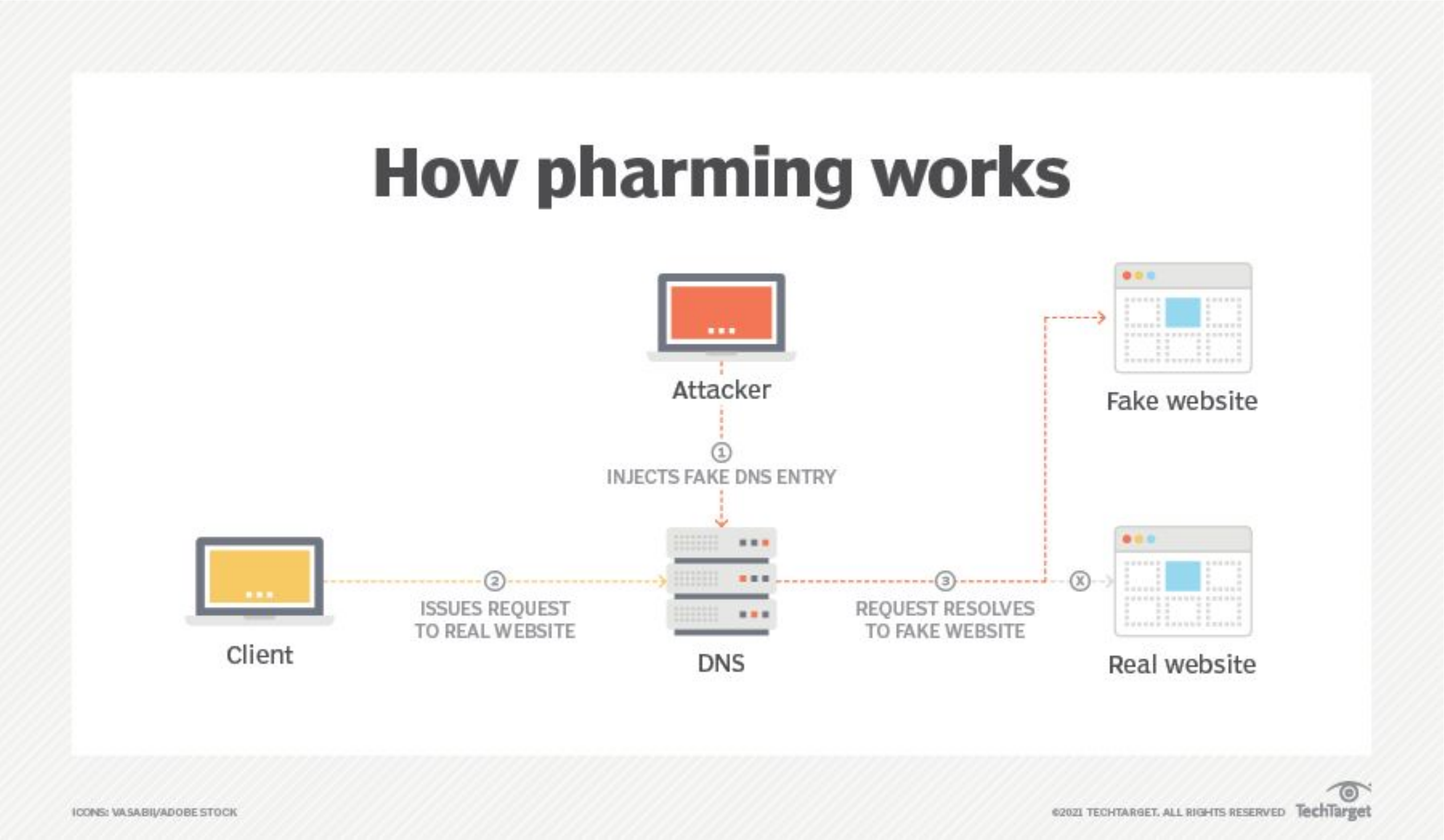
Phishing (continued)

Types of Phishing (continued)

7. Pharming - This is redirecting users from a legitimate website to a malicious one.

- Example: A victims enter their credentials into the fake site, thinking it’s real.

Does this feel like the same thing as another attack we have covered earlier this term?



How pharming works

Attacker
① INJECTS FAKE DNS ENTRY
Fake website
Client
② ISSUES REQUEST TO REAL WEBSITE
DNS
③ REQUEST RESOLVES TO FAKE WEBSITE
ⓧ
Real website

ICONS: VASABI/ADOBE STOCK

©2021 TECHTARGET. ALL RIGHTS RESERVED TechTarget

Image Credit
https://www.techtarget.com/searchsecurity/definition/pharming

Discussion Questions

Why do phishing attacks continue to be effective despite widespread awareness campaigns?

Is it possible to eliminate phishing entirely? Why or why not?

How do phishing attacks adapt to emerging technologies like AI and deepfakes? What does the future look like?

Image Credit

Pretexting

Pretexting

Pretexting is when the attacker creates a fabricated scenario—or pretext—to manipulate a target into divulging confidential or sensitive information.

Unlike phishing, which often casts a wide net, pretexting is more targeted and narrative-based, relying heavily on research, trust-building, and impersonation.

The attacker typically assumes a false identity (e.g., bank official, IT support, HR rep, law enforcement) and uses that cover story to make the interaction seem legitimate.

Image Credit

Pretexting (continued)

Key Characteristics:

1. Fabricated Persona or Storyline
   a. The attacker carefully crafts a believable backstory to justify their request.
2. Data Collection
   a. Pretexting often involves gathering specific details about the target in advance (job role, internal procedures, social connections).
3. One-on-One Interaction
   a. Typically conducted over the phone, email, or even in person; highly personalized.
4. Exploits Trust and Authority
   a. Attackers leverage perceived authority, urgency, or familiarity to lower the victim’s guard.

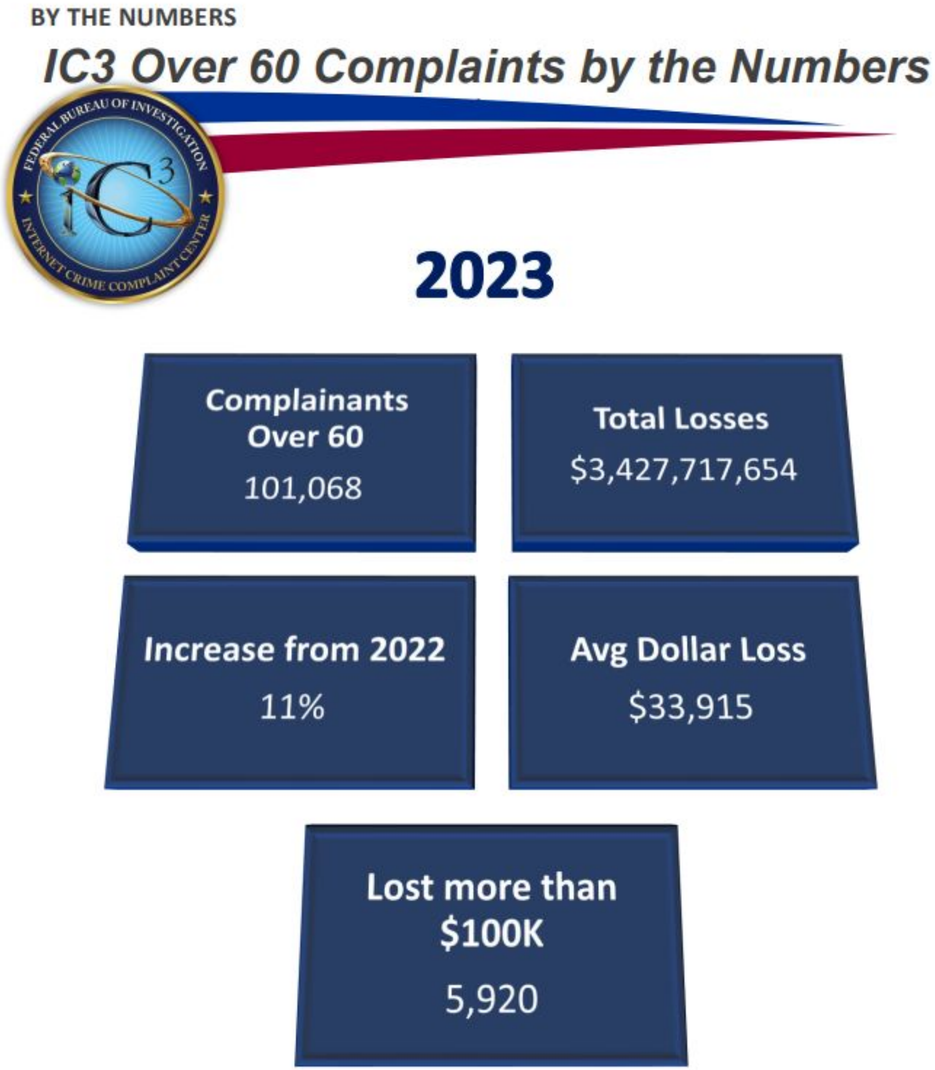
Pretexting (continued)

Example Scenarios:
IT Support - An attacker poses as a company's IT technician, saying they need the employee’s credentials to “run a critical update.”

Bank Official Scam - A person calls pretending to be from your bank, claiming suspicious activity and asking for account verification info.

HR Impersonation - A fraudster pretending to be from Human Resources calls a new employee to "update payroll" info—really to steal SSNs and bank details.

Image Credit



BY THE NUMBERS

IC3 Over 60 Complaints by the Numbers

2023

Complainants Over 60
101,068

Total Losses
$3,427,717,654

Increase from 2022
11%

Avg Dollar Loss
$33,915

Lost more than $100K
5,920

Image Credit
https://www.ic3.gov/AnnualReport/Reports/2023_IC3ElderFraudReport.pdf

Discussion Questions

How does pretexting differ from phishing in terms of method and psychological manipulation? How is it similar?

What factors make a pretexting attack more believable or successful? How can individuals train to spot them?

Should employees always verify identities—even those of internal colleagues or managers? What are the risks and benefits of doing so?

Image Credit

Baiting

Baiting

Baiting is where an attacker entices the victim with a tempting offer or object—the bait—in order to trick them into compromising their security.

<u>What are some things that attackers could use as bait?</u>

Image Credit

Baiting

Baiting is where an attacker entices the victim with a tempting offer or object—the bait—in order to trick them into compromising their security.

What are some things that attackers could use as bait?

The bait can be a physical item, a digital lure, or an “investment opportunity” that leads the target to install malware, reveal credentials, or open access to a secure environment.

Image Credit

Baiting (continued)

<u>Key Characteristics:</u>

1. Reward
2. Installation
   a. This isn't always necessary, but usually implants malware or opens a backdoor when the bait is accessed.
3. Action
   a. This can also requires user action, such as plugging in a device or clicking a link.
4. Information Extraction

Baiting (continued)

<u>Example Scenarios</u>

USB Drop Attack

- An attacker leaves infected USB drives in public places (e.g., parking lots, libraries, bathrooms). Then, individuals plug them into their computers, unintentionally installing malware or granting remote access.

Fake Download Links

- A website offers “free” versions of popular games, music, or software, but the download installs spyware or ransomware.

Online Giveaways

- This can be scam social media ads or emails offer “free gift cards” or products. Clicking the link leads to credential harvesting or malware.

Image Credit

Discussion Questions

How do cultural or situational factors (e.g., stress, workplace norms, urgency) influence the success of baiting attacks?

Would you consider baiting with digital rewards (e.g., fake app downloads) more or less dangerous than physical bait (e.g., USBs)? Why or why not?

Image Credit

Defenses

Defenses

Examples:

1. Security Awareness Training - We educate users about common tactics used in social engineering.

- What are some examples of how we could improve awareness?
- How often should we do this?

Defenses (continued)

Examples (continued):
2. Multi-Factor Authentication (MFA) - The credentials can be stolen through phishing or pretexting, and MFA can block unauthorized access.

3. Technical Controls - This can be any set of software/hardware-based security intended to secure users.

Image Credit

Defenses (continued)

Examples (continued):

4. Policies and Procedures

- Verification: We require confirmation for sensitive requests (e.g., wire transfers, password resets).
- Secure Physical Information: We prevent exposure of confidential info in physical spaces.
- Visitor Access Controls: We reduce risks of tailgating or impersonation.

Defenses (continued)

Examples (continued):
5. Principle of Least Privilege (PoLP) - We limit access to only what is necessary for a user's role.

6. Incident Response Readiness - We have clear reporting structure and rapid response process for suspected social engineering incidents.

- Do we want to encourage or punish our employees mistakes? Which do we think is more effective?

7. Behavioral Analytics & AI Tools - We use tools to detect anomalies in login behavior or communication patterns.

- Example: An unusual login location or urgent email from a normally slow-responding executive.

Discussion Questions

How can an organization measure the effectiveness of its social engineering defenses over time?

Which is more effective: user training or technical controls? You have to choose one. Why or why not?

Image Credit

Activity: Let’s Go Phishing

Activity: Let’s Go Phishing

You are going to create a fake phishing attack that is going to target Dr. Polanco. You must screenshot your fake phishing attack, and you can use either email or smishing (please don’t call me, smishing will require you to find my phone number). These are the guidelines:

1. You can *actually* try sending this to me, but you **cannot use a Kit** submission (I need to open all of those).
2. The link should just be to a YouTube video, keep it appropriate.
3. This is for purely academic purposes, it is meant to be fun. I may give a prize if someone successfully gets me to open the video.

You must screenshot your fake email and it should be submitted to kit along with the following questions (see next slide).

Image Credit

Activity: Let’s Go Phishing (continued)

1. What is the context of your phishing email (i.e., bank, IRS, etc.)?
2. What psychological techniques or social engineering tactics did you use in your message?
3. What visual or stylistic choices did you use to make the email look convincing?
4. What kind of YouTube video did you use to simulate this, and how did you disguise it?
5. How would a careful user detect that your email is a phishing attempt?
6. How did this exercise help you better understand phishing attacks and defenses?
7. If you were building an anti-phishing training program, what lesson or take away would you highlight based on your phishing attack?

Questions?