


PHISHING

Cybersecurity Awareness Training



Manipulation tactic designed to trick an individual to reveal sensitive/personal information, or to make them perform an action that they would not normally do.

SOCIAL ENGINEERING



Form of social engineering attack focused on stealing credentials or identity information.

The diagram consists of two dark blue chevron-shaped boxes pointing to the right, connected by a light blue chevron. The first box contains the text 'Form of social engineering attack focused on stealing credentials or identity information.' and the second box contains the text 'Uses a variety of communication media, including email and the web, in face-to-face interactions or over the phone.' The background is a solid blue color with some white diagonal lines in the bottom right corner.

Uses a variety of communication media, including email and the web, in face-to-face interactions or over the phone.

PHISHING

EXAMPLES OF PHISHING

From: Bank <Support@Citibanksecuremygateway.com>
Subject: Suspicious Activity



We've identified suspicious activity on your account. To secure your account, please click the link below to confirm your identity:
<https://secure.citibank-verification.com>

+63 910 023 9284

Hi there! I'm Emily from Indeed — hope I'm not catching you at a bad time.

We're currently hiring for a remote online position that pays \$100-\$600 per day.

✓ You'll work just 60-90 minutes daily, on your own schedule and from anywhere you like.

✓ Payment is made every day. Important: You must be at least 21 years old to apply.

If you meet this requirement and would like more details, please reply with "Yes" or "No."



Looking forward to your response!

The sender and other recipients are not in your contact list.

[Report Junk](#)

From: domain@domain-name.com
To: Your email
Subject: Apple Facetime Information Disclosure



National Security Department

A vulnerability has been identified in the Apple Facetime mobile applications that allow an attacker to record calls and videos from your mobile device without your knowledge.

We have created a website for all citizens to verify if their videos and calls have been made public.

To perform the verification, please use the following link:

[Facetime Verification](#)

This website will be available for 72 hours.

National Security Department

[PayPal]: Your account access has been limited

Team Support services@paypal-accounts.com
to me



Dear PayPal customer,

Your PayPal account is limited, You have 24 hours to solve the problem or your account will be permanently disabled.

We are sorry to inform you that you no longer have access to PayPal's advantages like purchasing, and sending and receiving money.

Why is my PayPal account limited?

We believe that your account is in danger from unauthorized users.

What can I do to resolve the problem?

You have to confirm all of your account details on our secured server by clicking the link below and following the steps.

[Confirm Your Information](#)

90% of all attacks begin with a phishing email.

57% of organizations experience phishing attacks daily or weekly.

Phishing is the most common entry point of ransomware attacks.

74% of security breaches involve human error or social engineering.

PHISHING STATISTICS

Several white lines of varying lengths and angles are positioned in the bottom right corner of the slide, creating a modern, abstract graphic element.

AUTHORITY – Respond to authority with obedience.

Email sent using an altered email of the CEO in which workers are informed that they must visit a specific website to fill out an important HR document.

SOCIAL ENGINEERING PRINCIPLES

INTIMIDATION – Authority, confidence or threat to motivate someone to follow orders or instructions.

Expanding on a previous email, it could include a statement claiming that employees could face penalty if they do not fill out the form promptly.

SOCIAL ENGINEERING PRINCIPLES

CONSENSUS – Taking advantage of a person's natural tendency to mimic what others are doing or have done in the past.

Attacker claiming that a worker who is currently out of the office promised a large discount on a purchase and that the transaction must occur with you as the salesperson.

SOCIAL ENGINEERING PRINCIPLES

SCARCITY – An object has a higher value based on the object's scarcity.

Attacker claiming that there are only two tickets left to your favorite team's game, and you should grab them now, or the opportunity will be lost. Often associated with urgency.

SOCIAL ENGINEERING PRINCIPLES

FAMILIARITY – Attempts to exploit a person's trust in that which is familiar (appearing to have mutual friends or experiences).

Attacker using phone with falsified caller ID as their doctor's office.

SOCIAL ENGINEERING PRINCIPLES

TRUST – Working on developing a relationship with a victim. Could take seconds or months.

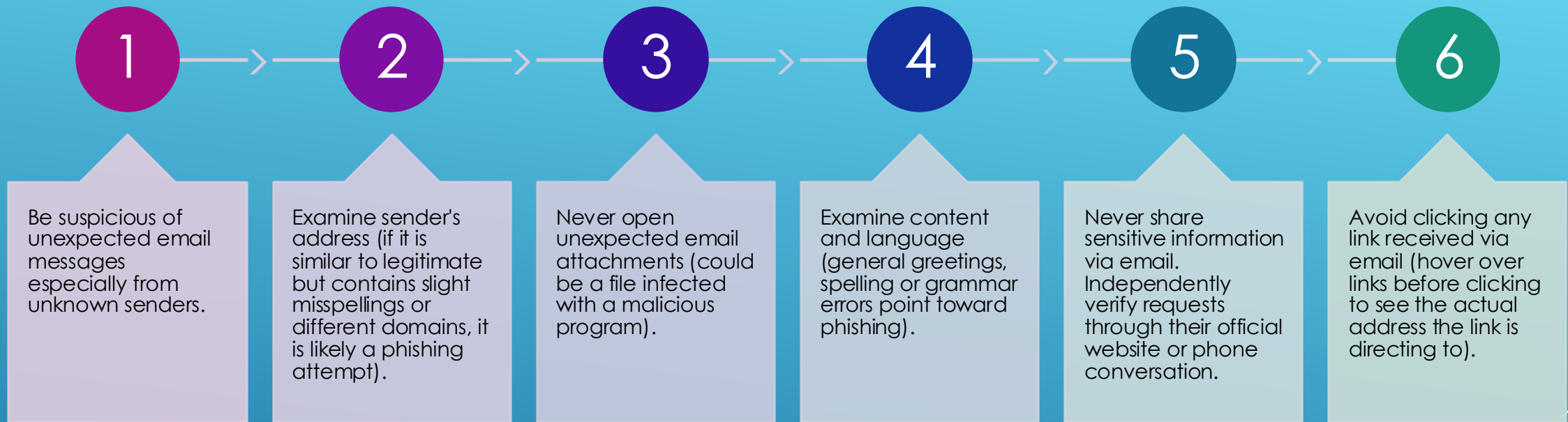
Fraudulent email from "Bank of America Security Team" with the subject "Security Alert: Suspicious Activity Detected" warns of unauthorized login attempts. It urges the recipient to "secure their account" by clicking a link that leads to fake login page.

SOCIAL ENGINEERING PRINCIPLES

URGENCY – Often used with scarcity as a method to get a quick response before a person has time to carefully consider or refuse compliance.

Attacker using an invoice scam through business email compromise (BEC) to convince you to pay an invoice immediately because either an essential business service is about to be cut off or the company will be reported to a collection agency.

SOCIAL ENGINEERING PRINCIPLES



HOW TO SPOT PHISHING ATTACKS

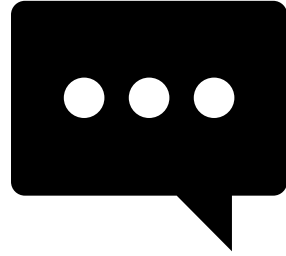
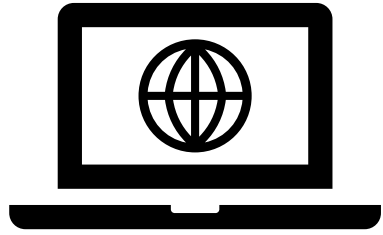
If you suspect that the email is a phishing attempt, delete or report it to the Security Operations team.



RECOGNIZE --> RESIST -->
DELETE/REPORT

SUSPICIOUS.
NOW WHAT?





REAL LIFE EXAMPLES

From: AppStore [<mailto:noreply-9@no-reply-to.com>]

1

Sent: Wednesday, February 15, 2017 7:12 PM

To: userLogin0349@Applelogcompain.com

Subject: Account temporarily unavailable

2

Dear Customer ,

3

Your apple ID has been disabled for security reasons

To get back into your apple account , you will need to confirm it ,

it's easy , fast and secure Click an the link below to open a secure browser window , during the verification process you will be asked to confirm your billing address

4

[Confirm my account now >>](#)

Best regards ,
Apple Support

<https://www.helpiapple.com/>

Click or tap to follow link.



Bank of America

Dear account holder,

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

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>

From: Your Boss <yourboss@fakeyourcompany.com>

Sent: 09 October 2018 11:06

To: Your Company Finance <finance@yourcompany.com>

Subject: IMPORTANT: Fund Transfer Done Today

Hi Gwen,

Could you do me a favour? There's a pending invoice from one of our providers and because I'm on holiday I need you to take care of it for me because I can't access the accounts from here.

They contacted me and I told them to send through the email to you as well (check spam filter incase it's accidentally blocked). Just click on the link in their email and transfer the amount to the account they specify.

This needs to be done TODAY so make it high priority.

If you do this for me it would be a huge favour.

Any questions then reply to this email. I can't take calls right now so just stick to replying to this email.


Thanks,
Your Boss

THANK YOU!!!

RECOGNIZE --> RESIST --> DELETE/REPORT