# Phishing Attacks


Dr. Ala Berzinji

1. **What is Phishing?**
2. **Why Phishing?**

# What is Phishing Attack

Phishing email messages, websites, and phone calls are designed to steal money or sensitive information. Cybercriminals can do this by installing malicious software on your computer, tricking you into giving them sensitive information, or outright stealing personal information off of your computer.

- Phishing is the most common way attackers illegally access systems.
- A phishing message is designed to trick you

Click Here!

USERNAME

**********

| Click an Unsafe Link | Open an Unsafe File | Type your Password | Transfer Funds |
| --- | --- | --- | --- |

Cyber attackers phish for different reasons, but they all phish.

## Criminals

Money

Fraud

Identity Theft

## Intelligence

Sensitive Data

Network Access

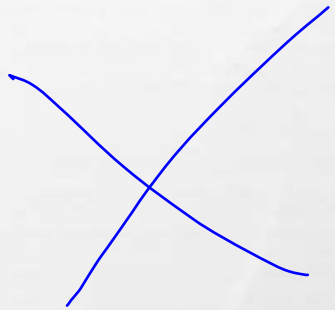
Infrastructure

## Hacktivists

Public Web Pages

Social Media

# Types of Phishing Attack



Social engineering exploits information readily available on social media profiles like Facebook or LinkedIn. This includes personal details such as name, date of birth, location, workplace, interests, hobbies, skills, relationship status, telephone number, email address, and even favorite foods. Cybercriminals can use this information to craft convincing messages or emails, increasing the likelihood of their deceit being perceived as legitimate.

# Types of Phishing Attack

1. **Link Manipulation** - Phishing is a deceptive tactic that frequently involves link manipulation. Cybercriminals mimic trusted sources by altering email links, often using misspelled URLs or subdomains to trick recipients. Email clients and web browsers sometimes preview linked destinations, aiding in detecting fraudulent links.

# Types of Phishing Attack

2. **Spear phishing** - Spear phishing, targeting specific individuals or organizations, involves gathering personal details through social engineering to enhance the success rate. This method dominates internet-based attacks, constituting 91% of all phishing attempts.

# Types of Phishing Attack

3. **Clone phishing** - Email spoofing involves creating a nearly identical copy of a previously sent email, including its content and recipient addresses. However, the attachment or link in the email is substituted with a malicious version. This spoofed email is then sent from an address made to look like it's from the original sender.

# Types of Phishing Attacks

4. **Voice Phishing** - Voice phishing, also known as "vishing," is a form of criminal activity wherein perpetrators use social engineering techniques via telephone to extract personal and financial data from individuals. This information is then exploited for monetary gain, often targeting credit card numbers or data crucial for identity theft schemes.

Phishing messages are designed to get you to react quickly without thinking too much.

Sense of Urgency

Offers of Money

Confirmations


Odd Requests

Rewards

IT Support

What should I do when I get a phishing email?

3 possible

1

Click

2

Delete

3

Report

What happens if I click?


Password Stolen

Malware Installed

| | | | |
|---|---|---|---|
| Identity Theft | Data Destruction | Data Leak | Account Takeover |
| Stolen Password | Remote Access | Network Compromise | Ransomware |

What happens if I delete?


# You're safe...for now.

What happens if I report?

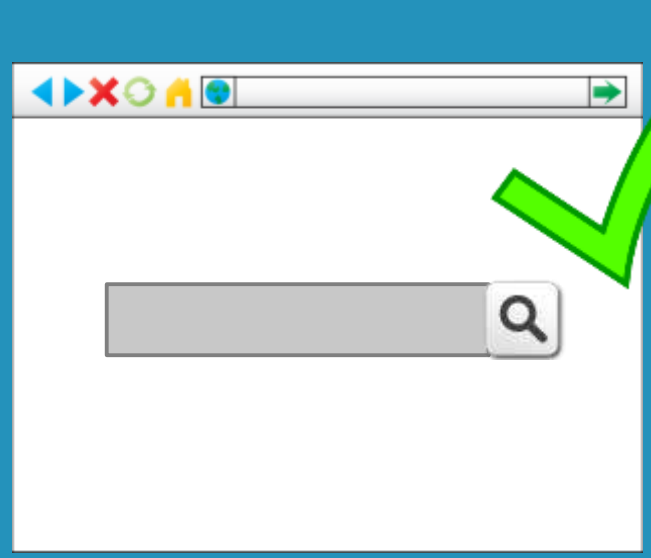
Review Links

Block Domains

Check Accounts

Remove Messages

If you aren't sure...

Or

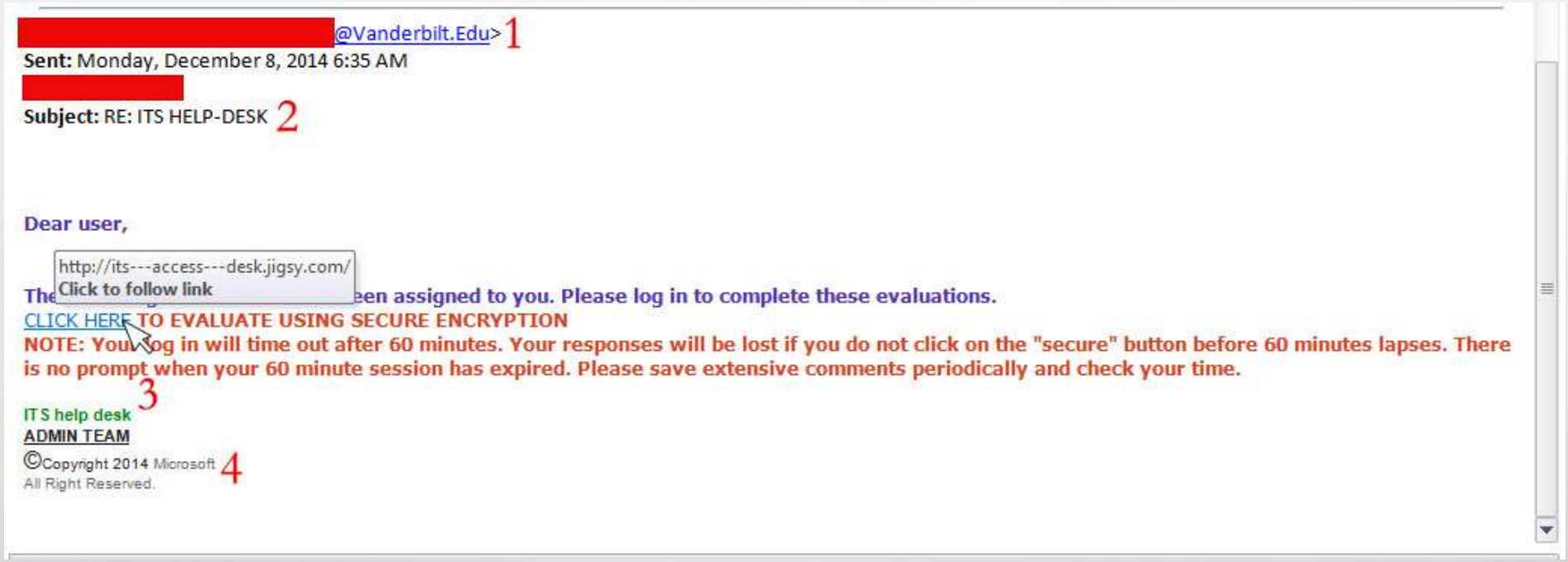
Skip the Link

Ignore the File

Go to The Source

# Some Examples!

# Phishing email



FROM Sara

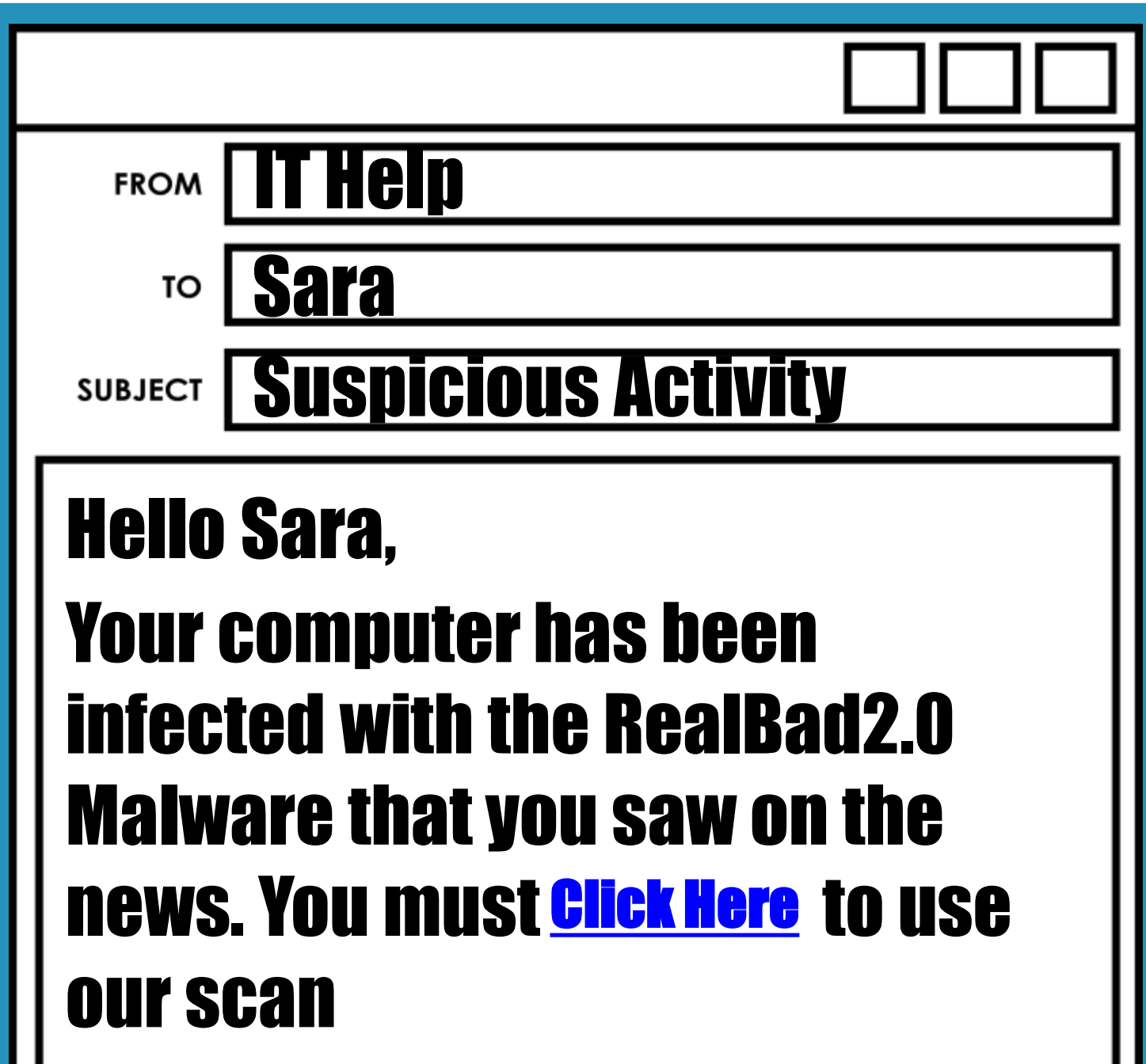
TO Ahmed

SUBJECT Transfer Problem

Hello Ahmed,

I am trying to get payment to a vendor. It is important they get paid by close of business. Can you please wire 7,540 to...

# #1 The Transfer




# #2 The IT Support Alert

FROM Super Shoppers, LLC

TO Sonia

SUBJECT Package Damaged

Dear Sonia,

We apologize in advance, but your recent order was damaged in delivery. We are unable to issue a refund until you confirm Account details with this form.

#3
Confirm
Now!

FROM Security@CrazyMail.Net

TO Maria Mailer

SUBJECT Password Compromise

**Dear Maria,**

**Your account has been locked due to potential compromise. You must go to this site to secure your account.**

**CrazyMail Secure Reset**

# #4 Password Reset

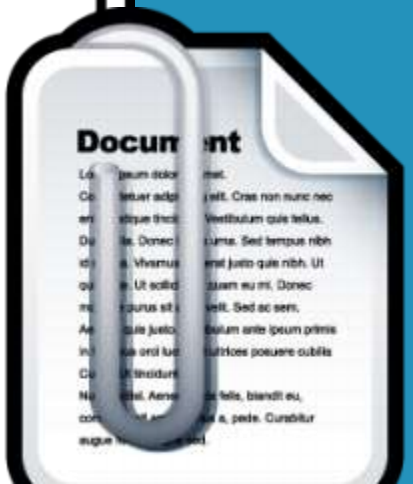
FROM N.Trouble@g.Harvard.edu

TO Ahmed

SUBJECT HELP!!!

HI,

I need to submit this file for class but it won't open on my computer. Can you PLEASE save as a PDF and send to me???



# #5 Cry for Help

FROM eFaxService@proserv.ly

TO Sara

SUBJECT Your

efax Premium User,

Your electronic fax is attached.
This file is intended only for the recipient and is considered confidential.

This is not my document.


# #6 Attach And Attack

# Tips to protect yourself from Phishing emails

- IT will **NEVER** ask for your password over email. Please be wary of any emails asking for passwords**. Never send passwords, bank account numbers, or other private information in an email.**
- Be cautious about opening attachments and downloading files from emails, regardless of who sent them. These files can contain viruses or other malware that can weaken your computer's security.
- If you are not expecting an email with an attachment from someone, such as a fax or a PDF, please **call** and ask them if they indeed sent the email. If not, let them know they are sending out Phishing emails and need to change their email password immediately.
- **Never** enter private or personal information into a popup window.
- If there is a link in an email, use your mouse to hover over that link to see if it is sending you to where it claims to be, this can thwart many phishing attempts.
- Look for '**https://**' and a **lock icon** in the address bar before entering any private information on a website.
- Look for spelling and bad grammar. Cybercriminals are not known for their grammar and spelling.