INFORMATION TECHNOLOGY SERVICES

HOW TO SPOT A PHISH!

Phil Kraemer

OVERVIEW

- What is Phishing?
- Types of Phishing Attacks
- Phishing Examples
- Protect Yourself from Phishing
- Additional Resources

WHAT IS PHISHING?

Definition of phishing

WHAT IS PHISHING?

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

TYPES OF PHISHING ATTACKS

Overview of various methods of phishing

TYPES OF PHISHING ATTACKS

Social Engineering

/ˈsōSHəl ˌenjəˈni(ə)riNG/
n. using deception to manipulate someone into giving up personal information that may be used for fraudulent purposes

- On your Facebook profile you can find:
  - Name
  - Date of birth
  - Location
  - Workplace
  - Hobbies
  - Relationship status
  - Email address
  - Favorite food …
- Everything a cybercriminal needs to fool you into thinking that the message or email is legitimate and coming from someone you know.

TYPES OF PHISHING ATTACKS

Spear Phishing

/spir fiSHiNG/ *n.* sending fraudulent emails from a known or trusted sender in order to trick targeted individuals into giving up confidential information

- Attackers may gather personal information (social engineering) about their targets to increase their probability of success

- Fast fact
  - Accounts for 91% of phishing attacks
  - Most successful form of phishing on the internet today

TYPES OF PHISHING ATTACKS

Clone Phishing

/klōn fiSHiNG/ *n.* replicating a legitimate, previously delivered email and replacing the attachment or link with a malicious version

- Tricky, tricky
  - Sent to the same recipient addresses as the original message
  - Sent from an email address spoofed to appear as though it's coming from the original sender

TYPES OF PHISHING ATTACKS

Voice Phishing

/vois fiSHiNG/ *n.* using social engineering over the phone to gain access to personal and financial information

- AKA: Vishing
- Typically used to steal credit card numbers or other information used in identity theft schemes

- Phrases to watch for
  - You've been specially selected for XYZ.
  - You'll get a free bonus if you buy our product.
  - You have to make up your mind right away.
  - We'll put the shipping charges on your credit card.
  - You trust me, right?

TYPES OF PHISHING ATTACKS

Link Manipulation

/liNGk məˌnipyəˈlāSHən/
n. phishing strategy in which a spoofed email link appears to belong to a legitimate organization or person

- Watch for:
  - Misspelled URLs
  - Subdomains

- Tip
  - Hover over or long tap a link to display the true URL and see if it's linking to a reputable website
  - Email clients or web browsers show previews of links in the bottom left of the screen

TYPES OF PHISHING ATTACKS

Display Name Spoofing

This highly targeted spam attack passes through mail-filtering solutions, unlike other spam emails. It involves mail sent from a registered email address on a valid domain (EG: spamuser@gmail.com), but with the display name set to a key contact or partner of a user within the recipient organization.

- Watch for:
  - The email displays the name of a key contact or someone you deal with regularly BUT the email address is incorrect.
  - The problem is people rely on the display name rather than looking or checking what the actual email address is.
  - Additionally, Outlook and most other email platforms show the display name over the email address for user friendliness.

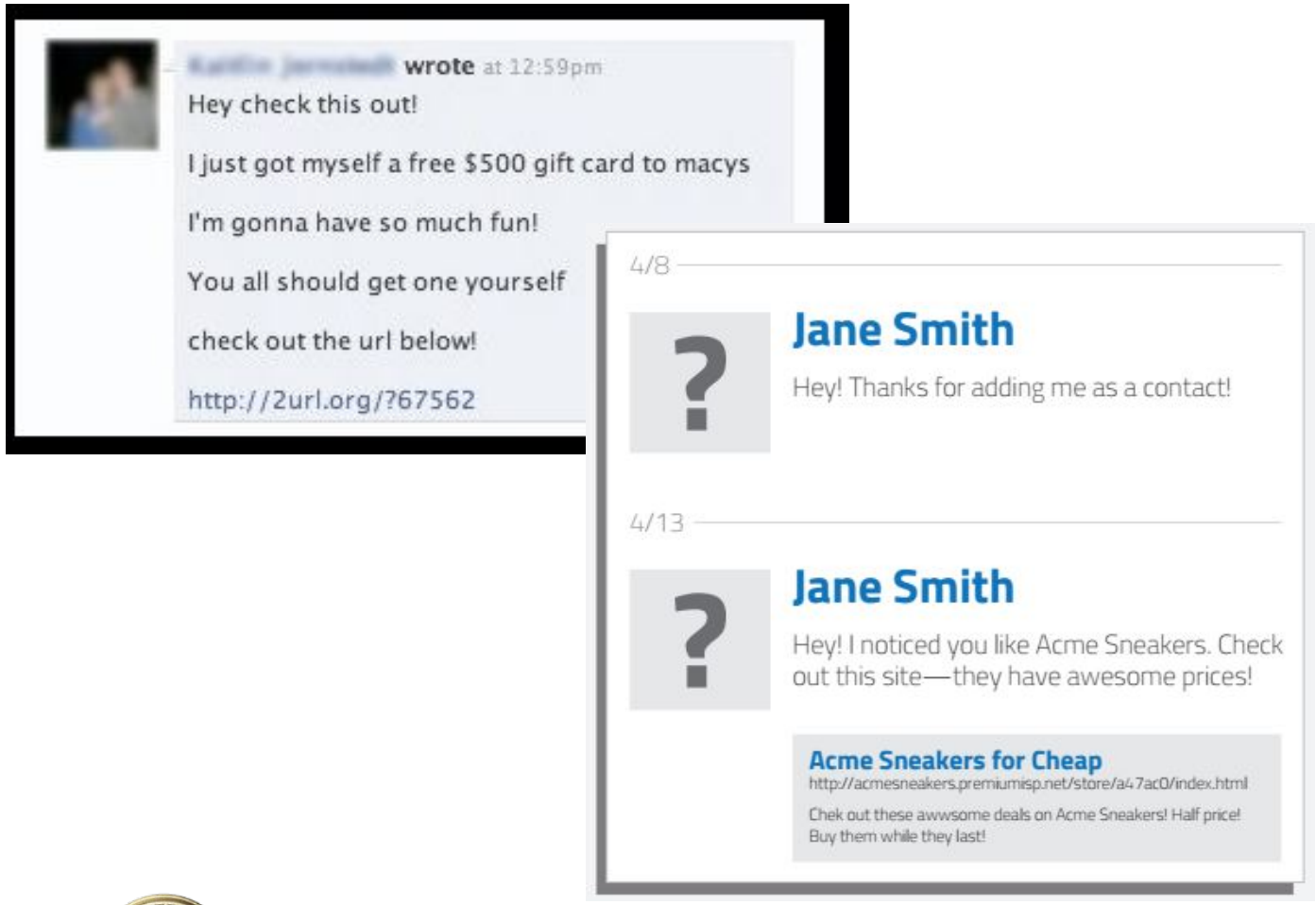
- Tip
  - Check not only the name of the sender but the email address
  - Implement verbal clarification to any email money requesting a transfer for large sums of money. If you receive an email requesting for a significant money transfer, call or text the person and confirm its legitimacy.

PHISHING EXAMPLES

Examples of real phishing attacks

PHISHING EXAMPLES – SOCIAL ENGINEERING

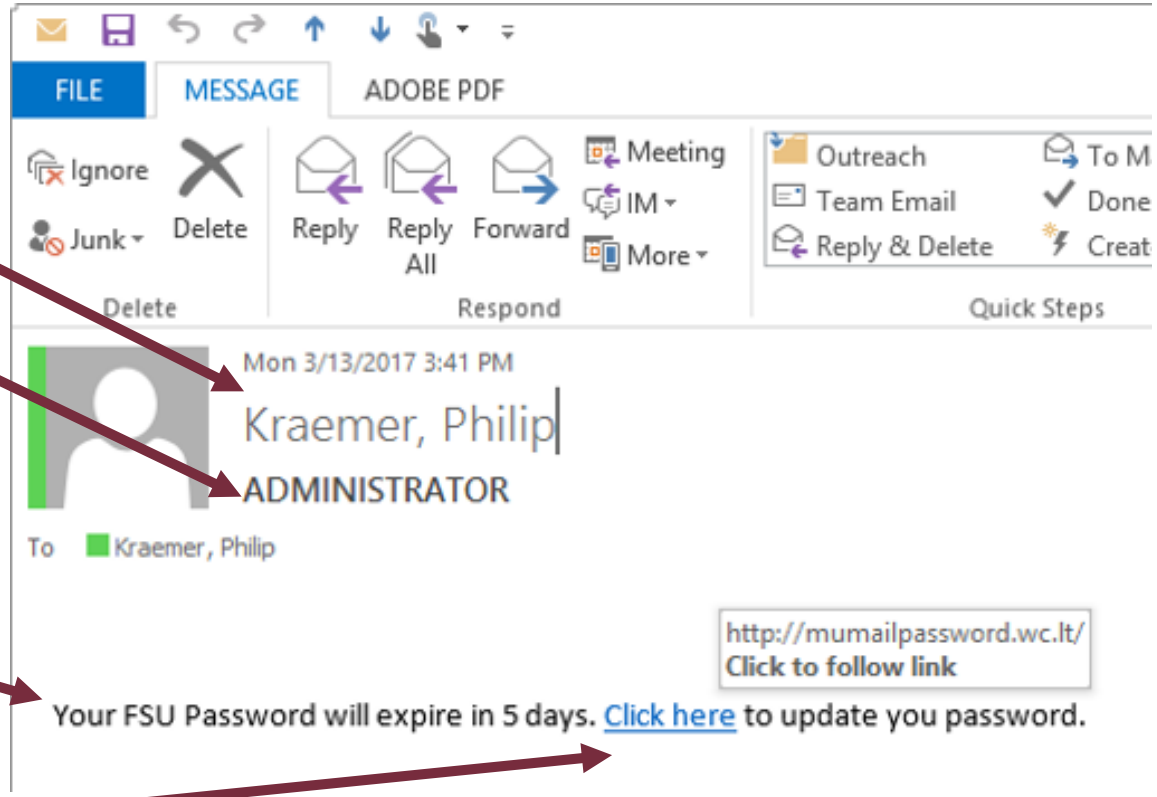
- Cybercriminals scan social media profiles for your interests, then send you a targeted message trying to get you to click a link
- Upon clicking the link, you would be prompted to sign in to a fake sign in page that would steal your username and password
- Then the cybercriminal takes over your profile and sends another phishing attack to your friends and contacts



PHISHING EXAMPLES – SPEAR PHISHING

Watch out for these tricks

- Sent from someone you don't know or from whom you weren't expending an email
- Subjects are in all caps or have lots of !!!!! to make you think the message is important and urgent
- When you hover over the link, you see it is taking you to an unknown site

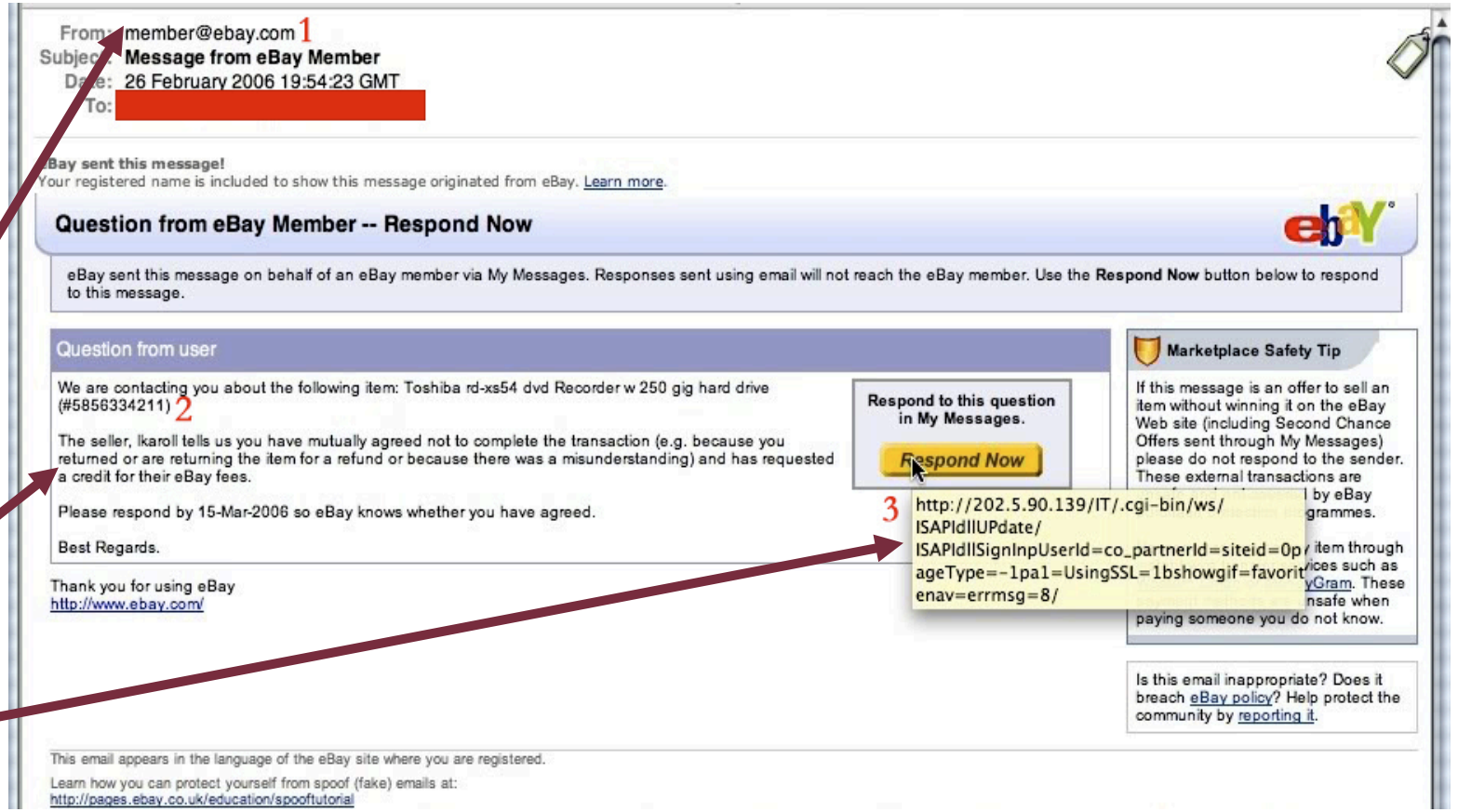


PHISHING EXAMPLES – CLONE PHISHING

These emails are harder to spot because they look like legitimate emails you would normally receive.

Watch out for these tricks

- Sent from a generic address
- Regarding a product you did not purchase
- When you hover over the link, you see it is taking you to an unknown or unexpected site

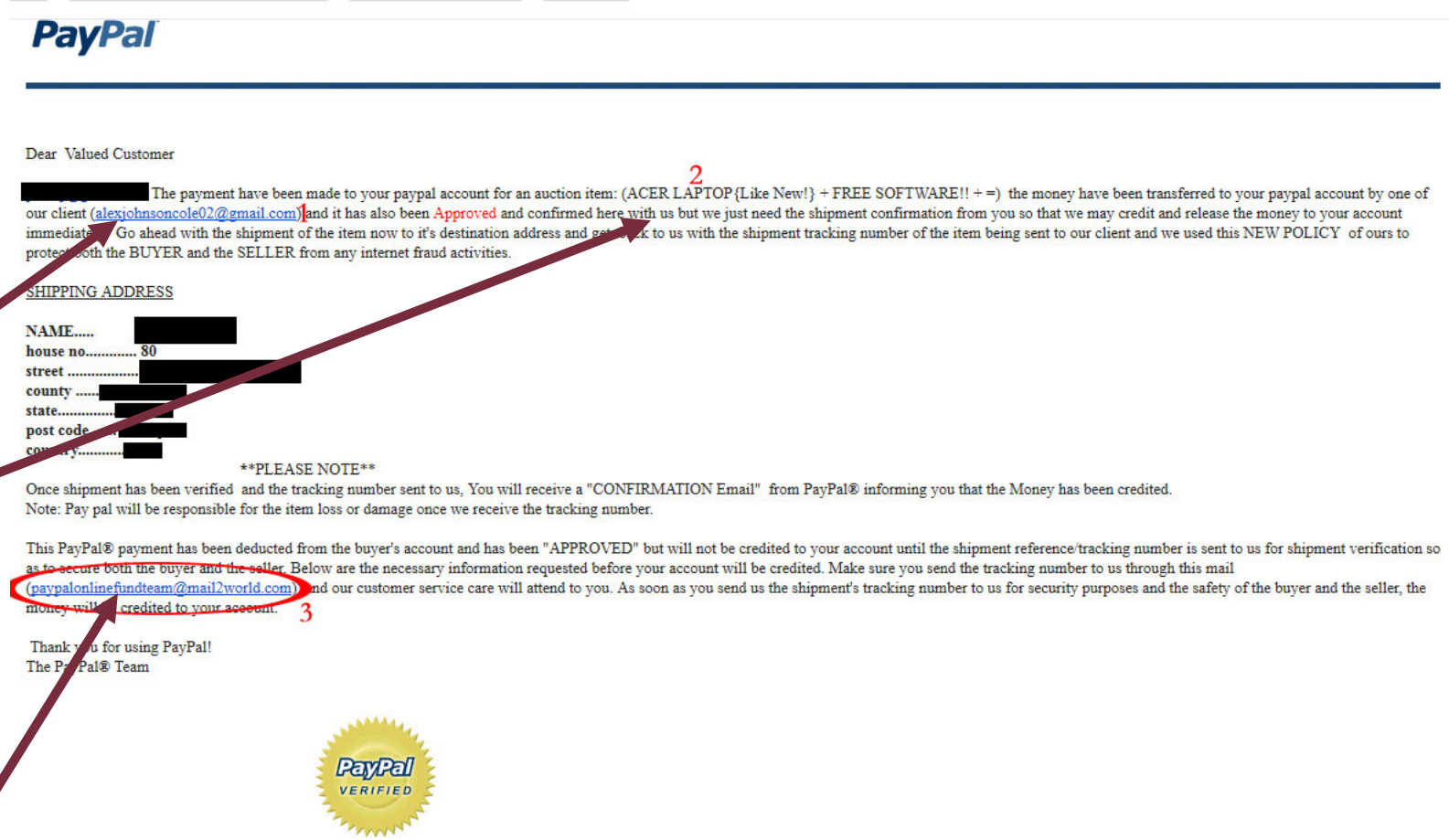


PHISHING EXAMPLES – CLONE PHISHING

Again, the email looks like an official company message.

Watch out for these tricks

- Do you recognize the sender?
- Did you purchase this product?
- Does the link or email point to a reputable site or person? (Example: If this was an official email from PayPal, it would end in “@paypal.com”)



PayPal

Dear Valued Customer

[redacted] The payment have been made to your paypal account for an auction item: (ACER LAPTOP{Like New!} + FREE SOFTWARE!! + =) the money have been transferred to your paypal account by one of our client (alexjohnsoncole02@gmail.com) and it has also been Approved and confirmed here with us but we just need the shipment confirmation from you so that we may credit and release the money to your account immediately. Go ahead with the shipment of the item now to it's destination address and get back to us with the shipment tracking number of the item being sent to our client and we used this NEW POLICY of ours to protect both the BUYER and the SELLER from any internet fraud activities.

SHIPPING ADDRESS

NAME..... [redacted]
house no..... 80
street ..... [redacted]
county .....
state.....
post code
country.....

PLEASE NOTE

Once shipment has been verified and the tracking number sent to us, You will receive a "CONFIRMATION Email" from PayPal® informing you that the Money has been credited.
Note: Pay pal will be responsible for the item loss or damage once we receive the tracking number.

This PayPal® payment has been deducted from the buyer's account and has been "APPROVED" but will not be credited to your account until the shipment reference/tracking number is sent to us for shipment verification so as to secure both the buyer and the seller. Below are the necessary information requested before your account will be credited. Make sure you send the tracking number to us through this mail (paypalonlinefundteam@mail2world.com) and our customer service care will attend to you. As soon as you send us the shipment's tracking number to us for security purposes and the safety of the buyer and the seller, the money will be credited to your account.

Thank you for using PayPal!
The PayPal® Team

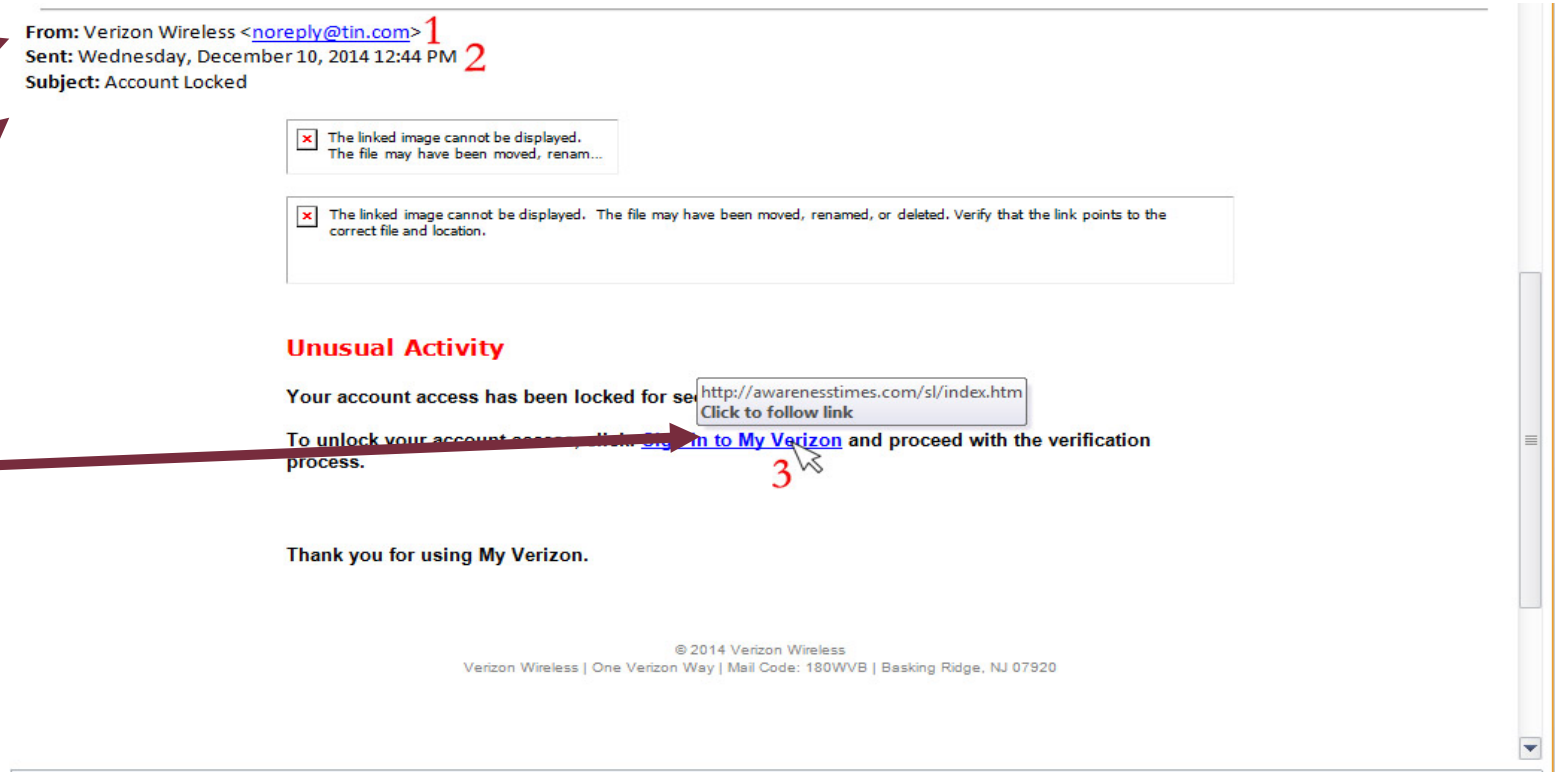
PayPal VERIFIED

1 2 3

PHISHING EXAMPLES – LINK MANIPULATION

Warning signs

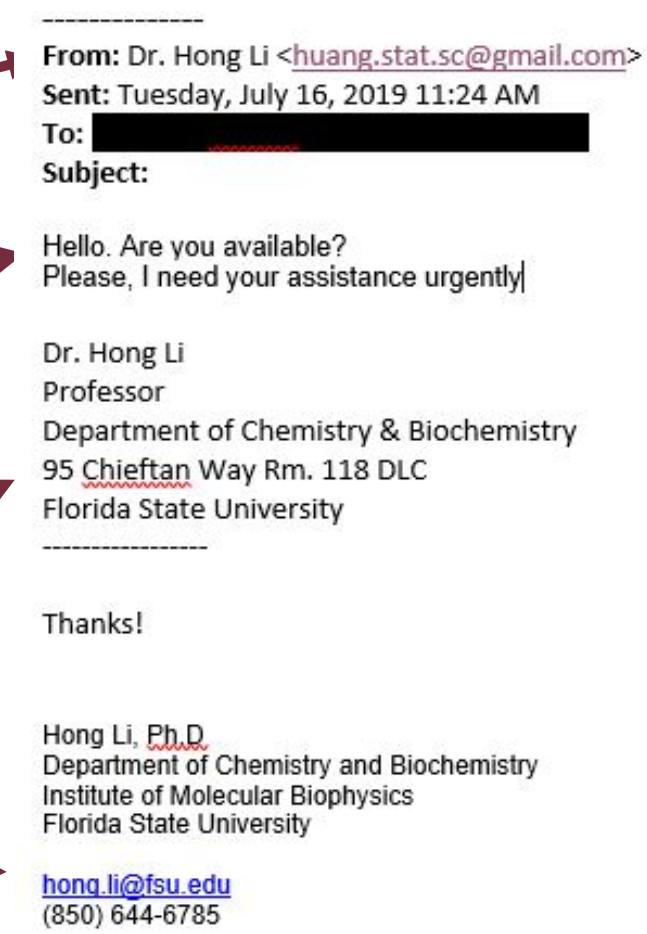
- Not an official Verizon email address
- "To" field missing
- Link is pointing to a strange and unfamiliar website



PHISHING EXAMPLES – DISPLAY NAME SPOOFING

Warning signs

- Not an official FSU email address
- Urgent request is a common sign of phishing
- Two signature blocks may be a sign of display name spoofing (note the second block appears to have a correct FSU email address)



From: Dr. Hong Li <huang.stat.sc@gmail.com>
Sent: Tuesday, July 16, 2019 11:24 AM
To: [redacted]
Subject:

Hello. Are you available?
Please, I need your assistance urgently

Dr. Hong Li
Professor
Department of Chemistry & Biochemistry
95 Chieftan Way Rm. 118 DLC
Florida State University

Thanks!

Hong Li, Ph.D
Department of Chemistry and Biochemistry
Institute of Molecular Biophysics
Florida State University

hong.li@fsu.edu
(850) 644-6785

PROTECT YOURSELF FROM PHISHING

Tips to protect yourself from phishing attacks

TIPS TO PROTECT YOURSELF FROM PHISHING

FSU will

NEVER

ask for your password over email

TIPS TO PROTECT YOURSELF FROM PHISHING

- Be wary of 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
- If you are not expecting an attachment from someone, call and ask them if they sent the email
- Never enter private or personal information into a popup window
- Hover over or long tap links in emails to display the true URL and see if it is linking to a reputable website
- Look for https:// and a lock icon in the website address bar before entering any private information on a website
- Watch for spelling and grammar mistakes

TIPS TO PROTECT YOURSELF FROM VISHING

- Don’t buy from unfamiliar companies
- Check out companies with the Better Business Bureau, National Fraud Information Center or other watchdog groups
- Verify a salesperson’s name, business identity, phone number, street address, mailing address and business license number before you transact business
- Don’t pay for a “free prize.” If a caller tells you the payment is for taxes, he is violating federal law.
- Never give out personal information such as credit card numbers and expiration dates, bank account numbers, dates of birth or SSNs to unfamiliar companies
- If you have been victimized once, be wary of calls offering to help you recover your losses for a fee paid in advance

WHAT TO DO WHEN YOU'VE BEEN PHISHED

Email

- DO NOT click any links or open any attachments in the email
- Forward the email to abuse@fsu.edu
- Check the phish bowl at https://its.fsu.edu/cybersecurity/phish-tank

Phone call

- Look up the phone number on Google or the following sites to see if the call is a scam
  - 800notes.com
  - callercenter.com
  - callercomplaints.com
- Report any caller who is rude, abusive or questionable
  - 877-FTC-HELP
  - ftc.gov/complaint

HOW IS FSU PROTECTING YOU?

- Multi-step verification (DUO)
- Phish Tank
- abuse@fsu.edu
- Training and outreach – call us to come to your organization

ADDITIONAL RESOURCES

More phishing online resources

ADDITIONAL RESOURCES

- http://its.fsu.edu/cybersecurity
- http://www.antiphishing.org/
- http://www.fraudwatchinternational.com/phishing-alerts
- http://phishme.com/
- http://www.onguardonline.gov/phishing
- http://www.consumer.ftc.gov/articles/0076-phone-scams
- http://www.fbi.gov/scams-safety/fraud

Questions?

CONTACT

Philip Kraemer

ISPO Security Training Coordinator
Information Technology Services
Florida State University
pkraemer@fsu.edu
(850) 645-3600
(850) 728-9841