Lesson Title: Something Is Phishy

Content Area: Privacy and Security

Overview:
This lesson shares how scammers can attempt to obtain personal information through phishing. Many times, electronic communication, such as e-mails and text messages, can appear to be coming from a trustworthy source, but they are actually fraudulent.

Objectives:
After participating in this lesson, adult learners will be able to:

- Identify the characteristics of trustworthy electronic communication
- Explain the importance of knowing how to avoid phishing attempts
- Distinguish between legitimate and fraudulent messages and phishing attempts

Materials & Supplies:
The following materials and supplies are needed for this lesson:

- Phishing examples (activity 1)
- Flip Chart & Markers (activity 2)
- Report Phishing cards (activity 2)
- Phishing examples (activity 3)
- Highlighters or pencils (activity 3)

Preparation:
In preparation for this lesson, facilitators should:

- Review lesson plan
- Print phishing examples
- Print and cut report phishing cards

Terminology:
The following terms will be discussed during the lesson:

- **Password**: a combination of keyboard letters, numbers, and characteristics that must be entered to gain admission into many online services (e-mail, social media accounts, online shopping accounts, etc.)
- **Phishing**: the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising as a trustworthy entity in an electronic communication

Background Information:
Phishing is a fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising as a trustworthy entity in an electronic communication. Many times, these e-mails or text messages appear if they are coming from a legitimate source and usually have a sense of urgency. Links in phishing e-mails typically take the user to an untrusted website to enter

sensitive information. Risks associated with phishing attempts include people obtaining your passwords, impersonating you to access your bank account and other financial services, purchasing items online, people impersonating you in social media networking sites, and accessing private information on your computer.

Activity 1: What is Phishing?

Distribute examples of a phishing e-mail and a phishing text.

Explain the following for the e-mail message:
The employee (who works for the University of Georgia) received this e-mail message. Her supervisor is Arch Smith, so she regularly receives e-mails from him. However, after further investigation, there are some suspicious things about this message:

- While the e-mail is from "Arch Smith," the sent e-mail address does not indicate that Arch sent the message. Since the correspondence is related to work, it's also suspicious that it did not come from an e-mail account associated with the University of Georgia.
- The spelling, grammar, and mechanics of the e-mail raise concerns. Words are capitalized that should not be. Punctation and grammar are incorrect in some instances.
- The e-mail isn't actually signed from Arch Smith. Most e-mails end with some sort of closing and signature.
- The e-mail seems very urgent and does not specifically cite why things are urgent. The sender also is not able to take phone calls (which would be considered a 'normal' practice in an emergency situation).

Explain the following for the text message:
The person banks with Wells Fargo and sometimes gets e-mail updates from the bank. However, after further investigation, there are some suspicious things about this message:

- The sender of this message uses the e-mail address customersatmbankingwells432@masbadar.com. It does not appear to be a legitimate e-mail address associated with Wells Fargo.
- The link embedded in the message is a bitly url. Bitly is a service that shortens urls – not showing the complete website url. While many groups use these services, you should only click on the shortened url when you know the sender.
- The spelling, grammar, and mechanics of the text raise concerns. The message is not complete.

Phishing is a fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising as a trustworthy entity in an electronic communication. Many times, people that reply to these types of e-mails are asked to do something that does not keep them safe online. They may also be asked to click on a link and share information. For example, they may be asked to share their password, financial information, pin codes, or asked to send money or buy items (such as gift cards). Many times, timing is urgent because "suspicious activity has been detected" or "your account is locked" until further actions.

Some features of a phishing e-mail include:

- Needing to verify account information (ex. e-mail account, banking account, money transfer account, etc.). Many times, the e-mail says your personal information has expired or needs to be verified.
- Link in the e-mail/text or attachment. Usually, the link does not provide you with the URL, so it's hard to determine what website it will redirect you to. Regardless, only click on links from reputable senders.
- Sense of urgency. Many times, phishing e-mails give you a limited amount of time (ex. 24 hours) to resolve a "problem" that doesn't exist.
- Too good to be true. Phishing e-mails could promise some sort of "return" such as cash or gift cards if you do something first (usually giving them personal/sensitive information).
- Spelling, grammar, and/or mechanics errors. An occasional typo sometimes happens in a legitimate e-mail, but an excessive amount of errors includes a phishing e-mail.
- Length. Some phishing e-mails can tend to be short. Others may be very long, explaining a circumstance (ex. why this person can't do something and why they need your help).
- Generic greeting. Many phishing e-mails don't have a greeting or simply start with 'hello.'

Activity 2: Dealing with Phishing Attempts

Why is it important to avoid phishing attempts? During the summer of 2019, a metro Atlanta city was scammed out of $800,000 because of phishing. A city employee thought they got an e-mail from a vendor with the water department, but the e-mail was from a cybercriminal instead. The e-mail said the vendor was updating/changing their banking account, so they needed to verify all their customer's records. The city employee sent over the city's banking information, and the cybercriminal was able to transfer nearly $800,000 from the account before someone realized the mistake. While the city does have insurance and the scam was reported to authorities, it is unlikely all of the money can be recovered. While this example applies to a city, anyone can be a victim of a phishing attempt.

Use the flip chart and markers to collectively brainstorm actions to take if you experience a phishing attempt. Examples include:

- Not clicking on any links or downloading any attachments. They might contain viruses or spyware.
- Don't reply to the e-mail or text message.
- Mark/categorize the e-mail as "junk" or "spam".
- If the e-mail references an account and you are concerned about that account, call the company. However, do not use any of the contact information in the e-mail or text. Many times, these criminals create fake phone numbers. Verify the company's contact information elsewhere first.
- Report the phishing e-mail to officials.

Phishing emails can be sent to the Federal Trade Commission (FTC) at spam@uce.gov and to the Anti-Phishing Working Group at reportphishing@apwg.org. Phishing attempts can be reported to the FTC at FTC.gov/complaint. Phishing text messages should be sent to 7726 (SPAM).

Activity 3: Spot the Phishing Attempt

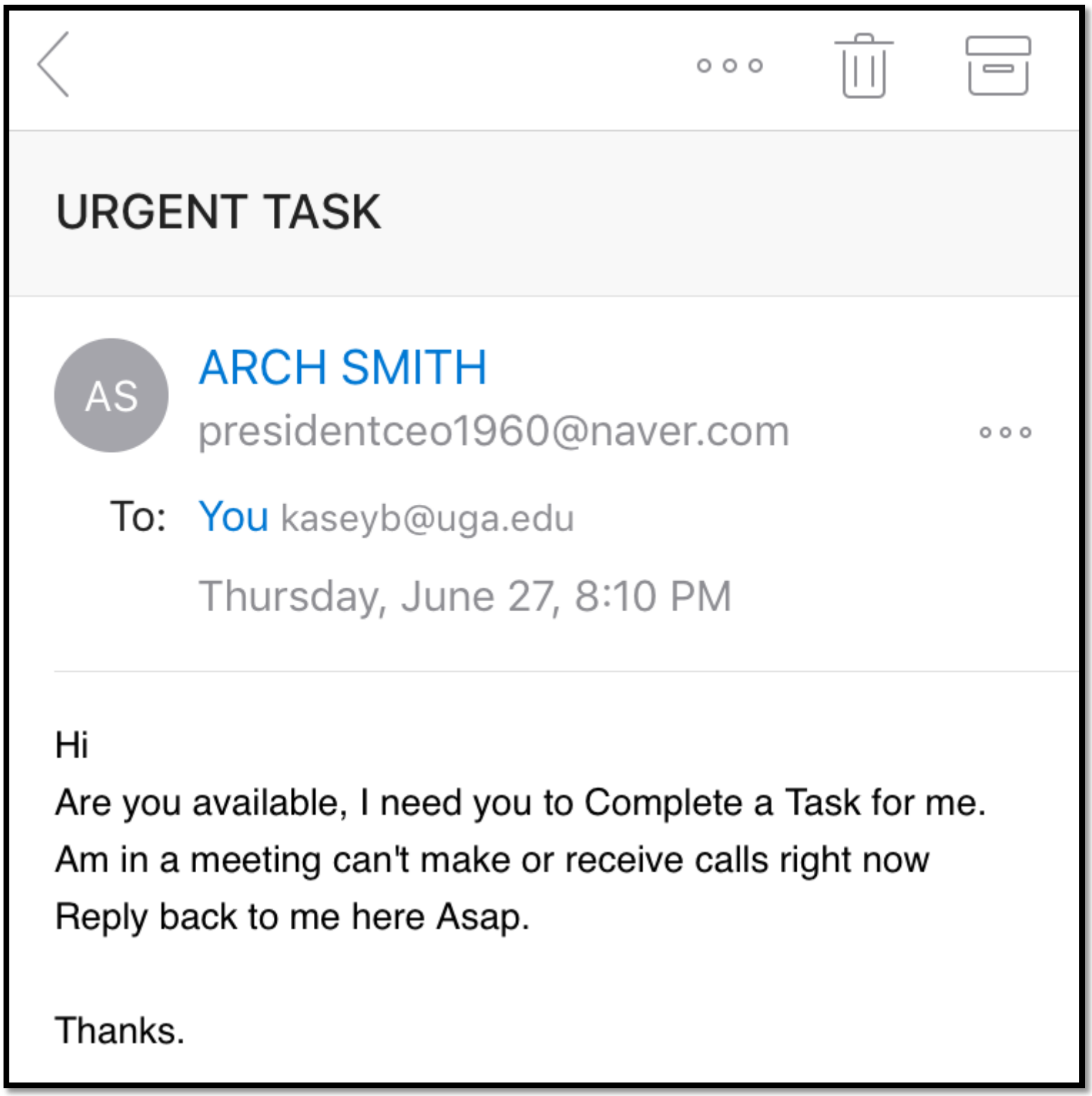
Depending on the size of the group, facilitators may choose to subdivide participants into smaller groups. Each group will get an example of a phishing attempt and highlight all of the features that indicate that the e-mail or text message is phishing. After each group has identified the different characteristics of phishing, facilitators should review the information for all the participants.

Reflection:
While the intent is for the activity to build privacy and security skills related to technology, it is important for the facilitator to lead a debrief discussion at the end of the lesson. Potential debrief questions could include:

- What are some characteristics of trustworthy electronic communications?
- What are some characteristics of fraudulent electronic communications?
- Why is it important to know how to avoid phishing attempts?
- What should you do if you receive an e-mail or text that you think is fraudulent?

Resources:

- https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams
- https://www.commonsense.org/education/digital-citizenship/lesson/dont-feed-the-phish
- https://www.commonsense.org/education/lesson/scams-and-schemes-6-8



URGENT TASK

AS

ARCH SMITH
presidentceo1960@naver.com

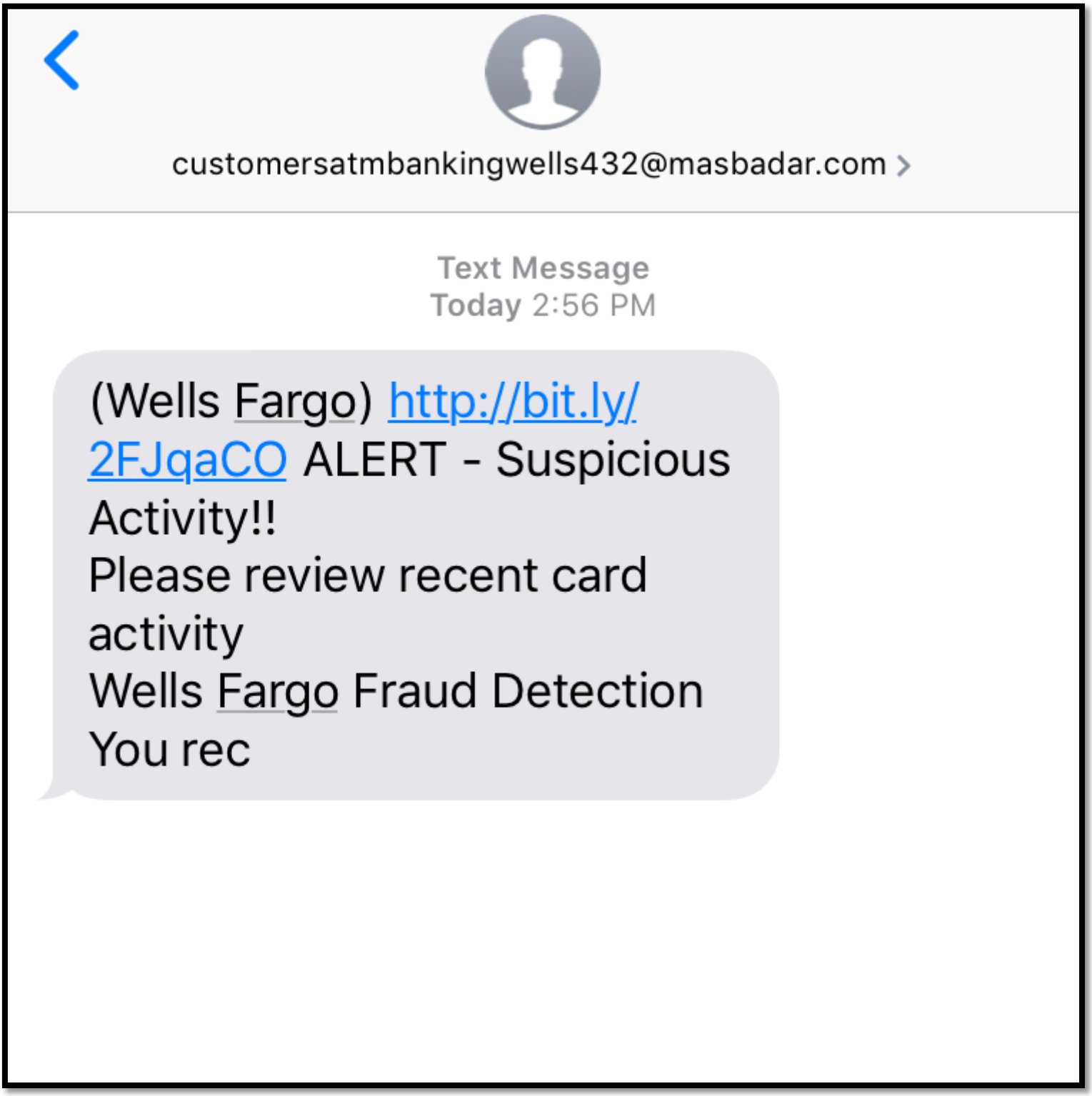
To: You kaseyb@uga.edu

Thursday, June 27, 8:10 PM

Hi
Are you available, I need you to Complete a Task for me.
Am in a meeting can't make or receive calls right now
Reply back to me here Asap.

Thanks.

to be used with to be used with Something is Phishy Lesson, Activity 1


customersatmbankingwells432@masbadar.com
Text Message
Today 2:56 PM
(Wells Fargo) http://bit.ly/2FJqaCO ALERT - Suspicious Activity!!
Please review recent card activity
Wells Fargo Fraud Detection
You rec

Report Phishing!

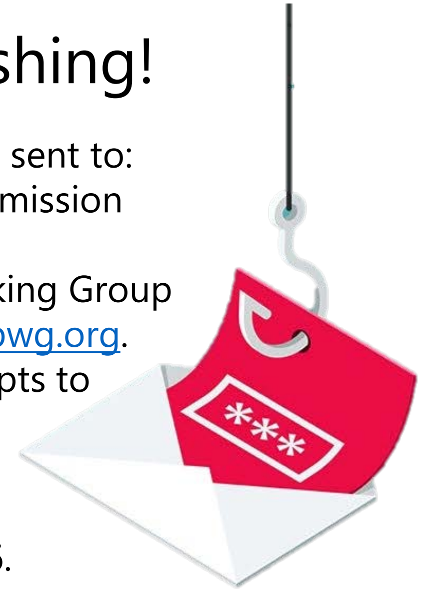
Phishing emails can be sent to:

- Federal Trade Commission spam@uce.gov
- Anti-Phishing Working Group reportphishing@apwg.org.

Report phishing attempts to FTC.gov/complaint.

Fishing text messages should be sent to 7726.

Report Phishing!



Phishing emails can be sent to:

- Federal Trade Commission spam@uce.gov
- Anti-Phishing Working Group reportphishing@apwg.org.

Report phishing attempts to FTC.gov/complaint.

Fishing text messages should be sent to 7726.

Report Phishing!

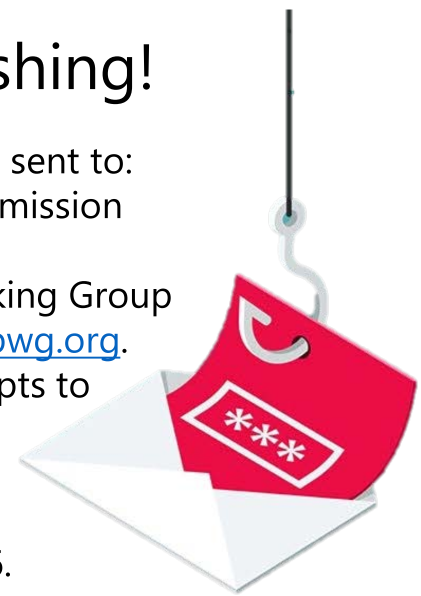
Phishing emails can be sent to:

- Federal Trade Commission spam@uce.gov
- Anti-Phishing Working Group reportphishing@apwg.org.

Report phishing attempts to FTC.gov/complaint.

Fishing text messages should be sent to 7726.

Report Phishing!



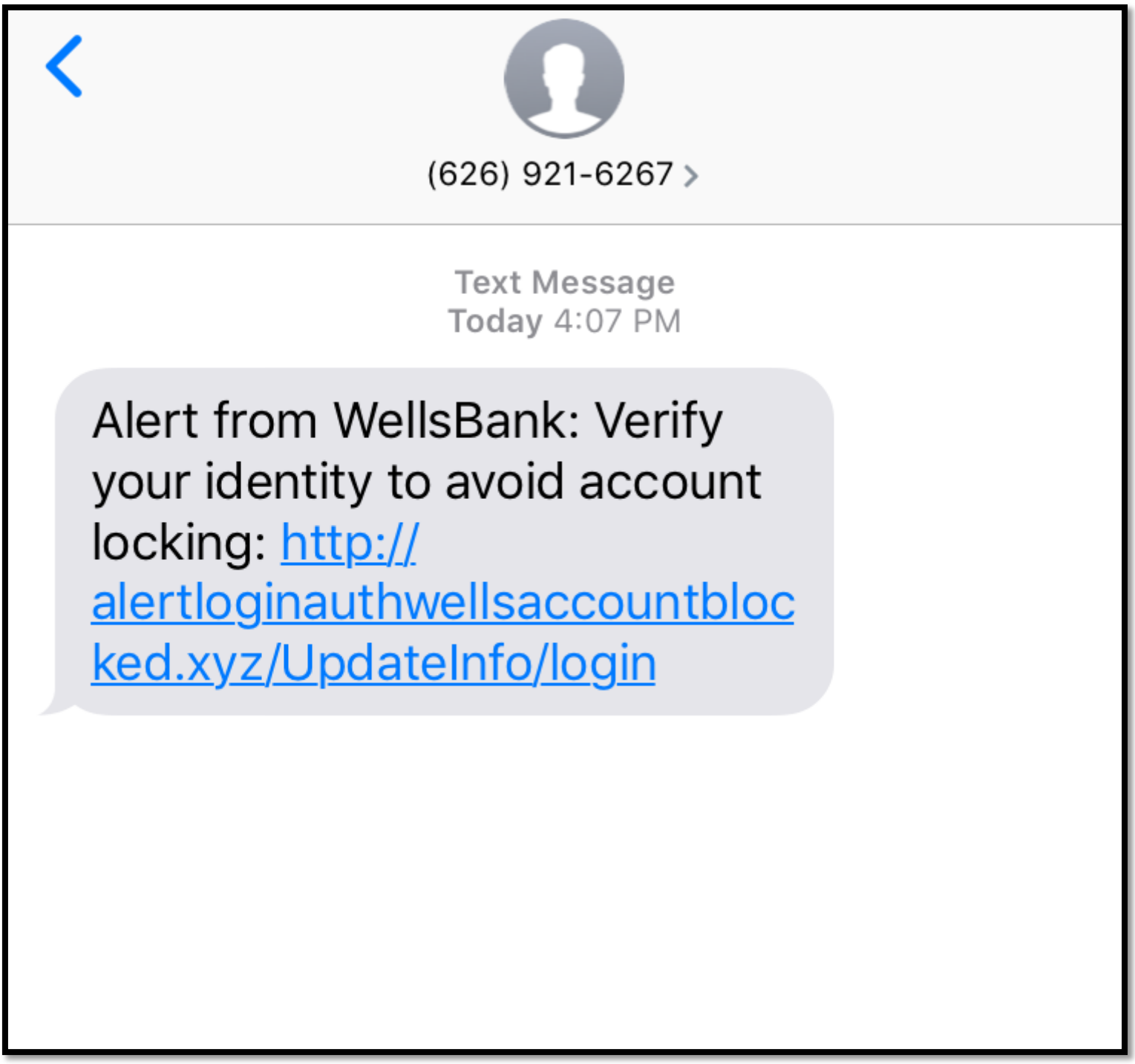
Phishing emails can be sent to:

- Federal Trade Commission spam@uce.gov
- Anti-Phishing Working Group reportphishing@apwg.org.

Report phishing attempts to FTC.gov/complaint.

Fishing text messages should be sent to 7726.

to be used with Something is Phishy Lesson, Activity 2



to be used with to be used with Something is Phishy Lesson, Activity 3

From: SALLY BROWN <directore8@gmail.com>
Sent: Monday, June 17, 2019 3:22 PM
Subject: Urgent request!

Hello,

I need a favor from you right now kindly email me back as soon as possible.

Regards,
SALLY BROWN,
EXECUTIVE DIRECTOR.

From: Nate Houghton <nate@quarterzero.com>
Sent: Tuesday, February 26, 2019 12:20 PM
Subject: Hi Kasey Lynn, Up to $600 off tuition for students

Hi Kasey Lynn,

I hope you're having a great day! I had a reminder pop up to reach out and see that you received my message below about partnering with Quarter Zero.

Let me know if this is a partnership that you would be interested in considering - I'd be happy to jump on the phone for a quick call anytime as well!

Thanks,

Nate

From: Joe W. Harrison Assistant Dean <limitedcable@aol.com>
Sent: Wednesday, March 6, 2019 1:23 PM
Subject: Hi

Hi

How are you doing? Kindly e-mail me your personal cell number.
Thank you.

Joe W. Harrison
Assistant Dean

From: self@mymedia.com
Sent: Friday, April 19, 2019 2:12 AM
Subject: The decision to suspend your account. Waiting for payment.

Hello!

I have very bad news for you.
21/10/2018 - on this day I hacked your OS and got full access to your account kaseyb@uga.edu. So, you can change the password, yes... But my malware intercepts it every time.

How I made it:
In the software of the router, through which you went online, was a vulnerability. I just hacked this router and placed my malicious code on it. When you went online, my trojan was installed on the OS of your device.

After that, I made a full dump of your disk (I have all your address book, history of viewing sites, all files, phone numbers and addresses of all your contacts).

Pay ONLY in Bitcoins!
My BTC wallet: 1H1K8MfLEJgjCCfDEkTJmv9GJjD3XzEFGR

You do not know how to use bitcoins?
Enter a query in any search engine: "how to replenish btc wallet".
It's extremely easy For this payment I give you two days (48 hours).
As soon as this letter is opened, the timer will work.

Do not hold evil! I just do my job.
Have a nice day!

From: Netflix <netflixrentals@gmail.com>
Sent: Monday, May 13, 2019 4:11 PM
Subject: Netflix Account

Your Netflix account will be suspended if you do not update your information within 24 hours.

Click here to update your information.

Netflix Administration

From: Bernhardt Betty <giordanopino75@gmail.com>
Sent: Wednesday, April 10, 2019 6:58 PM
Subject: help

Hello,
Good day to you, how are you doing? My name is Bernhardt Betty (CSM). I am a U.S. Marine Specialist [Command Sergeant Major] serving here in Syria. I found boxes containing the sum of $25,000,000.00 USD (Twenty Five Million United States Dollars) due to my status as a U.S. Army Specialist, I would not be able to transfer this funds to my account in United States. I need your help to evacuate this funds and also keep it until I finish my service here in few weeks and come get my share of it.
The box will be addressed as family valuables from me to you. If this is possible for you to do, I need your assurance that it will be safe in your care. You may be wondering why I decided to communicate with you, I have no one to discuss this with. I am an orphan. I am alone with no family. Please assist me to secure a brighter future. Trusting someone is very difficult, but I give you my trust and my word, and also i need your trust to make this a success. Your acceptance to this would really encourage me. Kindly let me know your conclusion to my request so we can proceed to get this completed as soon as you can. With a sincere heart, i am willing to give you 35% from the total sum for your assistance and willingness to help me. Please do not betray my trust and confidence in you. If you truly accept to help me, please reply me quickly.
srgtbernhardt@aol.com

From: E-bay <ebay@yahoo.com>
Sent: Tuesday, May 13, 2019 4:11 PM
Subject: E-bay

We have notices some unusual activity on your E-bay account. To verify your information, click here.

We appreciate you being a loyal customer.
E-bay