Title: Tips for Staying Safe Online: Identifying Phishing Emails

Introduction: The Tips for Staying Safe Online Video Series is led through slides as visual markers. Any images in the slides that are important to content, and share any additional information beyond the script, has been included here as Alt text.

Narrator: Welcome to the Help@Hand Identifying Phishing Emails Video. Help@Hand is a California multi-city and county collaboration created to help shape the future of technology-based mental health solutions and connect people to care across the state. These video tutorials are intended to empower California communities to make informed decisions about how they engage with technology. This is course [3] in a 4 course series called Tips for Staying Safe Online. The videos in this series can be viewed in order or in any order based on your interest.

Narrator: Many emails are harmless, but some emails that we receive can be sent by strangers who are trying to access our personal and financial information. The following tutorial will help you understand what phishing emails are and how you can spot them

Narrator: Phishing emails can seem real but often have links or attachments that can be harmful when we click on them. (click) The purpose of these emails is to get access to your information or to cause you to accidentally download malware and viruses which can damage your computer and further expose your data. Luckily, there are some clues that you can look for to help you identify a phishing email.

Image: Display of an email in a pop-out window. There is an email sender name that reads joykone and an email address that reads konemrskone10@gmail.com. On the left side of the email sender name there is a circle with an octagon in the center and an "X". Below the sender's name and email address there is a red box that reads "This message seems dangerous. Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information." There is also a clickable box that reads "Looks Safe." The message of the email reads " From Mrs Joy Kone, MY Dear, I wish to solicit your help, My name is Mrs Joy Kone, I am a widow. My husband and I worked with Tullow oil before he died seven years ago. I am interested in having you as my foreign investments partner to transfer a deposit of $18,300,000.00 USD to your country.

Narrator: The first tip is to look at the person or company who sent the message. Do you know them and is their email address spelled correctly? Once you've determined this, carefully read the subject line and message to see if there are any red flags. If there are a lot of spelling or grammar errors or it just doesn't sound like the person who has sent it make sure not to click on any of the links or attachments that may appear in the message. In this email example the sender of the message "Mrs. Joy Kone" is not known to the person receiving the email. The message itself is also quite suspicious. Why would Mrs. Kone share such personal information with someone she doesn't know and also offer to transfer such a large sum of money?

Image: Display of an email. The subject line reads “Fwd: for all” with a smiley face emoji. The sender name and email address reads “Michelle Vega lukaslogo@yandex.ru” the messages reads “I think you may find this interesting http://ub2l.ugtssxw.info/’

Narrator: This is another email example where the sender of the email is actually known to the person receiving the message. However, on closer review the email address is not associated with his person and the text in the message seems off because it contains a link with no other information explaining it. In this instance, it would not be a good idea to click on the link and risk exposing yourself to strangers who could steal your information. The better strategy would be to compose a separate message to Michelle to find out if she sent you the message. If not, it’s possible that Michelle’s computer has been exposed to a virus that is sending phishing emails to her contacts. If this is the case, it is especially important that you do not click on any links or attachments and that you don’t forward the email to others. Doing this could spread the virus further and make others vulnerable to the phishing attack.

Image: Display of an email in a pop-out window. The subject line reads “Request A Loan Today!- Up to $35k” then the sender name and email address reads “ChristmasCashNow <offer.chcf43264@cf607ntnv1rkk4.w1e5-aa8e.uclgk7w.gq.” On the left side of the email sender name there is a circle with an octagon in the center and an “!”. Below the sender’s name and email address there is a box that reads “Why is this message in spam? It is similar to messages that were identified as spam in the past. There is also a clickable box that reads “Report not spam.” The message of the email reads “Request a loan. With ChristmasCashFast, you can receive funding up to $35,000. We partner with over 100 authorized lenders. This allows us to coveralmost 50 states. The $35,00 is received quickly and from the privacy of you own home. Get Funds for Chirstmas! Fast online personal loans. All credit types welcome, funds directly deposited. Start Now!” The “Start Now!” test is in a clickable box.

Narrator: This leads us to tip number two. When you’re checking out an email you should always think carefully about what the message is saying. One thing to ask yourself is: “Is it too good to be true?” A lot of phishing emails contain notifications about winning big prizes or accessing questionable dating services. For example, this email makes it almost too easy to apply for a loan. It’s also suspicious that they are offering to deposit the funds directly into this person’s account as they would need all of the personal account information to do so. Again, if you have any doubts about an email it’s very important that you DO NOT click on any of the links in the message.

Image: Display of an email in a pop-out window with an ebay logo at the top. The sender name and email address reads “eBay Account Security Department” the subject line reads “Password change required” the message in the email reads “Password Change required! Dear Sir, We recently have determined that different computers have logged onto your eBay account, and multiple password failures were present before the logons. We strongly advice CHANGE YOUR PASSWORD. If this is not completed by March 8, 2007, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. Thank you for your cooperation. Click here to Change Your

Password. Thank you for your prompt attention to this matter. We apologize fo any inconvenience. Thank you for using eBay! Please do not reply to this email. Mail sent to this address cannot be answered.'

Narrator: Other fake emails use scare tactics to trick people into clicking on links or replying to the message with personal information. These emails will often seem urgent and will contain a warning that something bad will happen if the email recipient doesn't act quickly. In this message the person is told that they have a deadline for making the password change or else their account will be suspended. When you receive an email asking you to change your password, instead of clicking on the link it's usually a good idea to go to your web browser, type in the address for the site the email is coming from, make sure it's the real website and make any changes directly through the site. In this case, the person should go directly to their ebay account to see if they need to update their password. If the real ebay site does not mention that they need to change their password, then it is likely this email message was fake.

Image: Display of an email, the subject line at the top reads "Get a new Alarm Special + $100 Visa Card Bonus from Protect Your Home" under this there is a marker from the email platform that labels the email as spam. The sender name and email reads "Protect Your Home adtm43275@tl6ofeogvqj8b.wfcc-9101.gm8xuiii.ga" Below the sender's name and email address there is a box that reads "Why is this message in spam? It is similar to messages that were identified as spam in the past. There is also a clickable box that reads "Report not spam." The message of the email reads "What is You plan to help protect your home family? 87% of all Home Burglaries are Considered Preventable!* Did You Know: The average cost of damages by a home intrusion is $1000. According to FBI, a burglary occurs somewhere in the US every 15.4 seconds. Don't be an easy target!." At the bottom of the message is a clickable box that reads "FREE PILOT."

Narrator: In this email, the sender is trying to scare the person into clicking on the link by giving statistics about home burglaries and making the person feel pressure to act quickly in order to protect themselves and their families.

Image: Display of an email, the subject line reads "urgent respond" under this there is a marker from the email platform that labels the email as spam. The sender name and email reads " Shahinaz Zuthimalin fulltime343@yahoo.com." On the left side of the email sender name there is a circle with an octagon in the center and an "X". Below the sender's name and email address there is a red box that reads "This message seems dangerous. Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information." There is also a clickable box that reads "Looks Safe." The message of the email reads "Hello My Dear, Please do not feel disturbed for contacting you, based on the critical condition I find myself, though, it's not financial problem, but my health you might have know that cancer is not what to talk home about, I am married to Mr. Khalil Zuthimalin who worked with Tunisia embassy in Burkina Faso for nine years before he died in the year 2012. We were married for eleven years without a child. He deid after a brief illness that lasted for five days. Since his death I decided not to remarry, When my late husband

was alive he deposited the sum of US $ 9.2m (Nine million two hundred thousand dollars) in a bank in Burkina Faso, Presently this money is still in bank. And my Doctor told me that I don't have much time to live because of the cancer problem, Having known my condition I decided to hand you over this fund to take care of the less privileged people, you."

Narrator: A third tip is to pay attention to how your email provider labels these incoming messages. Your email account has settings to automatically filter dangerous messages that might be harmful to you. If an email is labeled as "spam" you should proceed with caution. If an email has a warning, the safest thing to do is to delete the message. This email has a warning telling the email recipient not to click on links, download attachments, or reply with any kind of personal information. This makes sense as the email has an urgent message from an unknown person who likely should not be trusted.

Narrator: So let's recap, keep these tips in mind when you're figuring out whether to trust an email message.

a. Tip 1. Think about the sender, do you know them? Are there spelling errors? Does it seem suspicious?
b. Tip 2. Consider what the message is saying and whether your email provider thinks it's safe or not. Is it too good to be true? Is there a sense of urgency?
c. Tip 3. If your email provider think it's dangerous it probably is. Did your email come with any spam or virus warnings?

Narrator: We hope you found this video valuable. While optional, we please take one minute to provide feedback on your experience, by clicking on the survey link that will display shortly. Thanks for joining and don't forget to check out the other Help@Hand videos.