SOUTH CAROLINA FAMILY AND COMMUNITY LEADERS

Affiliated with National Volunteer Outreach Network, Country Women's Council, U.S.A., Associated Country Women of the World and in partnership with Clemson University Cooperative Extension Service

SCFCL website: http://www.scfcl.com

Have You Been Targeted For An Email Phishing Scam?

Objectives:

The participants will be able to:

1. Learn how to spot a phishing email
2. Types of phishing emails that were dominate in 2022
3. What you should do if you receive a phishing email

Lesson Overview/Introduction:

You just received an email from Visa stating that suspicious activity has been detected on your credit card. You're instructed to click on a link to verify your security information.

Only thing is, you don't have a Visa card.

While it might be easy to avoid falling for this particular phishing email, many fake messages are harder to spot and ignore. Before you follow the links in a random email, follow these tips to keep from being lured into an online phishing scam.

Lesson:

Phishing is when attackers send malicious emails designed to trick people into falling for a scam. The intent is often to get users to reveal financial information, system credentials or other sensitive data.

Phishing emails are a huge problem in the United States and beyond. An estimated 3 billion phishing emails are sent around the world each day, with Google alone blocking 100 million of these malicious messages on its Gmail platform. The world's largest email provider also scans more than 300 billion attachments for malware every week.

Email phishing is a numbers game. An attacker sending out thousands of fraudulent messages can net significant information and sums of money, even if only a small percentage of recipients fall for the scam. Attackers will usually try to push users into action by creating a sense of urgency. These phishers, or scammers, can be very convincing, but there are ways to protect yourself from these criminals.

How a Phishing Email Works

Phishing emails attempt to connect with you on an emotional level. This manipulative method, known as social engineering, typically appeals to one of four emotional senses:

1. Kindness: Asks you to help a specific person or group accomplish something.
2. Fear: Invites you to protect your bank account or remove viruses from your computer.
3. Greed: Offers to help you make money quickly and easily.
4. Duty: Insists you perform a task requested by an authority figure.

These emails play on hopes and fears, and there's always a sense of urgency to them. Scammers know we're often too busy and not paying attention to the details or we're just too trusting. That's why phishing emails work — people don't take time to read them carefully and think about them.

How To Spot A Phishing Email:

1. An Unfamiliar Tone or Greeting - The first thing that usually arouses suspicion when reading a phishing message is that the language isn't quite right. If a message seems strange, it's worth looking for other indicators that this could be a phishing email. Is the "From" contact a person or organization that you know? Don't respond or give any information to anyone that you don't know. Look at the signature at the end of the email. A lack of details about who sent the email could indicate a phisher trying to impersonate someone.

2. Grammar and Spelling Errors - Misspelled words, incomplete sentences, missing punctuation, and odd phrasing are often found in phishing emails. Barring rare exceptions, most reputable organizations will proofread their messages before hitting Send, so take note if you receive a poorly-written email with obvious grammatical errors.

3. Inconsistencies in Email Addresses, Links & Domain Names – Another simple way to identify a potential phishing attack is to look for discrepancies in email addresses, links and domain names. Email addresses and domain names that seem obscure should raise concerns. For example, if the message comes from an address like info@mail.paypalco.com rather than info@paypal.com or a URL is spelled oddly (for instance, www.targit.com instead of www.target.com), chances are it's phony. Look at the email address. Is the email domain spelled incorrect and/or does not match the email sender name? Do you recognize it?

4. Threats or a Sense of Urgency - Emails that encourage you to act quickly to take advantage of a special offer to avoid penalties and other negative consequences are often phishing emails. This approach attempts to rush you to, say, provide a password or open an attachment before you've had time to study the message for clues that it's fake.

5. Embedded Links - Before clicking on any link embedded in an email, hover your mouse pointer over it to highlight the address where it's trying to direct you. If the URL looks strange, differs from the stated source of the email, or doesn't start with https:// to indicate it's a secure site, steer clear.

6. Suspicious Attachments - If an email with an attached file is received from an unfamiliar source, or if the recipient did not request or expect to receive a file from the sender of the email, the attachment should be questioned. Look out for unusual extensions (.zip, .scr, .exe, .bat, and .vbs, to name a few). When in doubt, don't click to download or open the file. Recipients should flag the file to be virus-scanned before opening.

7. Unusual Request - If the email is asking for something to be done that is not the norm, then that too is an indicator that the message is potentially malicious. For example, purchasing gift cards or items for the sender to be reimbursed later.

8. Short and Sweet - While many phishing emails will be stuffed with details designed to offer a false security, some phishing messages have also been sparse in information hoping to trade on their ambiguity.

9. Recipient Did Not Initiate the Conversation - Because phishing emails are unsolicited, an often-used hook is to inform the recipient he or she has won a prize, will qualify for a prize if they reply to the email, or will benefit from a discount by clicking on a link or opening an attachment.

10. Request for Credentials, Payment Information or Other Personal Details - One of the most sophisticated types of phishing emails is when an attacker has created a fake landing page that recipients are directed to by a link in an official looking email. The fake landing page will have a login box or request that a payment is made to resolve an outstanding issue. If the email was unexpected, recipients should visit the website from which the email has supposedly come by typing in the URL – rather than clicking on a link – to avoid entering their login credentials of the fake site or making a payment to the attacker. Remember that just because you recognize a logo

on an email, that doesn't mean the email came from that company. Anyone can save a logo and use it as an image in an email.

11. Too Good to Be True - Emails that claim you'll win a prize by clicking on a link or opening an attachment shouldn't be trusted. Offers that sound "too good to be true," usually are. If you receive an email with any kind of offer that seems unbelievable, don't believe it.

12. See Something, Say Something - Identification is the first step in the battle against phishers. However, chances are if one employee is receiving phishing emails, others are as well. Organizations need to promote phishing awareness and condition employees to report signs of a phishing email – it's the old adage of "If you see something, say something," to alert security or the incident response team.

6 Types Of Phishing Emails That Where Dominate In 2022

1. Pandemic Related Phishing Emails - If there's a worrying topic related to the pandemic, cyber criminals have sadly found a way to capitalize on it.
   Keywords to look out for include: New variant details, Vaccination schemes, Booster shots, Health department guidelines.

2. Brand Impersonation Phishing - Attackers trick you into thinking they're someone you can trust enough to give out confidential information to, or click on links they provide. ALWAYS double check the sender's email first for inconsistencies.
   Keywords to look out for include: Reset Password Required, Update payment information, Click on links, etc.

3. Delivery Or Customs Phishing - Postage-themed phishing emails have been making the rounds recently, whereby scammers ask you to pay a fee or track a fake package via a malicious link.
   Keywords to look out for include: Failed delivery attempt, Pending customs fees, Tracking links of items you don't recall ordering.

4. Emails Reflecting Urgency Or Reward - Email subject lines requesting further actions with a sense of urgency or reward are a phishing classic — even with changing times, trends and subject lines.
   Keywords to look out for include: Save your account, Grab your Bonus, Immediate Action required, Your Data will be lost.

5. Invoice-Themed Phishing - This type of phishing emails has been especially targeting Finance employees, preying on their sense of responsibility to check and investigate any payment issues. They then use fake links, attachments or even PDF files to steal your credentials, spread malware, etc.
   Keywords to look out for include: Overdue Invoice, Update Payment details, Pending Invoice, PO Attached.

6. Tax Related Phishing Emails - Fake tax related phishing emails have been super common recently, especially during tax season. They usually seek things like your Social Security Number, Banking details, or any other confidential information that can be used to impersonate you or hack your account(s).
   Keywords to look out for include: Your TAX Return for Year X, TAX Account Restricted, TAX Payment Deducted, TAX Refund Due, Update TAX Information.

What Should You Do If You Think You Received A Phishing Email?

1. Call the supposed sender of the email to ask if they sent you anything. If not, don't reply to the email or open any attachments. If there is contact information on the email, do not use it. Try to search for the contact information of the company online instead so that you do not call the phisher.

2. Don't give out any personal information or send any money. Legitimate banks and other companies will not ask for your personal information via email.

3. If someone claims to be related to you and asks for money, call them instead of replying to the email. Don't send money or personal information to relatives via email either.

4. Never click on links or attachments you aren't sure of or aren't expecting. Links in phishing emails can lead you to fraudulent websites. Attachments in phishing emails can contain viruses that can compromise your personal information and your computer's security.

5. Delete the email so you don't accidentally click on it in the future.

What to Do if You've Been Phished (Suggested by PenFed Credit Union)

If you accidentally respond to a phishing email, time is of the essence. You need to immediately:

1. Disconnect from the Internet. This will help reduce the risk of malware spreading to other devices on your network. It will also prevent hackers from remotely tapping into your system.
2. Back Up Your Files. Since data can be lost or erased when recovering from a phishing attack, you should regularly save copies of all digital files — including invaluable items like family photos and videos — to an external hard drive or cloud storage. But if you haven't backed up in a while, go ahead and do it now.
3. Scan for Malware. If you have anti-virus software on your computer (and you should), run a complete scan and follow the instructions to remove or quarantine any malware. If you don't have an anti-virus program, take your machine to a tech specialist like Geek Squad.

Once you've addressed the most pressing issues, you should quickly move to:

1. Change Online Credentials. From a secure connection, change the login information for all of your online accounts, including email, online banking, utilities, retailers, social media, and anything else you access via the internet. Make sure to use different usernames and passwords for each account.
2. Contact Your Bank. If you entered account information or credit card numbers, unauthorized withdrawals or charges are likely soon to follow. Your financial institution and credit card company will guide you through the process of locking down your accounts and minimizing the impact.
3. Notify Credit Bureaus. If you suspect or know that cyber thieves have gained access to your personal information, you should file a fraud alert with one of the three main credit bureaus and they will alert the other two.

You may also want to put a credit freeze on your credit report to prevent new credit accounts from being fraudulently opened in your name. With a freeze, you'll need to contact all three bureaus separately: Equifax, Experian, and TransUnion.

Lesson Summary:

While phishing emails keep changing to reflect the issues users care most about, if you look closer, you'll notice that the tell-tale signs don't change much.

Phishing Awareness is your first line of defense against phishing emails. Make sure you're aware of current phishing trends and how to spot and deal with them.

Sources

"How to Better Avoid Email Scams" by Nancy Hightower, Arkansas Cooperative Extension
Phishing Emails by PenFed Credit Union
10 Most Common Signs of a Phishing Email by Cofense
6 Types of Phishing Emails to Keep an Eye on in 2022 by Gat Labs

Lesson Prepared By: Pam Hanfland, South Carolina Family and Community Leaders

Lesson Review By: Connie N. Lake, Extension Agent & FCL State Advisor