SCN
SECURE COMMUNITY NETWORK
COLLABORATION · VIGILANCE · EMPOWERMENT

BULLET

SECURE COMMUNITY NETWORK
Phone: 212.284.6940
Website: www.securecommunitynetwork.org

Michael
National D

07 May 2018
No. 12

Please report all relevant information and direct all media inquiries to the SCN Duty Desk:

Email: DutyDesk@securecommunitynetwork.org | Phone: 212.284.6940

SCN CYBER BULLETIN

How to Identify and Report a Phishing Attack

OVERVIEW

Phishing attacks are among the most common cyber threats facing organizations of all sizes, and they are becoming increasingly sophisticated. Over the last year, it is estimated that phishing attacks increased 65 percent worldwide and accounted for 90 percent to 95 percent of all successful cyberattacks.[1] The rise in phishing attacks is primarily due to the low cost of launching an attack and the expected high return for the criminal, with the average phishing attack costing a mid-size organization $1.6 million.[2]

Phishing attacks aim to deceive recipients into believing a fraudulent email is from a trusted individual or organization and then luring the recipient into revealing sensitive information or clicking on a website containing malicious code. While many attempted attacks may easily be spotted by the recipient, it is increasingly difficult to identify a fraudulent email as cyber criminals become more sophisticated. According to the Verizon Data Breach Investigations Report, 30 percent of phishing messages get opened by targeted users and 12 percent of those users click on the malicious attachment or link.[3]

The best way to keep an organization safe is to increase staff awareness of the threat, enabling them to effectively identify phishing attacks and empowering them to be part of the solution. SCN has developed the attached SCN Poster on **How to Spot a Phishing Scam** for dissemination to stakeholders to raise awareness of phishing indicators and best practices for preventing phishing attacks. SCN is available to work with organizations to co-brand this poster with an organization specific seal.

REPORTING A PHISHING ATTACK

What should you do if you successfully identify a phishing attempt before your information or system is compromised? Consider the following steps when responding to and reporting a phishing attack:

1. DO NOT OPEN ANY LINKS OR ATTACHMENTS INCLUDED IN THE EMAIL. DO NOT RESPOND TO THE EMAIL.
2. Follow internal protocols. If your organization employs IT professionals, immediately notify them.
3. Report the incident to SCN's Duty Desk at DutyDesk@securecommunitynetwork.org. We will communicate the incident to the relevant agencies. Please include the following in your report to SCN:
    - The email address where the phishing attempt was received
    - The organization the recipient is affiliated with, if any.
    - The time the phishing attempt was delivered, and the time it was detected.
    - A brief description of the phishing attempt and any actions taken. Please include whether the phishing email was opened, if any links/attachments were opened, and whether any sensitive/confidential information was potentially compromised.
    - In order to capture the most information about the phishing attempt, SCN also asks that you copy and paste the phishing message's email header below your email report to SCN's Duty Desk. The email header contains the originating IP address and other helpful information to make your report most effective. For more information about how to obtain the email header, follow the link with your email provider:
        - Gmail, AOL, Yahoo, and Hotmail
        - Apple Mail
        - Outlook 2016, Outlook 2013, Outlook, 2010, and Outlook 2007
4. As a precaution, you may also want to run a computer and email anti-virus scan.

You have just become a victim of a phishing attack and revealed sensitive information or compromised your system. What should you do?[4]

1. If you believe you may have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network and IT administrators. They can be alert for any suspicious or unusual activity. Follow all internal protocols.
2. If you believe financial accounts may be compromised, contact your financial institution immediately and notify them of any accounts that may have been compromised. Watch for any unexplainable charges to your account.
3. Inform the credit bureaus and request a fraud alert on your credit report. This alerts the bureaus of possible phishing activity and prevents anyone from opening new credit accounts in your name. (Note: The bureaus share information, so one request will result in notification to all three.)
4. Immediately change any passwords you may have revealed. If you used the same password for multiple resources, make sure to change it for every account. Do not use that password in the future.
5. File a report with the Federal Trade Commission – This is a trusted, one-stop resource to help you report and recover from identity theft. Information provided here includes checklists, sample letters, and links to other resources.
6. File a Police Report at your local police station to report identity theft. Be sure to bring the following:
    - government-issued photo ID

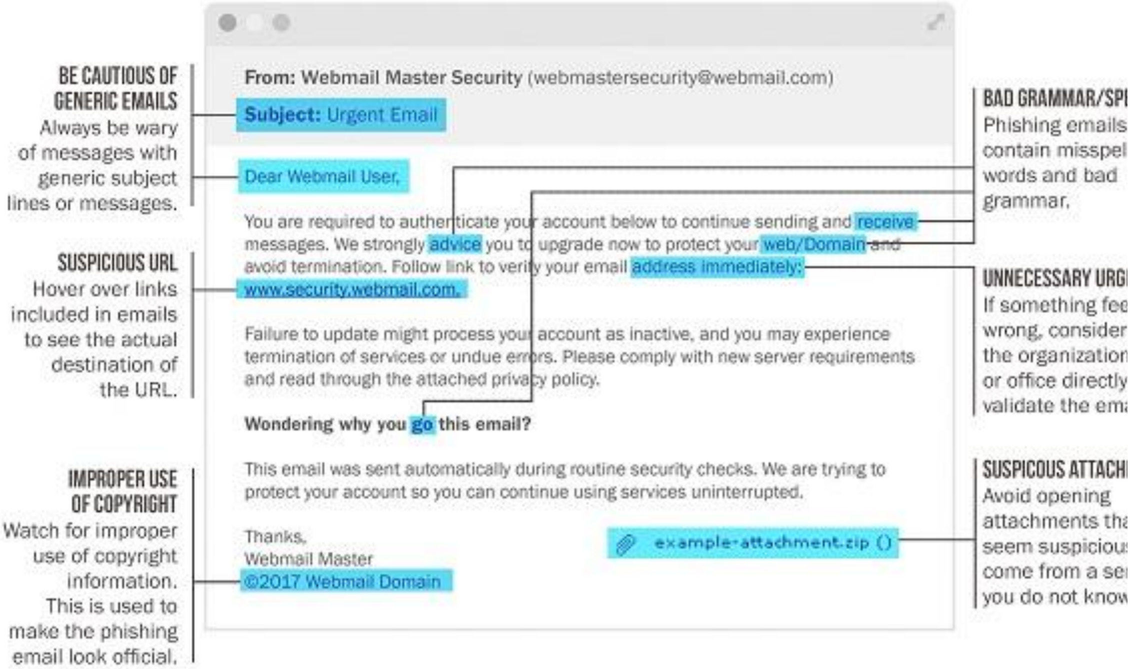
- proof of address (such as a utility bill or rental agreement/mortgage statement)
- proof of the theft (bills, IRS statements, etc.)
- a downloaded copy of the FTC Memo to Law Enforcement.

7. Report the incident to SCN's Duty Desk at DutyDesk@securecommunitynetwork.org. See instructions in the previous section.

Download SCN Cyber Poster Here

HOW TO SPOT A PHISHING SCAM

Phishing attacks are one of the most common forms of cybercrime and are a critical threat to any organization, especi as social engineering attacks become more sophisticated and difficult to identify. The best way to prevent a phish attack is to know how to identify a phishing email.



BE CAUTIOUS OF GENERIC EMAILS
Always be wary of messages with generic subject lines or messages.

SUSPICIOUS URL
Hover over links included in emails to see the actual destination of the URL.

IMPROPER USE OF COPYRIGHT
Watch for improper use of copyright information. This is used to make the phishing email look official.

From: Webmail Master Security (webmastersecurity@webmail.com)

Subject: Urgent Email

Dear Webmail User,

You are required to authenticate your account below to continue sending and receive messages. We strongly advice you to upgrade now to protect your web/Domain ~~and~~ avoid termination. Follow link to verify your email address immediately: www.security.webmail.com.

Failure to update might process your account as inactive, and you may experience termination of services or undue errors. Please comply with new server requirements and read through the attached privacy policy.

Wondering why you go this email?

This email was sent automatically during routine security checks. We are trying to protect your account so you can continue using services uninterrupted.

Thanks,
Webmail Master
©2017 Webmail Domain

example-attachment.zip ()

BAD GRAMMAR/SP
Phishing emails contain misspel words and bad grammar.

UNNECESSARY URG
If something fee wrong, consider the organization or office directly validate the ema

SUSPICOUS ATTACH
Avoid opening attachments tha seem suspiciou come from a se you do not know

"NCSAM Phishing Awareness 201
Department of Homeland Security, 25 Septemb

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency. Dissemination of FOUO is restricted to persons with “need-to-know.” Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties.

Typical FOUO requirements include:

1. FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.
2. The holder of the information will comply with access and dissemination restrictions.
3. Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

FOUO
For Official Use Only