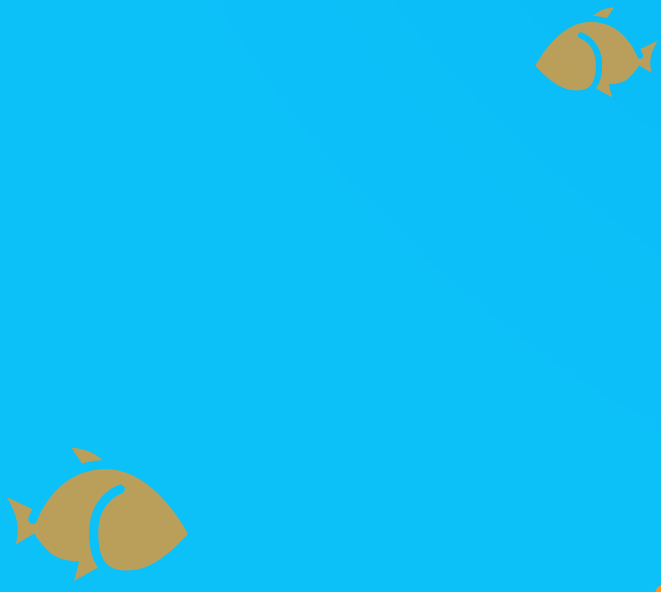
ONE PHISH TWO PHISH

How to Recognize and Deal with Phishing Scams

June 2019



SKYVIEW TECHNOLOGY

TABLE OF CONTENTS

Introduction.....2

What is Phishing?.....3

How to Identify Phishing.....4

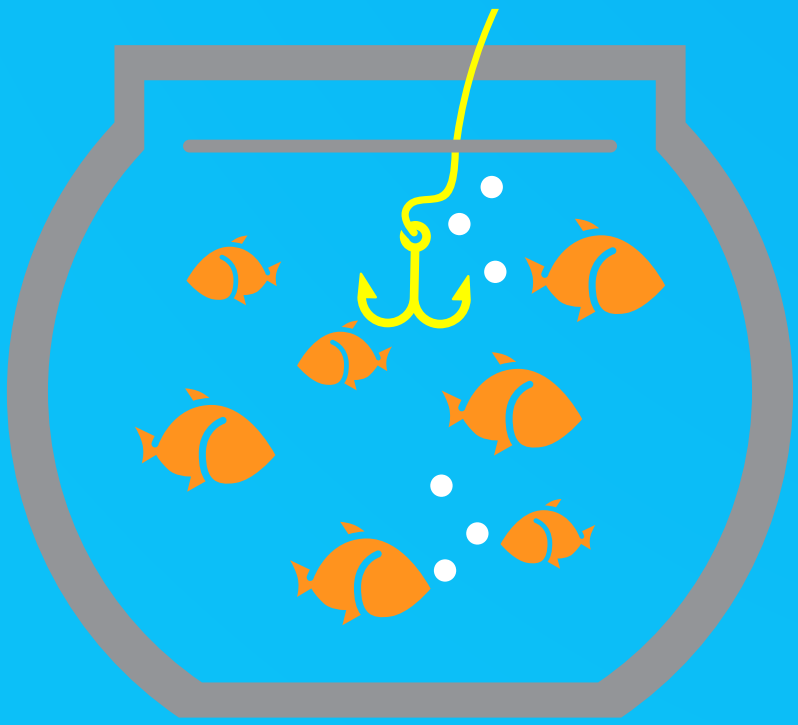
How to Avoid Falling Prey to Phishing.....6

Conclusion.....8

Additional Resources.....9

INTRODUCTION

For several decades, email has been the primary form of professional and casual communication on the internet. In April 2019, it was estimated that 293.6 billion emails are sent around the globe each day [1]. Because it is such a widely used form of communication, there are those who seek to take advantage of its scope and exploit it. Statista [2] reports that over 55% of emails sent are considered spam. Although spam inboxes assist in weeding these imposter messages out, there are still many that slip through filters and end up where trustworthy emails are sent. These emails, disguised as legitimate, are actually phishing scams that aim to attack users like you.



WHAT IS PHISHING

Phishing is the act of attempting to manipulate the recipient of a malicious email into opening and engaging with it. A sender of a malicious email intends to deceive a victim by making the email seem important and from a reputable source. These phishing emails may include harmful attachments, like PDF or Word documents, which once opened can cause harm to the user's computer by installing forms of malware, ransomware, or other unsavory software. Phishing emails can also contain malicious links in the body that can lead a user to a fraudulent site. These sites are used to collect confidential information such as usernames and passwords, or to install malware onto a device. Once the victim's information has been obtained, scammers will monetize the data by selling it to the highest bidder on Dark Web sites.

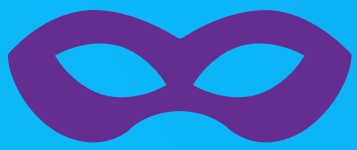
Deceptive Phishing is any attack by which fraudsters impersonate a legitimate company and attempt to steal people's personal information or login credentials.

Spear Phishing is when fraudsters customize their attack emails with a target's name, position, company, work phone number or other information in an attempt to trick the recipient into taking some action being requested by a known connection.

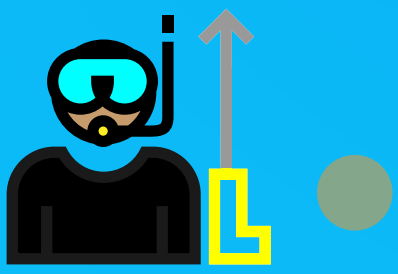
CEO Fraud is targeting an executive in an organization. Fraudsters attempt to isolate an executive and steal their login credentials. With these credentials they are able to perform a CEO scam. CEO scams occur when an email, seemingly addressed from a CEO or other member of senior management, is falsely created by a scammer in order to exploit the trust of employees. The imposter email seeks for the target to wire funds or share confidential information with the scammer.

TYPES OF PHISHING:

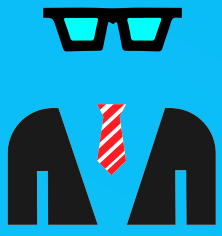
DECEPTIVE PHISHING



SPEAR PHISHING

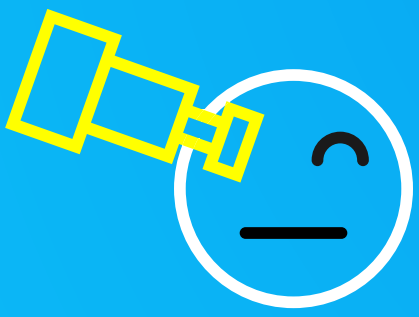


CEO FRAUD



HOW TO IDENTIFY PHISHING:

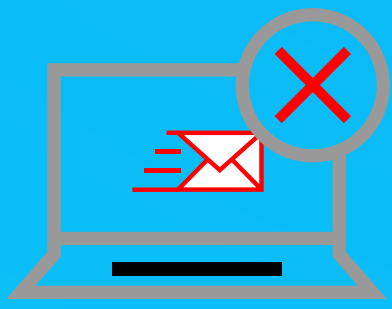
With the number of spam emails sent daily expected to increase to almost 190 billion a day through 2023 [3], it's increasingly important to be able to spot the tell-tale signs of a fraudulent email and protect your personal and business data, and your tech from malicious viruses and malware.



1. CONFIRMING PERSONAL INFORMATION

Often you will receive emails disguised to look authentic. They might mimic the style of your current company or an outside business such as a bank or credit card company. These emails may have requests for personal information that you would not usually provide, such as banking information or login credentials. It is important you don't click on or respond to these emails. Before responding, determine the legitimacy of the email by contacting an organization directly or searching on the internet.

2. FRAUDULENT EMAIL AND WEB ADDRESSES



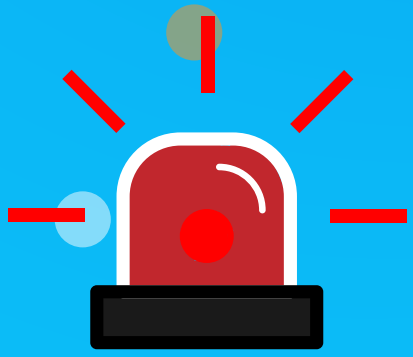
Phishing emails often come from an address that appears to be legitimate, but at a closer glance can have some discrepancies. These emails may contain the names of genuine companies and might be made to replicate the company's personal sites or email accounts. Brand logos and trademarks do not guarantee that an email is real. Hackers can use these images or download them from the internet to mimic an existing company. Even antivirus badges can be inserted into emails to persuade victims into thinking an email is from a legitimate source.

3. GRAMMAR

Phishing emails can sometimes contain poor language in the body of the message. Grammatical errors and conflictive sentence structure are common in these fraudulent emails. A legitimate company would have constructed an outbound communication professionally and checked for spelling errors and other mistakes. While poor grammar is a giveaway, not 100% of phishing emails will have sloppy grammar, so it is important to keep on your toes.

4. SCENARIOS

Many phishing emails tempt to instill a sense of worry into the recipient. The emails may give a scenario that depends on you entering your credentials to solve it. For example, an email may state that your account will be closed if you don't enter your personal information and act now. If ever unsure of what an email is asking of you and why, be sure to contact the company through other methods.



5. ATTACHMENTS

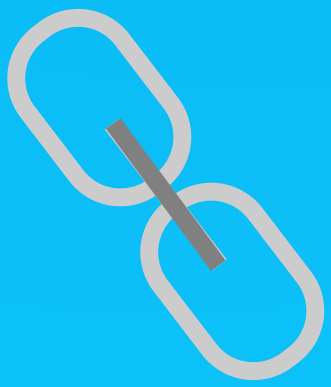
If you receive an email from a seemingly random company you do not affiliate with, and the email references something unexpected, the attachment might include some malicious malware or virus. These attachments may contain a URL or trojan horse designed to compromise your system, if opened. Send these emails to your security team instead of attempting to open them yourself.

HOW TO AVOID FALLING PREY TO PHISHING

Phishing attacks primarily disguise themselves as trusted organizations and people, preying on individuals' loyalty and exploiting it. You should be wary of email titles and phrases such as "your account has been locked," "update your record," "click to learn more," "you missed a delivery," "confirm your account," "suspended account," and unwarranted refunds on taxes or purchases. Emails can also be sent from seemingly reliable individuals such as your company's CFO or CEO. When in doubt, contact the sender or company directly through the official website or the individual in person. Do not click any of these links or attachments.

1. BE WARY OF LINKS

Hover over potential links in emails to verify the legitimacy before clicking on them, as this can prevent navigation to fraudulent sites or links that may contain malware. Hovering lets you see a site's full URL, and from here you can determine if the website is secure and the correct destination before visiting.



2. ANTI-PHISHING TOOLBARS

Some internet browsers can be fitted with anti-phishing toolbars that run checks on sites before you visit and compare them to lists of known phishing sites. This helps prevent you from navigating to fraudulent sites and decreases the risk of downloading any malicious content. Discuss this with your company's security team or MSP before adding.

3. VERIFY A SITE'S SECURITY

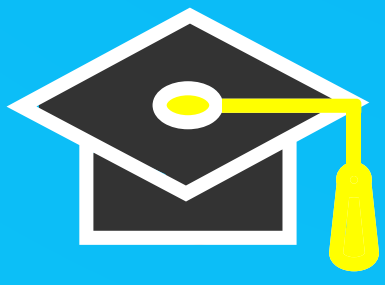
URLs that begin with "https" and have a closed lock icon near the address bar, are secure websites. These sites allow sensitive information to be entered with little risk.

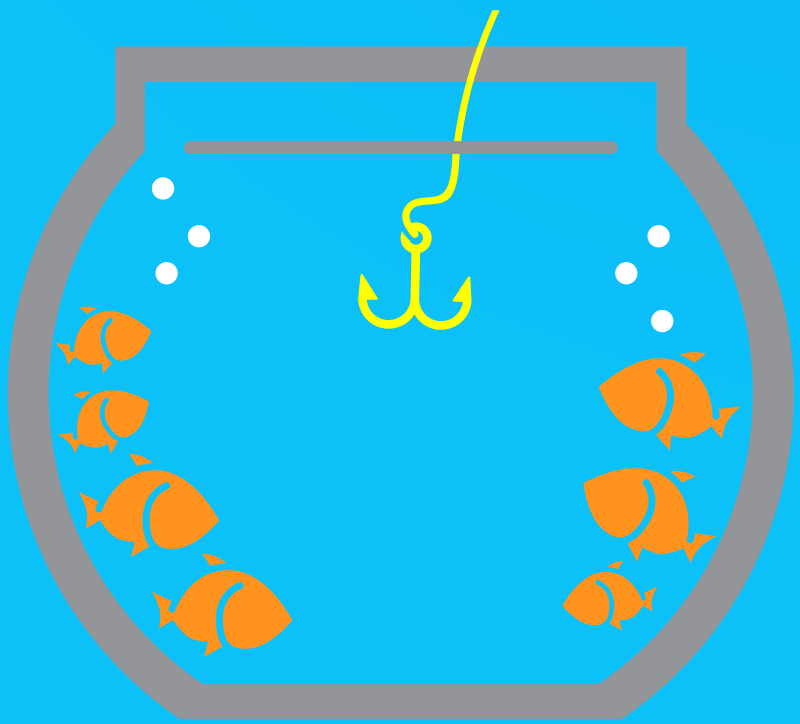
4. DON'T SEND PERSONAL FINANCIAL INFORMATION VIA EMAIL

You should only communicate secure information such as usernames, passwords or banking information via a secure website or over the phone. Don't fill out any forms in emails unless verified as legitimate.

5. EDUCATE

Many companies offer thorough training programs to help employees and individuals learn to identify and combat phishing techniques. Through necessary training, examples and procedures, you can reduce employee and individual susceptibility to different kinds of phishing.



CONCLUSION

Email being the main form of business communication poses different threats to organizations and individuals. Spam mail and phishing attacks can often be detrimental to an organization, these attacks can cause a breach of personal or clientele information, or a loss of funds. The best way to avoid and protect yourself from an attack is awareness and education. Knowing the different types of attacks, motives and identifying key features can help yourself and employees avoid malicious emails.