7 Tips for How to Spot Email Phishing.

Don Guilbeault - 2024-09-19 - Comments (0) - GENERAL

7 Tips for How to Spot Email Phishing.

Phishing is not a new phenomenon – it has been the most common attack vector for cybercriminals for several years. Due to the increasing complexity of phishing scams, knowing how to spot email phishing is becoming more important than ever before.

Despite advances in anti-virus protocols and detection technology, phishing attacks continue to increase in number and impact. Everyone is a target in today's cyberwar climate, but by educating your workforce about how to spot phishing and deal with phishing attacks appropriately, today's targets can become the primary defense sentinels of the future.

What Might be a Phishing Message?

A phishing message is an email or text that appears to be from a legitimate source but is sent by a threat actor with malicious intent.

Phishing messages can be sent through emails, websites, text messages or even through social media. These messages are often designed to appear like legitimate communications from banks, government agencies, online service providers or other organizations.

How to Spot Email Phishing?

The first step in how to spot email phishing comes with understanding what a phishing email is.

The most accurate definition of a phishing email is an email sent to a recipient with the objective of making the recipient perform a specific task. "**Call to Action**". The attacker may use social engineering techniques to make their email look genuine and include a request to click on a link, open an attachment, or provide other sensitive information, such as login credentials.

Socially engineered phishing emails are the most dangerous. They are constructed to be relevant and appear genuine to their targets. The recipient is more trusting of the email and performs the specific task requested in the email. The results can be devastating. If the recipient clicks on a link to a malware-infected website, opens an attachment with a malicious payload, or divulges their login credentials, an attacker can access a corporate network undetected.

Common Email Phishing Techniques:

SuperMailer Abuse is Now Responsible for 14% of All Credential Phishing

Threat detection agencies have observed a new phishing campaign that employs open redirect abuse, varied email senders, and URL randomization to bypass email security measures.

The Threat Actor Impersonates Email Security Providers to Steal User Credentials

Threat detection agencies have analyzed a phishing campaign impersonating email security providers that lure recipients into providing their user credentials via malicious HTML attachments.

Credential Phishing Attack Threatens Account deletion or closure

Threat detection agencies have observed a phishing campaign that uses an account deletion threat to create a sense of urgency and compel recipients to act quickly.

Phishing claiming to have EFT / e-Transfer / payment information

Threat detection agencies have seen an increase in payments transactions spoofing legitimate payment services to try and gain banking login credentials. With the increase in forms of electronic payment, would be thieves see this as an opportunity to target individuals that normally handle payment processes.

“Voicemail” attachments delivering ransomware payloads

Phishing emails sent to recipients claiming to contain a voicemail message as a HTML attachment, when opened redirects and delivers a payload to infect business networks with ransomware.

Why Socially Engineered Phishing Emails are So Effective:

It’s quite scary how much you can find out about an individual on the Internet without having to hack databases or trick somebody into divulging confidential information. Hackers can quickly accumulate personal information from social media sites, professional profiles, and other online publications to identify the triggers that people respond to.

It would not be too difficult to find details of an employee’s children, the school they attend, and an event happening at the school to send the parent an email inviting them to click on a link or open an attachment about their child’s participation in the event. With the advent of Machine Learning and Artificial Intelligence, phishers will be able to collate this information much more quickly in the future.

How to Spot Email Phishing with these 7 Tips

Socially engineered phishing emails often evade detection by email filters due to their sophistication. They have the right Sender Policy Frameworks and SMTP controls to pass the filter’s front-end tests and are rarely sent in bulk from blacklisted IP addresses to avoid being blocked by real-time global blacklist filters. Because they are often individually

crafted, they can even evade detection from advanced email filters with Grey listing capability.

However, phishing emails often have common characteristics. They are frequently constructed to trigger emotions such as curiosity, sympathy, fear and greed. If a workforce is advised of these characteristics – and told what action to take when a threat is suspected – the time invested in training a workforce in how to spot a phishing email can thwart attacks and network infiltration by the attacker.

1. Emails Demanding Urgent Action

Emails threatening a negative consequence, or a loss of opportunity unless urgent action is taken, are often phishing emails. Attackers often use this approach to rush recipients into action before they have had the opportunity to study the email for potential flaws or inconsistencies.

2. Emails with Bad Grammar and Spelling Mistakes

Another way to spot email phishing is bad grammar and spelling mistakes. Many companies apply spell-checking tools to outgoing emails by default to ensure their emails are grammatically correct. Those who use browser-based email clients apply autocorrect or highlight features on web browsers.

3. Emails with an Unfamiliar Greeting or Salutation

Emails exchanged between work colleagues usually have an informal salutation. Those that start “Dear,” or contain phrases not normally used in informal conversation, are from sources unfamiliar with the style of office interaction used in your business and should arouse suspicion.

4. Inconsistencies in Email Addresses, Links & Domain Names

Another way to spot phishing is by finding inconsistencies in email addresses, links, and domain names. Does the email originate from an organization that is corresponded with often? If so, check the sender’s address against previous emails from the same organization. Look to see if a link is legitimate by hovering the mouse pointer over the link to see what pops up. (Do not click the link) If an email allegedly originates from (say) Google, but the domain name reads something else, report the email as a phishing attack.

5. Suspicious Attachments

Most work-related file sharing now takes place via collaboration tools such as SharePoint, OneDrive or Teams. Therefore, emails with attachments should always be treated suspiciously – especially if they have an unfamiliar extension or one commonly associated with malware (.zip, .exe, .scr, .htm, .html, .png, etc). .htm and .html are some of the most common phishing attachments, even if other seemingly legitimate attachments are included. Bad actors will often include some basic non threating attachments to try and throw off the recipient when jumping through the additional malicious attachments.

6. Emails Requesting Login Credentials, Payment Information or Sensitive Data

Emails originating from an unexpected or unfamiliar sender that requests login credentials, payment information or other sensitive data should always be treated with caution. Spear phishers can forge login pages to look like the real thing and send an email containing a link that directs the recipient to the fake page. Whenever a recipient is redirected to a login page or told a payment is due, or you have received an electronic payment, they should refrain from inputting information unless they are 100% certain the email is legitimate.

7. Too Good to Be True Emails

Too good to be true emails are those which incentivize the recipient to click on a link or open an attachment by claiming there will be a reward of some nature. If the sender of the email is unfamiliar or the recipient did not initiate the contact, the likelihood is this is a phishing email.

How to Stop Email Phishing: "If You See Something, Say Something"

Conditioning employees on how to spot email phishing and report suspicious emails – even when opened – should be a workforce-wide exercise. The chances are that if one of your workforce is the subject of a phishing attack, other employees will be as well. "**If you see something, say something**" should be a permanent rule in the workplace, and it is essential that employees have a supportive process for reporting emails they have identified or opened.

The reporting of potential phishing attacks and opened suspicious emails enables security personnel to secure the network in good time – mitigating the risk that a threat will spread to other areas of the network and minimizing disruption.

FAQ

What is a Phishing Email?

A phishing email is an email sent with the objective of tricking the recipient into performing a specific task, "**Call to Action**". The action may be clicking a link that leads to a phishing or malicious website, or that downloads malware. The recipient may also be told to open a corrupt attachment or provide user credentials.

What Might be a Phishing Message?

In simple terms, a phishing message is an email or text that appears to be from a trusted source such as a bank, government agency, or well-known company. However, these messages are actually sent by cybercriminals with the sole purpose of tricking unsuspecting individuals into giving away their personal information or installing malware onto their devices.

What are signs of a Phishing email?

Emails that contain the following should be approached with extreme caution, as these are

common traits of phishing email:

- Urgent action demands
- Poor grammar and spelling errors
- An unfamiliar greeting or salutation
- Requests for login credentials, payment information or sensitive data
- Offers that are too good to be true
- Suspicious or unsolicited attachments
- Inconsistencies in email addresses, links, and domain names

How do I stop email phishing?

Even when software is in place to block malicious email, phishing can still get into employees' inboxes. It's important to report known or suspected phishing emails so they can be identified and removed. Reporting potential phishing attacks and opened suspicious emails allows security personnel to secure the network more quickly to mitigating the risk that a threat will spread. It's essential that employees have a process for reporting emails they've identified or opened.

Lastly when in doubt "**DELETE IT**", you can always contact the sender via other means to verify the legitimacy of the email and ask for the message to be sent again. Remember when reaching out to a sender for verification, never use any contact details provided in the suspicious email. Always search for contact details either from company directories, or search for their contact details on official websites.

Safe internet usage starts with you!