threatintelligencelab.com 18/02/2024

2024 PHISHING CHECKLIST

CLASSIFICATION
WHITE

THREAT INTELLIGENCE LAB.com

INTRO

25 CRUCIAL INDICATORS

Here are 25 crucial indicators to be vigilant for if you encounter a suspicious email. Elevate your skills in phishing detection and ensure this detailed guide is always within reach at your workstation. The digital landscape is fraught with potential threats, and you can never predict when the next phishing attempt might invade your inbox.

SCRUTINIZE THE "FROM" EMAIL ADDRESS

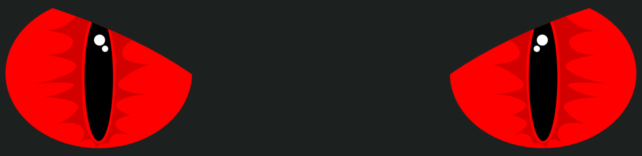
#1

One of the initial steps in identifying a phishing attempt is to carefully examine the sender's email address. Check the domain name closely—it should match the company or organization the sender claims to represent. Be especially vigilant for subtle misspellings or unusual characters, as these can be telltale signs of a phishing attempt.

LOOK OUT FOR SPELLING AND GRAMMAR MISTAKES

#2

Phishing emails often contain spelling and grammar errors. These mistakes can be due to the phisher's lack of proficiency in the language or reliance on automated translation tools. Any such errors in an email that's supposed to be from a professional organization should raise red flags.



VERIFY HYPERLINKS WITHOUT CLICKING

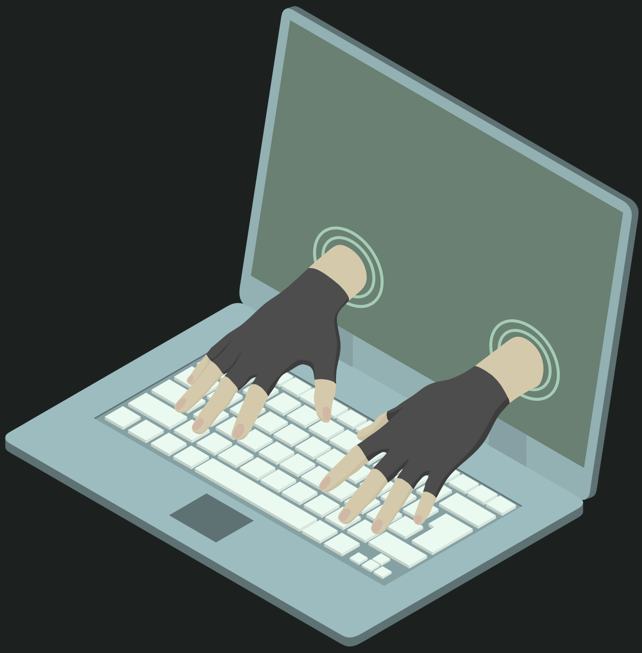
#3

Before clicking on any links in an email, hover over them to see the URL. This preview should match the expected destination's web address. Phishers often use legitimate-looking links that, when clicked, redirect to malicious sites. If in doubt, open a new browser tab and manually enter the website's address.

EXERCISE CAUTION WITH ATTACHMENTS

#4

Attachments in emails from unknown or suspicious sources should be treated with extreme caution. Never open an attachment unless you are completely sure of the sender's legitimacy. Malicious attachments can contain malware designed to compromise your system.



BEWARE OF URGENT OR THREATENING LANGUAGE

#5

Phishers commonly use urgent or threatening language to create a sense of panic or urgency, prompting you to act hastily. Always take a moment to critically assess the situation before responding to such emails.

GUARD YOUR PERSONAL INFORMATION

#6

Legitimate companies and organizations will never ask for sensitive personal information, such as passwords or Social Security numbers, via email. Any email requesting such information should be considered suspicious.

CHECK FOR PERSONALIZATION

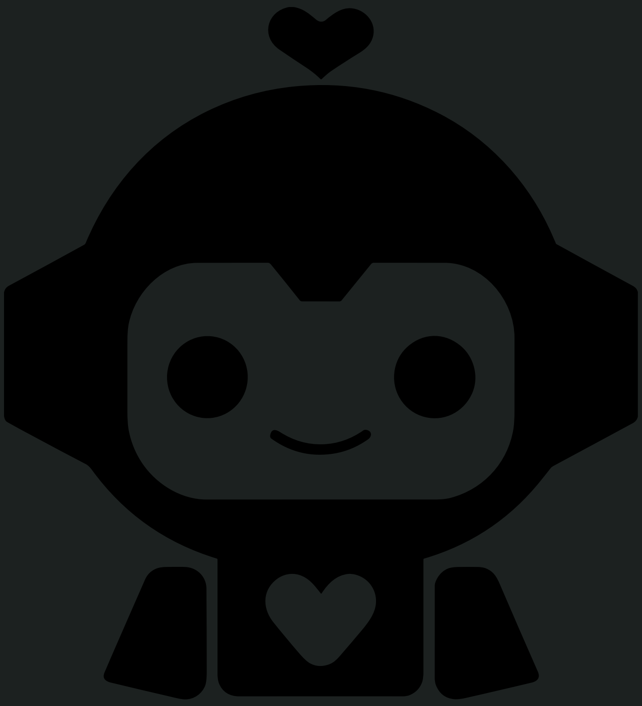
#7

Phishing emails are often generic and lack personalization. If an email addressed to you does not contain your name or contains incorrect details, it's likely a phishing attempt.

EVALUATE THE EMAIL'S GREETING

#8

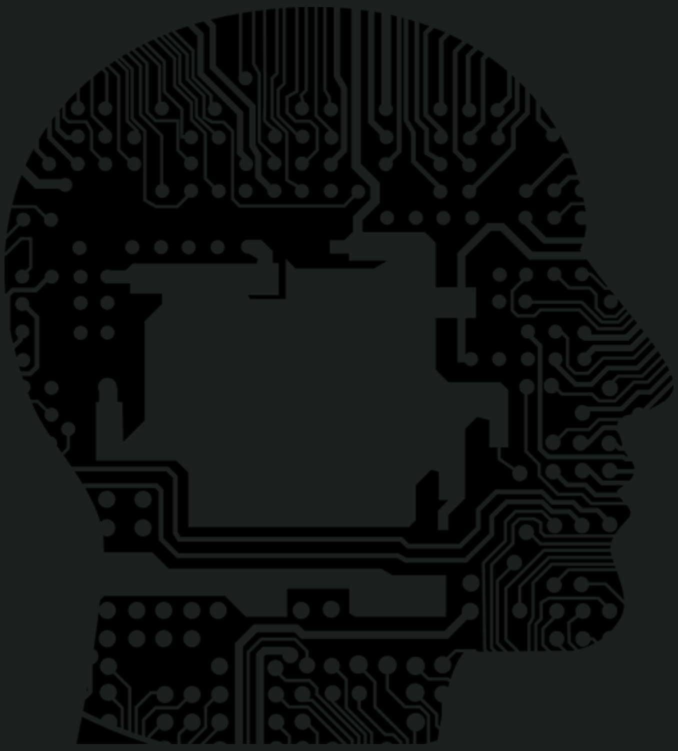
Be cautious of emails that use vague greetings like "Dear Customer" or "Dear User." Legitimate businesses often use personalized greetings with your name.



WATCH FOR INCONSISTENCIES IN ADDRESSES, LINKS, AND DOMAIN NAMES

#9

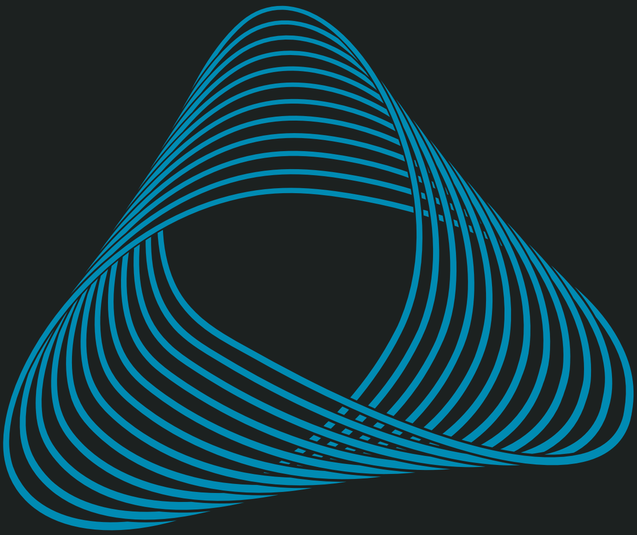
Analyze the email for any inconsistencies. For example, the email may claim to be from a reputable company but originate from a suspicious or unrelated email address.



USE EMAIL FILTERING OPTIONS

#10

Utilize your email service's filtering options to help identify and block phishing attempts. While not foolproof, these filters can reduce the number of phishing emails that reach your inbox.



UPDATE YOUR SOFTWARE REGULARLY

#11

Ensure that your operating system, web browsers, and security software are up to date. Software updates often include patches for security vulnerabilities that phishers exploit.

ENABLE TWO-FACTOR AUTHENTICATION (2FA)

#12

Implementing 2FA adds an additional layer of security, making it more difficult for attackers to gain unauthorized access to your accounts, even if they manage to phish your credentials.

EDUCATE YOURSELF ABOUT PHISHING TECHNIQUES

#13

Stay informed about the latest phishing techniques. Phishers constantly devise new strategies, so keeping abreast of these tactics can help you better recognize potential threats.

BE CAUTIOUS WITH PUBLIC WI-FI

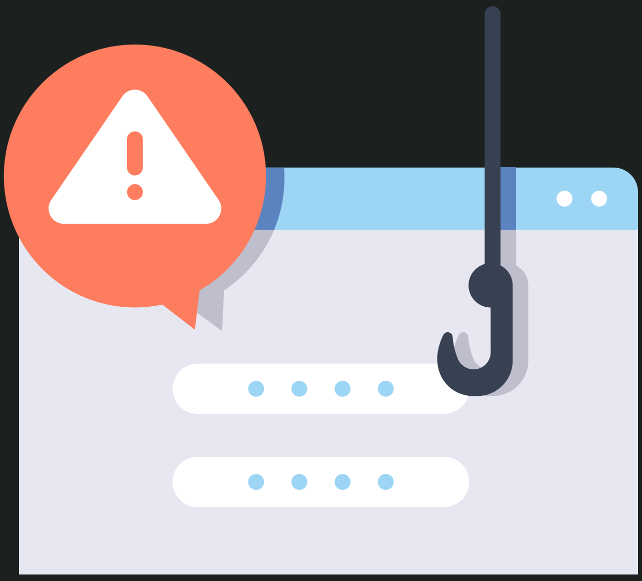
#14

Avoid accessing sensitive accounts or conducting important transactions over public Wi-Fi networks. Phishers can intercept data on these unsecured networks.

REGULARLY MONITOR YOUR ACCOUNTS

#15

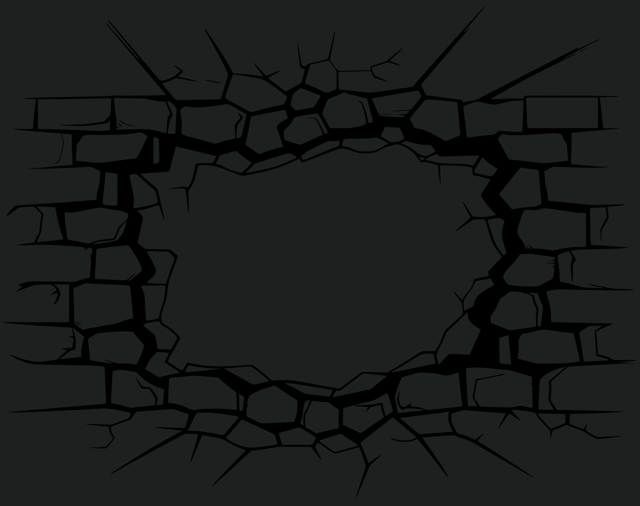
Regularly check your financial and personal accounts for any unauthorized activity. Early detection of suspicious activity can prevent significant damage.



USE SECURE WEBSITES

#16

When entering personal or financial information online, ensure the website is secure. Look for "https://" in the URL and a padlock icon in the address bar.



CONFIRM REQUESTS FOR SENSITIVE ACTIONS

#17

If you receive an email requesting sensitive actions, such as transferring money or providing confidential information, confirm the request through an alternative communication method.

BE WARY OF TOO-GOOD-TO-BE-TRUE OFFERS

#18

Phishing emails often lure victims with offers that seem too good to be true. Always approach such offers with skepticism.

REPORT SUSPECTED PHISHING EMAILS

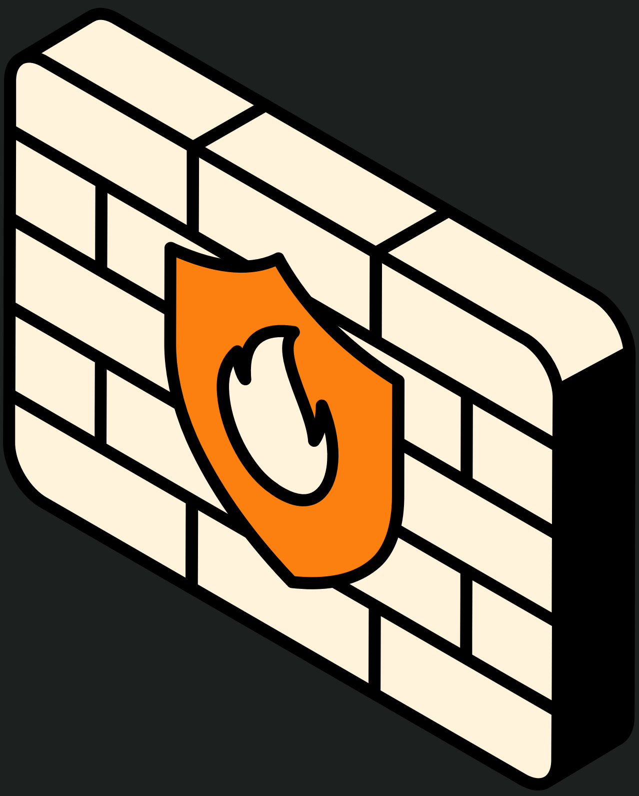
#19

Most email platforms allow you to report suspected phishing emails. Reporting these emails helps improve phishing detection for everyone.

USE A COMPREHENSIVE SECURITY SOLUTION

#20

Invest in a comprehensive security solution that includes antivirus, anti-malware, and anti-phishing features to protect your devices and data.



BACKUP YOUR DATA REGULARLY

#21

Regular backups can save your data in case of a phishing attack that leads to data loss or ransomware.

BE CAUTIOUS OF INFORMATION SHARED ONLINE

#22

The information you share online can be used by phishers to target you specifically. Be mindful of the personal details you post on social media and other platforms.

UNDERSTAND YOUR EMAIL CLIENT'S SECURITY FEATURES

#23

Familiarize yourself with the security features offered by your email client, such as phishing alerts and the ability to analyze email headers for authenticity.

PRACTICE SAFE BROWSING HABITS

#24

Develop safe browsing habits, such as avoiding clicking on pop-up ads or downloading files from untrusted websites.

TRUST YOUR INSTINCTS

#25

Finally, trust your instincts. If an email feels off in any way, it's better to err on the side of caution and verify its legitimacy before taking any action.

TRY OUR TOOLS AT

THREAT INTELLIGENCE LAB.com