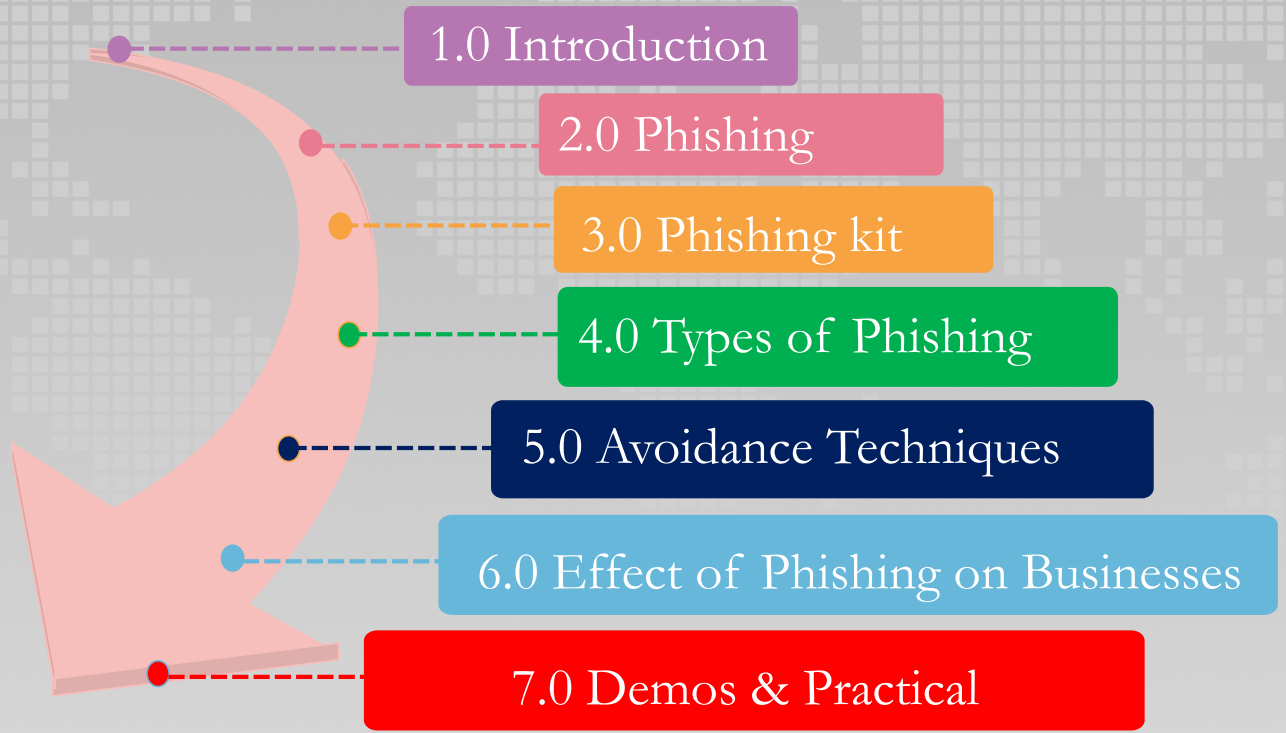
OWASP
Open Web Application Security Project

PHISHING IN DEPTH

(ATTACKS & MITIGATIONS)

Table of Content



INTRODUCTION

- ERIC NII SOWAH BADGER (NiiHack)
- Software Developer / Certified Ethical Hacker
- Penetration Tester / CTF Player on HackTheBox
- Member of Inveteck Global
- LinkedIn: Eric Nii Sowah Badger
- INSTAGRAM: ni1hack
- TWITTER: ens_nii

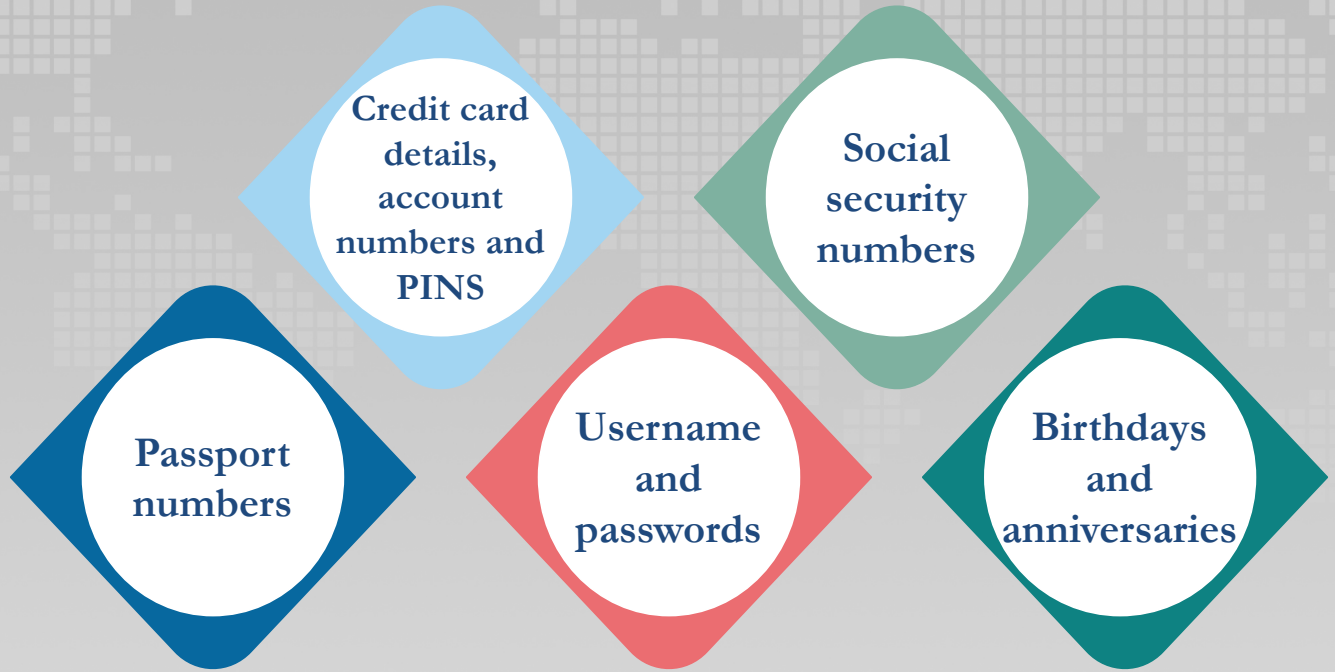
PHISHING

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

The recipient is tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

Phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack,

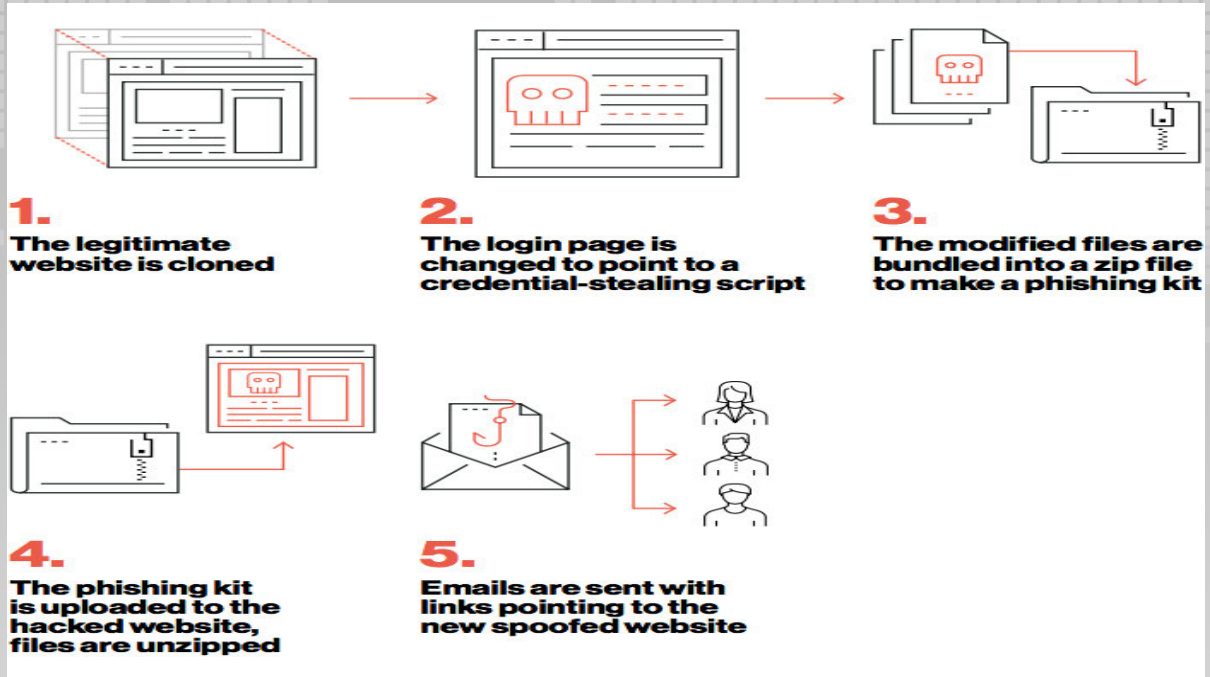
What kind data do criminals want from victims?



PHISHING KIT

- A phishing kit is the web component, or the back-end to a phishing attack.
- It's the final step in most cases, where the criminal has replicated a known brand or organization.
- Once loaded, the kit is designed to mirror legitimate websites, such as those maintained by Microsoft, Apple or Google.

ANATOMY OF A PHISHING KIT



STEPS IN CREATING A PHISHING KIT

TYPES OF PHISHING

EMAIL PHISHING

Usually appear to come from a well-known organization and ask for your personal information — such as credit card number, social security number, account number or password

VISHING

is the telephone equivalent of phishing. It is described as the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft.

WHALING

A method to masquerade as a senior player at an organization and directly target senior or other important individuals at an organization, with the aim of stealing money or sensitive information or gaining access to their computer systems for criminal purposes.

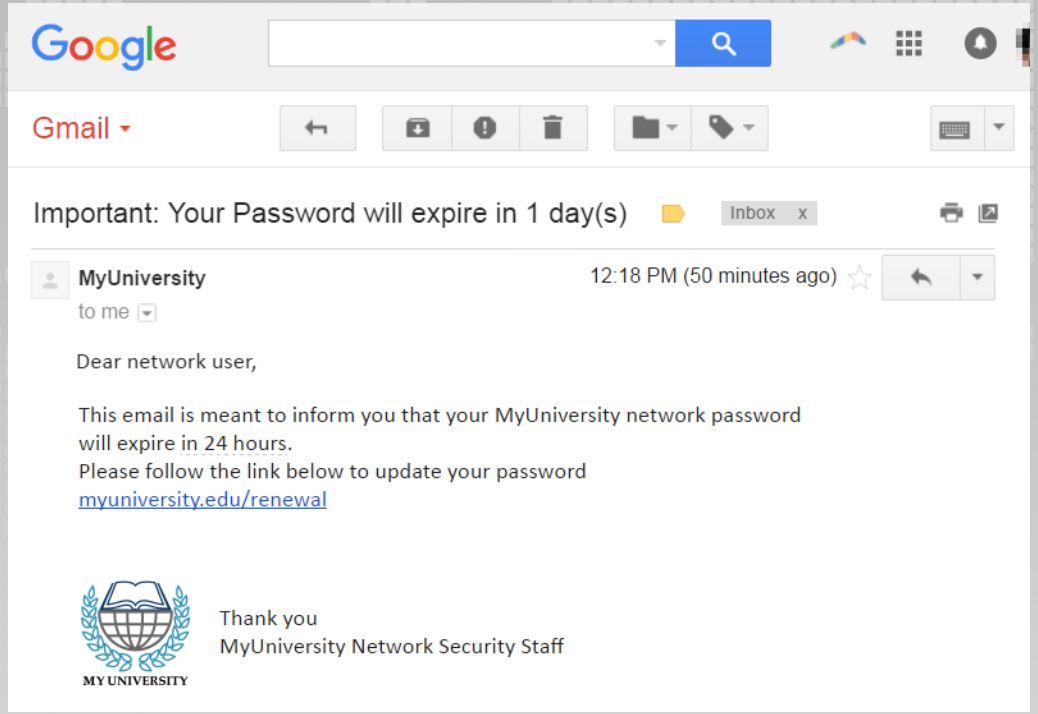
SMISHING

When someone tries to trick you into giving them your private information via a text or SMS message

SPEAR PHISHING

The fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information

EMAIL PHISHING



SAMPLE EMAIL PHISHING TO HAVEST PASSWORDS

SMISHING PHISHING

FREE DATA TO ALL MOBILE NETWORK USERS!!

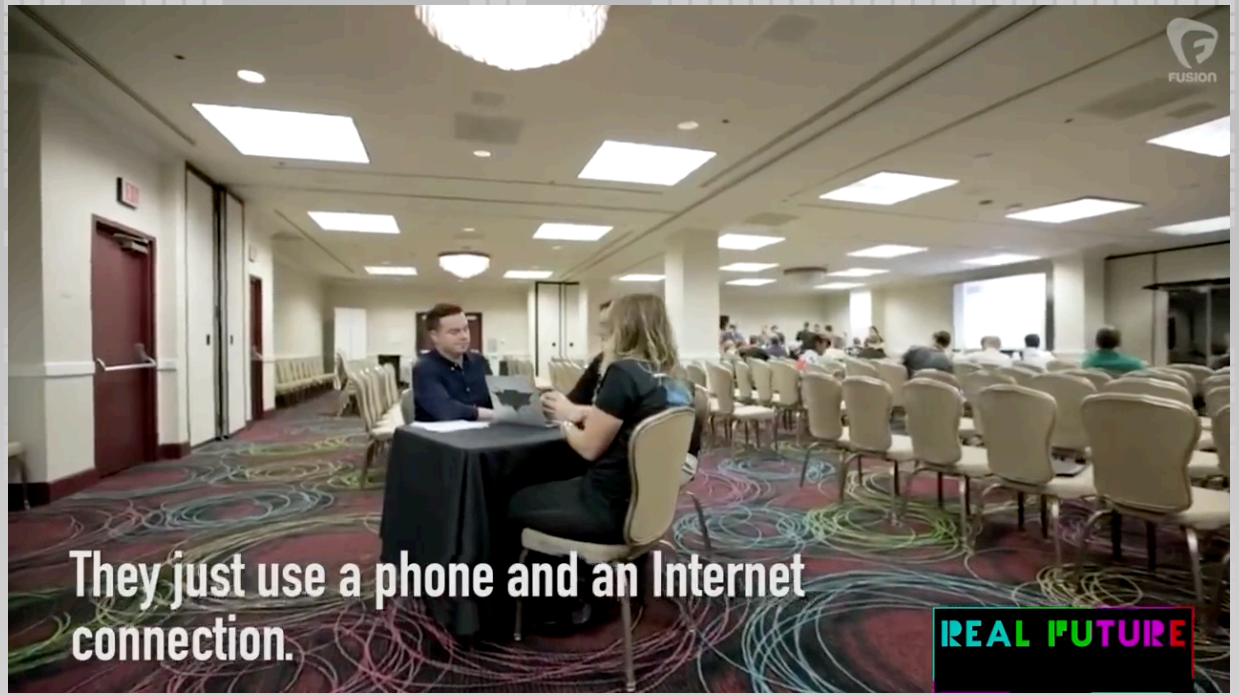
It's Today, Grab your Free 6GB Data Bundle, it will be given to only 2,000 people in the next 24 hours. I just received mine now. Hurry up before it Ends.
Tap the link below to get yours Now!!!.

https://bit.ly/today-free-data-offer

6:55 AM

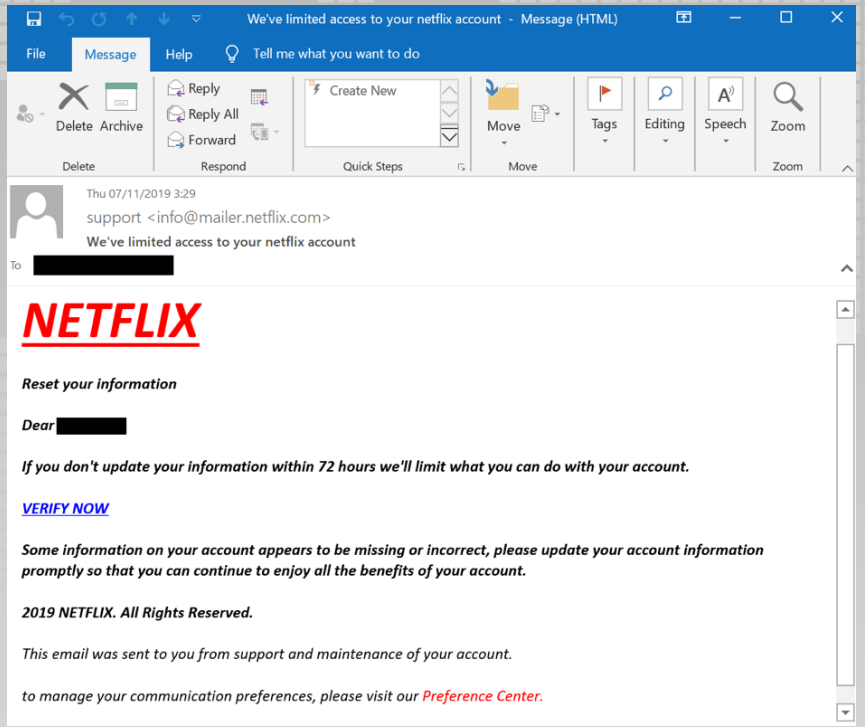
SAMPLE SMISHING MESSAGE TO HARVEST PERSONAL INFO

VISHING



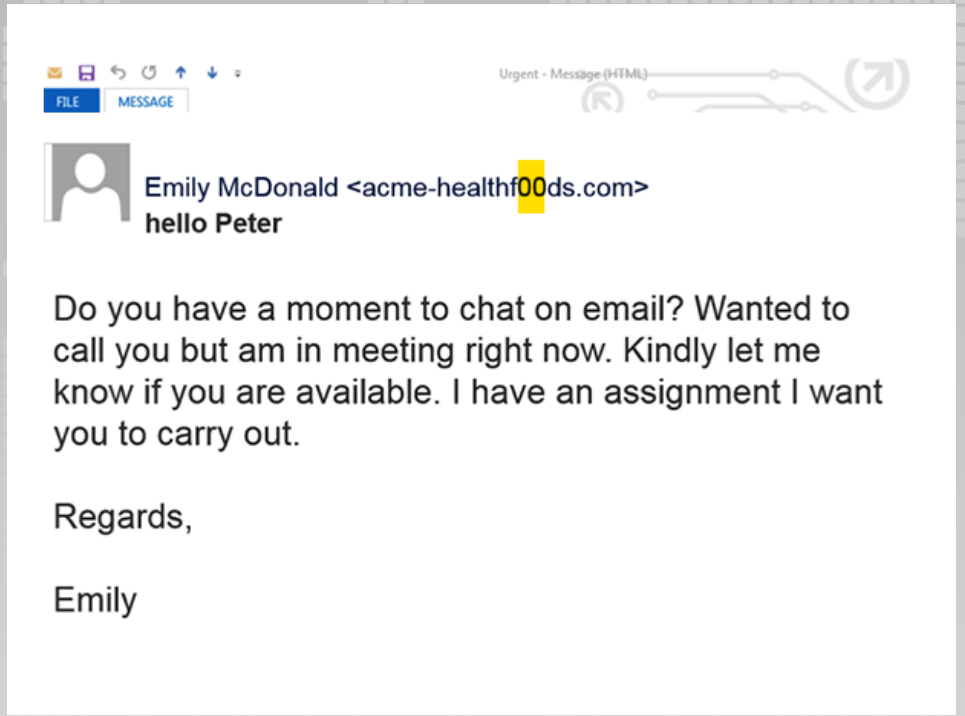
VIDEO DEMO OF A VISHING ATTACK TO GET SENSITIVE INFO

SPEAR PHISHING



SAMPLE SPEAR PHISHING MESSAGE TARGETED AT A NETFLIX USER

WHALING



SAMPLE WHALING MESSAGE TO GET PERSONAL INFO

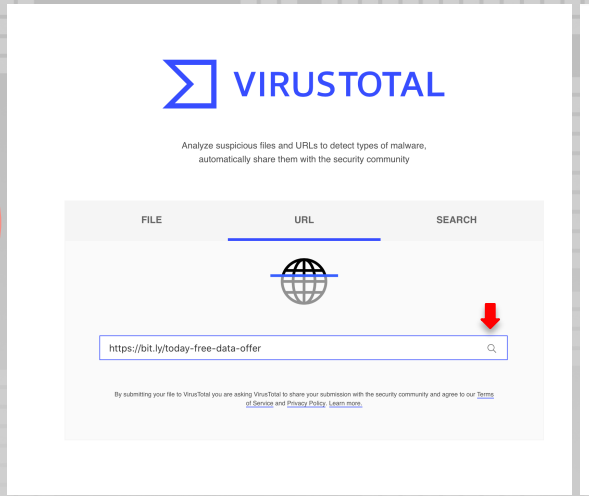
AVOIDANCE TECHNIQUES

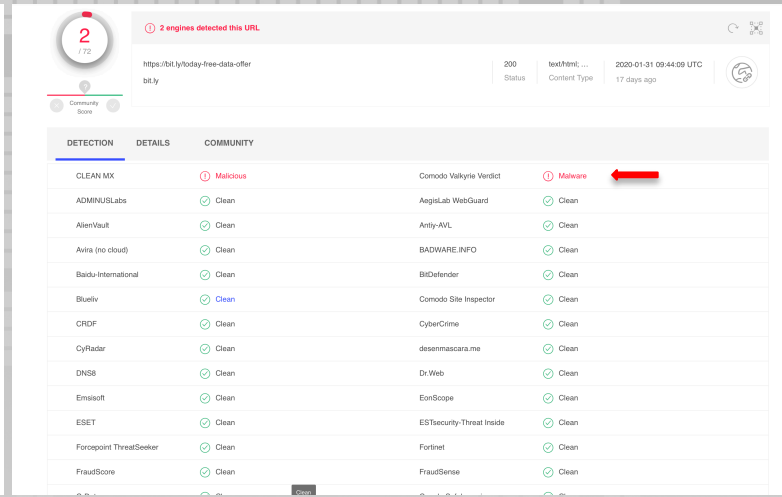
- Always, Always Think Twice Before Clicking
- Two Factor Authentication (2FA)
- Don’t click on links, type them directly in the URL
- Verify link first before clicking (www.virustotal.com)
- Hover mouse on link to be sure its legit before clicking

AVOIDANCE TECHNIQUES

- Always, Always Think Twice Before Clicking (There is no free lunch)
- Avoid clicking on any UNKNOWN messages with links
- Verify links if there are malicious(contains malwares or viruses) first before clicking (www.virustotal.com)
- Ignore and flags suspicious texts
- Do extensive research before replying to any message.

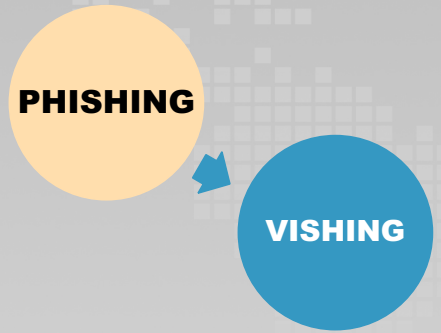
AVOIDANCE TECHNIQUES





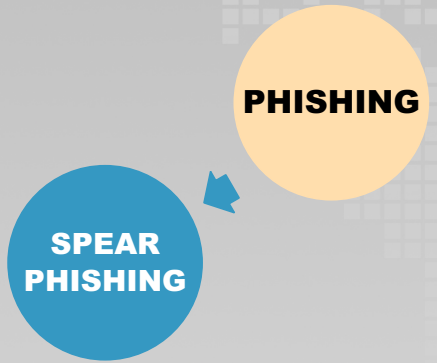
HOW TO USE VIRUSTOTAL TO VERIFY LINKS FOR MALWARES AND OTHER MALICIOUS CODES BEFORE CLICKING ON THEM
WWW.VIRUSTOTAL.COM

AVOIDANCE TECHNIQUES



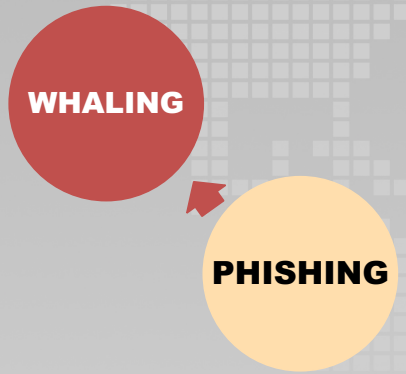
- Be very suspicious of any caller who asks you to share login information over the phone.
- If a caller asks you to provide account data or personally identifiable information, refuse to do so
- Security won't call you to request that you change logins, passwords, or network settings.
- Always do a 2nd Verification of suspicious calls

AVOIDANCE TECHNIQUES



- Don’t be swayed just because a correspondent
  seems to know a lot about you
- Don’t rush to send out data just because the other person tells you it’s urgent
- Don’t be afraid to get a second opinion
- Verify and validate
- Trust no one

AVOIDANCE TECHNIQUES



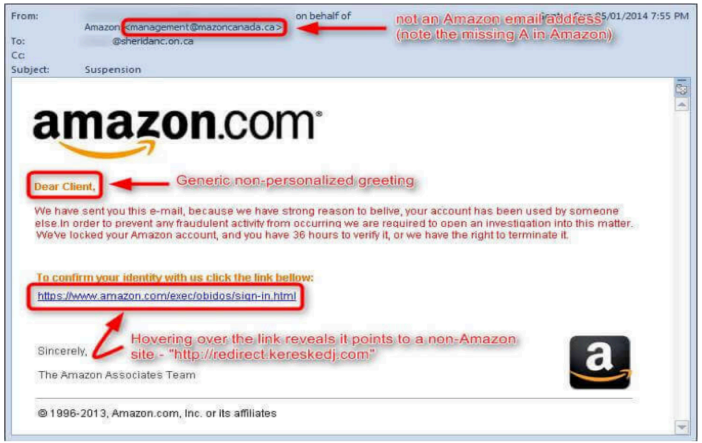
- Use two-factor authentication for email to avoid accounts becoming compromised.
- Establish a verification process for transferring funds, such as face-to-face verification or verification over the phone.
- Utilize an email filtering system for inbound emails that flags emails sent from similar-looking domain names.
- Use mock whaling attacks against employees to teach them how easy it is to be tricked.
- Enforce strict Passwords policies

AVOIDANCE TECHNIQUES

End users! Verizon's 2018 Data Breach Investigations Report showed that **93%** of security incidents are the result of phishing, and this is solely due to end user behavior.

Phishing attempts are only successful with user interaction. An unopened phishing email is basically harmless. To unleash its destructive capabilities, a human must reply with information, or click a malicious link.

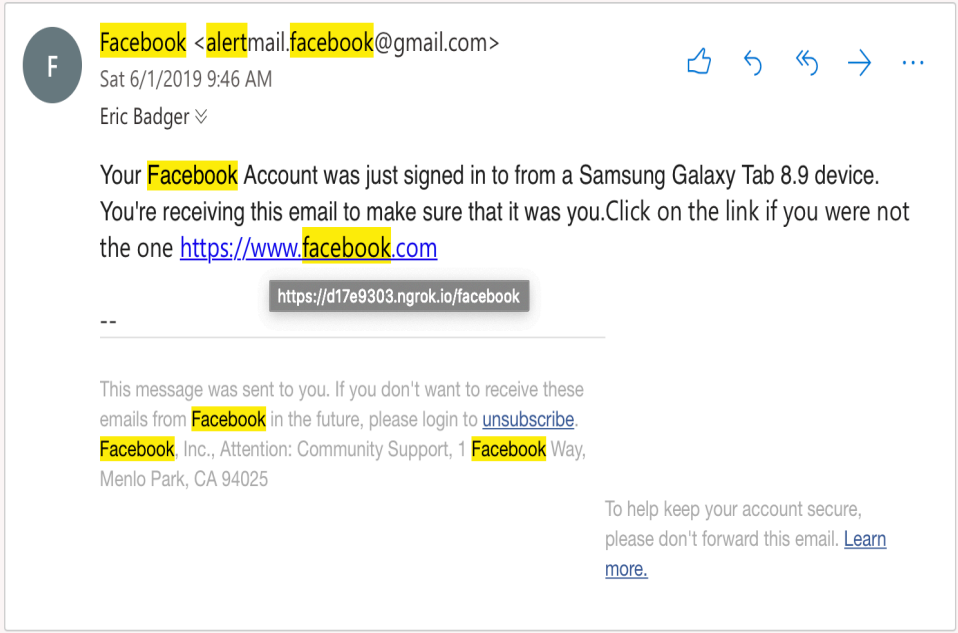
Here is a great example of how easy it is to be fooled by a phishing email.



If you're not paying attention, you may click on the malicious link, and infect your entire network.

No doubt about it, lack of phishing training is the weakest point of your organization's network.

Facebook



HOW TO DETECT PHISHING EMAIL

EFFECTS OF PHISHING ON BUSINESSES

1. Reputational Damage

Headlines like “British Airways data breach: Russian hackers sell 245,000 credit card details” and “Uber concealed massive hack that exposed data of 57m users and drivers”.

2. Loss of customers

After 157,000 of TalkTalk’s customers had their data compromised in 2015, customers left in their thousands. The company’s eventual financials revealed the true costs of the breach to be around £60m in 2016 alone.

3. Loss of company value

Following the compromise of Facebook user data in 2018, Facebook’s valuation dropped by $36bn – a loss from which (at the time of writing) the company is yet to fully recover. In public companies, the pattern is clear: following a breach, company value decreases.

4. Regulatory fines

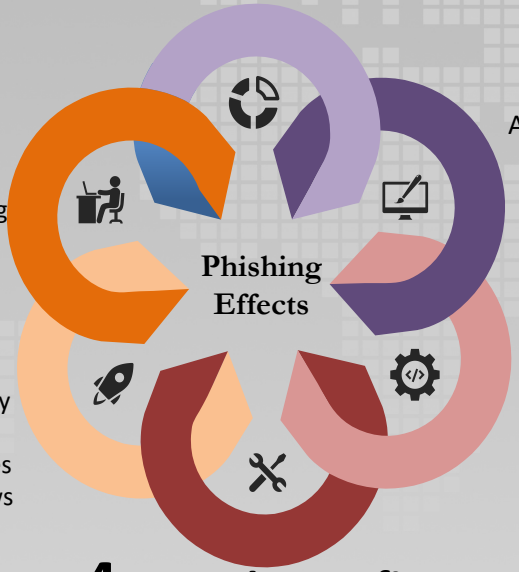
Financial penalties for the misuse or mishandling of data have been in place for decades. Under GDPR, the penalties can total €20 million or 4% of a company’s annual global turnover – whichever is higher.

5. Business disruption

After being infected by malware in 2017 (most likely following a phishing email), the advertising multinational WPP instructed its 130,000 employees to “immediately turn off and disconnect all Windows servers, PCs and laptops until further notice.”

6. Safeguarding against phishing

Phishing filters can help but, unfortunately, no phishing filter is 100% effective.



OWASP
Open Web Application Security Project

THE NEW INDIAN EXPRESS

NATION WORLD STATES CITIES BUSINESS SPORT GOOD NEWS MOVIES GALLERIES

Home › Nation

Military comes under phishing attack, Army points finger at crooks in Pak, China

A senior Indian Army officer said cyber attacks on India's critical infrastructure are originating either from Pakistan or China.

Published: 07th December 2019 03:48 PM | Last Updated: 07th December 2019 04:00 PM | A+ A A-

For representational purposes (Express Illustrations)

By IANS

EFFECTS OF PHISHING ON INDIAN ARMY

US Govt Warns Critical Industries After Ransomware Hits Gas Pipeline Facility

February 19, 2020 Ravie Lakshmanan

The U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) earlier today issued a warning to all industries operating critical infrastructures about a new ransomware threat that if left unaddressed could have severe consequences.

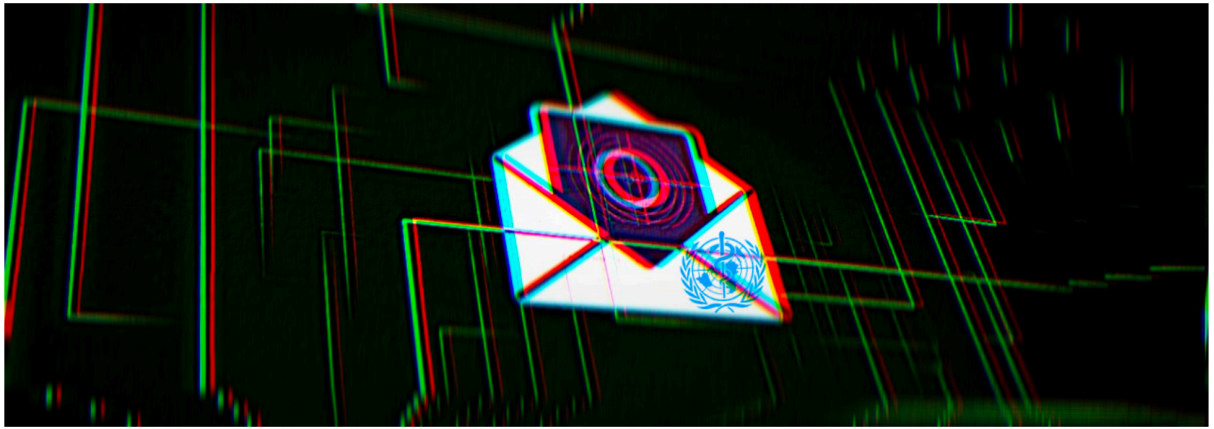
The advisory comes in response to a cyberattack targeting an unnamed natural gas compression facility that employed spear-phishing to deliver ransomware to the company's internal network, encrypting critical data and knocking servers out of operation for almost two days.

SPEAR-PHISHING ATTACK USED TO DELIVER RANSOMWARE TO A COMPANY'S INTERNAL NETWORK

World Health Organization Warns of Coronavirus Phishing Attacks

By Sergiu Gatlan

February 17, 2020 02:50 PM 1



The World Health Organization (WHO) warns of ongoing Coronavirus-themed phishing attacks that impersonate the organization with the end goal of stealing information and delivering malware.

"Criminals are disguising themselves as WHO to steal money or sensitive information," the United Nations agency says in the Coronavirus scam alert.

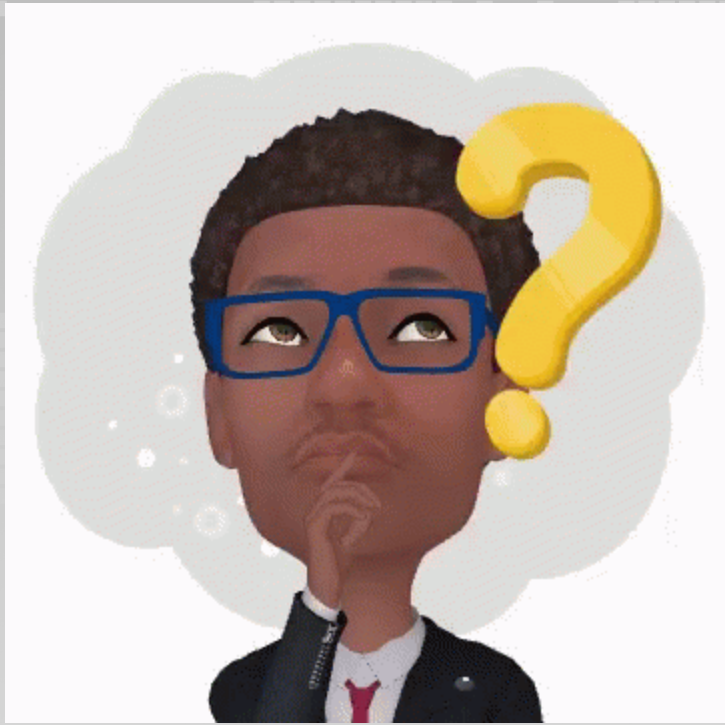
WORLD HEALTH ORGANIZATION WARNS OF CORONAVIRUS PHISHING ATTACKS

DEMOS & PRACTICALS

REFERENCES

- https://www.imperva.com/learn/application-security/phishing-attack-scam/
- https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing
- https://www.mimecast.com/blog/2018/10/4-simple-tips-for-stopping-vishing/
- https://www.ntiva.com/blog/how-phishing-affects-businesses
- https://www.newindianexpress.com/nation/2019/dec/07/military-comes-under-phishing-attack-army-points-finger-at-crooks-in-pak-china-2072861.html
- https://thehackernews.com/2020/02/critical-infrastructure-ransomware-attack.html?m=1

QUESTIONS



THANK YOU