Original Article

How to Deal with Phishing Scams During COVID19

Rishit Mishra

Security Manager, PwC, Dallas, TX, USA

Received Date: 30 March 2020
Revised Date: 13 May 2020
Accepted Date: 15 May 2020

Abstract - *With the world engrossed in COVID 19, threat actors are using this opportunity to perform cyberattacks on individuals and organizations. One of the most common forms of attack that is being observed currently is phishing attacks. In this article, we'll talk about the types of Phishing attacks that are being seen and how to protect yourself from those.*

Keywords - Cybersecurity, *security, Phishing, COVID – 19, vulnerabilities, social engineering, malware*

I. INTRODUCTION

The one word that is keeping everyone awake these days is "COVID-19". The pandemic has been in the headlines for the past few months and brought new terms such as "social distancing" on the lips of everyone you know. This pandemic has also greatly changed the way we work and has forced companies and employees to adapt to a remote working model. In this trying time, cybercriminals are more active than ever and are using every opportunity to exploit the situation. The number of cyberattacks since COVID 19 started has been steadily on the rise. In this article, we try to explore one of the most common and effective forms of attacks cybercriminals are using and how organizations/individuals can protect themselves from these.

II. WHAT IS PHISHING?

When someone thinks of COVID 19, cybersecurity or cyberattacks are not something that seems to come to mind or even seem interrelated. But if you think carefully and put your hacker hat on, you" find that, in fact, this time is a very fertile window for the cybercriminals to launch an attack. On April 8, 2020, a joint alert was issued by the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC), alerting on the exploitation by the cybercriminals and the mitigations that can be put into place.

A research organization noted a 667% increase in phishing attacks related to COVID 19. But how is that happening? The answer to this – Social Engineering.

Social engineering is and has been one of the oldest and most common ways used for cyber attacking by threat actors. In social engineering, the attacker interacts with the human by using his social skills and tries to obtain information that can compromise the information of an organization or its IT/computer systems. The attacker at times claims to be either a new employee or someone who's coming to repair and can even offer credentials that support his identity. Their aim is to piece together enough information about the organizations and their systems so that they can launch a cyberattack. The attacker might gather this information from one or many sources. In instances when one source is not enough, they use the information gained by the first source to have a conversation with the second source and use the information from the first source to try to gain their trust and establish credibility.

Phishing is a form of social engineering. These attacks use different methods such as email, malicious websites etc., to gain information which is mainly achieved by posing a trustworthy organization. A lot of times, we have received emails from reputable banks credit card companies asking for information stating that there is a problem. The user, without noticing what the URL is, clicked on the link and might land upon a site that might be an exact replica of the original site and put in the required information, thus compromising the information.

Several threat actors sometimes also ask users to open attachments which, when clicked, can result in downloading of malicious software. This malicious software also called malware, then can give the attacker access to your computer, the ability to log your keystrokes, access to your financial or personal information, which could result in identity theft.

III. TYPES OF PHISHING ATTACKS

Google recently published that it saw more than 18 million daily phishing and malware emails that were related to COVID 19. The way they work is that they use the fear and curiosity of the user and create a sense of urgency which forces the user to perform an action like responding with the information or clicking the malicious link.

Below is the different type of attack techniques that have been observed.

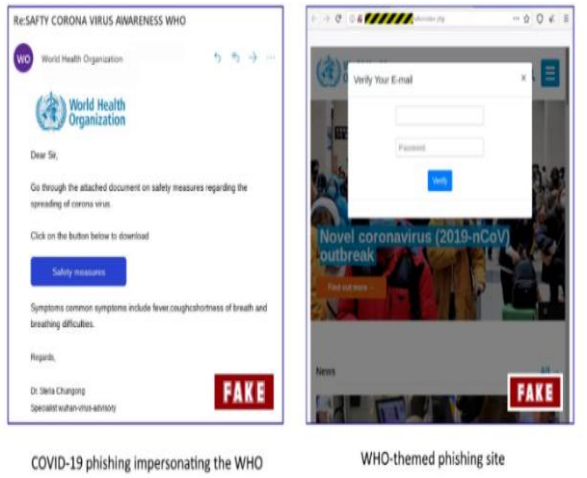
A. *Email Phishing*

Emails have been and are still the most common form of a cybersecurity attack. So, it's no surprise that even during the COVID 19 pandemic, email is the method that is being utilized most effectively to scam individuals. Using subject lines like Coronavirus Updates, New Confirmed cases in your area etc., the threat actors play on the victim's curiosity and force them to open the email.

Types of emails that have been seen include

a) Alerts

Cybercriminals are sending emails that look like alerts from the CDC (Centres for Disease Control) or WHO. It provides a list of cases within your area and urges you to click on the link.



Re:SAFTY CORONA VIRUS AWARENESS WHO

World Health Organization

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.

Click on the button below to download

Safety measures

Symptoms common symptoms include fever.coughshortness of breath and breathing difficulties.

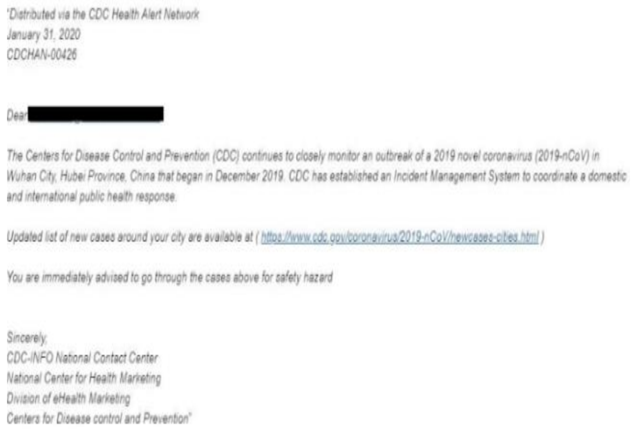
Regards,

Dr. Stella Chungong
Specialist wuhan-virus-advisory

WO
World Health Organization
FAKE
Verify Your E-mail
Password
Verify
Novel coronavirus (2019-nCoV) outbreak
Find out more
News
FAKE

COVID-19 phishing impersonating the WHO

WHO-themed phishing site



"Distributed via the CDC Health Alert Network
January 31, 2020
CDCHAN-00426

Dear [redacted]

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

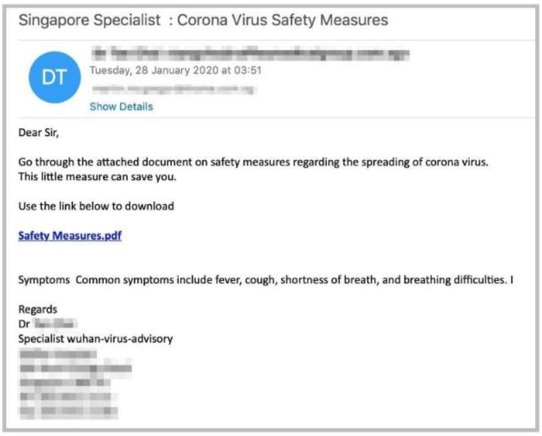
You are immediately advised to go through the cases above for safety hazard

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention"

Fig. 1 Example Phishing email alert

b) Health Advice

Claiming to be from experts, these types of emails aim to provide information on how to protect yourself from COVID 19



Singapore Specialist : Corona Virus Safety Measures

[redacted]
Tuesday, 28 January 2020 at 03:51
[redacted]
Show Details

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.
This little measure can save you.

Use the link below to download

Safety Measures.pdf

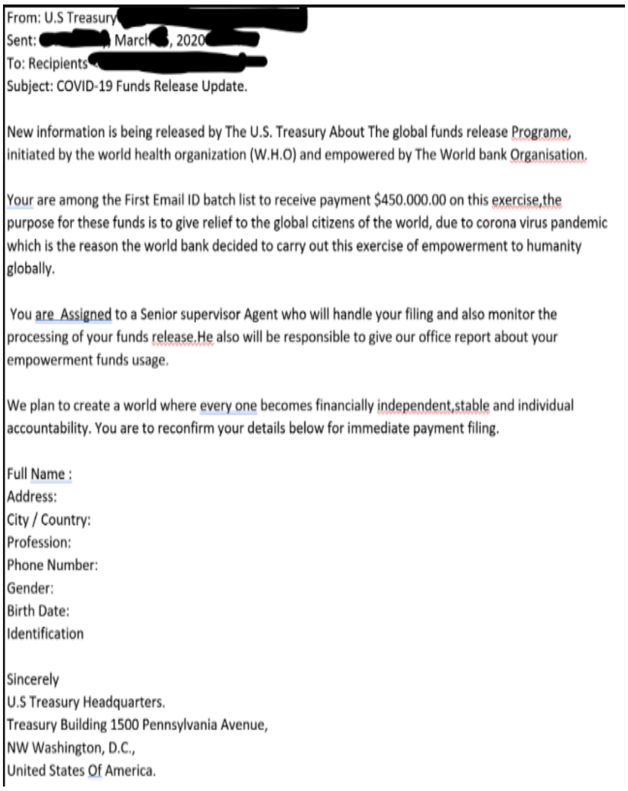
Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties. I

Regards
Dr [redacted]
Specialist wuhan-virus-advisory
[redacted]

Fig. 2 Example Phishing Health Advice Email

c) Fake Stimulus Check Emails

Emails like below which request users to provide personal information so that their stimulus checks can be released.



From: U.S Treasury[redacted]
Sent:[redacted] March[redacted], 2020[redacted]
To: Recipients[redacted]
Subject: COVID-19 Funds Release Update.

New information is being released by The U.S. Treasury About The global funds release Programe, initiated by the world health organization (W.H.O) and empowered by The World bank Organisation.

Your are among the First Email ID batch list to receive payment $450.000.00 on this exercise,the purpose for these funds is to give relief to the global citizens of the world, due to corona virus pandemic which is the reason the world bank decided to carry out this exercise of empowerment to humanity globally.

You are Assigned to a Senior supervisor Agent who will handle your filing and also monitor the processing of your funds release.He also will be responsible to give our office report about your empowerment funds usage.

We plan to create a world where every one becomes financially independent,stable and individual accountability. You are to reconfirm your details below for immediate payment filing.

Full Name :
Address:
City / Country:
Profession:
Phone Number:
Gender:
Birth Date:
Identification

Sincerely
U.S Treasury Headquarters.
Treasury Building 1500 Pennsylvania Avenue,
NW Washington, D.C.,
United States Of America.

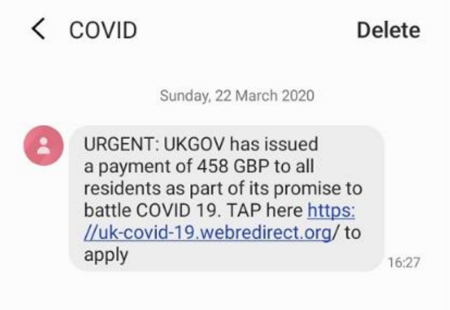
Fig. 3 Example Stimulus Check Email

A number of threat actors use these attacks in order to steal user credentials. Once the user clicks on the hyperlink in the email, he/she is pointed to a webpage that includes an option to provide a user name and password. A lot of the time, the website may look like a known website like that of your bank or your favourite social media site. Often a good way to know if the website is fake or not is by looking at the website URL. Once the user enters the password, his account is compromised, and the attacker has access to the users personal/financial information.

B. SMS Phishing

SMS Phishing, commonly known as smishing, is a type of social engineering which is triggered via SMS or text messages. These texts contain links that, when clicked, either automatically open a browser window or dials a number.

SMS Phishing attacks have mostly been used for a financial incentive where the victim is lured by informing them about a government payment or a tax rebate scheme. Given the economic impact of the COVID 19 crisis and with the different forms of stimulus payments provided by the government, scammers are using texts to dupe people.



Sunday, 22 March 2020

URGENT: UKGOV has issued a payment of 458 GBP to all residents as part of its promise to battle COVID 19. TAP here https://uk-covid-19.webredirect.org/ to apply

16:27

Fig. 4 Example SMS Phishing Text

IV. HOW TO PROTECT FROM PHISHING ATTACKS

Malicious attacks of this nature will continue coming, and cyber attackers are continuously evolving and adjusting their tactics to take full advantage of the situations. In this situation, the only thing we can do is to be vigilant and take these simple steps to avoid falling into their traps.

A. Never give sensitive information via email

Whenever there is someone asking for personal and financial information over email, think it through and do not provide that information.

B. Do not act on emails that tell you to act on immediately

The main reason why phishing attacks work is they create a sense of urgency in order to hinder our decision-making capability and ability to think straight. Take a minute and think through the request.

C. Check the email address

One of the easiest and best ways to avoid the trap is to be vigilant and check the email address to find out who the sender is and does the information match what the sender is claiming it to be.

D. Keep an eye out for spelling and grammatical mistakes

One of the things that give away a fake email/website is spelling mistakes or grammatical errors. The threat actors rely on the fact that humans make errors like how sometimes instead of "Google", we type "Goggle", and so forth.

E. Be sure you know the source who's sending the information

In this pandemic situation, everyone is eager to gather information which is the fact these threat actors are exploiting. Make sure you know the source and be wary of unknown or third-party sources. Big organizations such as the CDC and WHO will seldom send emails directly to us providing information on COVID-19.

F. Keep your systems up to date

More often than not, having an updated system can protect you from these attacks. The malware which might be embedded in the email tries to exploit a vulnerability that often has been corrected in the latest patch or updated by the vendor, but you might not have the latest version.

G. Device protection

Make sure you have the latest antimalware or antivirus software on your devices to protect your data.

V. WHAT HAPPENS IF YOU BECOME A VICTIM?

If you have become prey to one of these attacks by downloading and opening the attachment or clicking on the link, the first thing you should

- Update your antimalware or antivirus software and make sure to run a full scan.
- If you entered your login information on the link provided in the email or something, you should immediately change the credentials.
- If you have provided financial information, you should immediately contact your financial institution.
- Keep a watchful eye on any kinds of theft or any unexpected activities that you see on your accounts.

VI. CONCLUSION

This is a critical time for the world, and the last thing any person needs is to worry about identity theft or falling victim to cybercrime. Being vigilant and following simple practices can go a long way.

REFERENCES

[1] https://security.berkeley.edu/news/scammers-are-exploiting-coronavirus-fears-phish-users

[2] https://www.us-cert.gov/ncas/alerts/aa20-099a

[3] https://www.securitymagazine.com/articles/92157-coronavirus-related-spear-phishing-attacks-see-667-increase-in (2020)

[4] https://www.us-cert.gov/ncas/tips/ST04-014

[5] https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html

[6] https://www.us-cert.gov/ncas/alerts/aa20-073a

[7] https://www.cisomag.com/researchers-uncover-agent-tesla-malware-abusing-ms-office-vulnerabilities/

[8] https://www.theverge.com/2020/4/16/21223800/google-malware-phishing-covid-19-coronavirus-scams

[9] https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic