P: ISSN NO.: 2394-0344 RNI No.UPBIL/2016/67980 VOL-4* ISSUE-11* February- 2020
E: ISSN NO.: 2455-0817 Remarking An Analisation

Dealing with the New Era of Cyber Attacks – Analysing the Impact, Hazards & Prevention of Phishing, Vishing & Smishing

Avinash Agrawal
Assistant General Manager & Faculty,
State Bank Institute of Consumer Banking,
(Erstwhile SBI Staff College),
Hyderabad, India

Mukti Prakash Behera
Faculty (Marketing),
State Bank Institute of Consumer Banking,
(Erstwhile SBI Staff College),
Hyderabad, India

Abstract

As firms adapt the opportunities presented by avenues of cloud and mobile computing to connect with customers and maximize operations, they also meet new risks. Although the outdated IT limits are disappearing, the opponents now have new targets to attack. Companies face the risk of significant financial loss, damage to customer satisfaction and market reputation due to such attacks. The Article aims to inform the readers regarding the impact of Cyber Attacks on Individuals, Systems, Organization and the country. Further, the article attempts to explain and analyze the impact, hazards & prevention of Phishing, Vishing & Smishing.

Keywords: Cyber-attacks, Computer Emergency Response Team (CERT-In), NPCIL, Phishing, Vishing & Smishing, Digital World.

Introduction

Cyber-attacks are termed as "the deliberate action to disrupt or destroy computer systems or the information and programs". To further elaborate, cyber espionage refers to the penetration of enemy networks to acquire information for adverse purposes. In a digitally wired world, the weapons of Cyber attack are easy to use and they can generate gargantuan outcomes that range from defacing the website of a company/organization to even disruption of critical services.

Aim of the Study

The aim of this article is to sensitize digital and non-digital consumers regarding the knowledge, impact and prevention of cyber-attacks through Phishing, Vishing & Smishing. The review article further makes an attempt to explain in details the modus operandi of these techniques and advise prevention methods for safeguarding financial wealth.

The Larger Impact

The malware attack on Kudankulam Nuclear Power plant in India is a cause of worry as although it was successfully contained by The Nuclear Power Corporation of India Ltd (NPCIL). The Computer Emergency Response Team (CERT-In) reported that they noticed a malware attack that breached India's largest nuclear power facility's administrative network on September 4th, 2019. Investigating authorities were startled to discover that an anonymous user had attached a personal computer infected malware to the administrative network. Although it was reiterated by NPCIL that the operational systems of the nuclear power plant were separate and that the administrative network was no way connected to it.

Owing to the proximity of India's nuclear facilities from densely populated areas the threat of a potential nuclear attack on these critical establishments would always remain.

Dealing with Cyber Attacks: Are We Ready?

Today, cyber-attacks are considered as the fifth dimension in warfare after air, water, land and space and the invisible threat level are indeed high. As per Symantec (organization dealing with Cyber Threats), India is among the top three countries in the world after the US and China having constantly exposed to phishing and malware attacks. Other recent and relevant reports also divulge that the share of mobile malware in India is as high as 23.6 per cent and significantly by 2017, it was further reported that there is a security breach every 10 minutes in India. With many cybersecurity incidents going unreported, the data can be extrapolated logically to a larger extent.

Quantifying the Deadly Impact of Cyber Attacks

A study commissioned by Microsoft and Frost & Sullivan reveals that a large firms in India sustains economic loss to the tune of US$10.3 million from cyber-attacks vis-à-vis a mid-sized firm suffers losses of around US$11K. The impact of cybersecurity attacks has also impacted job losses across functions in more than three in five (64%) firms that have experienced cyber attacks.

The study further examines the existing cybersecurity approach of organizations in India. The findings are below:

1. Firms that have come across cybersecurity incidents, as the biggest concern, as they have the highest impact with the slowest recovery time.
2. Complex IT environment coupled with options to deal with several cybersecurity tools also increases the turnaround time.
3. A lack of cybersecurity strategy also impacts mid-sized and larger organizations.

(Source: A study commissioned by Microsoft and Frost & Sullivan titled “Understanding the Cybersecurity Threat Landscape in the Asia Pacific: Securing the Modern Enterprise in a Digital World”, 2018.)

The Economic Loss Model of Cybercrime

DIRECT LOSSESS	INDIRECT LOSSESS	INDUCED LOSSESS
Financial losses associated with the incident	The opportunity cost to the organization such as customer churn due to reputation loss incident	Impact on the broader ecosystem and economy, such as the decrease in consumer and enterprise spending

(Source: A study commissioned by Microsoft and Frost & Sullivan titled “Understanding the Cybersecurity Threat Landscape in the Asia Pacific: Securing the Modern Enterprise in a Digital World”, 2018.)

The economic loss model created to calculate the cost of cybercrime, takes into consideration losses which could be caused due to a cybersecurity attack. They are; direct losses (incident based financial losses); indirect losses (the opportunity cost); and induced losses (impacting the broader ecosystem and economy.

Phishing, Vishing & Smishing

Phishing, Vishing & Smishing are not new threats. They have all been there for years, but primarily it is the way the online criminals use these tools to defraud innocent customers that have changed. These techniques remain popular within fraudster circles for specific reasons.

1. The cost of execution to launch such attack is comparatively low
2. Little technical knowledge is required to set up an attack
3. The techniques work because the consumers are still tricked into believing the calls and divulge personal financial details online and over the phone

Phising

Phishing is frequently used to steal user data, login credentials, and credit card information. It happens when an invader, masked as a reliable entity, targets a victim into opening an email, instant message, or text message. It is a cybercrime in which a target(s) is contacted by someone pretending like a genuine institution to attract individuals into providing sensitive data such as personal information, banking, credit card details and passwords. This information is then used to access accounts and can result in identity theft and financial loss.

Modus Operandi of Phishing Attempt

Unbelievably True

Here, interesting offers and lucrative statements are created to attract the attention of the customer immediately. To illustrate, the message might contain that you have won a lottery, an iPad or a great prize. Such emails are false we are not supposed to click on these links.

Act Fast

The most preferred way for cybercriminals is the constant request to act fast as the lucrative deals are for a limited time frame. In fact, few of the callers will insist that you only have a minute to respond. In such situations, such calls and emails are better to be ignored. Further to it, the cybercriminals also advise you to all transactions in your account will be further suspended unless the customers updates the personal data immediately. It is for the customers information that all reputed and RBI approved financial institutions never ask customers to update personal data online. With such calls or emails, it is advisable to ignore such calls and visit the branch directly.

Misleading Hyperlinks

The link sent to consumers may not represent the real link of the bank or the financial institutions. The trick is to fly the cursor on the link and it will reveal the true (or the false) link. We can further realize that it may represent a popular website with a slightly different spelling. To exemplify, www.bankofarnerica.com, the letter “m” is replaced by “r” and “n”. Such instances call for extreme clarity and carefulness.

False Attachments

Here, unexpected or emails that do not make any sense needs to be avoided. Such mails often contain dangerous ransom ware and potent viruses that affects the entire system.

Unknown Senders

If the mail that you receive is from someone you are not aware about and you are suspicious about it, do not click on it.

How to prevent Phishing Attempt

To prevent Phishing attack suitable steps to be taken by both individuals and enterprises.

For Individuals, Vigilance is the Key

A spoofed message often contains subtle mistakes that expose its identity. It may include spelling mistakes or changes to domain names.

Operators should also stop and think about why they’re even receiving such an email.

For enterprises, several steps can be taken to mitigate phishing attacks:

1. To counter phishing activities, a two-factor authentication (2FA) process is the most efficient method as it further adds an extra layer of verification while logging into sensitive applications. This technique depends primarily on users having two essential attributes: initially, something that the user knows; such as the user name and password and something that they have i.e., a smart phone. The strength of a two-factor authentication (2FA) process is, even when the users are compromised, it further prevents the use of the compromised credentials as they are not sufficient to gain entry to the system.
2. Apart from this, firms should also enforce stringent password management policies. As an example, employees should be mandated to frequently alter their passwords and they should not be allowed to reuse a password for multiple times.
3. Training and awareness campaigns can help in eradicating phishing threats. Employees need to be educated on secure practices and avoid clicking on external email links.

Vishing

In short, Vishing is also called ‘voice phishing’. Here, fake user tries to extract your confidential information over the phone. It is an act of using the telephone to scam the user into surrendering private information that will be used for identity theft. The scammer generally shows to be a genuine business and fools the victim.

Impostors seek to extract your confidential information like passwords, Personal Identification Number (PIN), CVV and OTP. They then use this information to defraud you.

Modus Operandi of Vishing Attempt

A confident voice at the other end of the phone line claims to call from your bank, card company, the RBI, etc. He or she may possess some of your basic personal details and uses this to convince you about the genuineness of the call, and to part with critical details.

Similarly, the messages purporting to be from your bank or from the RBI can provoke you to share such confidential information. Some messages may also carry malicious links or phone numbers that you are urged on to click or call.

The excuses employed by fraudsters are many. They professionally reiterate that the information is required for a bonus claim or special offer scheme that the user is eligible for. If the user provides the required confidential data, it leads to the card being charged or the account being debited within no time.

How to Prevent Vishing Attempt?

It is utmost important to know that the user is not supposed to share personal banking details such as passwords, PIN, CVV and OTP with anyone. Alertness is key, and that saves the user from fraudulent activities. All users must be aware that neither the bank nor the card provider will ever ask for personal information as mandated by RBI.

Completely ignore such calls or messages and on priority raise a red flag. Cut them off and ignore them. Avoid links or attachments that get generated from suspicious sources. Report such instances to your bank, card company or the RBI.

Smishing

In Smishing the user is cheated to downloading a virus or other malware on his mobile phone. Smishing is a short form of "SMS phishing." Smishing is when someone tries to trick you into giving them your private information via a text or SMS message.

The technique is dangerous as users believe and trust the text message than the email as most users are aware of the security risks involved in clicking an external link.

Interest in smishing has gradually increased by the growth in smartphones with web browsing capabilities.

Modus Operandi of Smishing Attempt

Smishing cleverly uses the elements of social engineering and motivates users to share personal information. This technique affects the trust of the user to obtain personal information. Usually the smisher looks for online passwords or social security number or credit card information. Once the data is obtained, they violate the norms and put you in trouble.

Another option used by smisher is to say that if you don’t click a link and enter your personal information you would be charged per day for the usage of the service. Hence, if you have not registered for the service, then ignore the message. If you see any unauthorized charges on your credit card or debit card statement, then take it up with your bank or credit card company.

One news report highlights a smishing scam that tried to get victims to activate a new credit card. The messages provoked individuals to call a number and enter private information over the phone. Other smishing scams identified by the report include ones that tell users their online accounts (such as Bank ID) are expiring.

At times, smishing may lead users to install a virus on their devices. In these situations, the results may be worse for some users. A Research survey found that only 32 percent of Smartphone users install antivirus software on their devices.

Smishers essentially look for the missing piece of the puzzle. That could be a social security number, pin number, password, or any other private detail that will help them access your accounts.

How to Prevent it?

The most significant step is not to click on links that contains unfamiliar or unexpected text messages. While you are authorized to avoid any such suspicious links, but you will have a desire to call or respond to the scammers to stop it. A few tips may be used to avoid such smishing scam:

Do not Respond to The Text Message or Call Back The Number

The most important part is that even if the text message says “to stop receiving messages, please send STOP” never reply. If you are sure the message is coming from scam number, replying may result in more messages getting spammed to your phone. If you are calling the number to STOP sending messages, the same may happen. Normally, scammers do not know that the numbers they are trying are active. Sending a response to the message will verify to them that the number is active, leading them to continue and possibly increase the number of spam messages you’re receiving.

A most effective option is to block the number immediately, but some mobile phones do not have phone blocking options on their phones. In this case, you may install a number blocking an app from your phone’s app store.

Have a Web Search of Both the Number and The Message Content

It may happen that you are not the first person to receive that message. Check if a suspicious number or message has numerous others posting then it’s potentially a scam.

One such site for this is 800notes.com. When you get a call from a suspicious number, you may login the site to help and vet the number of potential scams or spam.

If The Phishing Message Is Deceiving A Company, Call The Company Directly

Many smishing messages will pretend to be a well-known company, such as a card or bank. If you believe the message is a scam, instead of calling or texting the scam number, look up that company’s customer care number from its official website. Contact the customer care and inquire about the message you received. If they confirm that it’s from them, then ignore it otherwise delete it.

Don’t Click on Any Links in the Message

Smishing generally try to manipulate the customers emotions. Often, scammers don’t need you to plainly give up passwords, pins, CVV and other security numbers. They will increase your interest enough to get you to click on a link and download a virus to your phone. There are chances that even though you do not click on a phishing link, your mobile device is already infected. Since such viruses are often hidden and you may not realize your phone is infected. However, you may get few clues i.e. if your handset started showing unsuspected memory usage or excessive heating up an issue or you get auto-messages while using your mobile phone web browser.Install an antivirus app and scan your device to prevent frequent smishing attempts. Antivirus app will block any virus installation attempts in the future, as well as block malicious websites.

Utilize a VPN on Your Mobile Device

We often overlook the fact that, smishing attack is the collection of location data. According to an internet security company, cybercriminals are increasingly using location data to better target individuals. Cybercriminals take advantage of this sensitive data to send you smishing messages that appear extremely local. If the message is having your personal information, chances to the response from victims are high.A VPN app may help in spoofing your location, making it seem like you are somewhere else.

Be Proactive

Most importantly, we must be proactive to avoid smishing scams. If a message does not seem genuine, don’t take any chances. A trustworthy company will never ask important business or personal data through a text message and will also never ask you to enter private account information through a text message or a suspicious link. If the message is genuine and important, the company will possibly call or send an email.

Methods to Block A Number on Android and iOS

If you are facing trouble with the arrival of SMS spam or phone calls to your Android or iOS device, you might have a few solutions available to you through your app store, or even through your phone’s operating system.

Block calls and text messages on iOS

After the introduction of iOS 7, Apple has included call and text message blocking as a software feature. To block a text message or mobile number, you must go to the settings option, message and blocked. Add the number(s) you want to block to reject all new messages.

Block Calls and Text Messages on Android

Since all Android phones are not unified in their technology, you may or may not have the option to add numbers to a block list. To find out how to block numbers on your phone, go for a Google search. For instance, you may search “how to block a text on Mi4i”. Such a search will bring up many results depending on your mobile and Android version.

A large number of SMS and call spam blockers are available in Google Play Store. For example; True caller, Caller ID, SMS spam blocking, Dialer app. These apps can intelligently block both spam SMS and phone calls. It also allows you to blacklist and whitelist the number.

Conclusion

Through the objective of the study, the authors have made an endeavour to identify the various threats of cyber attacks and their forms. Primarily, the impacts of the cyber attacks are significant and they are designed to exploit the vulnerabilities of electronic communication devices. In fact, in a mobile environment, such attacks are easier to set up and more convincing than traditional mass mailing techniques. It is critical to note that, although traditional phishing attacks depend on deceiving the user, in a mobile environment, the attack can take advantage of the limited security in mobile devices. It is about time, that apart from technology upgradtion in terms of Artificial Intelligence (AI), Machine Learning (ML), and creation of anti-phishing solutions, the end-user needs to be aware of the dangers that these cyber-attacks propose. Merely blaming technology will not help, awareness and carefulness is the key to prevent such attacks.

References

https://www.techopedia.com;
https://www.imperva.com;
https://www.phishing.org;
https://us.norton.com/
https://www.thehindubusinessline.com
https://news.microsoft.com