SN Computer Science (2021) 2:78
https://doi.org/10.1007/s42979-020-00443-1

REVIEW ARTICLE

Social Engineering Attacks During the COVID-19 Pandemic

Venkatesha Sushruth[1] · **K. Rahul Reddy**[1] · **B. R. Chandavarkar**[1]

Received: 24 November 2020 / Accepted: 28 December 2020 / Published online: 6 February 2021

Abstract
The prevailing conditions surrounding the COVID-19 pandemic has shifted a variety of everyday activities onto platforms on the Internet. This has led to an increase in the number of people present on these platforms and also led to jump in the time spent by existing participants online. This increase in the presence of people on the Internet is almost never preceded by education about cyber-security and the various types of attacks that an everyday User of the Internet may be subjected to. This makes the prevailing situation a ripe one for cyber-criminals to exploit and the most common type of attacks made are Social Engineering Attacks. Social Engineering Attacks are a group of sophisticated cyber-security attacks that exploit the innate human nature to breach secure systems and thus have some of the highest rate of success. This paper delves into the particulars of how the COVID-19 pandemic has set the stage for an increase in Social Engineering Attacks, the consequences of this and some techniques to thwart such attacks.

Keywords COVID-19 pandemic · Phishing attacks · Social Engineering Attacks · Social Engineering Attack mitigation

Introduction

The twenty-first century has seen an accelerated move of business, media, social interaction, education, etc. onto platforms on the Internet. As a result, the amount and importance of information flowing through the digital landscape has increased exponentially. This has led to increased criminal activity in the cyber-space which has materialized as data-breaches, malware, ransomware and phishing type attacks. There has been concentrated efforts by private organizations and governmental agencies to guard against these attacks and as a result in the past few years, traditional modes of attacks such as hacking have proven to be marginally less successful, but alternate areas of vulnerabilities have been exposed. One such area gaining attention is social engineering and its utilization in all modes of cyber-attacks [1].

Over the years, there have been a number of attempts to provide a concrete definition to the term 'Social Engineering Attacks' in the literature, each being slightly different but having the same overarching meaning. The term has been described by Conteh and Schmick as 'Human Hacking', an art of tricking people into disclosing their credentials and then using them to gain access to networks or accounts [2]. Ghafir et al. have defined the term as a breach of organizational security via interaction with people to trick them into breaking normal security procedures [3]. The lack of a structured definition has led to works that have focused solely on defining the term. One such work by Wang, Sun and Zhu has defined Social Engineering in cyber-security as a type of attack wherein the attacker(s) exploit human vulnerabilities by means of social interaction to breach cyber security, with or without the use of technical means and technical vulnerabilities [4]. Going forward, this paper will be using this definition by Wang et al., as the standard definition for the term 'Social Engineering Attack' (SEA) in this study.

SEAs have traditionally followed a template made up of 4 steps: (1) Target research; (2) Forming a relation with the

This article is part of the topical collection "Cyber Security and Privacy in Communication Networks" guest edited by Rajiv Misra, R K Shyamsunder, Alexiei Dingli, Natalie Denk, Omer Rana, Alexander Pfeiffer, Ashok Patel and Nishtha Kesswani.

✉ Venkatesha Sushruth
vsushruth21@gmail.com

K. Rahul Reddy
k_rahul_reddy@outlook.com

B. R. Chandavarkar
brcnitk@gmail.com

[1] Department of Computer Science and Engineering, National Institute of Technology Karnataka, Surathkal, Mangalore, India

target; (3) Exploit the relation and formulate an attack; (4) Exit without leaving behind traces [5]. With time the tools used in each step have evolved. Target research has gone from searching in the target's dumpster to extracting information from the target on social media platforms [6]. With the development of Machine Learning, steps (2) and (3) have become automated, with 'social bots' tracking and engaging with targets on social media [7]. The wide array of technologies and methodologies used for SEAs and the speed with which they evolve make developing software solution such as spam and bot detectors a game of cat-and-mouse.

The global situation that has come into existence due to the COVID 19 pandemic has changed the equation in this space. The increase in Work-from-home situations, online education, entertainment via online platforms has created a sharp uptick in the number of Internet Users worldwide and also the amount of time spent by users on the Internet. Industry analysts have reported an increase of over 47 percent in the amount of broadband data usage worldwide during the March to May period in 2020, as seen in Fig. 1 below [8]. This has also reciprocated into an increase in social engineering attacks that use Internet as a medium of contacting the target. Phishing, one of the staples in the SEA arsenal has seen a huge increase, with technology companies such as Google and Microsoft recording trends where the attackers masquerade as officials from organizations working on COVID-19 such as the World Health Organization [9, 10]

In this unprecedented situation brought on by the pandemic, having a deeper understanding of the various SEA strategies being deployed is valuable to both organizations and to private citizens. With this theme in mind, the second section of this paper gives an overview of how the participation of individuals in the Internet has changed and how SEAs have evolved as a response to the pandemic. The third section then takes up the task of providing guidelines as to how one can tackle these SEAs. These guidelines are presented based on the demographic that are most affected by these attacks. Guidelines particular to SEAs popular during the COVID-19 pandemic are also covered. The pandemic is currently an evolving situation and this paper aims to be a checkpoint from a time within this time-frame that will aid research and studies that will eventually be carried out after the end of this unprecedented time period.

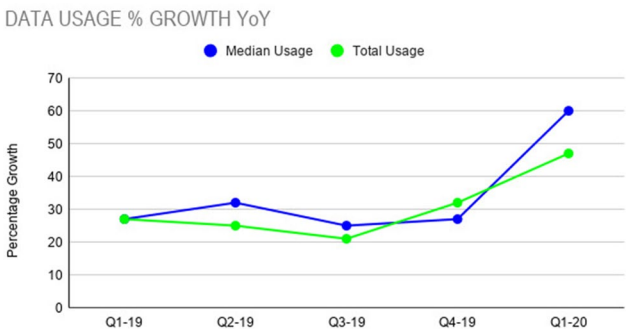

Fig. 1 Data usage growth year-on-year in percentage terms [8]

Social Engineering Attacks During COVID 19

Humans are social creatures. Our society is built upon the cooperation of various groups of people communicating, understanding each other, and building on each other's strengths. Throughout the history of the human species, this cooperation was only possible when all the parties were present at the same place at the same time. This changed with the invention of the Internet in the late 1960s and the launch of the World Wide Web in 1989. The commercial Internet allowed multitudes of online platforms that provided instant communication with anyone at anytime from anywhere. Technologies like instant messaging, video calling and video conferencing shrunk the world and allowed greater cooperation. Video conferencing especially is a technology that can truly replace the need for physical interactions as it allows the parties communicating to view each other's facial expressions. The ability to see facial expressions has been proven to be the most important aspect in communication [11]. But, even with such technologies, the primary mode of human communication remained physical contact. This status-quo is now being forcefully being changed by the effects of the COVID-19 pandemic.

There has been a mass migration of human activities and interactions to platforms on the Internet. This sudden increase in activity online, coupled with the mental anguish brought on by the pandemic, creates a perfect storm of conditions for bad actors to carry out SEAs. These bad actors can be a single individual, an organization of cybercriminals or even government-backed entities from various countries around the world. While the main incentive for the bad actors from the first two categories is financial, the incentive for government-backed entities is usually geopolitical in nature [12]. Google, the technology company, has been tracking phishing attacks deduced to have been originated from such government-backed entities. Figure 2 shows the scale of such attacks based on the number of accounts flagged by Google.

This section first looks at how the COVID-19 pandemic has affected human activities and the migration to platforms on the Internet. Then it looks at the changes seen in SEAs as a result of the pandemic and finally SEAs that have a theme pointing to the COVID-19 pandemic.

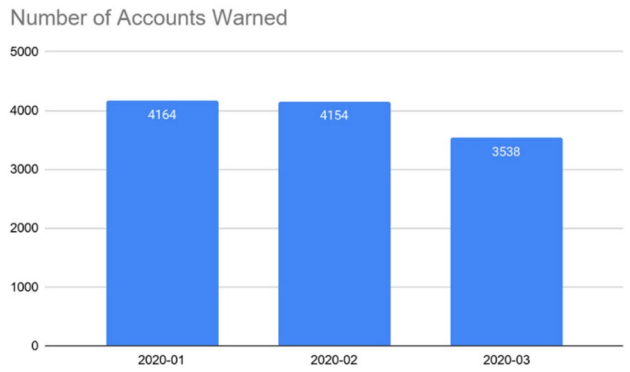

Fig. 2 Accounts that received a "government-backed attacker" warning each month of 2020 [9]

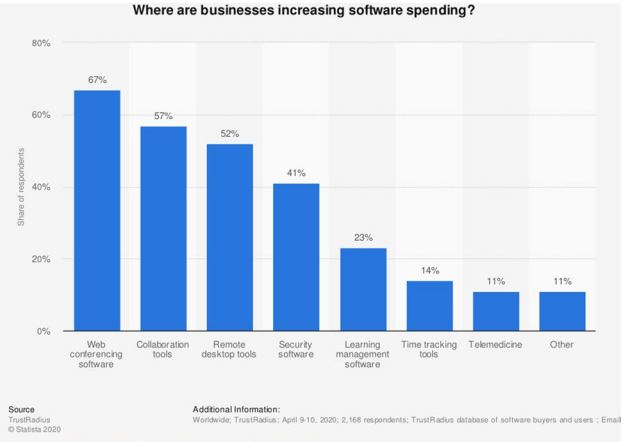

Fig. 3 Spending by business on software during the early stages of the COVID 19 pandemic [14]

Migration of Activities to Online Platforms

The main three activities that lead to humans venturing out of their homes in the modern world are business/work, commerce/shopping, and leisure. Business can be people going to their educational institutions or to their places of work. Commerce can be producers and sellers going to the marketplace to sell their products and consumers going there to procure their needs. Leisure can be a multitude of activities ranging from international tourism to strolls in the park. The COVID-19 global pandemic and the resultant lockdown measure enacted by various governments worldwide has caused disruptions to all such activities. At the height of the pandemic lockdown measure in April 2020, a total of a third of the world's population was estimated to be under various degrees of quarantine and social distancing measures.

The International Labour Organization(ILO) had estimated that 7.9 percent of the global workforce, that is, nearly 260 million people worked from home on a permanent basis before the COVID-19 pandemic. With the disruption in the normal work schedule brought on by the pandemic, according to the calculations of the ILO, the number of people working from home has the potential to reach 18 percent of the global workforce working from their homes permanently as a result of the pandemic. The report published by the ILO in April of 2020 suggests that this number is mainly made up of artisans, self-employed, business owners, freelancers, knowledge-based workers, and high-income earners [13]. This increase in remote work can easily be visualized by the spending patterns of various companies as shown in Fig. 3 below. Businesses worldwide have been investing in software products that support remote work and make the process more convenient.

Education is another area that has seen major disruption, with most of the countries closing their educational institutions in the early stages of the pandemic. In late April 2020, the World Economic Forum estimated that a total of 1.2 billion students from 186 countries have seen disruptions in their education brought on by the pandemic [15]. This has brought on a digital education revolution where the classes have been shifted onto platforms that allow remote learning. These platforms may come as lectures on the radio, as television programs, or full-fledged classroom education on platforms on the Internet. These platforms were used in over 110 countries and able to provide remote education during the pandemic, as seen in the UNESCO-UNICEF-World Bank Survey on National Education Responses to COVID-19 School Closures [16]. This study shows that pre-teenage children from over 70 countries have had to attend classes on platforms on the Internet. This is a worrying statistics as, without supervision, these children can become easy victims of Social Engineering Attacks.

Commerce has also seen the big jump onto online platforms that had been slowly going on in the background. The COVID-19 pandemic and the resulting social distancing measures have become a catalyst for the big migration of commerce onto the Internet. A joint survey conducted by the United Nations Conference on Trade and Development (UNCTD) and Netcomm Suisse E-commerce Association in October 2020 [17] in 9 representative countries has given an insight into the situation. The survey showed that consumers in emerging economies saw a greater shift to online shopping, with an increase in the number of customers for most product categories, as shown in Fig. 4 below. This can be seen as a one-to-one relation for the increase in participation on various Internet platforms while becoming a potent medium for Social Engineering Attacks.

Leisure activities which include any traveling have been severely curtailed due to the pandemic. In the early stages of the pandemic, when strict quarantine and lockdown measures were enacted, the simple act of going out for a walk was prohibited in man heavily affected areas around the world.

This lack of entertainment via outdoor activities has largely been compensated by entertainment via digital media such as television, social media platforms, and on-demand entertainment platforms on the Internet. Brightcove's Q2 2020 Global Video Index [18] has reported a staggering 40 percent increase in video content consumption over the three month period from April to June 2020. Reports have also shown a 30 percent increase in the time spent by Indians during the pandemic as compared to before, on over-the-top entertainment platforms on the Internet.

The statistics highlighted so far in this section provide a glimpse of the extent of online migration caused by pandemic and the reaction to it. Next we will see how this change has impacted SEAs

Changes to Social Engineering Attacks During the Pandemic

Cybercrime can be thought of as a business, one with bad intentions. But like any other business entity, the ultimate aim of any cybercriminal is to turn a profit for the work they put in. When cybercrime is seen through such a perspective, the COVID-19 pandemic can be seen as a new business opportunity. This unique opportunity is exciting to these cybercriminals as the pandemic pushes more people onto the Internet, increasing the number of Users that can be targeted.

As per reports from Google, most SEAs are now carried out as Phishing Attacks via emails or websites [9]. These attacks deploy multiple tactics using the brand identity of well-known entities by their trademarks such as their company names and logos, to develop phishing websites or send emails that appear authentic and lure users into entering sensitive information such as usernames, passwords, banking details and other details that can help in identifying them. Google has reported that they block more than 100 million phishing email every day, with a claimed accuracy of 99.9 percent [19].

Microsoft, another major industry player, has reported an increase in email phishing activities, stating that phishing type attacks make almost 70 percent of all attacks. The September 2020 published Digital Defense Report [20] reports that the attackers deploying SEA are now deploying significant time, money, and effort to develop scams and attack strategies to trick even the users being wary of such attacks. This development can be attributed to an increase in information available to the users about such attacks, heightened awareness among users and technological advancements in detection of attacks. Microsoft based on the telemetry from their business software offerings "Office 365" has reported [20] that users face three main types of phishing attacks—credential phishing, Business email compromise, or a mix of both.

Fig. 4 Number of customers on online platforms increased for most product due to COVID-19 [17]

Fig. 5 Outline of a credential phishing attack [20]

Credential phishing is carried out by the cybercriminal posing as a well-known service in an email template and trying to lure users into clicking on a link, which takes them to a fake login page. When the users enter their credentials on the page, those credentials can be used to further launch deeper and complex attacks to build a presence inside the organization by using cloud-only APIs and systems. This presence is then used to move around laterally to steal data, money, or otherwise breach the organization. An illustration of the process is shown in Fig. 5 above.

Business email compromise phishing attacks specifically target businesses and are in the limelight in this era of remote work. This type of attack is characterized by techniques that masquerade as someone the target usually takes notice of, such as the company CEO, CFO, or HR personnel. The attack can also involve a business-to-business transaction. For example, the attacker might fraudulently access a company's system and then act as that company to criminally request payment from another company. An illustration of the attack is showing above in Fig. 6.

Using phishing attacks as a vehicle to deliver malware or ransomware software is also common. During the pandemic period ransomware attacks are reported to be more common than malware because ransomware attacks can do the same

information collection job along with monetary payments from the target paid to decrypt files that the ransomware software encrypts.

The pandemic and the resultant shift of work as well as education online can be seen as a catalyst for an increase in both credential phishing attacks as well as business email compromise attacks. Ransomware attacks have also pipped malware attacks as a result of increased online activity during the pandemic. Although these changes have been recorded during the pandemic, the highlight is the shift in the attack strategies from generic subjects to themes related to the pandemic. This is seen in detail in the upcoming section.

COVID-19 Themed Attacks

The public health emergency brought on by the COVID-19 pandemic and the fear, anxiety, and uncertainty present in the general public, and the desire for information on the pandemic presents the ideal opportunity for exploitation by cybercriminals deploying SEAs. When news about the pandemic made headlines in the early months of 2020, SEAs with the over-arching theme about the pandemic shot up in frequency [21]. This trend is illustrated below in Fig. 6. Another report produced by consultancy firm Deloitte noted a 254 percent increase in new COVID-19 themed web and sub-domains registered per day in the early stages of the pandemic [22]. This has led to many government organizations such as the Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency in the USA and issuing warning about the trend.

Phishing emails that used the pandemic as their lure were seen to have subject lines such as "2020 Coronavirus Updates", "Coronavirus Updates", "2019-nCov: New confirmed cases in your City", and "2019-nCov: Coronavirus outbreak in your city (Emergency)". The above type of mails were targeting the human nature of curiosity, the instinct to gather information and the fear of missing out. The content of such emails contained attachments that deployed malware and ransomware or lead to fake sites to harvest user credentials. The contents were worded in such a manner that they encouraged users to visit websites that the attackers used to harvest valuable data, such as usernames and passwords, credit card information, and other personal information from the targets [23]. An example of how phishing emails changed after the pandemic can be seen below in Fig. 7.

Another common tactic used in phishing emails was the impersonation of trusted sources that provided information about the pandemic such as the World Health Organization (WHO) and the US Center for Disease Control. As a result of this trend, the US Federal Bureau of Investigation released a notice above impersonation of the US CDC by attackers [23]. Impersonation of WHO was a common trend that was picked up by the security services provided by Google in their email service [19]. An example of a phishing email impersonating the WHO can be seen in Fig. 8.

Multiple governments worldwide enacted measures that provided financial respite to their citizen through cash payments which were carried out via platforms on the Internet. This was another area where phishing emails and also in some cases phishing SMS were deployed. Figure 9 depicts one such phishing email example.

Other common subject matters used in phishing attack campaigns included notices about mandatory COVID-19 testing, news related to remote work settings, and news regarding social distancing and stay-at-home or quarantine rules and regulations. There was also a marked increase in

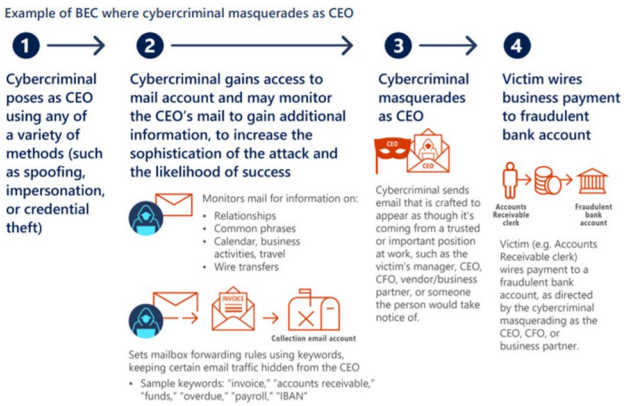

Fig. 6 Outline of a business email compromise attack [20]

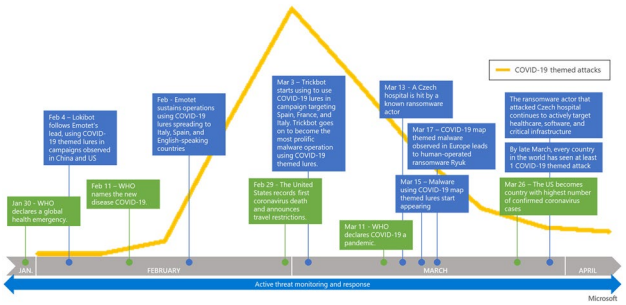

Fig. 7 COVID-19 themed SEAs [10]

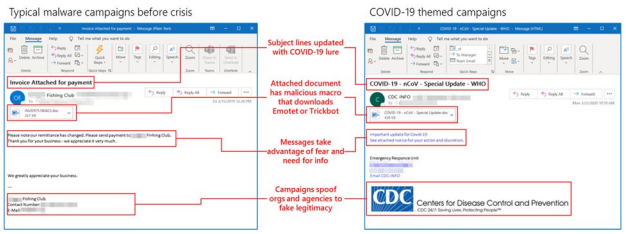

Fig. 8 Modifications to phishing emails in response to the pandemic [24]

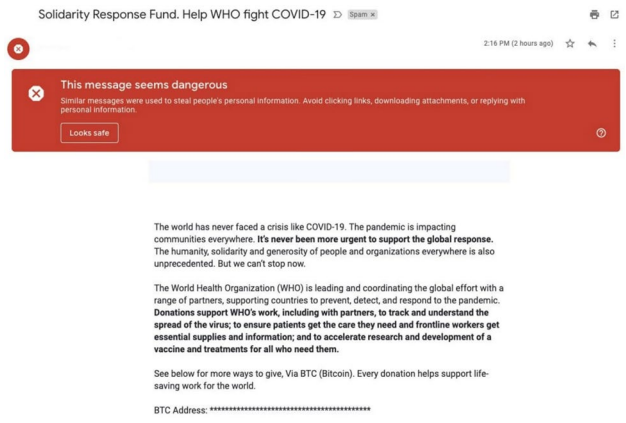

Fig. 9 Phishing email impersonating the WHO [19]

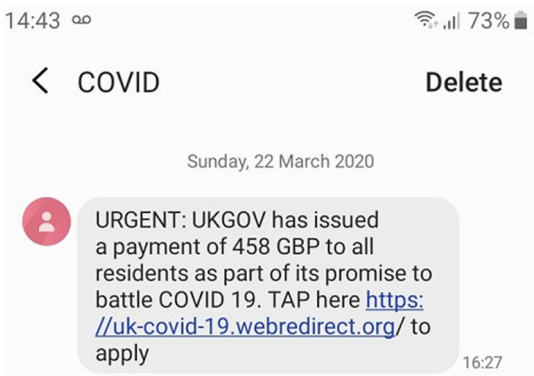

Fig. 10 Phishing SMS [23]

social media posting about the pandemic that carried misinformation (Fig. 10).

Tackling Social Engineering Attacks

This paper contains a survey on the affected demographic for Social Engineering attacks. It cover points factors which affect the demographic that are targeted by Social Engineering Attackers. Based on this, the paper provides guidelines to be followed by each of these groups. It also cover the demographic points and the guidelines for attacks during COVID. These guidelines are slightly different because of the reason that these attacks mainly use the fear of the population to their advantage [25]. The paper notes how these attacks target the vulnerable demographic with tactics involving pandemic panic and fear and presents guidelines considering all these factors.

General Guidelines

These guidelines are aimed towards social engineering attacks in general.

Social Engineering Attacks are most successful against those who were not aware at an early age [26] about the potential threats and attacks possible by fraudulent and malicious intent. The four major steps in Social Engineering Attacks include [27]

1. Gathering of information
2. Developing a relationship with the target
3. Exploiting the target based on a targeted attack strategy
4. Execute the Attack.

Affected Demographic

The Demographic analysis can be made based on the four common steps of Social Engineering Attacks mentioned above.

Gathering of Information

Most Social Engineering Attacks are directed towards a very large audience. The information gathered by attackers is of two types. One is the general contact information of as many targets as possible. This is used to make initial approach to these targets. Only after certain reciprocation activity by the targets, the attackers go further with the responding subset of targets. Once they have a lock on the specific targets, the attackers gather the other type of information. This is usually specific to the target [27]. This includes jargon and other terms that the target can associate themselves with. This information often helps the attacker in the next steps of the Social Engineering attack.

At this step of the Social Engineering Attack, the population which is unaware of the security consequences of information disclosure. The main mistakes made by the targets are that they do not understand the importance of the data to the social engineer, leading to the disclosure of information. These can involve revealing information that, from a security point of view, is apparently harmless from the eyes of the target, but can be beneficial to the attacker.

Developing a Relationship

The willingness of the target to share information and reciprocate plays a very crucial part in the attack. Only the subset of population that reciprocate to the initial approach made by the attackers are further targeted specifically. Based on the information gathered by the attacker in the previous step of the attack, they try to establish a relationship with the target. After foot-printing the target, attackers often use information about the target or any other contact of the target.

In the formation of relationships, an attacker exploits the inherent willingness of a target to be trusted and establishes relationships with them. The attacker will manoeuvre him into a position of confidence when establishing this partnership, which he can then manipulate. Human beings have the willingness to trust and care for others. In order to exploit and influence goals to create authenticity and gain confidence, social engineers often use these attributes. By touch, such as physical or interactive, the act of coercion can be performed. Digital contact is an interaction with media such as the telephone, e-mail or even social media. Manipulations such as overloading, reciprocating, and dissemination of transparency are universal psychological concepts.

Exploiting the Target

Social Engineering Attackers now have access to the target's information like location or other crucial information by using the relationship and confidence generated with the target through coercion during the previous stage, or by implementing other similar tactics. After gaining the trust, attacker exploits the target to obtain passwords or perform acts that would not occur under normal circumstances. At this point, the attacker could end or carry it forward to the next level.

At this stage, the affected demographic is the population who are unaware of these kinds of attacks and the ones who are gullible to trusting the attackers based on the footprinted information.

Executing the Attack

At this stage, the attackers utilize all the information available to make the final move and cash in from the target. If all the previous stages were successful, the attackers almost always get away with the attack.

Guidelines

We have identified two major factors which must be focused upon to mitigate these attacks: Contact information and Bank transactions. This section contains general guidelines for Social Engineering Attacks:

1. Be extra cautious about controls on payments and wary of emails containing an attachment or connection. Contact the information security or information technology department for a questionable message when in doubt.
2. Reconcile your accounts regularly and confirm by calling a checked number that business partners have received payments. Be vigilant with demands for payment and account changes and pay particular attention to whom you pay.
3. Keep contact details up to date with several workers now working from home, so that your bank can contact you quickly if they suspect a suspicious payment.
4. Don't trust any requests that come in from email alone for payments or account changes. Often allow callbacks from a record system to the person making the request using a recognized phone number.
5. Often conduct callbacks when changing business partners' contact details as well. Don't simply trust an email demanding that a trusted call-back number be updated.

There are also a lot of scope for organisational employees being targets of these attacks. A study [23] shows that Social Engineering attackers spend time on developing techniques to victimize top officials and experts as well. The following few guidelines can be followed to mitigate those attacks:

1. Wherever possible, allow multi-factor authentication, adding another layer of protection to any applications you use. In addition, a password manager can help deter risky behaviour, such as passwords being stored or exchanged.
2. Try using the Encrypted Network Connection VPN(Virtual Private Network) solution. Accessing IT resources within the organization and anywhere on the internet is secure for the worker.
3. The cybersecurity strategy of companies should be revised and home and remote work included. When the company adjusts to getting more individuals outside the workplace, make sure the strategy is appropriate. For employee access to documents and other information, they need to provide remote-working access management, the use of personal devices, and revised data privacy considerations.
4. Employees can communicate with colleagues using employer-provided IT equipment for official matters. In the context of business IT, there is also a variety of software installed that keeps people safe. The company and the employee could not be completely secured if a security incident has occurred on the personal computer of an employee.
5. Personal devices used to access working networks will leave organizations vulnerable to hacking without the right protections. If information is leaked from a personal computer or hacked, the company would be held responsible.

Tackling Attacks During COVID-19

These guidelines are aimed towards Social engineering attacks during current times, which are focused differently because of everything moving online.

Affected Demographic

Although the general demographic that was vulnerable to Social Engineering Attacks is still almost the same, the attackers are focusing more on the victims who could be manipulated based on health data. As discussed in the previous sections, gathering information and relationship development are very crucial parts of any Social Engineering Attack. During this global pandemic, everyone has moved to a place of fear. This allows the attackers to look for and target victims with existing health conditions and medical history [28]. These people are more susceptible for the attack and give out information willingly.

Guidelines

The paper presents few necessary guidelines to be followed by the demographics to overcome Social Engineering attacks during COVID-19 like times:

1. For Phishing attacks: Strong authentication can protect the users from the large number of identity attacks, reducing the possibility of security breaches with strong authentication. For the best protection and user experience, options for password less authentication are recommended. The preferred choice over SMS [23]/voice authentication is always the use of an authentication app.
2. For Healthcare related fraudulent calls: Verify all incoming calls for the authority. Do not share any information until and unless the contact made by the other person was expected. This is essentially to avoid reciprocation. Most attackers only proceed to attack those who reciprocate initial attempts of contact.
3. Avoid falling for targeted attack strategies: As discussed in the previous sections, the attackers gather information (footprint) about targets. This includes both personal information and that of their close members. This is essentially any information that the attackers can get their hands on. If a suspicious attempt with information of your past health history or that of any family member is made, it is possible that the attackers are targeting the victim based on some health based information received.
4. Health history based attacks: If any malicious attempt is made by quoting health history and medical records of the target or that of their family, trying to get this data validated and verified will help get out of this attacks.

Conclusion

This paper has discussed how the global pandemic has affected the Social Engineering Attacks. The pandemic has moved a range of daily practices to the Internet and online platforms. This increased the fraction of population online. This rise in the presence of people on the Internet is not accompanied by cyber security education and the different forms of attacks that an Internet user can be exposed to on a daily basis. We discuss a variety of these kinds of attacks and propose a few guidelines as to how to avoid and counter these. We present an analysis of the steps taken by these attackers from knowing(foot-printing) a target to successfully executing the attack. We present these guidelines based on the four major steps discussed.

This paper also presents a detailed analysis of COVID-19 themed attacks. Guidelines to avoid these targeted attacks like Phishing attacks, Healthcare related fraudulent calls, Health history based attacks have been presented too.

Compliance with Ethical Standards

Conflict of Interest Conflict of Interest: The authors declare that they have no conflict of interest. On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Verizon Communications. Data breach investigations peport, 2019. URL https://www.phishingbox.com/assets/files/images/Verizon-Data-Breach-Investigations-Report-DBIR-2019.pdf. Accessed 20 Oct 2020
2. Nabie C, Paul S. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. Int J Adv Comput Res. 2016;6:31–8. https://doi.org/10.19101/IJACR.2016.623006.
3. Ghafir I, Prenosil V, Alhejailan A, Hammoudeh M. Social engineering attack strategies and defence approaches. pp 145–149, 2016. https://doi.org/10.1109/FiCloud.2016.28.
4. Wang Z, Sun L, Zhu H. Defining social engineering in cybersecurity. IEEE Access. 2020;8:85094–115. https://doi.org/10.1109/ACCESS.2020.2992807.
5. Salahdine F, Kaabouch N. Social engineering attacks: a survey. Future Internet, 11(4), 2019. ISSN 1999-5903. https://doi.org/10.3390/fi11040089. URL https://www.mdpi.com/1999-5903/11/4/89. Accessed 24 Oct 2020
6. Algarni Abdullah, Yue Xu, Chan Taizan. An empirical study on the susceptibility to social engineering in social networking sites: the case of facebook. Eur J Inform Syst. 2017;26(6):661–87. https://doi.org/10.1057/s41303-017-0057-y.
7. Huber M, Kowalski S, Nohlberg M, Tjoa S. Towards automating social engineering using social networking sites. In: 2009 International Conference on Computational Science and Engineering, 2009;volume 3: pp 117–124. https://doi.org/10.1109/CSE.2009.205.
8. OpenVault. Broadband Insights Report (OVBI), April 2020. URL https://openvault.com/wp-content/uploads/2020/05/Openvault_Q120_DataUsage_FINAL.pdf. Accessed 28 Oct 2020
9. Huntley S. Findings on COVID-19 and online security threats. Google Threat Analysis Group Blog, April 2020. URL https://blog.google/threat-analysis-group/findings-covid-19-and-online-security-threats/. Accessed 29 Oct 2020
10. Microsoft 365 Defender Threat Intelligence Team. Exploiting a crisis: How cybercriminals behaved during the outbreak.

Microsoft Blog, June 2020. URL https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/. Accessed 04 Nov 2020
11. Frith C. Role of facial expressions in social interactions. 2009; pp 3453–3458. https://doi.org/10.1098/rstb.2009.0142.
12. Gidwani T. Identifying vulnerabilities and protecting you from phishing. Google Threat Analysis Group, March 2020. https://www.blog.google/technology/safety-security/threat-analysis-group/identifying-vulnerabilities-and-protecting-you-phishing/. Accessed 04 Nov 2020
13. International Labour Organization. Working from Home: Estimating the worldwide potential. *ILO Policy Brief*, April 2020. URL https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/briefingnote/wcms_743447.pdf. Accessed 03 Nov 2020
14. Liu S. Business software spending increases amid COVID-19 worldwide 2020. October 2020. URL https://www.statista.com/statistics/1116831/business-software-spending-covid19-forecast/. Accessed 04 Nov 2020
15. Li C, Lalani F. The COVID-19 pandemic has changed education forever. This is how. World Economic Forum, April 2020. URL https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/. Accessed 06 Nov 2020
16. UNICEF. COVID-19: Are children able to continue learning during school closures? A global analysis of the potential reach of remote learning policies. UNICEF Data, August 2020. URL https://data.unicef.org/resources/remote-learning-reachability-factsheet/. Accessed 06 Nov 2020
17. United Nations Conference on Trade, Development, and Netcomm Suisse Ecommerce Association. COVID-19 and Ecommerce: Findings from a survey of online consumers in 9 countries. October 2020. URL https://unctad.org/system/files/official-document/dtlstictinf2020d1_en.pdf. Accessed 06 Nov 2020
18. Brightcove. Q2 2020—Global Video Index. July 2020. URL https://www.brightcove.com/en/video-index#media. Accessed 05 Nov 2020
19. Kumaran N, Lugani S. Protecting businesses against cyber threats during COVID-19 and beyond. Google Cloud - IDENTITY SECURITY, April 2020. URL https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond. Accessed 06 Nov 2020
20. Microsoft Corporation. Microsoft Digital Defense Report. September 2020. URL https://aka.ms/digitaldefense. Accessed 05 Nov 2020
21. Blank Rome LLP. Flattening the Scam Curve: Be Prepared for Uptick in COVID-19 Social Engineering Cyber Attacks. *Blank Rome Cybersecurity Data Privacy*, April 2020. URL https://oacta.memberclicks.net/assets/docs/COVID-19%20Privacy%20Alert%20-%20FBI%20Alert%20Social%20Engineering%20Cyber%20Attacks.pdf. Accessed 08 Nov 2020
22. LORCA and Delloite. Social engineering attacks and COVID-19. May 2020. URL https://z3x0k1mf9pv4dfy4d3m15mq1-wpengine.netdna-ssl.com/wp-content/uploads/2020/05/Social-engineering-attacks-and-COVID-19.pdf. Accessed 07 Nov 2020
23. Cybersecurity and infrastructure security agency. COVID-19 exploited by malicious cyber actors. Alert (AA20-099A), April 2020. URL https://us-cert.cisa.gov/ncas/alerts/aa20-099a. Accessed 09 Nov 2020
24. Lefferts R. Microsoft shares new threat intelligence, security guidance during global crisis. *Microsoft Blog*, April 2020. URL https://www.microsoft.com/security/blog/2020/04/08/microsoft-shares-new-threat-intelligence-security-guidance-during-global-crisis/. Accessed 07 Nov 2020
25. Parthy P. P, Rajendran G. Identification and prevention of social engineering attacks on an enterprise. 2019; pp 1–5.
26. Nuseir M. Impact of misleading/false advertisement to consumer behaviour. Int J Econ Bus Res. 2018;16(4):453–65. https://doi.org/10.1504/IJEBR.2018.095343.
27. Hassan Chizari, Ahmad Zulkurnain, Ahmad Hamidy, Affandi Husain. Social engineering attack mitigation. Int J Math Comput Sci. 2015;1:188–98.
28. Ahmad T. Corona virus (COVID-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity. SSRN Electron J. 2020;. https://doi.org/10.2139/ssrn.3568830.