ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 6 | Issue: 10 | October 2020 || Journal DOI: 10.36713/epra2013 || SJIF Impact Factor: 7.032 ||ISI Value: 1.188

SOCIAL ENGINEERING ATTACKS AND THE CORONA VIRUS PANDEMIC

Ajayi Adebowale. O.[1]
[1] Lecturer,
Computer Science Department,
Babcock University,
Ilishan-Remo Ogun State,
Nigeria.

Ajayi Oluwabukola. F [2]
[2] Lecturer,
Computer Science Department,
Babcock University,
Ilishan-Remo Ogun State,
Nigeria.

ABSTRACT

Social engineering attacks are amongst the most successful and rampant cyber-attacks. The major focus of social engineering is the manipulation of human targets to further the objectives of an attacker. The present coronavirus pandemic has had a profound effect on how we live and work and has proved to be perfect fodder for the nefarious activities of cybercriminals. This study delineates the underlying problems in social engineering vis-à-vis the corona pandemic.

A descriptive survey was carried out on social engineering attacks and the corona virus pandemic including focused group discussions with some cyber attackers and regular users of information systems. A review of current covid-19 related social engineering schemes are presented. Insights gotten from synthesizing the knowledge gathered from the analysis of social engineering attacks during Covid-19 are also highlighted in this paper.

It is very likely that many people will continue to work from home or, at the very least, switch back and forth between home and traditional offices in their normal routines. The study therefore recommends that as the global community stays on high alert for signs of new pandemics or recurrence of the present one, safeguards will need to be put in place ensure that these anxieties don't expose enterprise IT assets to social engineering tactics.

KEYWORDS: ***social engineering, cyber-attacks, coronavirus pandemic, focused group discussions, descriptive survey***

I. INTRODUCTION

The pervasiveness of information technology also comes with its huge security and privacy concerns. Reports of security breaches abound in developed and developing countries as black hat hackers continue to have their way irrespective of degree of technological advancement [1]. The information security ecosystem is proliferated with security tools ranging from firewalls, to intrusion detection systems, intrusion prevention systems and cryptographic systems, yet security breaches abound. This calls for a more holistic approaches to information security and more specifically there is a need for human centred security interventions [2].

Like every other system, an information security system is only as strong as its weakest points and several empirical studies have concluded that users of information systems often represent the weakest part of the information security system. While research has been focussed on identifying vulnerabilities in networked systems, little attention has been given to the users of these systems despite their varying levels of computing expertise. It has become imperative to shift our focus to the human elements of information security as social engineering attacks [3] continue to lead the charts when it comes to successful cyber and information security attacks. A report by Computer emergency response team CERT and the national security agency in 2018 placed social engineering attacks at the top of security incidents, followed by SQL injection, spyware and ransomware.

A focus group discussion with Nigerian online scammers popularly known as yahoo boys revealed that a large number of their schemes is centred around social engineering. The major focus of their schemes borders on identifying potential victims and preying on their gullibility and naivety. Very little technical know-how is needed to be a successful yahoo boy as evidenced in the success recorded by inhabitants of towns and villages with low levels of literacy here in Nigeria. Some secondary students actually drop out of school to begin their black hat careers armed with just a laptop and an internet

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 6 | Issue: 10 | October 2020 || Journal DOI: 10.36713/epra2013 || SJIF Impact Factor: 7.032 ||ISI Value: 1.188

modem. Yet this semi-literate individuals con multinationals and educated individuals of their hard earned money. The success rate of these yahoo boys is so high that several literatures now delineate certain security hacks as 'nigerian scams' [4].

Though several schemes are used to lure victims into revealing sensitive and sometimes personal information or even to make them send money to perpetrators of social engineering attacks, the varying schemes can be characterised based on their mode of operation. Examples of security scams identified as Nigerian cyber fraud by certain sections of cyber security research includes and are not limited to: impersonations on online dating sites, posting false advertisements on classified sites like craiglist.com, lottery scams and phishing scams. In all of these aforementioned scams, the attackers aim to get the trust of unsuspecting victims, lure them away from the medium of contact after establishing sufficient trust and then proceed into executing the attack either by asking for payments through several payment options (Paypal, Western Union, Moneygram, wire transfers, gift cards, cryptocurrencies among others).

Detecting these personal cyber attacks remain a difficult problem given the stealth and sometimes complex process of the attacks. For example, After luring an unsuspecting victim from craiglist, an attacker could use google talk to engage his potential victim. This leaves little data points on the craiglist platform to help inform any detection system running on the craiglist servers. Secondly, after engaging the victim on google talk, the potential victim could be given a legitimate bank account belonging to another unsuspecting victim of a phishing attack which would then forward such funds to the final recipients or use the funds to buy gift cards or other tangibles to be sent to the attackers themselves [5].

Trailing social engineering attacks therefore remains a very arduos task and are nearly impossible to detect by implementing a detection software or hardware as they mostly comprise of apparently legitimate steps [6]. Proper education therefore remains the only viable defence to effectively combat attacks on our personal space.

Another type of personal cyberattacks involves large organisations. Among Nigerian yahoo boys, such scams are categorised as Chief financial officer (CFO) scams and Ali Baba scams. These scams are considered the most lucrative and tedious of scams and sometimes involves more than one attacker for a successful operation. A group of scammers obtain corporate mails from the dark web and infiltrate the mail domain while studying the organisational culture regarding wire transfers. The attackers remain undetected by the company's mail domain intrusion detection systems through te use of malware attached to company emails. These kinds of attack can be categorised as Advanced Persistent Threats as they can remain undetected for a long period as the attacker receive company receipts and other valuable communication while sometimes waiting for the opportuned moment to strike.

Successful CFO attacks occur when the company's CFO receives a mail purportedly coming from the CEO, Chairman or Managing director to send huge sums to an offshore account, Most especially while such higly placed person (CEO, chairman) is on holidays. The attackers sometimes monitor company mails for close to a year to identify when influential company figures go on breaks before striking. If unsuccessful the attacker simply looks for more creative ways to use acquired company documents, they have been privy to via metamorphosed attacks.

A successful CFO attack on the other hand is said to guarantee a minimum of fifty thousand dollars and annually billions of dollars are lost to perpetrators. Like the previously elucidated examples these attacks require proper security education for staffs of organisations in conjuction with adoption of state-of-the-art intrusion detection systems. It is widely accepted in certain corners of the information security world that security is an illusion. As long as valuables remain in the cyber space there are bound to be cyber pirates threatening the peace and well-being of the cyberverse. The onus therefore lies on the users of these important resources to harm themselves with sufficient levels of paranoia befitting the value of domiciled information.

It is well established that criminals capitalize on the fears of their victims and the present COVID-19 pandemic has so far proved to be the perfect fodder for cybercriminal activities. Every aspect of the COVID-19 crisis has been exploited by opportunistic hackers, terrorists, and other criminals. In addition to capitalizing on rampant fear, uncertainty, and doubt, attackers are targeting a fresh new honeypot of federal aid, in the form of payouts from unemployment checks, stimulus checks, and the Paycheck Protection Programs.

II. SOCIAL ENGINEERING CYBERATTACKS AND PANDEMIC ANXIETIES

Pervasive social engineering attacks are hindering the world's coordinated response to the COVID-19 emergency. As noted in this recent press report, cyberattacks have spiked during the first half of 2020 [7]. The FBI noted that as of May 28, it had received nearly the same number of complaints for this calendar year as for all of 2019.

Preying on social engineering factors, cyberattackers exploit the following facets of society's collective response to the pandemic:

- **Demand for accurate information on the crisis**: A swelling number of malicious COVID-

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 6 | Issue: 10 | October 2020 || Journal DOI: 10.36713/epra2013 || SJIF Impact Factor: 7.032 ||ISI Value: 1.188

19 websites and emails claim to offer useful information on the coronavirus and how to protect oneself. It's no surprise that thousands of COVID-19 scam and malware sites are being created daily. Many spread false narratives about the COVID-19 outbreak's progression and impact while stirring anxiety, selling bogus treatments and cures, price gouging for face masks and other needed supplies, and otherwise taking advantage of nervous people's gullibility.

- **Deepened online dependence**: DDoS attacks have bombarded websites people depend on for their quarantined existence. In addition, hackers are targeting DDoS attacks at the enterprise VPN ports and protocols used for remote access, thereby crippling employees' ability to get their work done from the coronavirus-free comfort of home. Hackers may initiate thousands of SSL connections to an SSL VPN and then leave them hanging, exhausting memory and thereby preventing legitimate users from using the service.
- **Expanded use of email and social media**: Phishing attacks have increased. They are frequently cloaked in emails that include pandemic maps or other content related to the coronavirus. In addition, social media is being used as a broadcast platform for predatory and deceptive content, while the companies that run those communities attempt to nip it in the bud. Social engineering tactics in phishing and spam campaigns trick people into disclosing passwords and other sensitive personal and financial information.
- **Sudden mandate to work from home**: People working from home for the first time are acutely exposed to cybersecurity intrusions. Many remote workers may fail to use prudent cybersecurity practices. These lapses often include not securing their passwords effectively, opting not to use multifactor authentication, or neglecting the need for a virtual private network. Corporate IT staff may themselves be working from home, lacking the resources needed to monitor and secure a huge remote workforce's access to corporate IT assets effectively. In addition, there has been a spurt of voice phishing attacks where callers pretend to be from workplace technical support and thereby convince employees to disclose passwords or to enter authentication information into malicious websites.
- **More vulnerable economic situations**: More COVID-19-related ransomware attacks via email exploit people and organizations' increasingly desperate straits due to job losses and the general recession. Some attacks involve hacking enterprise routers to direct users to bogus COVID-19 websites that trick people into downloading malware onto their computers. An uptick in text message phishing perpetrates such scams or dupes targets into loading malicious content onto mobile devices.
- **Community efforts to mitigate pandemic risks**: Cyberattacks on public-sector healthcare coordinating bodies have ramped up. The U.S. Department of Health and Human Services was recently the target of a cyberattack apparently designed to undermine the country's response to the coronavirus pandemic. In addition, a state-sponsored hacking group attempted, albeit unsuccessfully, to breach IT systems at the World Health Organization. The FBI has detectedcybersecurity attacks against the healthcare industry since the start of the outbreak, such as email fraud campaigns designed to solicit donations for nonexistent healthcare-related organizations and bogus contact-tracing apps that download malware onto a user's device.

III. SOCIAL DISTANCING DEEPENS CYBERSECURITY VULNERABILITIES

Social distancing has become the critical response for flattening the curve of COVID-19. As in-person encounters become less frequent, we'll have to rely on each person to ensure that they don't fall victim to these tactics in their myriad virtual and online interactions. That will place more of a burden on the IT infrastructure—and personnel—to guide everybody in the new normal of vigilance against these risks [8].

Exacerbating it all is the fact that many IT professionals have been thrown off balance by their own need to work from home while supporting a vastly expanded home-based workforce. The increasing demand for social distancing, lockdowns, and shutdowns has made it difficult for many IT vendors, including big cloud service providers, to keep the lights on in their facilities. As users find it harder to receive 24x7 support for cybersecurity issues that pop up during the COVID-19 emergency, the attacks on their computers, data, and other online assets will grow [9].

Robotics, postperimeter, and AI are key cyberdefenses against social engineering tactics

If there's any hope to reduce society's exposure to pandemic-stoked social engineering hacks, it comes in the form of AI-driven robotics. To the extent that we can automate more of the tasks in our lives, we'll reduce the need for human decisions and our vulnerability to cyberscams. Fortunately, the COVID-19 crisis has brought robotic systems to the front lines in every conceivable scenario: in industry,

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 6 | Issue: 10 | October 2020 || Journal DOI: 10.36713/epra2013 || SJIF Impact Factor: 7.032 ||ISI Value: 1.188

commerce, and the consumer worlds, including (especially) in the back-end data centers that are the beating hearts of the modern economy.

Postperimeter security will be another key defense against social engineering hacks in the postpandemic economy. It ensures that users access cloud apps only from managed devices and secure apps. Enterprise IT can block users from falling prey to social engineering tactics, such as requests to connect their mobile devices to unsupported or risky cloud services. In this way, postperimeter security gives people who work from home access to many resources beyond the enterprise perimeter while also giving corporate IT fine-grained control over what, when, and how they do this.

Artificial intelligence (AI) will play a pivotal role in postpandemic defenses against social engineering hacks. Automated systems can't have hard-and-fast rules for detecting the zillion potential cybersecurity attack vectors. But they can use AI's embedded machine learning models for high-powered pattern recognition, detecting suspicious behavior, and activating effective countermeasures in real time. For example, AI-based defenses can proactively isolate or quarantine threatening components or traffic after determining that a website is navigating to malicious domains or opening malicious files, or after sensing that installed software is engaging in microbehaviors that are characteristic of ransomware attacks.

However, AI-based defenses are no panacea, especially when monitoring social engineering attacks that have complex signatures and evolve rapidly. AI-based defenses detect and block abnormal behavioral patterns involving endpoints, or in the network, or in how users interact with devices, applications, and systems. If the AI-learned attack vector is too broad, it's at risk of blocking an excessive number of legitimate user behaviors as cybersecurity attacks. If the pattern is too narrow, the cybersecurity program risks permitting a wide range of actual attacks to proceed unchecked.

IV. SOCIAL ENGINEERING LESSONS FROM COVID-19

Unless we do something proactively, social engineering's impact is expected to keep getting worse as people's reliance on technology increases and as more of us are forced to work from home.

Contact tracing, superspreaders, flattening the curve — concepts that in the past were the domain of public health experts are now familiar to people the world over. These terms also help us understand another virus, one that is endemic to the virtual world: social engineering that comes in the form of spear-phishing, pretexting, and fake-news campaigns.

As quickly as the coronavirus began its spread, news reports cautioned users about social engineering attacks that tout fake cures and contact-tracing apps. This was no coincidence. In fact, there are a number of parallels between the human transmission of COVID-19 and social engineering outbreaks:

Just like coronavirus transmits from person to person through respiratory droplets, social engineering also passes from users through infected computing devices to other users. Because of this transmission similarity, just as infected people — because of their physical proximity to many others — act as superspreaders for COVID-19, some technology users act in a similar way. These tend to be people with many virtual friends or those subscribing to many online services who consequently have a hard time discerning a real notification or communication from one of these personas or services from a fake one. Such users are prime targets for social engineers looking for a victim who can provide a foothold into an organization's computing networks.

The vast majority of people infected with this coronavirus have mild to moderate symptoms. The same is the case with most victims of social engineering because hackers usually lurk imperceptibly as they make their way through corporate networks [8]. They often go undetected for months — on average, at least 101 days — showing no signs or symptoms.

Just as no one has immunity from COVID-19, no one is immune against social engineering. By now everyone, all over the world, has been targeted by social engineers, and many — trained users, IT professionals, cybersecurity experts, and CEOs — have fallen victim to a spear-phishing attack.

COVID-19's outcomes are worse for people who have prior health conditions and for people who are older. Similarly, the outcomes of social engineering are worse for users with poor computing habits and poor technical capabilities. Many of these tend to be senior citizens and retired individuals who lack updated operating systems, patches that protect them from infiltration, and access to managed security services.

Finally, personal hygiene — hand washing, use of masks, social isolation — is the primary protection against coronavirus infection. Likewise, for protecting against social engineering, digital hygiene — protecting devices, keeping updated virus protections and patches, and being careful when online — is the only protection that everyone from the FBI to INTERPOL has in their arsenal.

But beyond these similarities, social engineering outbreaks are actually harder to control than coronavirus infections:

Social engineering infections pass through devices wirelessly, making it hard to contact-trace infection sources, isolate machines, and contain them. Unlike the COVID-19 pandemic, social

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 6 | Issue: 10 | October 2020 || Journal DOI: 10.36713/epra2013 || SJIF Impact Factor: 7.032 ||ISI Value: 1.188

engineering infections are hard to trace and isolating infected systems will not curb its spread

There are well-established scientific processes that the medical community has developed to identify knowledge gaps about coronavirus. This helps researchers focus. In contrast, even the fundamentals of social engineering — such as when it's correct to call an attack a breach or a hack — lacks clarity. It's hard to do research in an area when there is no consensus on what the problem should be called or where it begins and ends.

While human hygiene is well researched, digital hygiene practices aren't. For instance, in 2003, NIST developed password hygiene guidelines asking that all passwords contain letters and special characters and are changed every 90 days. The guideline was developed by studying how computers guessed passwords, not how humans remembered them. Consequently, users the world over reused passwords, wrote them down on paper to aid their memory, or blindly entered them on phishing emails that mimicked various password-reset emails — until 2017, when these problems were recognized and the policy was reversed.

Evidence points to those who have recovered from coronavirus having at least short-term immunity to it. In contrast, organizations that have had at least one significant social engineering attack tend to be attacked again within the year. Because hackers learn from every attack, this suggests that the odds of being breached by social engineering actually increase with each subsequent attack.

Our response to COVID-19 is informed by reporting throughout the healthcare system. Unfortunately, there is no similar reporting mechanism for social engineering. For this reason, a hacker can conduct an attack in one city and replicate it in an adjoining city, all using the same malware that could have easily been defended against had someone notified others. We saw this trend play out in ransomware attacks that crippled computing systems in Louisiana's Vernon Parish in November 2019, quickly followed by six other parishes, and continuing through the rest of the state in February 2020.

Because of these factors, the economic impact of social engineering continues to grow. There has been a 67% increase in security breaches in the past five years, and last year companies were expected to spend $110 billion globally to protect against it. This makes social engineering one of the biggest threats to the worldwide economy outside of natural disasters and pandemics.

Just as we are fighting the pandemic, we must coordinate our efforts to combat social engineering. Without it, there will be no vaccine or cure. To this end, we must develop intraorganizational reporting portals and early-warning systems to warn other organizations of breaches. We also need federal funding for basic research on the science of cybersecurity along with the development of evidence-based digital hygiene initiatives that provide best practices that take into account the user and their use cases. Finally, we must enlist social media platforms for tracing the superspreaders in their users, and develop open source awareness and training initiatives to protect them and the cyber-vulnerable from future attacks.

V. CONCLUSION

Unless we do something proactively, social engineering's impact is expected to keep getting worse as people's reliance on technology increases and as more of us are forced to work from home, away from the protected IT enclaves of organizations. We may in the end win the fight against the coronavirus, but the war against social engineering has yet to begin.

These and other cyberdefenses will crystallize into a new normal for enterprises in the postpandemic era. It's likely that many people will continue to work from home or, at the very least, switch back and forth between home and traditional offices in their normal routines. As the global community stays on high alert for signs of new pandemics—or recurrence of the present one—safeguards will need to ensure that these anxieties don't expose enterprise IT assets to social engineering tactics perpetrated by hackers, terrorists, and other criminals.

REFERENCE

1. *A. Alzahrani and C. Johnson, "AHP-based Security Decision Making: How Intention and Intrinsic Motivation Affect Policy Compliance," Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 6, 2019, doi: 0.14569/IJACSA.2019.0100601.*
2. *N. A. G. Arachchilage, S. Love, and K. Beznosov, "Phishing threat avoidance behaviour: An empirical investigation," Comput. Human Behav., vol. 60, pp. 185–197, 2016, doi: 10.1016/j.chb.2016.02.065.*
3. *J. D'Arcy, A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach," Inf. Syst., vol. 20, no. 1, pp. 79–98, 2009.*
4. *Y. Park, J Jones, D. McCoy, E. Shi and M. Jakobson "Scambaiter: Understanding Targeted Nigerian Scams on Craigslist" http://damonmccoy.com/papers/scambaiter.pdf (accessed oct 9, 2020)*
5. *T. Jagatic, N. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," Commun. ACM, vol. 50, no. 10, pp. 94–100, 2007.*
6. *National Cyber Security Centre, "Phishing campaign," 2018. https://www.ncsc.gov.uk/news/phishing-campaign (accessed Oct 2, 2020).*
7. *N. Kumaran and S. Lugani, "Protecting against cyber threats during COVID-19 and beyond,"*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 6 | Issue: 10 | October 2020 || Journal DOI: 10.36713/epra2013 || SJIF Impact Factor: 7.032 ||ISI Value: 1.188

2020. https://cloud.google.com/blog/products/ identity-security/protecting-against-cyber-threats-during-covid-19-andbeyond (accessed Sept 23, 2020).

8. *National Cyber Awareness System, "COVID-19 Exploited by Malicious Cyber Actors," 2020. https://www.us-cert.gov/ncas/alerts/aa20-099a (accessed Sept 7, 2020).*
9. *K. Okereafor and O. Adebola, "Tackling The Cybersecurity Impacts of the Coronavirus Outbreak as a Challenge to Internet Safety," J. Homepage http//ijmr. net., vol. 8, no. 2, 2020.*
10. *C. Mu-Hyun, "South Korea sees rise in smishing with coronavirus misinformation," ZD Net, 2020. https://www.zdnet.com/article/southkorea-sees-rise-in-smishing-with-coronavirusmisinformation/#ftag=RSSbaffb68 (accessed Sept 7, 2020).*