International Journal in IT & Engineering (IJITE)
Volume 8 Issue 2, February 2020 ISSN: 2321-1776 Impact Factor: 6.493
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

TACKLING THE CYBERSECURITY IMPACTS OF THE CORONAVIRUS OUTBREAK AS A CHALLENGE TO INTERNET SAFETY

Kenneth Okereafor, PhD, PhD [1]
[1] Deputy General Manager - Database Security,
Department of Information and Communications Technology,
National Health Insurance Scheme (NHIS) Abuja, NIGERIA.
Olajide Adebola [2]
[2] Chief Technology Officer,
Home Plus Medicare Services Ltd. Abuja, NIGERIA.

Abstract

The world is currently ravaged by the novel coronavirus which has so far affected 82,410 persons in 50 countries with a death toll of 2,808 as at 27th February 2020, and code-named COVID-19 by the World Health Organization (WHO) on 11th February 2020. Research findings indicate that due to the contagious nature of the virus, there is so much anxiety over its spread and mode of infection. As the world awaits a possible cure or a remedy to curb the spread of COVID-19, every online information that makes direct or indirect reference to the word "coronavirus" tends to attract fast attention of internet users. As a result, cybercriminals are exploiting the fear and uncertainty surrounding the coronavirus outbreak to distribute malicious software with the motive of stealing confidential data, disrupting digital operations and making illicit ransom money from an outbreak that has been declared a global health emergency by the WHO. Does the coronavirus outbreak have any significant impact on user privacy and computer security? This paper reviews the cyber security effects of the coronavirus panic on digital systems and the cyberspace. The paper makes recommendations for safer internet usage and privacy protection in the face of rising coronavirus-related online scams.

Keywords: *Coronavirus, cybercriminals, cyber security, malicious code, scam, social engineering.*

1.0: INTRODUCTION

Coronaviruses (CoV) are a large family of viruses that cause illnesses ranging from the common cold to more severe diseases such as Middle East Respiratory Syndrome (MERS-CoV) and Severe Acute Respiratory Syndrome (SARS-CoV). The novel coronavirus (formally nCoV) which was officially renamed **COVID-19** (WHO, 2020), (Coronavirus disease named Covid-19, 2020), (The Verge, 2020), (COVID-19: WHO renames deadly coronavirus, 2020) by the World Health Organization (WHO) on 11th February 2020 is a new strain that has not been previously identified in humans (Coronavirus). Coronaviruses are zoonotic, meaning that they are transmitted between animals and people through pathogens shared with wild or domestic animals. Zoonotic diseases are naturally transmitted from animals to humans (or vice versa) either by the consumption of contaminated food and water, exposure to the pathogen during preparation, processing or by direct contact with infected animals or humans (Sanyaolu, Okorie, Mehraban, & Ayodele, 2016), (Karesh, Dobson, &

Lloyd-Smith, 2012). Other examples of zoonotic diseases are Ebola virus disease and salmonellosis. The COVID-19 which was first spotted in Wuhan, China in December 2019, has currently spread to 50 countries accounting for over 82,410 infections with a rising death toll of 2,808 cases as at 27th February 2020, leaving 14% of the affected in serious/critical conditions (WUHAN CORONAVIRUS OUTBREAK, 2020). On the 30th of January 2020, the WHO declared the coronavirus outbreak a public health emergency.

The WHO's declaration increased the global perspective of the disease and equally created greater apprehension, making anything that purports to relate to coronavirus a source of attention, as the world is desirous of information that can stop the spread of the virus as well as lead to a lasting solution such as a vaccine or curative therapy. While the search is ongoing, cybercriminals are taking advantage of people's desperation and fear to sell non-existing products, disseminate unsubstantiated claims (China coronavirus: Misinformation spreads online about origin and scale, 2020) and fake news and in the process steal valuable confidential data using various malicious software (malware) to package their arsenal.

The rest of this paper is organized as follows: Section 2 examines how digital behaviors are changing as a result of the coronavirus outbreak. Section 3 reviews the economic importance of the coronavirus to cybercriminals. Section 4 discusses the human weaknesses which cybercriminals exploit to attract victims and discusses some of the most common tactics used by internet fraudsters to attack digital systems and internet resources. Section 5 makes recommendations on how to prevent, detect or respond to threats that tend to take advantage of the coronavirus panic to attack internet users and systems. Section 6 summarizes the entire discuss.

2.0: EFFECTS OF CORONAVIRUS OUTBREAK ON DIGITAL BEHAVOUR

The disease outbreak has a huge impact on digital behavior of computer and internet users not only in the affected localities but across the globe. On the global stage, authorities such as the World Health Organization (WHO) and China's National Health Commission (NHC) are using digital systems to send and receive information about the nature and magnitude of infections, educate the public on how to prevent transmissions and instruct on what to do if infected. Governments are using high speed telecommunications facilities to securely issue travel advice to their citizens home and abroad. In Wuhan for example, after the lockdown by the Chinese Government, videos of nationals of other countries trapped in Wuhan started surfacing on the internet and social media platforms, necessitating Governments to plan for evacuation of their citizens in record time. At some point when face masks to prevent transmission was out of stock in some badly affected localities, authorities had to resort to the use of digital systems to locate countries where masks could be sourced and shipped from. With daily updates disseminated through digital systems and internet resources, people tend to access ready information hoping to know more about the coronavirus.

In addition to the use of drones to advice the public, Chinese authorities have released a mobile App that tracks people and alerts them if they have been in "close contact with someone infected" with the new coronavirus (China launches coronavirus app to detect whether users have come in 'close contact' with the sick, 2020). The App uses WeChat, Chinese most popular messaging and social media platform, to allow users to submit their name, phone number and Government-issued ID number to request information about

whether they have been in close contact with anyone infected by the virus (As Chinese Internet Users Try To Track The Coronavirus, Their Government Is Tracking Them, 2020), (WeChat now lets you report information on the Wuhan coronavirus, 2020). They can also report and share up-to-date information on the disease.

Knowing that such a deadly disease also causes despair among people, the outbreak of COVID-19 has had its impact on digital behaviors of digital consumers particularly internet users. In the short term, users shall continue to rely heavily on digital resources while seeking for information to protect them and avoid travelling to places affected with the disease. This will limit global trade and economic growth with a negative impact on individuals whose trades are directly affected. Such people will continue to use digital systems to look out for the appropriate time when infections are under control especially with China being an exporting nation. Until such a time when a reasonable control of the coronavirus outbreak is achieved, or a vaccine to prevent future infections is discovered, the attitude towards the use of digital systems to better understand the situation will continue to increase.

3.0: CYBERSECURITY IMPACTS OF THE CORONAVIRUS OUTBREAK

Cybersecurity focuses on preventing unauthorized alteration of data and protecting users from falling prey to computer-based scams that threaten the confidentiality, integrity and availability of digital information on the internet and the entire cyberspace. The word coronavirus is perhaps one of the most searched words on the internet today, and the reason is obvious. A search engine is a software used to find data faster on the internet or a website using specific textual keywords to narrow the search. Internet search engines are currently overwhelmed with keywords containing the strings *corona, virus, coronavirus, COVID-19, china*, *Wuhan disease*, and other related keywords. The desperation to access updated information related to the spread of the coronavirus leads to an increase in internet network traffic, and particularly a rise in the chances of spreading malicious codes in disguise of authentic coronavirus information. A malicious code is the term used to describe any computer software/program that is intended to cause undesirable effects, security breaches, privacy infringements, or damage to a system (Neil DuPaul). A malicious code that successfully finds its way into a poorly protected computer system can lead to several detrimental outcomes including stealing confidential information, exposing sensitive and private financial data, spying on the user's online transactions, or installing a number of other malicious codes that can be activated at a later date or to be triggered by certain specific occurrence such as logic bombs.

4.0: CYBERATTACKS ON HUMAN WEAKNESSES USING CORONAVIRUS FEAR

The despair and anxiety exhibited by people in the face of seeking for coronavirus information also exposes inherent vulnerabilities that make humans easy targets of cybercrime. Just as computers and other digital assets exhibit vulnerabilities and weaknesses, human beings have weaknesses too that can be taken advantage of by cybercriminals and internet fraudsters to obtain sensitive information or to gain unauthorized access. The art of cleverly gathering sensitive and confidential information from a person by exploiting human weaknesses is known as social engineering (Lohani, 2019). Social engineering is a

psychological exploitation which scammers use to skilfully manipulate humans and carry out emotional attacks on innocent people (Atkins & Huang, 2013). Social engineering methods use psychological tricks to create deception, which in turn makes people to perform actions or divulge personal and corporate confidential information (Choudhary, Kumar, & Kumar, 2016) innocently. These deceptive methods remain a major global threat as more organizations digitize operations and increase connectivity through the internet (Aldawood & Skinner, 2019) and as more people rely on the internet for updated information on the coronavirus outbreak. The term typically applies to trickery or deception for the purpose of information gathering, fraud, identity theft, or computer system access (Choudhary, Kumar, & Kumar, 2016). Social engineering targets human vulnerabilities, weaknesses and flaws including anxiety, desperation, urgency, fear, loyalty, compassion, confusion, respect, honesty, persuasion, etc. The social engineering aspect of the coronavirus pertains to the exploitation of people's fears of infection to spread dubious health advice (China coronavirus: Misinformation spreads online about origin and scale, 2020), malware and other cyber threats (Alex Scroxton, 2020). People are anxious to learn how to avoid contacting the virus as well as desperate for new of a possible containment of the spreading outbreak. This anxiety leads to an unusual clinging to the digital systems to know more about the situation. As a result, any message that carries the connotation of coronavirus receives easy attention including spam emails, fake websites and malicious attachments which internet fraudsters use to steal information through deception and falsehood.

4.1: Coronavirus malware

A malicious software (malware) is any software that has been deliberately designed to cause data loss, harmful or undesirable outcome including unauthorized alteration. Cybercriminals are using emails that claim to originate from authorized public health facilities, with the malicious code embedded in an attachment such as a Microsoft Word document that purportedly contains instructional information and advice on safeguard and defence measures against contracting the coronavirus disease. Majority of the cybersecurity gimmicks exploiting the coronavirus episode purport to offer updates and health information relevant to the global health emergency. A popular coronavirus-related malware is the Emotet, a banking trojan malware program which secretly obtains financial information from victims by concealing and injecting a destructive computer code into an infected programme such as a Microsoft Word document, allowing sensitive data to be stolen in the process (Ishita Chigilli Palli, 2020). Such an attack could result in disclosure of confidential proprietary information and financial loss as well as disruption to operations and harm to corporate reputation (Mathew J. Schwartz, 2020). Undetected malware residing permanently in a system can become a perpetual source of spying and exporting confidential data from the victim's computer to a remote malicious hacker. Such malware also called an Advanced Persistent Threat (APT) would find easy distribution channel using coronavirus-related scams and deceitful web portals claiming to disseminate genuine COVID-19 information.

4.2: Coronavirus spam emails

Cyber criminals use a technique called *social engineering* to obtain confidential information from vulnerable victims and use such information to launch other attacks. Social engineering is the use of human weaknesses to compel action and obtain a secret. A typical example of social engineering is phishing/spam email where an attacker sends a deceptive email to an unsuspecting target or a group with the intention of obtaining classified information such as login credentials, passwords and security codes. In the case of the coronavirus, cybercriminals are currently using an advanced form of phishing called spear phishing usually targeted at chief executives of corporate entities or influential personalities. Spear phishing is a customized version of the phishing scam where accurate profiles and details of the target recipient are smartly presented in the body of the email to make the correspondence appear real, authentic and believable. A classic spear phishing scam would address the target in his correct official designation (e.g. The Chief Medical Officer), precise salutation (e.g. Dear Dr. Martins), and his exact designation/responsibilities. Coronavirus spam emails would address a victim in a tone that suggests familiarity while offering a service or product that claims to have latest information on the disease. Oftentimes scammers construct spam mails using expressions and keywords that create a sense of urgency and fear both of which are human vulnerabilities that facilitate social engineering attacks.

4.3: Fake coronavirus information websites and online portals

A fake or cloned website is a replica or imitation of the authentic website hosted by cyber criminals with the intention of misleading users (China coronavirus: Misinformation spreads online about origin and scale, 2020) and gathering confidential information that can later be used to steal data, alter financial information or disrupt digital operations. Fake commercial websites are springing up advertising products and services purportedly related to coronavirus spread, prevention and awareness, and compelling users to either make instant purchases, place orders online or subscribe to free COVID-19 information. If a web portal portrays payment facilities, it is a good practice to inspect the website properly before initiating payment processes. The website inspection for payment genuineness must observe the procedures listed under recommendations below.

5.0: RECOMMENDATIONS FOR MAINTAINING ONLINE SAFETY AMID CORONAVIRUS SCAMS

The following recommendations and guidelines are essential for preventing, detecting and responding to cyber threats that particularly take advantage of coronavirus anxiety to distribute malware or steal confidential information. These guidelines are useful advice to help individual and corporate internet users to safeguard their online operations and protect digital assets from unauthorized access amid coronavirus scams and several other online threats.

5.1: Test commercial websites before making payments

i. Look out for names and/or expressions on the website that do not completely reflect the identity or focus of the claimed entity you intend to pay to.

ii. Watch out and beware of spelling mistakes and grammatical errors on the website. Inconsistent grammatical expressions are indicative of fakeness.
iii. Watch out for contradictory statements and ambiguous instructions within the website.
iv. Look out for instructions that imply a sense of urgency particularly referring to a well-known critical incident such as the coronavirus outbreak.
v. Be alert to ambiguous contact details displayed on the website including unreachable phone numbers, wrong email addresses, untraceable physical addresses, misleading designations, and many other details whose portrayals are suspicious.

Any or combination of these is enough to suspect the website, at which point the transaction must be aborted. Never supply your bank details to a suspicious website. Verify first by contacting a customer service personnel via phone or email where applicable.

5.2: Be vigilant with spam emails

Every email with a string of coronavirus appendage should be handled with caution as it could be a potential cyber security threat disguised as a genuine resource, more so if the email carries an attachment. Any email with a strange sender's address and sent to you as a blind copy (bcc) should be treated as suspicious. If the email carries a strangely looking or unsolicited attachment such a *coronavirus information pack*, latest *COVID-19 statistics*, etc, then the suspicion should increase. All such suspicious emails should either be ignored or deleted. Never open a suspicious email or try to download its attachment except if you are sure of the source and have a good antivirus software on your system.

5.3: Install an effective anti-malware software

Anti-malware programmers such as antivirus software are software designed to identify contents that are potentially harmful to the computer particularly those disguised as coronavirus resources. Having a functional anti-malware tool on all internet-connected devices is a good approach for users desirous of preventing malwares and averting their huge consequences. A good antivirus or anti-malware solution is able to apply an advanced detection mechanism (Dixit & Mishra, 2012) to detect the most common strings of malicious codes and can take actions to protect systems and data. Prior to choosing and installing an antivirus tool, users should take note of performance features, and support given by the antivirus software providers (Devi & Kumar, 2016). It is also important to keep all antivirus software fully updated for maximum efficiency.

5.4: Keep a good social engineering vigilance and cyber awareness

Social engineers usually take advantage of human weaknesses to obtain confidential information from unsuspecting victims. It is important for users to exhibit caution and calmness, and not allow their desperations and anxiety over the spreading coronavirus disease to dictate their online behaviours or to negatively influence their choices. With vigilance, some of the indicators can be detected from messages that ordinarily would appear innocent and genuine.

5.5: Avoid opening suspicious attachments

All attachments that do not appear normal either due to unrealistic size or clumsy display format should be ignored or deleted. Abnormal attachments include word documents with an .html extension, excessively large documents, and attachments sent to multiple recipients in a chain-like manner. These and other related indicators should be monitored closely and once a pattern is established, an appropriate response action should follow to forestall falling prey to cyberattacks using coronavirus information as a bait.

5.6: Avoid clicking on questionable web addresses and URLs

A Uniform Resource Locator (URL) is the technical name for the address or identity of a website. To verify the authenticity of a suspicious web address, users are encouraged to carry out the hover test on any URL (or referenced website address) before clicking to open. Simply place or hover the mouse pointer above the suspicious URL and look out for the display that pops up. Confirm that the path displayed is similar to the purported web resource being referenced to. Any deviation in information content should be suspected, and appropriate action taken including aborting the operation.

5.7: Keep a functional backup of data

In the event of a cyber-breach involving the successful implantation of a malicious code disguised as legitimate coronavirus information through a deceitful email attachment or fake website, a previous local or remote backup comes very handy to minimize the impact of data loss. As a precautionary measure, it is advisable to perform regular data backup to forestall the possibility of huge data loss in case of a breach.

5.8: Verify information source

There is currently an overload of digitized information on the COVID-19 outbreak purporting to be genuine and credible, and so the need to obtain authentic information cannot be over emphasized. A disease that comes with despair requires verification of information sources before an individual out of fear takes the wrong steps. Verifiable up-to-date information is available from health institutions at global, regional and national levels. WHO maintains a web portal that offers courses on methods for detection, prevention, response and control of emerging respiratory viruses, including COVID-19 at https://openwho.org/courses/introduction-to-ncov (Emerging respiratory viruses, including nCoV: methods for detection, prevention, response and control, 2020). Similarly the WHO website contains standard recommendations for the general public to reduce exposure to and transmission of a range of illnesses, e.g. to protect oneself and others from getting sick, and to stay healthy while travelling (Updated WHO advice for international traffic in relation to the outbreak of the novel coronavirus 2019-nCoV, 2020), (Emerging respiratory viruses, including nCoV: methods for detection, prevention, response and control, 2020). Since not all information out there is factual and correct, consumers of digital services must know who to follow in the cyberspace and where to search for the right information about coronavirus on digital platforms.

5.9: Fine-tune digital readiness

It is very imperative to fine-tune surveillance and monitoring systems to ensure speedy contact-tracing in case the COVID-19 arrives. The use of Geographic Information System (GIS) resources in addition to data analytics tools can provide a view of the spread of the disease to help citizens avoid unnecessary visits to such places. At the National level, a combination of multiple initiatives made up of contemporary messaging Apps, cybersecurity technologies, data analytics tools, high speed telecommunications and an informed digital consumer base makes the cyberspace ever ready to play a facilitating role in disseminating up-to-date authentic information on the spread and containment of the coronavirus disease.

6.0: CONCLUSION

The ability of the coronavirus to infect more people across many countries outside the epicentre of the outbreak makes the nature and magnitude of the virus peculiar in comparison with previous health emergencies of global dimension such as the 2014 Ebola virus outbreak. With such peculiarities, it is only natural that humans will continue to display desperation for information leading to its control and eradication. Even as countries struggle to curtail the spread of the COVID-19, and drug makers work desperately to develop vaccines and therapies that could combat the new virus that is more contagious than SARS and could cost the global economy four times more than the about $40 billion gulped by the 2003 SARS outbreak (Coronavirus deaths exceed Sars fatalities in 2003, 2020), (Doctors in China Are Starting Human Trials for a Coronavirus Treatment, 2020), (China sends Coronavirus treatment guide to Nigeria, 2020) unfortunately cybercriminals are cashing in on human desperation to deceive internet users and distribute harmful software. The paper concludes that this desperation which is premised on the fact that every available literature on the virus appears attractive to internet users, increases the chances of downloading adware, spyware, ransomware and other malicious software. The panic and anxiety associated with the coronavirus have increased online vulnerabilities and ignited a wave of cyberattacks using social engineering as a tool, whereby cybercriminals are taking advantage of human fear and apprehension to distribute destructive codes in the guise of authentic coronavirus information and stealing confidential information in the process. The paper recommends that proper awareness is essential to distinguishing genuine information from those with malicious, misleading or false intent (China coronavirus: Misinformation spreads online about origin and scale, 2020).

Notwithstanding the strength of security deployed to detect and prevent cyberattacks masquerading as candid online coronavirus information, it is important for digital users to have a plan for recovery from successful cyber breaches in order to minimize their impacts if they occur. Recovery plans are essentially anticipated through routine data backup strategy on all mobile and remote online systems, cyber awareness and adherence to safe digital ethics particularly on mobile devices and internet applications.

ABOUT THE AUTHORS

Kenneth Okereafor, PhD, PhD is a Cybersecurity and Biometric specialist trained by the International Telecommunication Union (ITU), UNESCO International Centre for Theoretical Physics (ICTP) Italy, US Foreign Service Institute's (FSI) School of Advanced Information Technology (SAIT) Washington DC and Swiss Centre for Biometrics Research and Testing, Switzerland. He is currently a Deputy General Manager with Nigerian National Health Insurance Scheme (NHIS) where he oversees Database Security Operations and leads Digital Health and Automation Projects.

He previously worked with the US Department of States, supporting the US Embassy's Cybersecurity programmes in Abuja. As former Cybersecurity Manager at the National Institute for Democratic and Legislative Studies (NIDLS), he supervised the automation of the legislative reporting system at the National Assembly Abuja. He is currently the Chair of the Security, Safety and Privacy Working Group on ISO/TC215 Health Informatics with responsibilities to develop Cybersecurity standards for Nigeria's digital health ecosystem. With dual PhD degrees in Cybersecurity from Azteca University Mexico, and IT Administration from Central University of Nicaragua, Kenneth has over two decades of experience in Cyber Threat Mitigation Technologies spanning industry, government and academia. He possesses advanced expertise and certifications in IT Governance, Project Management Methodologies, Automation Strategies and Technology Change Management Principles.

In addition to many published works, his extensive research at ICTP Italy resulted in a novel Cybersecurity concept - *the Multi Modal Random Trait Biometric Liveness Detection System (MMRTBLDS) framework* – which has received attention from the University of Cambridge, the Institute of Electrical and Electronic Engineers (IEEE) Computer Society, and the International Journal of Simulation, Systems, Science & Technology (IJSSST), among others.

Dr. Olajide Joseph Adebola is a medical graduate of University of Ilorin, Kwara State, Nigeria, and Associate Chattered Project Manager of International Academy of Management, Nigeria with Master of Science degree in Global eHealth from the University of Edinburgh.

He is currently the Chair National Technical and Mirror Committee on ISO/TC215 Health Informatics, Nigeria.

His career in eHealth spans over fifteen years with focus on mHealth, Telehealth/Telemedicine, User Centered Design and Health Informatics. He has attended several local and international trainings, conferences and courses in eHealth. He has acquired professional skills and expertise in Medicine, Strategic Planning, Training and Development, Global eHealth, Consumer Health Informatics, Ethics and Governance of eHealth, Health Informatics Core Technologies, Health Informatics, Change Management , Project Management, mHealth, Research and Evaluation in eHealth, Telehealth, Telemedicine, Public Health Informatics, User Centered Design in eHealth, Organisational Management and Leadership, Standards for Data Content, Health Information Exchange, and Interoperability, eHealth Standardization and Standard Development Process.

References

[1] WHO, "Novel Coronavirus (2019-nCoV) Situation Report – 22," World Health Organisation, Geneva, 2020.

[2] "Coronavirus disease named Covid-19," BBC News, 11 February 2020. [Online]. Available: https://www.bbc.com/news/world-asia-china-51466362. [Accessed 11 February 2020].

[3] "The Verge," The illness caused by the new coronavirus gets a new name: COVID-19, 11 February 2020. [Online]. Available: https://www.theverge.com/2020/2/11/21133107/coronavirus-name-covid19-illness-who-new. [Accessed 11 February 2020].

[4] "COVID-19: WHO renames deadly coronavirus," Aljazeera, 11 February 2020. [Online]. Available: https://www.aljazeera.com/news/2020/02/covid-19-renames-deadly-coronavirus-200211172638418.html. [Accessed 11 February 2020].

[5] "Coronavirus," World Health Organization (WHO), [Online]. Available: https://www.who.int/health-topics/coronavirus. [Accessed 4 February 2020].

[6] A. Sanyaolu, C. Okorie, N. Mehraban and O. Ayodele, "Epidemiology of Zoonotic Diseases in the United States: A Comprehensive Review," Journal of Infectious Diseases and Epidemiology, vol. 2, no. 3, pp. 1 - 8, 2016.

[7] W. B. Karesh, A. Dobson and J. O. Lloyd-Smith, "Ecology of zoonoses: natural and unnatural histories," The Lancet Medical Journal, vol. 380, no. 1, pp. 1936 - 1945, 2012.

[8] "WUHAN CORONAVIRUS OUTBREAK," 10 February 2020. [Online]. Available: https://www.worldometers.info/coronavirus/. [Accessed 10 February 2020].

[9] "China coronavirus: Misinformation spreads online about origin and scale," BBC Trending, 30 January 2020. [Online]. Available: https://www.bbc.com/news/blogs-trending-51271037. [Accessed 11 February 2020].

[10] "China launches coronavirus app to detect whether users have come in 'close contact' with the sick," Health and Science, 10 February 2020. [Online]. Available: https://www.cnbc.com/2020/02/10/china-launches-coronavirus-app-to-detect-whether-users-have-come-in-close-contact-with-the-sick.html. [Accessed 11 February 2020].

[11] "As Chinese Internet Users Try To Track The Coronavirus, Their Government Is Tracking Them," Buzz Feed News, 7 February 2020. [Online]. Available: https://www.buzzfeednews.com/article/ryanhatesthis/as-chinese-internet-users-try-to-track-the-coronavirus. [Accessed 11 February 2020].

[12] "WeChat now lets you report information on the Wuhan coronavirus," South China Morning Post, 27 January 2020. [Online]. Available: https://www.scmp.com/tech/article/3047763/wechat-now-lets-you-report-information-wuhan-coronavirus. [Accessed 11 February 2020].

[13] Neil DuPaul, "MALICIOUS CODE," VERACODE AppSec Knowledge Base, [Online]. Available: https://www.veracode.com/security/malicious-code. [Accessed 4 February 2020].

[14] S. Lohani, "Social Engineering: Hacking into Humans," INTERNATIONAL JOURNAL OF ADVANCED STUDIES OF SCIENTIFIC RESEARCH (IJASSR), vol. 4, no. 1, pp. 385 - 393, 2019.

[15] B. Atkins and W. Huang, "A study of social engineering in online frauds," Open Journal of Social Sciences, vol. 1, no. 3, p. 23, 2013.

[16] M. Choudhary, A. Kumar and N. Kumar, "Social Engineering in Social Networking Sites: A Survey," International Journal of Engineering Research & Management Technology (IJERMT), vol. 3, no. 1, pp. 123 - 129, 2016.

[17] H. Aldawood and G. Skinner, "Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal," International Journal of Security (IJS), vol. 10, no. 1, pp. 1 - 15, 2019.

[18] Alex Scroxton, "First coronavirus cyber threats seen in the wild," Computer Weekly, 30 January 2020. [Online]. Available: https://www.computerweekly.com/news/252477578/First-coronavirus-cyber-threats-seen-in-the-wild. [Accessed 4 February 2020].

[19] Ishita Chigilli Palli, "Fake Coronavirus Messages Spreading Emotet Infections," Bank Info Security, 31 January 2020. [Online]. Available: https://www.bankinfosecurity.com/fake-coronavirus-messages-spreading-emotet-infections-a-13675. [Accessed 3 February 2020].

[20] Mathew J. Schwartz, "Emotet Malware Alert Sounded by US Cybersecurity Agency," Data Breach Today, 23 January 2020. [Online]. Available: https://www.databreachtoday.com/emotet-malware-alert-sounded-by-us-cybersecurity-agency-a-13640. [Accessed 3 February 2020].

[21] N. K. Dixit and L. Mishra, "THE NEW AGE OF COMPUTER VIRUS AND THEIR DETECTION," International Journal of Network Security & Its Applications (IJNSA), vol. 4, no. 3, pp. 79 - 96, 2012.

[22] K. D. Devi and K. M. Kumar, "An Analysis of Various Anti-Virus Software Tools Based On Different Effective Parameters," International Journal of Computer Science Trends and Technology (IJCST), vol. 4, no. 4, pp. 104 - 110, 2016.

[23] "Emerging respiratory viruses, including nCoV: methods for detection, prevention, response and control," World Health Organization, 2020. [Online]. Available: https://openwho.org/courses/introduction-to-ncov. [Accessed 11 February 2020].

[24] "Updated WHO advice for international traffic in relation to the outbreak of the novel coronavirus 2019-nCoV," World Health Organization, 27 January 2020. [Online]. Available: https://www.who.int/ith/2019-nCoV_advice_for_international_traffic/en/. [Accessed 11 February 2020].

[25] "Coronavirus deaths exceed Sars fatalities in 2003," BBC News, 9 February 2020. [Online]. Available: https://www.bbc.com/news/world-asia-china-51431087. [Accessed 11 February 2020].

[26] "Doctors in China Are Starting Human Trials for a Coronavirus Treatment," Bloomberg News, 3 February 2020. [Online]. Available: https://time.com/5776682/coronavirus-drug/. [Accessed 11 February 2020].

[27] "China sends Coronavirus treatment guide to Nigeria," Punch News, 11 February 2020. [Online]. Available: https://punchng.com/china-sends-coronavirus-treatment-guide-to-nigeria/. [Accessed 11 February 2020].

As Chinese Internet Users Try To Track The Coronavirus, Their Government Is Tracking Them. (2020, February 7). (Buzz Feed News) Retrieved February 11, 2020, from https://www.buzzfeednews.com/article/ryanhatesthis/as-chinese-internet-users-try-to-track-the-coronavirus

China coronavirus: Misinformation spreads online about origin and scale. (2020, January 30). (BBC Trending) Retrieved February 11, 2020, from https://www.bbc.com/news/blogs-trending-51271037

China launches coronavirus app to detect whether users have come in 'close contact' with the sick. (2020, February 10). (Health and Science) Retrieved February 11, 2020, from

https://www.cnbc.com/2020/02/10/china-launches-coronavirus-app-to-detect-whether-users-have-come-in-close-contact-with-the-sick.html

China sends Coronavirus treatment guide to Nigeria. (2020, February 11). (Punch News) Retrieved February 11, 2020, from https://punchng.com/china-sends-coronavirus-treatment-guide-to-nigeria/

Coronavirus deaths exceed Sars fatalities in 2003. (2020, February 9). (BBC News) Retrieved February 11, 2020, from https://www.bbc.com/news/world-asia-china-51431087

Coronavirus disease named Covid-19. (2020, February 11). (BBC News) Retrieved February 11, 2020, from https://www.bbc.com/news/world-asia-china-51466362

COVID-19: WHO renames deadly coronavirus. (2020, February 11). (Aljazeera) Retrieved February 11, 2020, from https://www.aljazeera.com/news/2020/02/covid-19-renames-deadly-coronavirus-200211172638418.html

Doctors in China Are Starting Human Trials for a Coronavirus Treatment. (2020, February 3). (Bloomberg News) Retrieved February 11, 2020, from https://time.com/5776682/coronavirus-drug/

Emerging respiratory viruses, including nCoV: methods for detection, prevention, response and control. (2020). (World Health Organization) Retrieved February 11, 2020, from https://openwho.org/courses/introduction-to-ncov

The Verge. (2020, February 11). (The illness caused by the new coronavirus gets a new name: COVID-19) Retrieved February 11, 2020, from https://www.theverge.com/2020/2/11/21133107/coronavirus-name-covid19-illness-who-new

Updated WHO advice for international traffic in relation to the outbreak of the novel coronavirus 2019-nCoV. (2020, January 27). (World Health Organization) Retrieved February 11, 2020, from https://www.who.int/ith/2019-nCoV_advice_for_international_traffic/en/

WeChat now lets you report information on the Wuhan coronavirus. (2020, January 27). (South China Morning Post) Retrieved February 11, 2020, from https://www.scmp.com/tech/article/3047763/wechat-now-lets-you-report-information-wuhan-coronavirus

WUHAN CORONAVIRUS OUTBREAK. (2020, February 10). Retrieved February 10, 2020, from https://www.worldometers.info/coronavirus/

Aldawood, H., & Skinner, G. (2019). Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal. *International Journal of Security (IJS), 10*(1), 1 - 15.

Alex Scroxton. (2020, January 30). *First coronavirus cyber threats seen in the wild*. (Computer Weekly) Retrieved February 4, 2020, from https://www.computerweekly.com/news/252477578/First-coronavirus-cyber-threats-seen-in-the-wild

Atkins , B., & Huang, W. (2013). A study of social engineering in online frauds. *Open Journal of Social Sciences, 1*(3), 23.

Choudhary, M., Kumar, A., & Kumar, N. (2016). Social Engineering in Social Networking Sites: A Survey. *International Journal of Engineering Research & Management Technology (IJERMT), 3*(1), 123 - 129.

Coronavirus. (n.d.). (World Health Organization (WHO)) Retrieved February 4, 2020, from https://www.who.int/health-topics/coronavirus

Devi, K. D., & Kumar, K. M. (2016). An Analysis of Various Anti-Virus Software Tools Based On Different Effective Parameters. *International Journal of Computer Science Trends and Technology (IJCST), 4*(4), 104 - 110.

Dixit, N. K., & Mishra, L. (2012). THE NEW AGE OF COMPUTER VIRUS AND THEIR DETECTION. *International Journal of Network Security & Its Applications (IJNSA), 4*(3), 79 - 96.

Ishita Chigilli Palli. (2020, January 31). *Fake Coronavirus Messages Spreading Emotet Infections*. (Bank Info Security) Retrieved February 3, 2020, from Bank Info Security: https://www.bankinfosecurity.com/fake-coronavirus-messages-spreading-emotet-infections-a-13675

Karesh, W. B., Dobson, A., & Lloyd-Smith, J. O. (2012). Ecology of zoonoses: natural and unnatural histories. *The Lancet Medical Journal, 380*(1), 1936 - 1945.

Lohani, S. (2019). Social Engineering: Hacking into Humans. *INTERNATIONAL JOURNAL OF ADVANCED STUDIES OF SCIENTIFIC RESEARCH (IJASSR), 4*(1), 385 - 393.

Mathew J. Schwartz. (2020, January 23). *Emotet Malware Alert Sounded by US Cybersecurity Agency*. (Data Breach Today) Retrieved February 3, 2020, from https://www.databreachtoday.com/emotet-malware-alert-sounded-by-us-cybersecurity-agency-a-13640

Neil DuPaul. (n.d.). *MALICIOUS CODE*. (VERACODE AppSec Knowledge Base) Retrieved February 4, 2020, from Veracode: https://www.veracode.com/security/malicious-code

Sanyaolu, A., Okorie, C., Mehraban, N., & Ayodele, O. (2016). Epidemiology of Zoonotic Diseases in the United States: A Comprehensive Review. *Journal of Infectious Diseases and Epidemiology, 2*(3), 1 - 8.

WHO. (2020). *Novel Coronavirus (2019-nCoV) Situation Report – 22.* Geneva: World Health Organisation.