Internet Threats and Mitigation Methods in Electronic Businesses Post Covid-19

E.E. Odokuma
Department of Computer Science
Captain Elechi Amadi Polytechnic,
Port Harcourt, Nigeria

M.O. Musa
Department of Cyber Security,
Faculty of Computing,
University of Port Harcourt,
Port Harcourt, Nigeria

ABSTRACT

With the advent of COVID-19 and the imposed lockdowns, many businesses were forced online. A number of these business owners had no prior knowledge of internet technology use and were therefore devoid of the knowledge of internet security threats. Many businesses still operate the e-business model even after the restrictions were lifted, due to the merits of the model. E-Business organizations were one of the main victims of internet fraud during the pandemic for various reasons. In this work, the most common threats and their mitigation measureshave been presented using the semi-systematic literature review method. Knowledge and adherence to these mitigation measures, especially education of staff and customers will save electronic business owners from falling victim to internet fraud.

General Terms

Cyber security, eBusiness, Post COVID-19

Keywords

Internet, eCommerce, Security Threats, Fraud, Mitigation

1. INTRODUCTION

The year 2020 began like every other year for most people, where plans for improvements were made by individuals and corporate organizations, including plans to start new businesses and improve on existing ones. But, before the end of the first quarter, COVID-19 was declared as a pandemic by the World Health Organization (WHO), [1] and people were asked to stay at home to curtail the spread of the Corona Virus. Governments around the world declared lockdown on major cities, and offices, markets, shops, schools, places of worship and other public places were closed down, forcing people to work from home.

Internet based businesses began to thrive, offline businesses then had reasons to go online and avenues for creating new businesses emerged. This development also posed challenges for business owners, their staff and customers. Businesses used social media platforms like Facebook, Instagram, WhatsApp, Telegram, Snapchat and others, for staff and customer engagements. Electronic businesses have inherent challenges, the transition to work from home was urgently imposed on businesses and adequate preparations were not made for this move, further posing new challenges to the business. [2]

Working from home meant that the e-Business owner or employee used internet enabled devices such as desktop, laptops, tablets, smart phones etc., to connect to a broadband network, mobile hotspot or shared wireless network. These devices are oftentimes shared with family and/or neighbours. The data traffic flow is not controlled and covers a wide range of activities including personal email and educational needs. Some of these devices have default passwords for administration that are left unchanged by the home user or have rudimentary security for encryption of traffic. These devices and networks expose the electronic businesses to internet threats. [3]

The aim of this work is to identify internet threats that newcomers to the e-Business space due to COVID-19 may be exposed to and the mitigation methods needed to safeguard them.

2. THEORETICAL BACKGROUND

2.1 Internet Threats

Internet threat refers to any method that unapproved parties can use to gain access to sensitive information, networks and applications. Some of these threats may take the form of a human, computer viruses, botnets, application attacks and phishing scams, among others, [4].

2.2 E-Business and E-Commerce

Electronic commerce is a form of electronic business. An e-business is any business that incorporates online technologies into the business model, [5]. That could be something as simple as a physical store using social media marketing to bring in more customers. Even though there’s no transaction occurring within that setup, the use of online technology for business purposes makes it an e-business. On the other hand, e-commerce refers to a company that offers an online monetary transaction process, [6]. Figure 1 shows that e-commerce is a component of e-business

E-Business
E-Commerce

Figure 1: E-Business and E-Commerce

Whereas E-commerce is conducted exclusively on the internet, E-business can be conducted on the internet, intranet, or extranet. The main difference is that a company may be considered an e-business even if it only uses internet technology within the organization, [7].

2.3 Related Work

Samuel et al. [8], studied Social Engineering Attacks. They noted that the rapid development of technology has also introduced an advancement of security risks and threats. Their work highlighted various Social Engineering attack methods, and how to mitigate them for internet users.

Ahmad [9], examined the Pandemic and Work from Home from the perspective of challenges of cybercrimes and cybersecurity. It was observed that "As the home-working becomes the new normal, criminals are seeking to capitalise on the widespread panic – and succeeding, alas. New coronavirus-themed phishing scams are leveraging fear, hooking vulnerable people and taking advantage of workplace disruption. Therefore, the people working from home should immediately get educated about their cyber privacy and cybersecurity failing which the global cybercrime damage may costs as much as double by the end of this year.

Pranggono and Arabo [2], studied the COVID-19 pandemic cybersecurity issues and observed that "the pandemic has also raised the issue of cybersecurity in relation to the new normal of expecting staff to work from home (WFH), the possibility of state-sponsored attacks, and increases in phishing and ransomware." They encouraged healthcare organizations to improve protecting their important data and assets by implementing a comprehensive approach to cybersecurity.

Summer et al. [10], performed a Survey on Deceptive Phishing Attacks in Social Networking Environments and in which provided an overview of social engineering attacks, the detection methods of social engineering and phishing attacks, the education and training techniques for preventing social engineering and phishing attacks, as well as the susceptibility of users to social engineering and phishing attacks.

De Bona and Paci [11], performed a real-world study on employees' susceptibility to phishing attacks and found that employees were more vulnerable to phishing attacks when urgency principle was exploited. The study also showed no significant effect of employees' demographic data on susceptibility to phishing. Embedded training was perceived as effective by employees but it did not reduce their susceptibility to phishing.

Madson et al. [12], studied the Federated identity management for protecting users from ID theft and argues that, while such linkages do undeniably increase the potential scope of a successful theft of identity information, this risk is more than offset by the much greater value federated identity, in combination with strong authentication, offers in preventing such theft in the first place.

Zou et al. [13] examined the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices and observed that security practices were more widely adopted than privacy and identity theft protection practices. Manual and fully automatic practices were more widely adopted than practices requiring recurring user interaction. Participants' gender, education, technical background, and prior negative experience are correlated with their levels of adoption. Furthermore, practices were abandoned when they were perceived as low-value, inconvenient, or when users overrode them with subjective judgment.

3. METHODOLOGY

A semi-systematic review of literature was conducted on web searches, Google Scholar and ResearchGate scholarly literature indexes using several combinations of the search terms: ebusiness, ecommerce, security threats, mitigation and COVID-19 with limitations set for 2020 to 2022 as dates and English as the language of interest. Available literature was studied to identify the internet security threats to e-businesses and the recommended mitigation methods.

4. OVERVIEW OF EBUSINESS THREATS

There are many threats to the success of electronic businesses. Attackers are after financial gain or disruption of service [14]. The threats affecting e-businesses during the pandemic were mainly:

Hacking: Hacking is the activity of identifying weaknesses in computer systems or networks, with an aim to exploit the security and gain access to personal or business data. An example of computer hacking can be: using a password cracking algorithm to gain access to a computer system.

Identity theft: Identity theft/fraud refer to crime in which fraudster illegally obtains and uses another person personal information in some way that involves deception or fraud to gain something of value. Identity theft/fraud is the most serious crime for the person whose information is stolen as well as the financial institution.

Phishing: Phishing is a cyber attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need a request from their bank, for instance, or a note from someone in their company and to click a link or download an attachment, [15]. The e-mail appears to be sent from a legitimate organization to trick people in order to reveal sensitive information. On clicking the attachment or the hyperlink the computer system gets infected with malware. During the next online transaction, the malware will activate and steal private and personal financial information, including credit card numbers, PIN number which is used by fraudster to steal money from the account. Malware or "Malicious Software" is software which includes computer viruses, worms, Trojan Horses, spyware and other malicious software, [16].

Vishing: It is the practice of leveraging IP-based voice messaging technologies (primarily Voice over Internet Protocol, or VoIP) to socially engineer the intended victim into providing personal, financial or other confidential information for the purpose of financial reward. The term "Vishing" is derived from a combination of the words: "voice" and "Phishing." [17]

Malware: Software that performs a malicious task on a target device or network. It may corrupt existing data, take over the operation of a system or perform some other unwanted tasks.

Spoofing or Website cloning: This is an act of creating a hoax web site or to say duplication of a website for criminal use. The fraudsters use legitimate companies name, logos, graphics and even code. This usually take form of know chat room or trade sites where in people would innocently giving out personal information to criminals or make a fake purchase of a product the does not exist.

Ransomware: An attack that involves encrypting data on the target system and demanding a ransom in exchange for letting the user have access to the data again. These attacks can range from low-level nuisances to serious incidents that affect a good number of users at the same time.

Denial of Service attack or Distributed Denial of Service Attack (DDoS): DDoS occurs where an attacker takes over many (perhaps thousands) devices and use them to invoke the functions of a target system so that the system become overwhelmed and may result in a system crash

Data Breaches: A data breach is a theft of data by a malicious actor. Motives for data breaches may include crime (identity theft), a desire to embarrass an institution, spying and others.

Credit card fraud: Scammers fraudulently acquire credit or debit card details from their victims and use it to collect money, purchase goods and services or acquire property.

Overpayment scams: An e-business owner may receive a fake check or bank transfer receipt from a customer which if honoured will cause loss of revenue to the business. [18]

Men and women running e-Businesses were asked if they have knowledge of these threats. Figure 2 shows their responses in percentage. The responses show that whereas a good percentage of e-Business owners are aware of the threats, there are a number of persons that are uninformed, which exposes them to attacks.

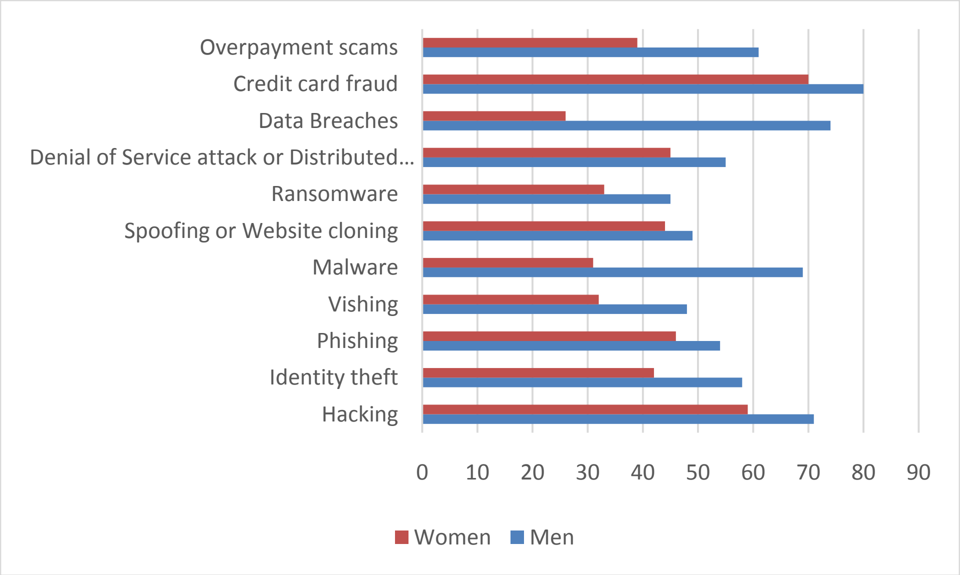

Figure 2: Awareness of the most popular e-Business threats among e-Business owners in a metropolis, South- South, Nigeria.

5. MITIGATION METHODS

Mitigating and preventing threats are not a trivial task. There are practical approaches that can reduce the risk of threats:

User Education: Security is only as strong as its weakest link. People are considered the weakest link in many security systems. Therefore, developing cybersecurity awareness among users by means of constant training is important to reduce the risks of threats on an organization and its personnel [16].

Use of Virtual Private Network (VPN): VPN is an encrypted communication channel between two points on the Internet to protect the data that is sent and received. The use of a VPN to surf the Internet is the new normal. A VPN provides two aspects of security: confidentiality and integrity and allows organizations to extend security policies to remote workers. VPNs protect against

Use of multi-factor authentication (MFA): MFA strengthens security by requiring a username and password plus a one-time code sent to mobile phone via SMS or an authentication app. MFA is an important factor to mitigate against password guessing and theft such as brute force threats. An employee attempting to access her company's network from home will need to provide both her username and password and a one-time code sent to her mobile phone to verify her identity before being allowed to access the internal network.

Regular Update of Operating System and Firmware: Ensure all devices firmware is up-to-date: Ensure that all devices and equipment firmware/OS are up-to-date with the latest security patches implemented to inoculate them against known vulnerabilities. Regular and up-to-date patches may reduce the risk of a zero-day attack.

Use of Up-To-Date Anti-Malware Protection: Ensure that up-to-date anti-malware software is activated in all network connected devices: Cyber criminals targeting vulnerable people by spreading various types of malware. As millions of new malware and its strain are generated every year, regular and up-to-date anti-malware may reduce the risk of threats caused by malware.

Segmentation and Separation: Do not use the same network for work and play. Provide a network strictly for work and another for home, family entertainment and children homework, [19].

Provide Physically Security for the Home Office: Make sure your doors and locks are working properly. It is important to physically protect home office devices. Practical ways include ensuring you do not leave work devices unattended, use a lock screen or lock the laptop, always log off devices after use, etc, [6].

6. CONCLUSION

Electronic Businesses have come to stay. Today, most businesses operate both offline and online in a hybrid model. Even in the offline businesses, payments are often made using electronic means. eBusiness organizations are one of the main victims of threats during the pandemic for various reasons. The objective of this study was to identify the various threats that militate against e-businesses during the Covid-19 pandemic and to find mitigative measures to overcome them. User education is key to avoiding these threats. Use of Virtual Private Network (VPN), use of multi-factor authentication (MFA), regular update of OS, firmware and malware protection software, Segmentation and Separation, and physical Home Office security, were the mitigative measures discussed.

7. RECOMMENDATIONS FOR FUTURE WORK

It is important that eBusiness organizations improve protecting their important data and assets from threats by leveraging on the tools and techniques discussed. Safeguarding an electronic business from internet threats should begin with staff and customer education. User education will keep them betterinformed and more cautious when using the internet for e-Business.

There are different directions that this research can take in the future, one of it may be to investigate the effectiveness the discussed toolsbetween educated and uneducated uses.

8. ACKNOWLEDGMENTS

Many thanks to the heads of the institutions of the authors for providing a conducive environment for research and innovation.

9. REFERENCES

[1] Tedros, A. G. (2020). Retrieved May 19, 2022, from Who.int website: https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020

[2] Pranggono, B., and Arabo, A. (2020). COVID- 19 pandemic cybersecurity issues. Internet Technol. Lett. Doi: 10.1002/itl2.247

[3] Walker, A. (2021). What Is Threat Modelling? Retrieved 19th May, 2022, from https://learn.g2.com/threat-modeling

[4] Nigeria 2020 Crime & Safety Report: Abuja. (2021). Retrieved 19th May, 2022, from https://www.osac.gov/Content/Report/04a87fa7-8575-4ce1-b5bb-188e5cb9d1d8

[5] Max, D. (2020). What is E-Business: Meaning, Types, Components, Model and Features. Temok Hosting Blog. Retrieved 17th May, 2022, from https://www.temok.com/blog/what-is-e-business/

[6] Nigeria – e-Commerce. (2021). Retrieved from https://www.trade.gov/knowledge-product/nigeria-ecommerce

[7] Furnell S, and Shah J. N. (2020) Home working and cyber security–an outbreak of unpreparedness? Computer Fraud and Security. (8):6-12.

[8] Samuel Adu-Gyimah, George Asante and Oliver Kufuor Boansi. Social Engineering Attacks: A Clearer Perspective. International Journal of Computer Applications184(8):53-62, April 2022

[9] Ahmad, T. (2020, April 05). Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity. Doi: 10.2139/ssrn.3568830

[10] Summer, A. and Yuan X. (2019) Mitigating Phishing Attacks: An Overview Publication: Proceedings of the 2019 ACM Southeast Conference April 2019. Pages 72–77 https://doi.org/10.1145/3299815.3314437

[11] De Bona M. and Paci F. 2020 Real world study on employees' susceptibility to phishing attacks. Proceedings of the 15th International Conference on Availability, Reliability and Security. August 2020 Article No.: 4 Pages 1–10 https://doi.org/10.1145/3407023.3409179

[12] Madsen, P., Koga, Y., & Takahashi, K. (2005). Federated identity management for protecting users from ID theft. Association for Computing Machinery. Proceedings of the 2005 workshop on Digital identity management, November 2005 Pages 77–83 https://doi.org/10.1145/1102486.1102500

[13] Zou, Y., Roundy, K., Tamersoy, A., Shintre, S., Roturier, J., and Schaub, F. (2020). Examining the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices. Association for Computing Machinery. CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems April 2020 Pages 1–15. Doi: 10.1145/3313831.3376570.

[14] Malecki F. Overcoming the National Cyber Security Centre (NCSC) and Cybersecurity and Infrastructure Security Agency (CISA) (2020). Advisory: COVID-19 exploited by malicious cyber actors. https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory

[15] Ali, M., Qaseem, Dr. M., and Rahman, M. (2020). A Survey on Deceptive Phishing Attacks in Social Networking Environments. Doi: 10.1007/978-981-15-1480-7_37

[16] National Cyber Security Centre (NCSC), and Cybersecurity and Infrastructure Security Agency (CISA), (2020). Advisory: APT groups target healthcare and essential services. https://www.ncsc.gov.uk/news/apt-groups-target-healthcare-essential-services-advisory.

[17] FraudWatch. (2019, February 25). Retrieved May 19, 2022, from Digital Brand Protection – FraudWatch website: https://fraudwatch.com/what-is-vishing-voice-phishing-scams-explained-how-to-prevent-them/

[18] How To Spot, Avoid, and Report Fake Check Scams. (2020, January 29). Retrieved 19th May, 2022, from Consumer Advice website: https://consumer.ftc.gov/articles/how-spot-avoid-report-fake-check-scams

[19] Pedley D, Borges T, Bollen A (2020, March 12). Cyber Security Skills in the UK Labour Market 2020. Retrieved May 19, 2022, from GOV.UK website: https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020