BOOK CHAPTER | Phishing Scenario

A Review of Cyber Phishing Attack Cases

Ukim Joshua Okon
Akwa Ibom State University, Ikot Akpaden
Akwa Ibom State, Nigeria
Department of Computer Science.
E-mail: ukimjosh18@gmail.com
Phone: +2348135028313

Abstract

Internet security has over time become a major area of trepidation for internet users, as cyber criminals exploit unskilled cyberspace user, stealing private credentials, hijacking user devices and spying on victims. Phishing is a social engineering cybercrime, which involves luring the user into proving sensitive and confidential information to the attackers. Qualitative Survey was conducted in this research to richly tackle the menace of cyber phishing attack by giving expository phishing evidences, processes, cause of these attacks and counter measures to combat further incidents.

Keywords: Phishing, cyberspace, social-engineering, anti-phishing.

Introduction

In recent times, the internet has proven to be a useful tool in coordinating and driving modern needs of human society. Cyber criminals over time have also developed new methods for stealing information and user credentials by tricking unsuspecting victims. Cyber security experts continue to provide technological applications, processes and controls measure to protect systems, networks programs, devices and data from cyber-attacks. Social-engineering-based attacks so far, have proven to be the most effective approach for cyber criminals. One of the social engineering crimes that allow the attacker to carry out such malicious attack is called Phishing attack. Phishing is an example of a highly effective form of cybercrime that enables criminals to deceive users and steal important data. Some critical statistics which supports the above points is that, as malicious actors rely more on phishing to access network systems, there is a correspondent decrease of 40% on breaches involving malware, further shifting the cyber security focus from anti-malware solutions to anti-phishing solutions. Nearly 65% of the active phishing attacks relied on spear-phishing in 2019 (Comparitech, 2021). There are many targets for phishing including end-user, business, financial services (i.e., banks, credit card companies, and PayPal), retail (i.e., eBay, Amazon) and, Internet Service Providers (wombatsecurity.com, 2018).

Citation: Ukim Joshua Okon (2022). A Review of Cyber Phishing Attack Cases.
SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series

The most impersonated brands overall for the first quarter of 2020 were Apple, Netflix, Yahoo, WhatsApp, PayPal, Chase, Facebook, Microsoft eBay, and Amazon (Checkpoint, 2020). Cyber Phishing attack, records it successes mostly when the human factor fail in its security role, as it remains the weakest link in cyber security, owing to this fact, cyber criminals will continue to exploit the human element vulnerabilities ranging from:Un-unravelable quest to secure goods and services at incredibly cheap rates or at zero cost.

1. Inability to detect phishing websites and links due to lack, obsolete or inadequate information on URL structure, domain name and its component.

Cyber Phishing Attack Case Studies

A Case in Study is a phishing website discovered to be impersonating the United State Government. In this case, cyber adversaries pretending to be representing United State Government and are offering fully funded scholarships and paid internship in Boston in attempt to steal user credentials. This site was launched on July 11, 2021 and research shows that the intended phishing attack has so far been successful as reports of its visit records over 92,675 visitors to the site. The site is believed to have originated from Kenya or it is targeted at Kenyans because they account for highest visit rating 53.12% when compared to United States and Egypt hitting 9.38% and 6.25% respectively.

Fig. 1: Case Study Phishing Website (Source:https://scholarship.get-offerr.online/)

Summary
Successful Phishing attack relies on the ignorance of cyber users on domain name structure and the character of ccTLD to steal private documents, sensitive data and user credential. Also noting the rush to obtained free gifts, scholarships, extreme bonuses and giveaway.

Case No 2: Upsher-Smith Laboratories – Loss of Nearly $39 Million
Though this incident happened sometime in 2014, it has tremendous significance because it is one of the classic email examples of the CEO Fraud category. CEO fraud is a cyber-attack carried out by malicious actors wherein they send phishing emails to the organization's employees by posing as the organization's CEO. In this case, cyber adversaries pretending to be the organization's CEO emailed the Accounts Payable Coordinator at Upsher-Smith Laboratories, a Maple Grove-based drug establishment, to follow the instructions from the CEO and the organization's lawyer. The instructions were to make nine wire transfers to the fraudster's accounts for amounts exceeding $50 million. The organizations loss was upwards of $39 million (Source: https://www.phishprotection.com).

Summary
In this case, Employee Negligence Factor was recognized as fail point, as the employee was negligent and took the emails at face value. He/she could have contacted the CEO's office to confirm the origin of such emails, especially if they were not following the standard procedures. The bank handling the transfer is also negligent of missing the multiple red flags, especially the amounts and the frequency of transfers, suspicious beneficiaries, and the failure to include a second signatory to the requests. Such phishing emails come with an urgency factor and also insist on confidentiality, a precautionary phone call could have stopped this crime from happening. Hence do not to take any email at face value. It does not cost much to confirm.

Case No 3: Twitter Phishing Case – 2020
The Twitter Phishing case of July 2020 is a classic case of threat actors compromising the employees' passwords to gain unauthorized access. In July 2020, several Twitter employees became victims when malicious actors posed as Twitter IT administrators and emailed/phoned Twitter employees working from home, asking them to share user credentials. Using these compromised accounts, the cyber adversaries gained access to the administrator's tools. It enabled them to reset the Twitter accounts of celebrities like Elon Musk, Barack Obama, Jeff Bezos, Apple, Uber, and many more to tweet scam messages asking for Bitcoin contributions. As these celebrity accounts have a massive following, many Twitter users transferred at least $180,000 in Bitcoins to scam accounts. Luckily, the scam messages were published and noticed by the press. It forced Twitter to take immediate action. Twitter experienced a 4% fall in its share price due to its failure in detecting and mitigating the scam in time. Twitter also had to stop its release of the new API to update security protocols. Though the financial loss was insignificant, Twitter lost its reputation of being one of the most secure social media platforms. (Source: https://www.phishprotection.com)

Summary
Twitter did not follow proper cyber security strategies as the compromised employees did not have appropriate email phishing protection solutions installed on their devices. Privileged access management solutions and monitoring user and entity behavior could have prevented this scam from happening. Also educating employees on potential social engineering attacks is crucial to preventing future occurrences of this attack.

Case No 4: FACC (€42 million)
In January 2016, an employee at the Austrian aerospace parts manufacturer FACC received an email asking the organization to transfer €42 million to another account as part of an "acquisition project".

The message appeared to come from the organization's CEO, Walter Stephan, but was in fact a scam. Unable to spot the true nature of the email, the employee complied with the request. Few details were revealed about exactly what went wrong, but there is reason to believe that Stephan was at least partially at fault. That's because FACC fired him following an internal investigation, claiming that he had "severely violated his duties". It also fired its chief financial officer. FACC sought €10 million in legal damages from both executives.

Recommendation

Remedial measures for mitigating these cyber phishing attacks include:

1. **User Education**: Investing in educating cyberspace users to recognize phishing and adhering to internet best practices.
2. **Technical Solution**: Timely installations of phishing security software to aid combat threat at early stage and stop its activation on devices.
3. **Security Report Enforcement**: reporting suspicious traffic, sites, links, mails, activities etc. to relevant law enforcement agencies to serve as deterrent control, and investigators where attacks have already been carried out. Agencies like EFCC, FBI, can be contacted.
4. **Proactive measures:** Constant reviews of phishing attack case studies, counter measures and communicate same to the public via social networks, compendiums, news agencies, talk shows, conference etc.
5. **Recommended security sites**: Cases of scam should be reported or checked for proper safety prevention and effect control measure. Visit:
    i. www.ReportFraud.ftc.gov
    ii. www.identityTheft.gov
    iii. www.cisa.gov
    iv. www.efccnigeria.org, Email: scam@efccnigeria.org and info@efccnigeria.org
    v. www.nigeriapolice.org
    vi. www.fbi.gov
    vii. reportphishing@apwg.org (if scammers contact you by text or call)

Conclusion

The analysis in this research shows that prospective attacks in future is projected to be on the increase as cyber-criminals will continue to threaten the safety of cyberspace, it is therefore paramount that corresponding cyber security proactive and counter measures are duly communicated and followed to the later. This study therefore examines cyber Phishing attacks, proposes detection solutions, and provides threat awareness scenarios which can be used to make better decision in future. It also proposes strategies to better arm cyberspace users against cyber-criminal elements and their adverse intentions.

References

1. Akarshita Shanka et, al. (2019) "A review on Phishing Attacks. International Journal of Applied Engineering Research ISSN 0973-4562, Volume 14, Number 9 (2019) pp. 2171-2175.
2. Biggest Phishing Scam Available at https://www.itgovernance.eu/blog/en/the-5-biggest-phishing-scams-of-all-time Retrieved 7th January, 2022.
3. Checkpoint, (2020) Available at https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/ Retrieved 11th January, 2022
4. Cyber security Phishing attack analysis Available at https://www.comparitech.com/blog/vpn-privacy/phishing-statistics-facts/ Retrieved 7th January, 2022.
5. Phishing attacks case study Available at https://www.phishprotection.com/blog/phishing-case-studies-learning-from-the-mistakes-of-others/ Retrieved 3rd January, 2022.
6. wombatsecurity.com, (2018) Available at www.wombatsecurity.com. Retrieved 2nd January, 2022.