ISSN 2581 – 3781

AJCSE
ASIAN JOURNAL OF COMPUTER SCIENCE ENGINEERING

Available Online at www.ajcse.info
Asian Journal of Computer Science Engineering 2022;7(2):48-52

RESEARCH ARTICLE

Online Attack Types of Data Breach and Cyberattack Prevention Methods

Muhammad Ahmad Baballe[1], Adamu Hussaini[2], Mukhtar Ibrahim Bello[3], Usman Shuaibu Musa[2]

[1]Department of Computer Engineering Technology,School of Technology, Kano State Polytechnic, Kano, Nigeria, [2]Department of Computer Science and Information Sciences, Towson University, USA, [3]Department of Computer Science, School of Technology, Kano State Polytechnic, Kano, Nigeria

Received on: 10/02/2022; Revised on: 25/03/2022; Accepted on: 13/04/2022

ABSTRACT

Phishing attacks are a common tactic used by cybercriminals to lure unsuspecting users into providing their private information. The need to look for and develop methods of detecting different threat kinds is determined by the detection of the cybersecurity (CS) state of Internet of Things (IoT) devices. To prevent some built-in protective mechanisms from the perspective of a possible intruder, software and hardware modifications are made easier thanks to the unification employed in the mass production of IoT devices. It becomes necessary to provide universal techniques for assessing the degree of device CS utilizing thorough methods of data analysis from both internal and external information sources.

Key words: Cyberattacks, Cybercrime, Cybersecurity, Internet of things, Internets

INTRODUCTION

Internet applications are now essential to almost every part of our life, including education, online commerce, software services, and entertainment. As a result, a specific secure account is in charge of all of the user's important data, including their online banking account.[1] Security in the digital age and online is becoming more and more crucial. Digitalization is quickly becoming the norm in all areas of human endeavor. Science and technology trends analysis reveals a rising reliance on digital tools by people, databases in networks by businesses, digital payments by banks, and computer technology and software by nations to manage strategic weapons. Every day, organized gangs of skilled cybercriminals acquire control of the devices and computers of others, regardless of who owns them, and start a series of destructive programs against websites. ATMs, businesses, phone lines, and even the presidential websites of the world's superpowers all stop working in a couple of seconds. The globe has a propensity to pay more attention to information resource management and cybersecurity. Nobody could have foreseen that the financial crisis of 2007–2008, which started with the US housing crisis, bank failures, and declining stock prices, would cause a global economic disaster (also known as the "Great Recession"); this is because it was unforeseeable.[2] The next threat to humanity was a contagious illness that was discovered in humans for the 1st time in December 2019 in China.[3] An outbreak of the illness led to its spread into a pandemic. The SARS-CoV-2 coronavirus was the disease's primary cause.[4,5] The illness has had a terrible impact on both human health and the entire global economy. A sizable portion of the global population was compelled by the illness to think about the issue of distant work. Institutions of higher learning have shifted to online instruction. Every day, there are a lot of online conferences, meetings, and business gatherings. Unquestionably, this sparked a tendency toward extending the use of digital technologies. Given the aforementioned, it was impossible to predict the financial crisis and contagious diseases like "black swans" in time to establish effective countermeasures.[6] Therefore, one should not rule out the possibility of devastating, global cyberattacks in the future. The social, economic, and political ramifications of the internet ceasing, even for a day, are currently impossible to anticipate. It should be mentioned that our digital operations and personal and business computer networks need to be securely protected.

Address for correspondence:
Muhammad Ahmad Baballe
E-mail: mbaballe@kanopoly.edu.ng

RELATED WORKS

There is no clear strategy to properly stop all sorts of cyberattacks since they are so complex. There are essentially two different types of security strategies: Raising user awareness and making use of additional programmed tools.[7] In response to several phishing scams designed to trick people into giving their personal information, a number of techniques for spotting phishing websites have been developed during the past decade. Cyberattacks including phishing can typically be stopped using one of several techniques, such as list-based detection, machine-based learning detection, heuristic detection, or deep learning methods.[8] However, more recent methods have modified machine learning (ML) algorithms to evaluate the reliability of websites. The use of ML techniques to strengthen the identification of phishing websites has been covered in this section's survey of recent detection methods. Rajithaet and VijayaLakshmi (2016) proposed oppositional Cuckoo search and fuzzy logic categorization to identify harmful cyberattacks. The OCS algorithms have been used to pick the most important features from the four different types of features during the feature selection step. To calculate the fuzzy score, the second stage involves training the selected features with FLC. A fuzzy score is used in the testing stage to identify harmful universal research locators (URLs).[9] A twin support vector machine (SVM)-based heuristic technique was proposed by Rao *et al*. in 2020. By comparing the differences between hyperlink and URL properties for both the URL of the visited page and the home page to categorize phishing websites, this method detects malicious phishing sites registered on susceptible servers.[10] To increase the accuracy of phishing detection, Tan *et al*. have extracted a new characteristic. The suggested approach starts with the extraction of hyperlinks from the webpage and a group of related URLs. To create a web graph and a classifier to recognize phishing web pages, the page linking data were gathered during this procedure.[11] The research study carried out by ALI and Malebary determines the weighting of various features using the particle swarm optimization method. Websites that are phishing can be recognized. According to the findings of their research, using fewer website features allow suggested ML algorithms to identify phishing websites more accurately.[12] Convolutional neural networks have been utilized by Aljofey *et al*. to identify phishing websites. It is possible to record URL strings without being aware of phishing. They then accelerate the current URL classification using the sequential pattern functionality.[13] Convolutional layers in a deep neural network were suggested by Wei *et al*. To identify fraudulent URLs, our work just analyzes URL text. In contrast to earlier studies, this technique finds 0 day attacks more quickly. The performance of mobile devices can also be used with it without suffering considerably.[14] Using extraction and representation paradigms, Feng *et al*. suggested a hybrid deep learning network to identify phishing websites. The approach first treats the architectures of HTML, Document Object Model, and URL as a string of characters. The representations of webpages are automatically learned using representational technology, and these representations are then submitted to a deep learning hybrid network made up of a coevolutionary neural network and a bidirectional memory network to retrieve local and global information.[15] A SVM binary classifier was used by Anupam and Kar to predict if a website was valid or not using several aspects of the URL (intellectual property [IP] address length, and HTTP request). The Firefly, the Bat, the Grey Wolf, and the Whale are offered to identify the ideal hyperplane of the SVM in addition to the help of four optimization algorithms.[16] To replace the knowledge base of the expert system, Mahdavifar and Ghorbani developed a knowledge base by employing Deep Embedded Network Expert Systems to extract precise rules from a trained deep network architecture.[17] By combining the best possible set of characteristics and criteria, Kumar and Indrani proposed a phishing detection method that uses a deep neural network classifier and fuzzy logic to categorize websites into three categories: Phishing, non-phishing, and suspicious. In addition, the Frequent Rule Reduction algorithm has created a greedy selection algorithm to find the best subset of rules with the most accurate prediction of phishing websites.[18] An artificial neural network-based anti-phishing model for a company has been put up by Sankhwar *et al*. The Fuzzy Inference System is used to construct the URL categorization procedures and provide results with erroneous data on

social attributes utilizing two ANNs (Levenberg-Marquart and feed-forward backpropagation). To reduce phishing cyberattacks, this methodology is effective at figuring out if emails are known or unknown phishing emails.[19] To learn how to imitate them, Tharani and Arachchilage displayed and discussed a collection of phishing URLs. They may entice users to carry out harmful actions like clicking on malicious links. On a phishing dataset, IG and Chi-squared feature selection approaches are utilized along with dual ML techniques.[20] By depending on URLs on the mobile device, Haynes *et al*. recommend using phishing detection-based lightweight algorithms. Only phishing websites are detected by deep transformers (BERT and ELECTRA).[21] Spear phishing, clone phishing, and whaling attacks are the three main types of phishing cyber-attacks. The first type monitors user and victim information to maximize the likelihood of a successful assault, targeting individuals, or numerous organizations. The second kind of attack spreads from a victim who is already infected and is historically and properly identified by getting cloned or mirror emails with attachments. The third kind of phishing is spear phishing, designed for top executives, and other high-rated individuals. An overhead manager is used to compose the text that is sent to the destination [Figure 1].[22]

HERE ARE A FEW INSTANCES OF TYPICAL CYBERATTACKS AND DIFFERENT KINDS OF DATA BREACHES

1. Identity theft, fraud, extortion
2. Malware, phishing, spamming, spoofing, spyware, Trojans, and viruses

Figure 1: A model of cyber security

3. Stolen hardware, such as laptops or mobile devices
4. Denial-of-service and distributed denial-of-service attacks
5. Breach of access
6. Password sniffing
7. System infiltration
8. Website defacement
9. Private and public web browser exploits
10. Instant messaging abuse
11. IP theft or unauthorized access.[23]

TECHNIQUES TO STOP CYBERATTACKS

Train your staff

Your employees are one of the most typical ways that cybercriminals obtain your data. They will send phony emails asking for personal information or access to specific files while posing as a member of your company. Untrained eyes frequently mistake link for trustworthy sources and it's simple to fall for the trick. Employee awareness is essential because of this. Educating and training your staff on how to prevent cyberattacks and all other forms of data breaches are one of the most effective ways to protect against them.
They need to:

- Check links before clicking them
- Check email addresses from the received email
- Use common sense before sending sensitive information.

Keep your software and systems fully up to date

Cyberattacks frequently occur because outdated systems or software leave gaps that can be exploited. These flaws are used by cybercriminals to get into your network. It's frequently too late to take precautions once they are inside. A patch management solution, which will oversee all software and system updates and keep your system resilient and current, is a wise investment to combat this.

Ensure endpoint protection

Remotely bridged networks are safeguarded by endpoint protection. Security threats can gain

access to corporate networks through mobile devices, tablets, and laptops. Specific endpoint security software must be used to secure these paths.

Install a firewall

There are a huge variety of sophisticated data breaches, and new ones appear daily and occasionally even make a reappearance. One of the best ways to protect yourself from any cyberattack is to place your network behind a firewall. We can assist you in setting up a firewall system that will stop brute force assaults on your network and/or systems before they can cause any harm.

Backup your data

You must have a backup of your data in case of a disaster (typically a cyberattack) to prevent significant downtime, data loss, and significant financial loss.

Control access to your systems

Unbelievably, physical attacks are one of the types of attacks that can be made against your systems. It is crucial to have control over who can access your network. Someone can easily access your entire network or infect it by entering your workplace or business and plugging a USB key with infected data into one of your PCs. Controlling who has access to your computers is crucial. Installing a perimeter security system is a great approach to prevent both break-ins and cybercrime.

Wi-Fi security

In 2020, who won't own a Wi-Fi capable device? And exactly therein lies the risk. By joining a network, a device has the potential to become infected. Your entire system is seriously at risk if this infected device subsequently connects to your company network.

The safest thing you can do for your systems is to secure and hide your Wi-Fi networks. There are thousands of devices that can connect to your network and compromise you as wireless technology continues to advance.

Employee personal accounts

Every application and program require a unique login from each employee. Multiple individuals connecting with the same credentials can endanger your company. You can lessen the number of attack vectors by having unique logins for each employee. Users will only use their own set of logins and will only log in once each day. You'll gain better usability in addition to increased security.

Access management

One of the dangers of running a business and employing people is that they might put software on company-owned devices that could damage your systems. Your security will benefit from having managed admin permissions and preventing your personnel from installing or even accessing specific files on your network. Protect your enterprise; it is yours.

Passwords

It can be risky to use the same password for everything. If a hacker discovers your password, they have access to every file on your computer and any program you use. Your security will greatly benefit from having unique passwords set up for each application you use, and frequent password changes will keep your defenses against internal and external threats strong.[23]

CONCLUSION

As more sophisticated phishing kits are released, the number of phishing websites has been rising dramatically. The attackers use these kits to propagate the phony pages. The overlapping between the selected characteristics is also considerable, which results in remarkable misclassification for conventional algorithms that rely on isolated features. Phishers always try to use these distinct qualities to their advantage. To improve the classes, phishing detection mechanisms need to be developed. Also covered in detail are the ways to stop this cyberattack.

REFERENCES

1. Raja SE, Ravi R. A performance analysis of software defined network based prevention on phishing attack

in cyberspace using a deep machine learning with CANTINA approach (DMLCA). Comput Commun 2020;153:375-81.
2. Jordà Ò, Schularick M, Taylor AM. The great mortgaging: Housing finance, crises and business cycles. Econ Policy 2016;31:107-52.
3. Zhao JY, Yan JY, Qu JM. Interpretations of "diagnosis and treatment protocol for novel coronavirus pneumonia (trial version 7)". Chin Med J (Engl) 2020;133:1347-9.
4. Zhou H, Chen X, Hu T, Li J, Song H, Liu Y, *et al*. A novel bat coronavirus closely related to SARS-CoV-2 contains natural insertions at the S1/S2 cleavage site of the spike protein. Curr Biol 2020;30:2196-203.e3.
5. Wu C, Liu Y, Yang Y, Zhang P, Zhong W, Wang Y, *et al* Analysis of therapeutic targets for SARS-CoV-2 and discovery of potential drugs by computational methods. Acta Pharm Sin B 2020;10:766-88.
6. Aven T. On the meaning of a black swan in a risk context. Saf Sci 2013;57:44-51.
7. Vijayalakshmi M, Shalinie SM, Yang MH. Web phishing detection techniques: A survey on the state-of-the-art, taxonomy and future directions. IET Netw 2020;9:235-46.
8. Trisanto D, Rismawati N, Mulya MF, Kurniadi FI. Effectiveness undersampling method and feature reduction in credit card fraud detection. Int J Intell Eng Syst 2020;13:173-81.
9. Rajitha K, VijayaLakshmi D. Oppositional cuckoo search based weighted fuzzy rule system in malicious web sites detection from suspicious URLs. Int J Intell Eng Syst 2016;9:116-25.
10. Rao RS, Pais AR, Anand P. A heuristic technique to detect phishing websites using TWSVM classifier. Neural Comput Appl 2021;33:5733-52.
11. Tan CL, Chiew KL, Yong KS, Abdullah J, Sebastian Y. A graph-theoretic approach for the detection of phishing webpages. Comput Secur 2020;95:101793.
12. Ali W, Malebary S. Particle swarm optimization-based feature weighting for improving intelligent phishing website detection. IEEE Access 2020;8:116766-116780.
13. Aljofey A, Jiang Q, Qu Q, Huang M, Niyigena JP. An effective phishing detection model based on character level convolutional neural network from URL. Electronics 2020;9:1514.
14. Wei W, Ke Q, Nowak J, Korytkowski M, Scherer R, Woźniak M. Accurate and fast URL phishing detector: A convolutional neural network approach. Comput Netw 2020;178:107275.
15. Feng J, Zou L, Ye O, Han J. Web2Vec: Phishing webpage detection method based on multidimensional features driven by deep learning. IEEE Access 2020;8:221214-221224.
16. Anupam S, Kar AK. Phishing website detection using support vector machines and natureinspired optimization algorithms. Telecommun Syst 2021;76:17-32.
17. Mahdavifar S, Ghorbani AA. DeNNeS: Deep embedded neural network expert system for detecting cyber attacks. Neural Comput Appl 2020;32:14753-80.
18. Kumar MS, Indrani B. Frequent rule reduction for phishing URL classification using fuzzy deep neural network model. Iran J Comput Sci 2021;4:85-93.
19. Sankhwar S, Pandey D, Khan RA, Mohanty SN. An anti-phishing enterprise environ model using feed-forward backpropagation and Levenberg-Marquardt method. Secur Privacy 2021;4:e132.
20. Tharani JS, Arachchilage NA. Understanding phishers' strategies of mimicking uniform resource locators to leverage phishing attacks: A machine learning approach. Secur Privacy 2020;3:e120.
21. Haynes K, Shirazi H, Ray I. Lightweight URL-based phishing detection using natural language processing transformers for mobile devices. Procedia Comput Sci 2021;191:127-34.
22. Barraclough PA, Fehringer G, Woodward J. Intelligent cyber-phishing detection for online. Comput Secur 2021;104:102123.
23. Available from: https://www.leaf-it.com/10-ways-prevent-cyber-attacks