A Comprehensive Survey on Phishing Attack Detection

***Amita Contractor*[1], *Rutvik Mehta*[2], *Sumitra Menaria*[3]**

Department of Computer Science Engineering[1], *Department of Information Technology*[2, 3]

PIET, Parul University, India

Email: *190303201007@paruluniversity.ac.in*[1], *rutvik.mehta@paruluniversity.ac.in*[2], *sumitra.menaria@paruluniversity.ac.in*[3]

DOI:- https://doi.org/10.47531/SC.2022.05

Abstract

Phishing attack detection is one of the most challenging challenges currently facing online social network users. This study presents a different phishing detection technique to identify gaps and offer solutions to current phishing detection problems. As shown, no techniques have been proposed to address phishing, including Machine Learning (ML) based, Nature Inspired (NI) based, heuristic, blacklist based and whitelist based techniques. However, the ML-based techniques give more accuracy in terms of classification.ML algorithms cannot deal with big datasets; hence they can be combined with NI algorithms to build fast and improved models for phishing detection. Although some surveys on phishing detection techniques exist, very few focused on ML-based and Ni-based techniques. Therefore, this study presents ML-based and NI-based phishing detection techniques. The survey reveals the various shortcomings of phishing detection techniques, including limited dataset, use of third-party services (age of the domain, search engine query, etc.), use of small feature set, use of classification rules, use of blacklist and whitelist, etc. There is an obvious need for efficient and reliable solutions for phishing detection.

Keywords: *- Phishing detection; Phishing website; Phishing email; Machine learning; Nature-inspired techniques; Social engineering*

INTRODUCTION

Network security is the most critical issues that need to be considered and emphasized in the network, especially in an organization, such as offices, banks, and clinics.[1]

The organization has to keep up its security arrangement to guarantee the protection and privacy of its management and worker information. This arrangement ensures that the information, particularly the delicate information, such as the worker information, can be secured within the server. For example, to get online money, we ought to have confirmation to get to our account. This is done by giving a username and password to the login page of the online money. Authentication is needed in this scenario so that our sensitive data is not exposed to an unauthorized user such as a hacker. [1]

Although there's Associate in Nursing implementation of network security in a company,

© MANTECH PUBLICATIONS 2021. All Rights Reserved

still there's a network attack that happened. Sometimes, the network attack includes phishing, denial-of-Service attack, and name System (DNS) spoofing. This attack can contribute to financial and privacy loss to the victims.

For example, if the hacker attacks sensitive data of an online banking account, they will use this data to retrieve the victim's account and steal their cash within the account. This can also be applied to the workplace organization, whereby the hacker can gain sensitive knowledge and use it to commit online crimes, like stealing the office's cash.[1]

Phishing is one network security attack, which is derivational of the word 'Fishing' by replacing the 'F' with 'Ph'. Usually, the phishing email will redirect the user to the infected website and asking them to provide their sensitive information, such as their details and bank account information, which will be used to hack the information whatever the user enters.

The phishing attack is always related to the spamming email received by the victim. Those spam emails are also vulnerable to phishing attack because some spam emails may contain links that redirect the victim to phishing websites.[1]

By the end of the 20th century, the internet had grown immensely, and it had radically changed a significant part of our economic and social life. This change has played a significant role in the development of Online Social Networks (OSNs).

Many OSNs are web-based they allow users to upload text, images, and videos to their profiles; comment about products; communicate their health problems, and share many other subjects with other users online. In terms of massive amounts of social relation networks and the data they contain, OSNs emerged as an exciting research area receiving a great deal of attention from researchers.[2]

LITERATURE SURVEY

Phishing is a treacherous effort to steal private data from users like address, Aadhar number, PAN card details, credit/debit card details, etc. [28]

Through such attacks, the phisher tries to obtain confidential information from the user, to use it fraudulently against himself or its organization. [28]

Phishing starts with a fallacious email or alternative communication that's designed to lure a victim. The message is created to appear as it comes from a sure sender. If it fools the victim, they are coaxed into providing direction, usually on a scam website. Typically, malware is additionally downloaded onto the target’s laptop.[28]

Phishing may be a style of fraud. However, the assaulter tries to amass personal data together with, however not restricted to, login credentials or account data by masquerading as an estimable entity through either a fake or taken identity. It's also, as represented by Microsoft, a kind of malicious online fraud. The primary effectively results in the second. Users on social networking sites, and not solely those frequented by adulterers, are quick turning into the simplest targets for phishers. Their strategies can broadly be grouped into two categories:[29]

- The use of links to fake websites to steal your login and password details (or other personal information), and;[29]

© MANTECH PUBLICATIONS 2021. All Rights Reserved

- The harvesting of seemingly unimportant personal details you unwittingly share with friends, colleagues, and strangers.[29]

TYPES OF PHISHING ATTACKS

Social engineering – A malicious assault maneuverer that involves tricking individuals into breaking traditional security procedures, usually hoping on greed, AN charm to self-importance or kindness, or threat of authority and intimidation. this kind of phishing is related to the bug of classical mythology, and its main purpose is military operation by making an illusion of reality.[29]

Pretexting – A fake but seemingly legitimate scenario is created to gain access to a victim's confidential data, e.g. requiring their details to confirm their identity before claiming a prize; or pretending to be the human resource department of their previous company that needs to update their records.[29]

Doxing – Private information gained in a phishing attack is leaked on social media, making victims vulnerable to other scams, like stalking, harassing, and stolen identities. This psychological tactic is usually exclusively malicious, designed to intimidate victims for little reason other than so-called fun.[29]

Pharming – A victim is lured to a spoofed website and invited to log in using their Facebook or email account. The victim's login details are hijacked, and their information used to access other accounts, including their email address.[29]

Spear phishing is an email spoofing fraud attempt targeting a specific organization or individual seeking unauthorized access to confidential data.[29]

APPROACHES FOR PHISHING ATTACK DETECTION

1. List-based approach

In this approach, the legitimate sites are maintained in a white list while the illegitimate sites are maintained on the blacklist. The site to be evaluated can be matched against the two lists to determine if it is hazardous or not. A site might be legitimate and classified as illegitimate or might be illegitimate and classified as legitimate. [4]

2. Heuristic-based approach

In this method, a set of features can be extracted from a webpage to be used as a query to be searched on any popular search engine. These features may include text from certain tags or images, or URLs.[4]

3. Visual similarities-based approach

Machine learning algorithms are used to map the similarity between authentic and phishing websites. Features are extracted from the website, such as text, images/graphics, etc., detection by reducing the similarity in appearance with the authentic website.[4]

4. Machine-learning algorithm

One of the popular methods of malicious websites' detection is the use of machine learning methods. Mainly, the detection of a phishing attack is a simple classification problem. To develop a learning-based detection system, training data must contain many features related to phishing and legitimate website classes. Using a learning algorithm can easily detect the unseen or not classified URLs with a dynamic mechanism.[5]

5. Natured inspired algorithm

ML algorithms cannot effectively handle big datasets. Hence they can be combined with NI

© MANTECH PUBLICATIONS 2021. All Rights Reserved

algorithms to build fast and improved models for phishing detection. [5]

6. Deep learning algorithm

The global impact of phishing attacks will continue to intensify. Thus, a more efficient phishing detection method is required to protect online user activities and address this need, focused on designing and developing a deep learning-based phishing detection solution.[.[22]

ANALYSIS OF PHISHING ATTACK DETECTION

We discuss other techniques to prevent phishing attacks and their result. We discuss some techniques used to prevent social engineering attacks as phishing attacks. Nowadays, phishing attackers have become so smart that sometimes skilful people cannot distinguish between suspicious and legitimate pages, necessitating a surf technique. This portion is divided into two parts. The first part contains a review of the literature. The second part includes observation which I have observed after reading papers.

REVIEW OF LITERATURE

The working of different papers is explained individually after that comparative table is created to compare methodology and limitations/future scope. Nathezhtha., Sangeetha. D, Vaidehi.V proposed a three-phase attack detection named as Web Crawler based Phishing Attack Detector (WC-PAD) [6]

Megha N, K R Remesh Babu, Elizabeth Sherly The proposed approach detects phishing sites and websites with malicious content. [7]

Merlin .V.Kunju, Mrs Esther Dainel, Heron Celestie Anthony, Sonali Bhelwa This study gives brief knowledge about several machine learning techniques such asked Algorithm, Naïve Bayes, Decision Tree, Support Vector Machines, Neural Network and Random Forest algorithm for predicting phishing sites. [8]

Jitendra Kumar, A. Santhanavijayan, B. Janet, Balaji Rajendran, Bindhumadhava BS, compared different machine learning techniques for the phishing URL classification task and achieved the highest accuracy [9]

Federico Concone, Giuseppe Lo Re, Marco Morana, and Claudio Ruocco address the problem of spam detection on Twitter, providing a novel method to support the creation of large-scale annotated datasets.[10]

Mohd Fazil and Muhammad Abulaish present a hybrid approach for detecting automated spammers by amalgamating community-based features with other feature categories, namely metadata-, content -, and interaction-based features.[11]

Seow Wooi Liew, Nor Fazlida Mohd Sani∗, Mohd. Taufik Abdullah, Razali Yaakob, Mohd Yunus Sharum propose an effective security alert mechanism using a classification model derived from a supervised machine learning technique of Random Forest (RF) and the identified 11 best classification features.[12]

Iv'an Ortiz-Garc'es, Roberto O. Andrade, and Mar´ıa Cazares present an investigation about the analysis of anomalous behaviour related to phishing web attacks and how machine learning techniques can be an option to face the problem.[13]

Raghav Kaul, Shahriar Badsha, Shamik Sengupta address these two issues by formulating a robust

© MANTECH PUBLICATIONS 2021. All Rights Reserved

framework for fast and automated phishing URL detection. [14]

Vaibhav Patil, Pritesh Thakkar, Chirag Shah, Tushar Bhat, Prof. S. P. Godse discuss three approaches for detecting phishing websites. The first is by analyzing various URL features. The second is by checking the website's legitimacy by knowing where it is hosted and who is managing it. The third approach uses visual appearance-based analysis to check the website's genuineness.[15]

Ankit Kumar Jain1 • B. B. Gupta1 proposed approach has divided the hyperlink specific features into 12 different categories and used these features to train the machine learning algorithms.[16]

Brij B. Gupta, Ankit Kumar Jain proposed a search engine-based method that uses a lightweight, consistent and language-independent search query to detect the legality of the suspicious URL[17].

Ozgur Koray Sahingoz, Ebubekir Buber, Onder Demir, Banu Diri proposed real time anti-phishing system, which uses seven different classification algorithms and natural language processing (NLP) based features.[18]

Bryan Espinoza, J'essica Simba, Walter Fuertes, Eduardo Benavides Roberto Andrade, and Theofilos Toulkeridis make a combination of the Naive Bayes, and decision tree algorithms have been constructed using the typical cycle of Machine Learning (ML) modelling.[19]

Aliya Begum and Srinivasu Badugu studied different techniques for detecting malicious URLs and discussed their merits and demerits.[20]

Ankit Kumar Jain, Sakshi Parashar, Palak Katare, Isha Sharma proposed a search-based method with weighted TF-IDF performs better than conventional TF-IDF. [4]

Sarabjit Singh & Jaiteg Singh & Sukhjit Singh proposed algorithm was implemented in the Android application using the Open Street Map dataset. GNSS spoofing attacks were simulated and detected in real-time.[21]

Moruf Akin Adebowale, Khin T. Lwin and M. A. Hossain An extensive experimental analysis was conducted to evaluate and compare the effectiveness of the IPDS in detecting phishing web pages and phishing attacks when applied to large data sets.[22]

Shuichiro HARUTA, Hiromu ASAHINA, Fumitaka YAMAZAKI, Iwao SASASE propose a hue signature auto-update system for visual similarity-based phishing detection with tolerance to a zero-day attack.[23] Yiwei Lu, Noman Mohammed, Yang Wang introduce a new unpaired homoglyph attack detection system using a convolutional neural network.[24]

Filipo Sharevski, Paige Treebridge, Peter Jachim, Audrey Li, Adam Babin, Jessica Westbrook introduces an alternate way of provoking or silencing social media discourse by manipulating how users perceive authentic content. This manipulation is performed by man-in-the-middle malware that covertly rearranges [25]

Aritz Arrate, José González-Cabañas, Ángel Cuevas, and Rubén Cuevas compromise the security of the users that receive those ads. This practice is referred to as Malvertising. Some reports have estimated the economic loss caused by malvertising to the online advertising sector[27]

© MANTECH PUBLICATIONS 2021. All Rights Reserved

Observation Table

Table 1: Literature review

Sr. No	Paper Name	Publication Year	Conference/journal	Methodology/tool/techniques used	Future scope
1	WC-PAD: Web Crawling based Phishing Attack Detection [6]	2019	IEEE	The three phases of WC-PAD include 1) DNS blacklist 2) Heuristic based approach and 3) Web crawler-based approach.	Third-party features can be removed
2	An Intelligent System for Phishing Attack Detection and Prevention [7]	2019	IEEE	SVM, ANN	Add more features
3	Evaluation of Phishing Techniques Based on Machine Learning [8]	2019	IEEE	kNN Algorithm, Naïve Bayes, Decision Tree, Support Vector Machines, Neural Network and Random Forest	High reliability is BIGGER CHALLENGES
4	Phishing Website Classification and Detection Using Machine Learning [9]	2020	IEEE	Naïve Bayes Classifier	Incorporate a rule-based prediction based on the content analysis of a URL.
5	Assisted Labelling for Spam Account Detection on Twitter [10]	2019	IEEE	Spam detection on Twitter	Analysis to non-English tweets
6	A Hybrid Approach for Detecting Automated Spammers in Twitter [11]	2018	IEEE	Random forest Decision tree Bayesian network	Temporal evolution of spammer
7	An effective security alert mechanism for real-time phishing tweet detection on Twitter [12]	2019	ELSEVIER	Random forest	REMOVE THIRD PARTY FEATURES

© MANTECH PUBLICATIONS 2021. All Rights Reserved

8	Detection of Phishing Attacks with Machine Learning Techniques in Cognitive Security Architecture [13]	2019	IEEE	Artificial Neural Networks	Not to open a shortened URL
9	An Automated Framework for Real-time Phishing URL Detection [14]	2019	IEEE	Detect phishing URLs using machine learning algorithms.	Collect more URLs.
10	Detection and Prevention of Phishing Websites using Machine Learning Approach [15]	2018	IEEE	Checking the legitimacy of website	Much richer feature to feed to the machine learning algorithm that would result in much higher accuracy.
11	A machine learning-based approach for phishing detection using hyperlinks information [16]	2019	SPRINGER	Hyperlinks found in the HTML source	Also detect non-HTML websites with high accuracy
12	Phishing Attack Detection using a Search Engine and Heuristics-based Technique [17]	2020	Journal of Information Technology Research	Detect the legality of the suspicious URL.	Cannot filter phishing webpages hosted on hacked or compromised domains.
13	Machine learning-based phishing detection from URLs [18]	2019	ELSEVIER	Seven classification algorithms NLP-based features	Improve efficiency deep learning can be used.
14	Phishing Attack Detection: A solution based on the typical Machine Learning modelling	2019	IEEE	Random Forest, Logistic Regression and Fictitious Classifier	Redesign this model using unsupervised learning techniques such as Deep Learning

© MANTECH PUBLICATIONS 2021. All Rights Reserved

	cycle [19]				
15	A Study of Malicious URL Detection Using Machine Learning and Heuristic Approaches [20]	2020	SPRINGER	Techniques for detecting malicious URL	Redesign this model using unsupervised learning techniques such as Deep Learning,
16	PhishSKaPe : A content-based Approach to Escape Phishing Attacks [4]	2020	SPRINGER	manipulate the TF-IDF score	Some additional features can be added to improve the accuracy.
17	Mitigating Spoofed GNSS Trajectories through Nature Inspired Algorithm [21]	2020	SPRINGER	Open Street Map dataset.	Deep learning can be used for improvement
18	Intelligent phishing detection scheme using deep learning algorithms [22]	2020	JEIM	Convolutional neural network (CNN) and the long short-term memory (LSTM)	A deep learning algorithm can be used to protect users in real time.
19	Hue Signature Auto Update System for Visual Similarity-Based Phishing Detection with Tolerance to Zero-Day Attack [23]	2019	IEICE TRANS. INF. & SYST	We propose a hue signature detection with tolerance to zero-day attack	Detecting phishing websites with the low computational cost is a challenge for all signature-based phishing detection scheme.
20	Homoglyph Attack Detection with Unpaired Data [24]	2019	SEC	Convolutional neural network	Building a web interface for users to check the legitimacy of a name before clicking will better serve to prevent data breaches.
21	Beyond Trolling: Malware-Induced	2020		The original Facebook post and comments	Social interaction is a decision making

© MANTECH PUBLICATIONS 2021. All Rights Reserved

	Misperception Attacks on Polarized Facebook Discourse [25]			The MIM Facebook post and comments	factor
22	Poster: Understanding User's Decision to Interact with Potential Phishing Posts on Facebook using a Vignette Study [26]	2019	Conference on Computer & Communications Security	Vignette study	Including who posts it, where it is posted, and the type of post. Attackers seeking to phish users on Facebook likely leverage this kind of information to craft their attacks, so it is crucial to understand designing mechanisms to protect users.
23	Malvertising in Facebook: Analysis, Quantification and Solution [27]	2020	MDPI	The primary goal of the paper is to analyze the impact of malvertising on Facebook	It can be used for other online social networks like Twitter.

CONCLUSIONS

Phishing detection is one of the most challenging problems faced by the cyber community and has led to the loss of millions of US dollars. Many phishing detection techniques have been proposed in the literature; however, ML-based techniques achieved the best results. ML-based cyber security systems can discover new cyber-attacks in real time, thus producing better prediction accuracy than other techniques. This study presents a comprehensive survey of phishing detection techniques with a focus on MTL-based and NI-based techniques. Its primary goal is to empower the research community with beneficial insights to enhance the design and development of improved phishing detection systems. Moreover, this survey provides a clear picture of various methods and algorithms applied to phishing detection irrespective of limitations.

REFERENCES

1. Arrate, Aritz & González-Cabañas, José & Cuevas, Ángel & Cuevas, Rubén. (2020). Malvertising in Facebook: Analysis, Quantification and Solution. Electronics. 9. 1332. 0.3390/electronics9081332.
2. Can, Umit & Alatas, Bilal. (2019). A new direction in social network analysis: Online social network analysis problems and applications. Physica A: Statistical Mechanics and its Applications. 535. 122372. 10.1016/j.physa.2019.122372.

© MANTECH PUBLICATIONS 2021. All Rights Reserved

3. Adil, Muhammad & Khan, Rahim & Khan, Abdul & Ghani, M & Ghani, Ul. (2020). Preventive Techniques of Phishing Attacks in Networks.10.1109/ICACS47775.2020.905594 3.
4. Jain, Ankit & Parashar, Sakshi & Katare, Palak& Sharma, Isha. (2020). PhishSKaPe: A content-based Approach to Escape Phishing Attacks. Procedia Computer Science. 171. 1102-1109. 10.1016/j.procs.2020.04.118.
5. Akinyelu, Ayo. (2019). Machine Learning and Nature Inspired Based Phishing Detection: A Literature Survey. International Journal on Artificial Intelligence Tools. 28. 1930002. 10.1142/S0218213019300023.
6. Nathezhtha, T. & Sangeetha, D. &Vaidehi, V.(2019). WC-PAD: Web Crawling based Phishing Attack Detection. 1-6. 10.1109/CCST.2019.8888416.
7. Megha, N & Raman, K R Remesh & Sherly, Elizabeth. (2019). An Intelligent System for Phishing Attack Detection and Prevention. 1577-1582. 10.1109/ICCES45898.2019.9002204.
8. Kunju, Merlin &Dainel, Esther & Anthony, Heron &Bhelwa, Sonali. (2019). Evaluation of Phishing Techniques Based on Machine Learning. 963-968. 10.1109/ICCS45141.2019.9065639.
9. Kumar, Jitendra & Santhanavijayan, A. & Janet, B. & Rajendran, Balaji & Bindhumadhava, Bapu. (2020). Phishing Website Classification and Detection Using Machine Learning. 1-6. 10.1109/ICCCI48352.2020.9104161.
10. Concone, Federico & Lo Re, Giuseppe &Morana, Marco &Ruocco, Claudio. (2019). Assisted Labeling for Spam Account Detection on Twitter. 359-366. 10.1109/SMARTCOMP.2019.00073.
11. Fazil, Mohd & Abulaish, Muhammad. (2018). A Hybrid Approach for Detecting Automated Spammers in Twitter. IEEE Transactions on Information Forensics and Security. PP. 1-1. 10.1109/TIFS.2018.2825958.
12. SeowWooi, Liew & Sani, Nor Fazlida Mohd& Abdullah, Mohd Taufik & Yaakob, Razali & Sharum, Mohd. (2019). An Effective Security Alert Mechanism for Real-Time Phishing Tweet Detection on Twitter. Computers & Security. 83. 10.1016/j.cose.2019.02.004.
13. Garces, Ivan & Cazares, Maria & Andrade, Roberto. (2019). Detection of Phishing Attacks with Machine Learning Techniques in Cognitive Security Architecture. 366-370. 10.1109/CSCI49370.2019.00071.
14. Sadique, Farhan & Kaul, Raghav & Badsha, Shahriar & Sengupta, Shamik. (2019). An Automated Framework for Real-time Phishing URL Detection. 10.1109/CCWC47524.2020.9031269.
15. Patil, Vaibhav & Thakkar, Pritesh & Shah, Chirag & Bhat, Tushar & Godse, Sachin. (2018). Detection and Prevention of Phishing Websites Using Machine Learning Approach. 1-5. 10.1109/ICCUBEA.2018.8697412.
16. Jain, Ankit & Gupta, B B. (2018). A machine learning-based approach for phishing detection using hyperlinks information. Journal of Ambient Intelligence and Humanized Computing. 10.1007/s12652-018-0798-z.
17. Gupta, B B& Jain, Ankit. (2020). Phishing Attack Detection using a Search Engine and Heuristics-based Technique. Journal of Information Technology Research. 13. 94-109. 10.4018/JITR.2020040106.
18. Sahingoz, O. K., Buber, E., Demir, O., &Diri, B. (2018). Machine Learning-Based Phishing Detection from URLs. Expert Systems with Applications. 10.1016/j.eswa.2018.09.029

© MANTECH PUBLICATIONS 2021. All Rights Reserved

19. Espinoza, Bryan & Simba, Jessica & Fuertes, Walter & Benavides, Eduardo & Andrade, Roberto & Toulkeridis, Theofilos. (2019). Phishing Attack Detection: A Solution Based on the Typical Machine Learning Modeling Cycle. 202-207. 10.1109/CSCI49370.2019.00041.
20. Begum, A., &Badugu, S. (2019). A Study of Malicious URL Detection Using Machine Learning and Heuristic Approaches. Advances in Decision Sciences, Image Processing, Security and Computer Vision, 587–597 10.1007/978-3-030-24318-0_68.
21. Singh, Saravjeet & Singh, Jaiteg & Singh, Sukhjit. (2020). Mitigating Spoofed GNSS Trajectories through Nature Inspired Algorithm. GeoInformatica. 10.1007/s10707-020- 00412-z.
22. Adebowale, Moruf&Lwin, Khin & Hossain, Alamgir. (2020). Intelligent Phishing Detection Scheme Algorithms Using Deep Learning. Journal of Enterprise Information Management. Ahead-of-print. 10.1108/JEIM-01-2020-0036.
23. Haruta, Shuichiro & Asahina, Hiromu & YAMAZAKI, Fumitaka & Sasase, I.. (2019). Hue Signature Auto Update System for Visual Similarity-Based Phishing Detection with Tolerance to Zero-Day Attack. IEICE Transactions on Information and Systems. E102.D. 2461-2471. 10.1587/transinf.2019EDP7079.
24. Lu, Yiwei & K, Mahesh & Mohammed, Noman & Wang, Yang. (2019). Homoglyph attack detection with unpaired data. 377-382. 10.1145/3318216.3363337.
25. Sharevski, Filipo & Treebridge, Paige &Jachim, Peter & Li, Audrey &Babin, Adam & Westbrook, Jess. (2020). Beyond Trolling: Malware-Induced Misperception Attacks on Polarized Facebook Discourse.
26. Seng, Sovantharith & Kocabas, Huzeyfe & Al-Ameen, Mahdi Nasrullah & Wright, Matthew. (2019). Poster: Understanding User's Decision to Interact with Potential Phishing Posts on Facebook using a Vignette Study. 2617-2619. 10.1145/3319535.3363270.
27. Arrate, Aritz& González-Cabañas, José & Cuevas, Ángel & Cuevas, Rubén. (2020). Malvertising in Facebook: Analysis, Quantification and Solution. Electronics. 9. 1332. 10.3390/electronics9081332.

Web References

1. https://www.cisco.com/c/en_in/products/security/email-security/what-is-phishing.html
2. https://resources.infosecinstitute.com/category/enterprise/phishing/the-phishinglandscape/phishing

© MANTECH PUBLICATIONS 2021. All Rights Reserved