LITERATURE SURVEY

[1] Author Name: Mahmoud Khonji, Youssef Iraqi, Andrew Jones

Phishing attacks target vulnerabilities that exist in systems due to the human factor. Many cyber-attacks are spread via mechanisms that exploit weaknesses found in end-users, which makes users the weakest element in the security chain. The phishing problem is broad and no single silver-bullet solution exists to mitigate all the vulnerabilities effectively, thus multiple techniques are often implemented to mitigate specific attacks. This paper aims at surveying many of the recently proposed phishing mitigation techniques. A high-level overview of various categories of phishing mitigation techniques is also presented, such as: detection, offensive defense, correction, and prevention, which we belief is critical to present where the phishing detection techniques fit in the overall mitigation process.

[2] Author Name: AZEEZ NURENI AYOFE

Phishing is a form of social engineering or website forgery whereby attackers mimic a trusted website or public organization or sending e-mails in an automated manner in order to steal sensitive information or credentials of online users. This is done in a way the user does not realize he is in a phishing environment and in turn reveals his sensitive information such as credit card information, employment details, online shopping account passwords and bank information. Phishers are still having their ways to succeed in their various nefarious activities and attacks. Different anti-phishing schemes however have emerged but phishers still find their ways around by breaking through various existing techniques. Against this backdrop, this project aims at developing a web enabled anti-phishing technique using enhanced heuristic approach.

[3] Author Name: Jason Hong

Phishing attacks are a significant threat to users of the Internet, causing tremendous economic loss every year. In combating phish, industry relies heavily on manual verification to achieve a low false positive rate, which, however, tends to be slow in responding to the huge volume of unique phishing URLs created by toolkits. Our goal here is to combine the best aspects of human verified blacklists and heuristic-based methods, i.e, the low false positive rate of the former and the broad and fast coverage of the latter.

[4] Author Name: Hiba Zuhair

Phishing has become a substantial threat for internet users and a major cause of financial losses. In these attacks the cybercriminals carry out user credential information and users can fall victim. The current solution against phishing attacks is not sufficient to detect and work against novel phishes. This paper presents a systematic review of the previous and current research waves done on Internet phishing mitigation in different areas of expertise and highlighted phishing attacks types and some existing anti-phishing approaches.

[5] Author Name: Jun Ho Huh

We propose a new phishing detection heuristic based on the search results returned from popular web search engines such as Google, Bing and Yahoo. The full URL of a website a user intends to access is used as the search string, and the number of results returned and ranking of the website are used for classification. Most of the time, legitimate websites get back large number of results and are ranked first, whereas phishing websites get back no result and/or are not ranked at all.

[6] Author Name: skr aaa

Phishing websites, fraudulent sites that impersonate a trusted third party to gain access to private data, continue to cost Internet users over a billion dollars each year. In this paper, we describe the design and performance characteristics of a scalable machine learning classifier we developed to detect phishing websites. We use this classifier to maintain Google's phishing blacklist automatically. Our classifier analyses millions of pages a day, examining the URL and the contents of a page to determine whether or not a page is phishing. Unlike previous work in this field, we train the classifier on a noisy dataset consisting of millions of samples from previously collected live classification data.

[7] Author Name: Dr.Ammar Almomani

Phishing is the fraudulent acquisition of personal information like username, password, credit card information, etc. by tricking an individual into believing that the attacker is a trustworthy entity. It is affecting all the major sector of industry day by day with lots of misuse of user's credentials. So, in today online environment we need to protect the data from phishing and safeguard our information, which can be done through anti-phishing tools. Currently there are many freely available anti-phishing browser extensions tools that warns user when they are browsing a suspected phishing site. In this paper we did a literature survey of some of the commonly and popularly used anti-phishing browser extensions by reviewing the existing anti-phishing techniques along with their merits and demerits.

[8] Author Name: Tommy Chin, Kaiqi Xiong and Chengbin

Authors designed a system with a detection technique involving a fresh approach for phishing website detection named PhishLimiter. The proposed system used Deep Packet Inspection (DPI) along with Software-Defined Networking (SDN) through web communications and emails for identifying malicious activities. The real-time DPI and phishing signature classification based on SDN programmability provided PhishLimiter, the flexibility to address phishing attacks in real-time. This also helped in better network traffic management and evaluated attacks in real-world environments proving an effective solution to identify phishing attacks.

[9] Author Name: L. MacHado and J. Gadge

This article surveys the literature on the detection of phishing attacks. Phishing attacks target vulnerabilities that exist in systems due to the human factor. Many cyber-attacks are spread via mechanisms that exploit weaknesses found in end-users, which makes users the weakest element in the security chain. The phishing problem is broad and no single silver-bullet solution exists to mitigate all the vulnerabilities effectively, thus multiple techniques are often implemented to mitigate specific attacks. This paper aims at surveying many of the recently proposed phishing mitigation techniques.

[10] Author Name: Solomon Ogbomon Uwagbole

In this paper, the authors proposed a system for phishing website detection using machine learning algorithms. The system used a domain name-based approach for determining the phishing website URL. The Random Forest algorithm was used to train the classifier by importing the dataset and extracting features for classification purposes. In total 10 URL features including the host-based and lexical features were extracted from the obtained dataset. The testing phase of this model achieved an accuracy of 96 percent for the Random Forest classifier using the labeled dataset