LITERATURE SURVEY

- **Phish Guard- An Automatic Web Phishing Detection System**

AUTHORS:

Smiti Poddar ; Harsh Salkar ; Priya Agarwal ; Deepak Karia ; Milind Paraye ; Dayanand Ambawade ; Narendra Bhagat

DESCRIPTION:

People are being compelled to adopt a "work from home" strategy because of the COVID-19 outbreak. In today's world, the Internet has evolved into a powerful tool for social connection. People's reliance on digital platforms creates opportunities for deception. Phishing websites are one of the types of internet security issues that target human vulnerabilities rather than software flaws. It is defined as the act of impersonating someone else to steal sensitive information such as usernames and passwords from online users. In this research, we provide an intelligent system for identifying phishing websites that work as an extension to an internet browser and automatically warn the user when a phishing website is detected.

YEAR: 2022

https://ieeexplore.ieee.org/document/9862857

- # WC-PAD: Web Crawling based Phishing Attack Detection

AUTHORS:

T. Nathezhtha ; D. Sangeetha ; V. Vaidehi

DESCRIPTION:

Phishing is a criminal offense which involves theft of user's sensitive data. The phishing websites target individuals, organizations, the cloud storage hosting sites and government websites. Currently, hardware based approaches for anti-phishing is widely used but due to the cost and operational factors software based approaches are preferred. The existing phishing detection approaches fails to provide solution to problem like zero-day phishing website attacks. To overcome these issues and precisely detect phishing occurrence a three phase attack detection named as Web Crawler based Phishing Attack Detector(WC-PAD) has been proposed. It takes the web traffics, web content and Uniform Resource Locator(URL) as input features, based on these features classification of phishing and non phishing websites are done. The experimental analysis of the proposed WC-PAD is done with datasets collected from real phishing cases. From the experimental results, it is found that the proposed WC-PAD gives 98.9% accuracy in both phishing and zero-day phishing attack detection.

YEAR: 2019

https://ieeexplore.ieee.org/document/8888416

- # Phishing Web Page Detection Methods: URL and HTML Features Detection

AUTHORS:

Humam Faris; Setiadi Yazid

DESCRIPTION:

Phishing is a type of fraud on the Internet in the form of fake web pages that mimic the original web pages to trick users into sending sensitive information to phisher. The statistics presented by APWG and Phistank show that the number of phishing websites from 2015 to 2020 tends to increase continuously. To overcome this problem, several studies have been carried out including detecting phishing web pages using various features of web pages with various methods. Unfortunately, the use of several methods is not really effective because the design and evaluation are only too focused on the achievement of detection accuracy in research, but evaluation does not represent application in the real world. Whereas a security detection device should require effectiveness, good performance, and deployable. In this study the authors evaluated several methods and proposed rules-based applications that can detect phishing more efficiently.

YEAR: 2021

https://ieeexplore.ieee.org/document/9359694

- # A Machine Learning Approach for URL Based Web Phishing Using Fuzzy Logic as Classifier

AUTHORS:

Happy Chapla ; Riddhi Kotak ; Mittal Joiser

DESCRIPTION:

Phishing is the major problem of the internet era. In this era of internet the security of our data in web is gaining an increasing importance. Phishing is one of the most harmful ways to unknowingly access the credential information like username, password or account number from the users. Users are not aware of this type of attack and later they will also become a part of the phishing attacks. It may be the losses of financial found, personal information, reputation of brand name or trust of brand. So the detection of phishing site is necessary. In this paper we design a framework of phishing detection using URL.

YEAR: 2019

https://ieeexplore.ieee.org/document/9002145

- # Detection and Prevention of Phishing Websites Using Machine Learning Approach

AUTHORS:

Vaibhav Patil; Pritesh Thakkar; Chirag Shah; Tushar Bhat; S. P. Godse

ABSTRACT:

Phishing costs Internet user's lots of dollars per year. It refers to exploiting weakness on the user side, which is vulnerable to such attacks. The phishing problem is huge and there does not exist only one solution to minimize all vulnerabilities effectively, thus multiple techniques are implemented. In this paper, we discuss three approaches for detecting phishing websites. First is by analyzing various features of URL, second is by checking legitimacy of website by knowing where the website is being hosted and who are managing it, the third approach uses visual appearance based analysis for checking genuineness of website. We make use of Machine Learning techniques and algorithms for evaluation of these different features of URL and websites. In this paper, an overview about these approaches is presented.

YEAR: 2018