LITERATURE SURVEY

DOMAIN: APPLIED DATA SCIENCE
TOPIC: WEB PHISHING DETECTION

1.A MACHINE LEARNING APPROACH TO PHISHING DETECTION AND DEFENSE:

AUTHORS: OA Akanbi, E Fazeldehkordi

ABSTRACT: Phishing is one of the foremost widely-perpetrated shapes of cyber attack,utilized to accumulate delicate data such as credit card numbers, bank accounts and client logins and passwords, as well as other data entered through a website. The creators of A Machine-Learning Approach to Phishing Detection and Protection have conducted inquire about to demonstrate how a machine learning calculation can be utilized as an viable and proficient instrument in recognizing phishing websites and assigning them as data security dangers.

REFER LINK: **Amiri: A machine-learning approach to phishing
detection... - Google Scholar**

2.PHISHING

AUTHORS: Koceilah Rekouche

ABSTRACT: Phishing may be a sort of social building where an aggressor sends a false(eg.,spoofed,fake, or something else deceptive) message planned to trap a individual into revealing delicate data to the aggressor or to send malicious program on the victim's foundation like ransomware.Phishing assaults have gotten to be progressively sophisticated and regularly straightforwardly reflect the location being targeted,permitting the aggressor to watch everything whereas the casualty is exploring the location, and transverse any extra security boundaries with the casualty.As of 2020,phishing is by distant the foremost common assault performed by cybercriminals,the FBI's Web Wrongdoing Complaint Middle recording over twice as numerous occurrences of phishing than any other sort of computer wrongdoing.

REFER LINK:
https://en.wikipedia.org/wiki/Phishing#History

3.TEXAS SCHOOL DISTRICT IOSES $2.3 MILLION TO PHISHING SCAM,BEC,2020.AVAILABLE AT:

AUTHORS: Trend Micro

ABSTRACT: House Free School Locale (MISD) in Texas is investigating an email phishing assault after a arrangement of seemingly typical school-vendor exchanges come about within the loss of an evaluated US$2.3 million. Agreeing to the explanation posted on Twitter, the area is collaborating with the House Police Division and the Government Bureau of Examination (FBI), and energized the community to share Any data related to the incident.

REFER LINK:

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/texas-school-district-loses-2-3-million-to-phishing-
Scam-bec

4.FACEBOOK AND GOOGLE WERE CONNED OUT OF $100M IN PHISHING SCHEME:

AUTHOR: Gibbs S

ABSTRACT: Google and Facebook were phished for over $100m, it has been detailed, demonstrating not indeed the greatest innovation companies within the world are safe from the progressively sophisticated assaults of online scammers. Final month it was reported that two major tech companies were deceived by a Lithuanian man into sending him over $100m (£77m). Evaldas Ramanauskas, 48, was charged with wire extortion, money washing and irritated character burglary for impersonating Quanta Computer – a Taiwanese hardware manufacturer that incorporates Google, Facebook and Apple as clients.

REFER LINK:

https://www.theguardian.com/technology/2017/apr/28/facebook
google-conned-100m-phishing-scheme

5.VADE SECURE DISCOVERS NEW PHISHING ATTACK TARGETING 550 MILLION EMAIL USERS GLOBALLY ’. AVAILABLE AT

AUTHORS: Haldey E

ABSTRACT: Vade Secure has found a modern phishing assault that represents more than 550 million emails sent since Q1 2018. First identified in early January, the phishing assault is focusing on consumers around the world. Nations with tall concentrations of affected mail clients incorporate the US, UK, France, Germany, and the Netherlands. The phishing assault endeavors to take users’ bank account details by advertising them a coupon or rebate in trade for participating in a test or online challenge. The emails masquerade as well known brands, online spilling administrations, and telecom administrators based on the nation of the beneficiaries. Examples incorporate Canada Drug stores within the US, as well as Orange and Carrefour in France. Additionally, the substance of the messages is adjusted according to the neighborhood dialect.

REFER LINK: **https://www.vadesecure.com/en/phishing-attacktargets-550-million/**

6.PHISHING ACTIVITY TRENDS REPORTS, 2020. AVAILABLE AT

AUTHORS: M. Wisecrackers

ABSTRACT: The APWG Phishing Activity Patterns Report analyzes phishing assaults reported to the APWG by its part companies, its Worldwide Inquire about Accomplices, through the organization's site at http://www.apwg.org, and by email submissions to reportphishing@antiphishing.org. APWG measures the advancement, multiplication, and engendering of crimeware by drawing from the investigation of our part companies. Phishing could be a criminal component utilizing both social building and specialized subterfuge to take consumers' individual personality information and monetary account credentials. Specialized subterfuge plans plant crimeware onto PCs to take qualifications specifically, frequently utilizing frameworks to intercept shoppers online account client names and passwords -- and to degenerate neighborhood navigational foundations to mislead consumers to fake Web locales (or true Web locales through phisher-controlled intermediaries utilized to screen and intercept consumers' keystrokes).

REFER LINK:
https://docs.apwg.org//reports/apwg_trends_report_h1_2017.

7.GOOGLE SAFE BROWSING, 2020.
AVAILABLE AT
AUTHORS: Tewari A
ABSTRACT: Google Safe Browsing makes a difference to ensure over four billion gadgets every day by appearing notices to clients when they endeavor to navigate to perilous locales or download unsafe records. Secure Browsing informs webmasters when their websites are compromised by malevolent on-screen characters and makes a difference in analyzing and resolving the issue so that their guests remain more secure. Secure Browsing securities work over Google items and control safer browsing encounters over the Web.

Our Transparency Report incorporates points of interest on the dangers that Safe Browsing distinguishes. The Transparency Report incorporates our Location Status demonstrative apparatus that you just can utilize to see whether a location right now contains substance that Secure Browsing has determined to be unsafe. Secure Browsing launched in 2007 to ensure clients over the net from phishing assaults, and has evolved to allow clients apparatuses to assist in securing themselves from web-based dangers like malware, undesirable computer programs, and social building over desktop and portable stages. Our Safe Browsing building, item, and operations groups work at the cutting edge of security, inquire about and innovation to build frameworks that offer assistance clients secure themselves from hurt. Check out our Investigate and the Google Security Web journal for updates on Secure Browsing and other Google security technology.

REFER LINK:https://safebrowsing.google.com/

8.PHISHING PAGE DETECTION VIA LEARNING CLASSIFIERS FROM PAGE LAYOUT FEATURE

AUTHORS: Mao J. Bian J. Tian W

ABSTRACT: The web technology has ended up the foundation of a wide range of stages, such as portable administrations and smart Internet-of-things (IoT) frameworks. In such stages, users' information are totaled to a cloud-based stage, where web applications are utilized as a key interface to get to and configure client information. Securing the net interface requires solutions to bargain with dangers from both specialized vulnerabilities and social components. Phishing assaults are one of the most commonly misused vectors in social building attacks.

REFER LINK:[**Mao: Phishing page detection via learningclassifiers... - Google Scholar**]

9.NEW RULE-BASED PHISHING DETECTION METHOD

AUTHORS: Moghimi M. Varjani A

ABSTRACT: An unused rule-based strategy to distinguish phishing assaults in internet banking. Our rule-based strategy utilized two novel include sets, which have been proposed to decide the webpage personality. We utilized approximate string coordinating algorithms to decide the relationship between the substance and the URL of a page in our first proposed highlight set.

REFER LINK:[**Moghimi: New rule-based phishing detectionmethod - Google Scholar**]

10.A PHISH DETECTOR USING LIGHTWEIGHT SEARCH FEATURES

AUTHORS: Varshney G. Misra M

ABSTRACT: Web phishing could be a well-known cyber-attack which is utilized by attackers to get imperative data such as username, password, credit card number, social security number, and/or other credentials from Web clients through duplicity. A number of web phishing detection solutions have been proposed and implemented within the later a long time. These arrangements incorporate the use of phishing dark list, look motor, heuristics and machine learning, visual closeness methods, DNS, get to list and proactive phishing.

REFER LINK:

Varshney: A phish detector using lightweightsearch features - Google Scholar