International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 02 | Feb -2020 ISSN: 2582-3930

Phishing

Supriya. M, Sushmitha .M, Vanaja, Ajitha basilica
Department of computer science
St philomena college,Bannimantap, Mysore-570015

ABSTRACT:

In this paper, we seek to highlight the concept of computing, phishing is a criminal activity using social engineering techniques. Phishes attempt to frugality to acquire sensitive information, such as passwords and credits cards details, by masquerading as a trustworthy person.

Phishing is a typically carried out using email or an instant message, although phone contact has been used as well. Attempts to deal with a growing number of reported phishing incidence include legislation, user training and technical measures. Some phishing scams use JavaScript commands in order to alter the address bar. This is done either by placing a picture of the legitimate entity's.URL over the address bar or by closing the original address bar and opening a new one containing the legitimate URL.phishing generally requires the fake website but, not all phishing attacks requires a fake website, the term phishing is a variant of phishing, probably influenced by freaking and alludes to the use of increasingly sophisticated lures to "fish" for users financial information and passwords.

HISTORY

Phishing is one of the most organized crimes of the 21st century .it is defined as a type of malware or a term for where someone sends out a spoofed email to random victims to try to get personal information about them. More specifically in computing, phishing is a criminal activity using social engineering techniques to fraudulently acquire sensitive information such as user names and passwords by attempting to trick users of popular websites by emailing them fake versions of the website to provide their credentials to .

This may seem easy to avoid but the advances in the phishing community are making phishing scams harder and harder to identify from the victim stand point. The term phishing has evolved from the almost poorly constructed instant messaging attack into spoofing entire websites to fool users into providing personal information .an example of a phishing attempt made to some of the email users of the authors. For this article, we survived the literature to study the current state of phishing and existing solutions. To address the many new developments in phishing, such as spear phishing, pharming and social phishing, and the way that phishers are also developing more and more convincing sites and emails to deceive users, we have designed a three-step approach to prevent and control phishing. Based on the proposed phishing solution frame work, the attack can be stopped before it reaches the user, once the user is at the phishing site or by training users to avoid it by themselves.

The objective of this article is to provide a clear analysis of the current state of phishing and recommend practical solutions. Phishing has been a major issue for security for a long time without a good solution in place. The problem with phishing is that a holistic solution that works to protect users securely from being phished does not exist. As a result, the need for more advanced methods of security to identify phishing scams is important. Phishing is a major threat to all internet users and is difficult to trace or defend against since it does not present itself as obviously malicious in nature. In today's society, everything is put online and the safety of personal credentials is at risk. Phishing can be seen as one of the oldest and easiest ways of stealing information from people and it is used for obtaining a wide range of personal details. It also has a fairly simple approach –send an email, email sends victim to a site, site steals information.

In reality, phishing has become a complex and escalating threat to everyone's internet security. By gathering even a small amount of information about a victim, the attacker can produce a personalized and believable email. These phishers are not easy to catch either, as most of them can hide the location of their servers and work in almost complete anonymity. Even a user with excellent security software can fall victim to a phishing attack, because for the most part they depend entirely on information typed into a form, not malware infection of a computer. However there are many ways to protect against phishing attempts. An attack can be detected before it reaches the user, once the user has reached the phishing site, or the user can be trained to be aware of the attack. Using these approaches together, a secure and safe environment for a user can be created. Phishing has become so advanced and stealthy that, according to Forbes, it results in about $500m in losses per year to US business alone. And the advances in targeted spear –phishing attacks-and how easily they can find data just by searching publicly available sources are astonishing. The breakdown of the phishing process is described in a stage-by-stage process that helps to create the concept of a typical phishing attack. We can visualize the the damaging effects from phishing on victims using three different angles: enterprise, customer and government authority, another malicious type of mass phishing is pharming. The paper looks at the pharming attack process and how it differs from phishing. Pharming leverages malicious code such as viruses, worms, Trojans and spyware to carry out sophisticated attacks including host file modification, DNS cache poisoning and so on, and the user will not be aware of it, there are few solutions that are proposed to prevent phishing attacks.

Online frauds in banks with phishing: this presents a more detailed look into the implications of phishing frauds in online banking. This study explains the most common frauds with online banks and how these are associated with phishing.many different definitions that can be used for phishing are outlined here.further,this work outlines the various phishing techniques that attackers may use. This paper describes the reasons foe the increased prevalence of phishing attacks and outlines a few examples of actual organizations affected by these malicious actions. It provides a detailed action plan on how to combat bank fraud by phishing .various tables of data include the top hosting methods for phishing sites and reports of attacks increasing over the years .the current state of phishing attacks: in this work, the

author analysis the state of phishing attacks. The paper describes how attacks will trick victims with multiple types of malware. The anatomy of a phishing attack is explained through the concepts of fake phishing emails, setting up fake websites and monetizing stolen information. The psychology behind why phishing attacks work is explained briefly. Phishing causes damage to organizations' and costs lots of money every year.countermeasure recommendations are covered, with different approaches to keep someone from becoming a victim of phishing scams. Classification of phishing email using random forest machine learning technique, the primary focus of this research work is the application of machine learning to identify phishing emails.First,it introduces the concept of phishing and problems that are associated with it the concept of machine learning is also described for its use in discovering phishing emails. Most email filtering methods have not evolved with the phishing techniques which is why machine learning for discovering patterns in phishing emails is important. The classification of a phishing email used in the machine learning detection system is described based on a set of rules. It approaches phishing using an experiment based on a algorithm for detecting phishing emails. The results were encouraging for this technique, with few fake positives.

Spear phishing can be defined as the preliminary stage of an advanced persistent threat (APT) attack, to create a point of entry into the organization. This article is mainly focused around the concept of spear phishing and how it works differently from just generic phishing. It covers how phishing affects victims and what is gained by the attacker using these methods brief description of how to avoid spear phishing is also provided. The many ways that a victim's personal information can be mined and exploited using data that can easily be found online are discussed. An attacker can use various social networking sites to produce a focused and much more effective phishing tactic. The paper describes research that was carried out by browsing and documenting relationships freely available to the public on such sites and using that information to launch a mock phishing attack on their subjects. During this procedure, the authors describe the methods social phishing attacks employ to steal user credentials. Finally the paper discusses the results of the experiment and the demographics of the subjects that fell for the attacks. Phishers have become more skilled at forging websites to appear identical to the expected location, even including logos and graphics in the phishing emails to make the phishing emails to make them more convincing. there are dangerous new advanced methods that utilize personal information that is easily available to the public in order to produce plausible and believable attacks that directly target victims. Methods such as social phishing and context aware phishing are perfect examples of attacks utilizing the massive amount of public information to increase the effectiveness of their scams. One study shows that victims are 4.5 times more likely to fall for a phishing attempt if it is from a personal contact or personally relates to them.

References:

google,

wikipedia

www.researchgate.net