International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 04 | April - 2023 Impact Factor: 8.176 ISSN: 2582-3930

Phishing Attack and its Counter Measures

Shatakshi, Vijay Laxmi (A.P. CSE department)

B.Tech. Computer Science, PDM University Bahadurgarh, Haryana, India

ABSTRACT

Phishing is a type of cybercrime in which attackers impersonate real persons/ organizations by impersonating them as persons or organizations via e-mail or other communication media. In this type of cyberattack, the attacker sends malicious links or links via phishing emails that can perform various tasks, including obtaining the victim's credentials or account information. These emails causedamage to victims of loss of money and identity theft. One of the biggest problems in internet technology is unwanted spam. Well-concealed phishing emails come as part of spam and currently the inbox is very active. While phishing is often seen as a consumer problem, scams used by phishers are now hurting businesses as well. In this article, we identify various types of phishing attacks and outline some defenses that can be avoided. We first discuss different types of phishing attacks in theory, and then we examine some examples of attacks in practice and common defensesagainst them. We also mentioned new statistics on phishing scams to predict the problem.

INTRODUCTION

Phishing is defined as the fraudulent obtaining and misuse of confidential information from the intended recipient. Phishing attacks are usually carried out via email. An example of phishing; The email appears to be coming from a known website, users' bank, credit card company, email or Internet service provider. Often times, personal information such as a credit card number or password is requested to update the account. With the development oftechnology, the internet and e-mail have become an important part of people's lives.

Unfortunately, the changes brought about by technological advances have also made criminals more adaptable. There are many problems, one of them is theft. A new form of phishing that has become a major security threat is phishing targeting email users. Phishing is the act of sending fake emails and fake websites to users in order to trick users into submitting their personal information and lead to identity theft.A phishing email is sent to many victims' mailboxes and often includes a link. This is to trick into fooling the recipient into believing that the email they received is from a trusted source, so the recipient opens and clicks on a hyperlink provided by that connects them to a fake website where they will eventually delete the Personal Information. Attackers fake in email mail sites can use really good logos and fake websites. We want to emphasize that user education is important in combating phishing, because users who don't know about can run into problems even with the best protection and top-notch stuff. Phishing often uses to find out someone's password or credit card information.

Thanks to the e-mails prepared as if they were coming from a bank or branch, computer users are directed to fake websites. In general, the information stolen by phishing attacks is as follows:

- User ID Number
- User Password and User name
- Card Information
- ***Internet*** Banking Information

FIG 1 (Life cycle of phishing threat)

Types of Phishing Attacks

Phishing attacks usually involve usernames, passwords, social security numbers, passport numbers, credit card numbers, bank account numbers, PIN, date of birth, parent name, etc. targets confidential information such as Phishers can easily target intel, sit from the comfort of their home or hacker's office, and retrieve sensitive information from. Email scammers will register a fake number that looks like a real organization and send thousands of requests. Pseudo-fields often include character changes, such as using 'r' and 'n' side by side to create 'rn' instead of 'm'. Alternatively, they will use the organization's name in the email address's domain (such as shatakshi@domainregistrar.com), hoping that the sender's name will only appear as "State". The subscriber is in the inbox of recipients. There are many ways to detect phishing emails, but as a general rule you shouldalways check email addresses for questions to click on links or download attachments.

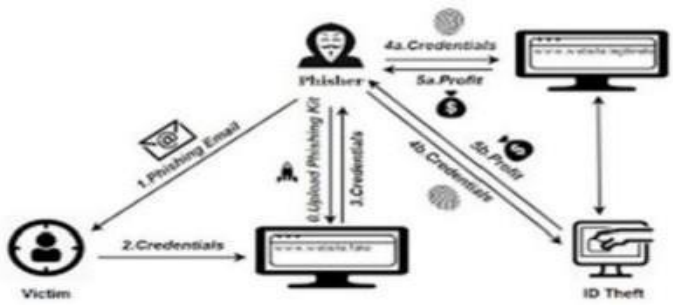

FIG 2 (Email Phishing)

Spear Phishing

There are two other types of scams involving email. The first, spear phishing, describes malicious emails sent to specific individuals. The perpetrators who did this already had some or all of the following information about 4,444 victims:

- Their names;
- Workplaces;
- Business name;
- Email address; and
- Specific information aboutstudies.

One of the most famous hacks in recent history, the hack of the Democratic National Committee, was done with the with the help of spear phishing. The initial attack sent emails containing malicious information to more than 1,000 email addresses. Its success led to another campaign to persuade group members to share theirpasswords.

FIG 3 (Spear Phishing)

Whaling

Whaling attacks more by targeting big bosses. While the end goal of whaling is the same as other phishing attacks, the process seems nuanced. Cheats like fake links and malicious URLs won't work in this case because the criminals are trying to be a high profile person. Fraud involving false tax returns is a more common form of competition. Tax returns are highly valued by criminals as they contain valuable information such as names, addresses, social security numbers and bank details.

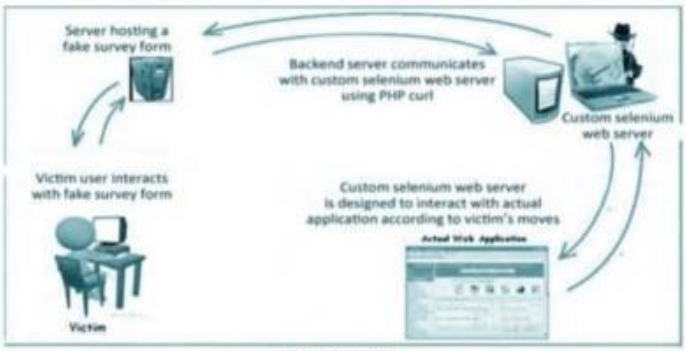

FIG 4 (whaling)

Smishing and vishing

Fraud and phishing through phone calls replacing email as a means of communication. Phishing involved 4,444 criminals sending text messages (with similar content to email phishing) and phishing involved 4,444 phone calls. A scam involving a criminal act as a fraud investigator (from a credit card company or bank) The effect of informing victims that their account has been compromised Criminals require the victim to provide a payment card to verify their identity or to transfer funds to a "secure" account they refer to as the criminal's account. will want.

FIG 5 (Smishing)

Angler phishing

According to the new attack, social media has many offensive ways to fool people. fakeURLs; cloned websites, posts and tweets; and instant messaging (actually phishing) can be usedto trick people into disclosing sensitive information or downloading malware.
Alternatively, terrorists can use information that people voluntarily share on social media to carry out attacks.
In 2016, tens of thousands of Facebook users took the advice they gave in the message.
The message is initiated by the terrorist, who initiated the attack on two levels.
The first step downloads a Trojan horse program containing the malicious Chrome browser extension to the user's computer.
The next time a user logs into Facebook using an infected browser, criminals can steal theuser's account. It can alter privacy, steal data, and spread viruses from the victim'sFacebook friends.

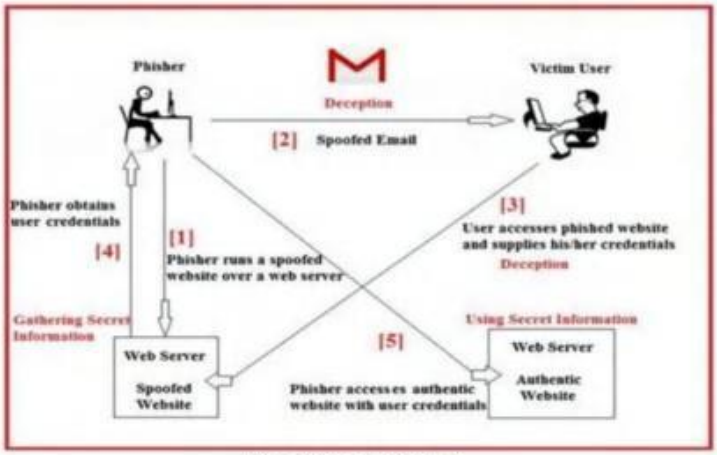

FIG 6 (Angler phishing)

Tools for Phishing Attacks

Nexphisher: Advanced Phishing Tool for Linux

NexPhisher is a phishing tool built for Termux and Linux. Zphisher
Phishing page from the GNU General Public License v3.0. This tool includes 37 phishingpage templates for 30 websites. There are 5 ways to forward including Localhost.

Features: -

- Newest landing page
- New Instagram auto followpage
- Newest export port
- Works on all devices

FIG 7 (Nexphisher)

ZPhisher: Automatic Phishing Tool
Zphisher is an updated version of Shellphish. Source code taken from Shellphish. But I didn' t repeat it exactly. I upgraded
and cleaned
junk files. It has 37 phishing page templates; Including Facebook, Twitter and PayPal.

Features:-

- Last Page
- New Instagram Auto Follow Page
- All Kinds of Editing
- Suitable for Beginners


FIG 8 (Zphisher)

Pickl3 : Windows Active User Credential Phishing Tool

Pickl3 is a Windows Active User Credential Phishing Tool. You can complete Pickl3 and phishing for user credentials. Today, there are about 200 sandbox search methods published. In particular, the sandbox for analysis in the Hypervisor layer is not affected by this detection process. But the sandbox isn't very good at user interaction yet. You can benefit from using Pickl3 on malware you create. For example, the target of red teamwork today is often end users, the target end user has a password, unless your target user enters the correct password, can prevent your malware from running and bypassing sandbox management. However, you'd better prevent your malware from running with administrative privileges when the first is installed. Because in the sandbox, malware is usually analyzed according to the rules.

FIG 9 (Pickl3)

Evil SSDP: Creates a rogue UPnP device to phishing for credentials: -

Evil SSDP responds to SSDP multiple discovery requests, acting like a UPnP client. Your fake device will magically appear as in Windows Explorer on a computer on your local network.

Users trying to unlock the device are presented with a phishing page setup. This page can upload more than SMB encrypted images allowing you to capture or export NetNTLM messages/responses. templates are also provided to capture the correct certificate by verifying facts and data entry, and it's quick and easy to create your own custom templates.

This does not require completion of existing credentials and also works on networks where Responder attack is protected by not using NETBIOS and LLMNR. Any OS or application that uses SSDP/UPNP can be targeted, but the is currently targeting Windows 10 with most guns.

As an additional feature, the tool can also detect and use the zero-day in the space of Windows 10's XML parsing engine.

If it detects a weak device, it will warn you in the UI, then raise your SMB report or delete the XML External Encoder (XXE) attack file without affecting user interaction.

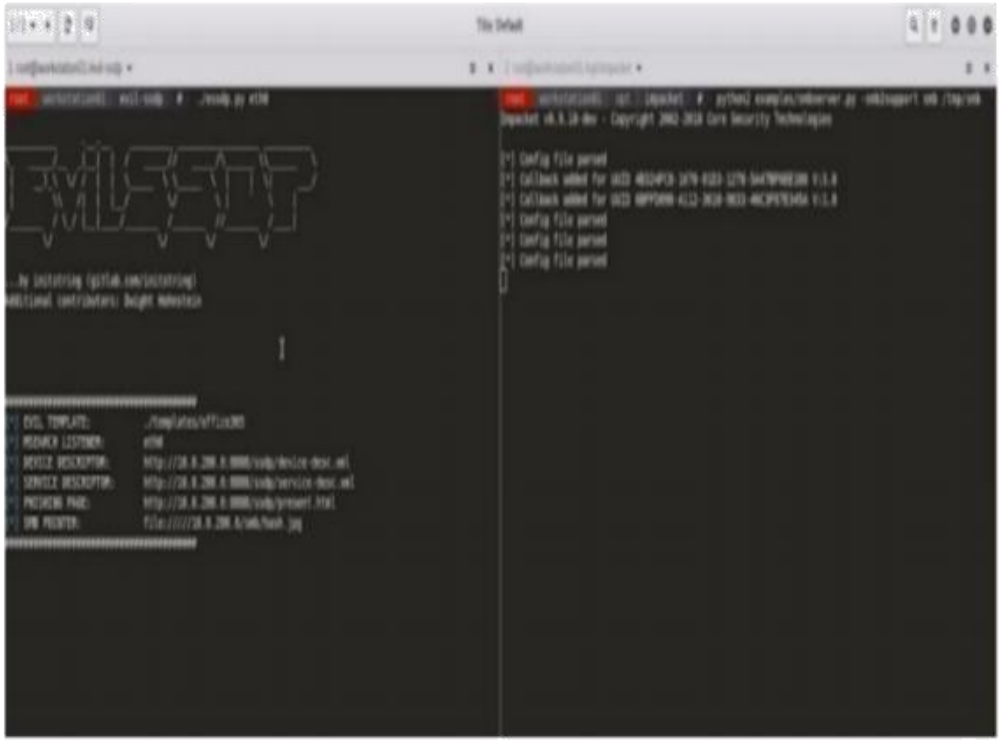

FIG 10 (Evil SSDP)

ShellPhish: phishing tool for 18 social media

ShellPhish is a phishing tool for 18 social media such as Instagram, Facebook, Snapchat, Github, Twitter, Yahoo, Protonmail, Spotify, Netflix, Linkedin, WordPress, History, Steam, Microsoft, InstaFollowers, Atlantis,Pinterest.

It is illegal to use this tool to attack the target without the prior consent of both parties. It is the end user's responsibility to comply with all local, state and federal regulations. The developer takes no responsibility and assumes noliability for any misuse or damage to caused by this program.

FIG 11 (ShellPhish)

Phishing Scam Statistics and Analysis

According to the FBI, phishing is the most common type of crime in 2020 – the frequency of phishing incidents nearly doubled from 114,702 in 2019 to 241,324 in 2020 to According to the FBI, there were 4,444 phishing scams reported in 2020, an11-fold
increase compared to 2016. According to Verizon's 2020 Data Protection ResearchReport
(DBIR), 22% of crimes in 2019 involved phishing. Although this is down 6.6 percent from last year, it remains the "the most common threat" that can lead to crime.

This is 30% higher than the world average and 14% higher than last year. Want to learn how to prevent attacks? Visit this page to learn about
BEC protection. ESET's Threat Report shows that malicious email detections increased by 9% between Q2 and Q3 2020. Previously, there was a 9% increase from the first quarter to the second quarter of 2020.

How Phishing Attacks Work

Hackers increasingly rely on stolen credentials through phishing attacks to gain accessto
systems and data. This is one of the reasons why malware-related crimes have decreased by over 40%. In 2019, PDFs and Microsoft Office files are the distribution tool of choice for cybercriminals today, according to Sonic Wall's 2020 Cyber Report. From where? Because this information is trusted throughouttoday's workplace.

When it comes to targeted attacks, 65% of active groups rely on spear phishing as their primary infection. This was followed by websites (23%), Trojan software updates (5%), web server exploits (2%), and data storage (1%). Of the 4,444 phishing attacks, 96% came via email. Another 3% came from malicious websites and only 1% came from phone calls. We call it Phishing when done on the phone, and Phishing when done in text messages. According to Symantec's 2019 Internet Security Threat Report (ISTR), the top fiveattacks related to email marketing vulnerabilities (BECs):

1. Urgent
2. Request
3. Important
4. Payment
5. Warning

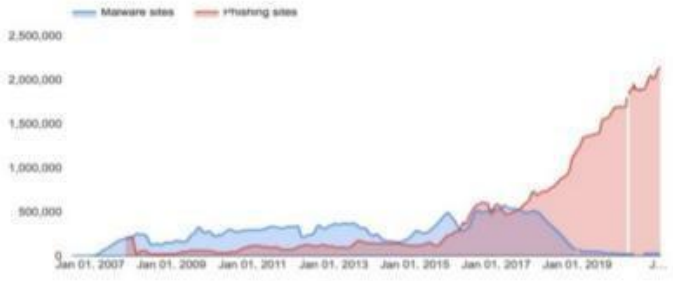

FIG 12 (Analysis of phishing)

How Cybercriminals Are Abusing Virus-19 In 2020

As millions of people struggle to learn the truth about worldwide epidemics from world leaders, the ethical cybercrime community is seeing its time. Phishing emails, "Do you have Covid-19 in your area?" and "News from the World Health Organization". Our main target in COVID-19-related phishing email has been revealed.Scammers focus their efforts on:

1. Fundraising for fake charities
2. Credential Collection
3. Malware distribution

Criminals are taking the opportunity to use fake logins and download the increasingly popular web chat Skype, one of which is really surprising struggles how obscure most ofthem are. Europol's report IOCTA 2020, "COVID-19 shows how cybercrime - at its core - has remained the same, but criminals have changed the description. 8 This reflects F5 Labs' previous findings that the Mirai botnet was lazily cloned to contain information about COVID-19. For UK ICOs, the number of phishing incidents reported per quarter in 2019 and 2020 averaged 289, while the latest figures released between April and June 2020 show a drop of, with only 185. F5 Security Operations Center (SOC), It showed a similar trend with the initial general phishing statistics following last year's model, but dropped to March-April, peaking in early 2020, and showed another significantincrease in Spring and early. write (see Figure 12)

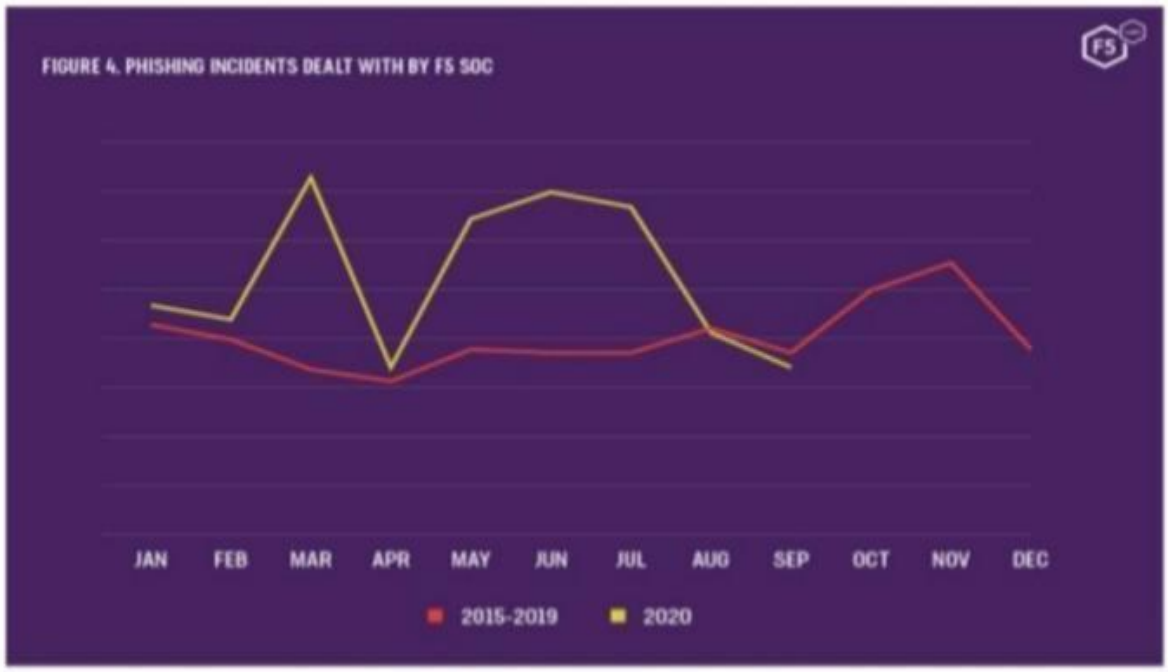

FIG 13 (Analysis of covid phishing)

In SOC data from July to September, we found 320 malicious characters using special words "covid" or "corona" in their URLs. Many other malicious sites use deliberate errors to attack or simply use irrelevant names. We can also search for specific words or values in HTTPS certificates using the Certificate Transparency engine. When the Pandemic was announced in March, it's not surprising that certificates created with the words "covid" or "corona" peaked at 14,940 (see figure 13) 4,444 Security Expert content, but if these patterns show us everything, those who want to know are end users - our staff. and our customers -. Phishing awareness training should teach the message that attackers can jump into the new model.

Users should be extra cautious with emails, voicemails, and text messages that appear to relate to general topics in advertising or popular culture.

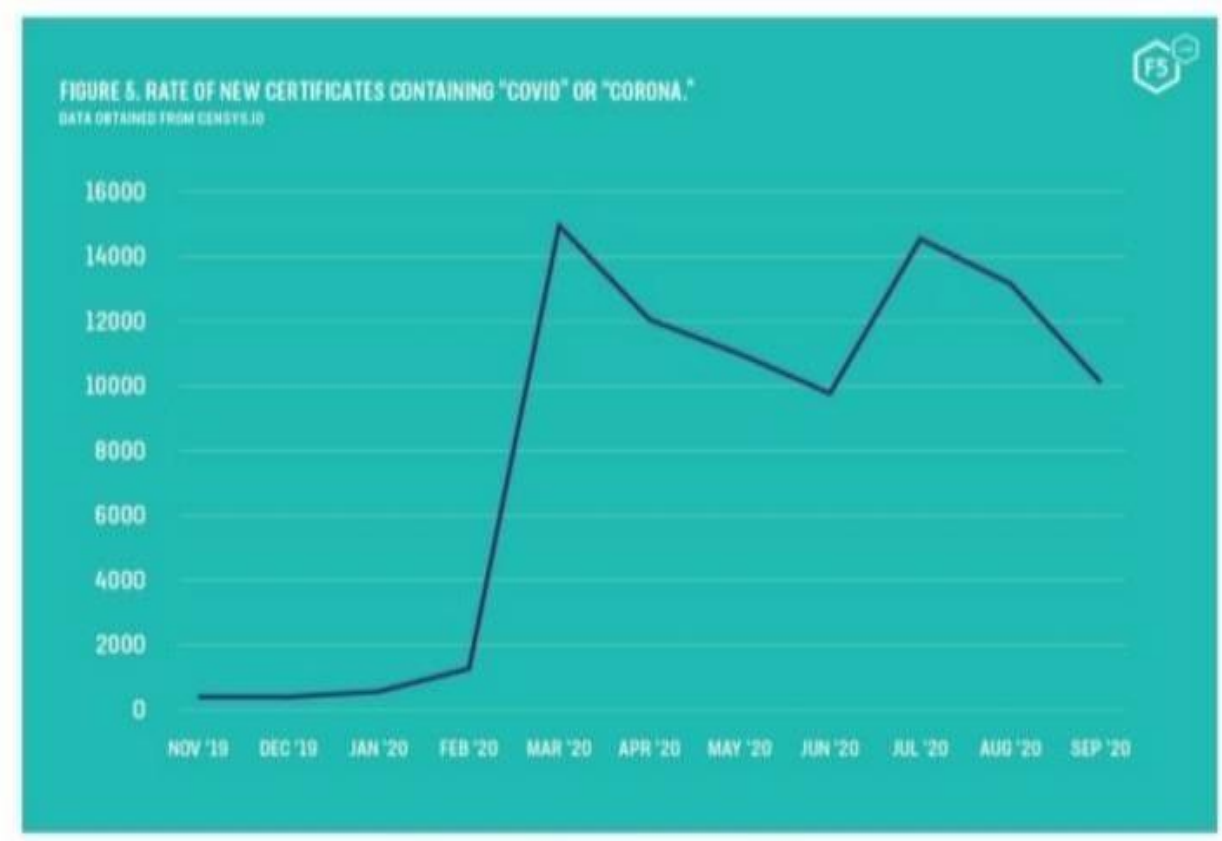

FIG 14 (Analysis of covid phishing)

Protection Against Phishing Scams

There are several steps a user or organization can take when dealing with spamand phishing emails. Here are some common measures that can prevent phishing at the user level:

1. Do not click hyperlinks in phishing emails as they will not take the user tothe site properly.
2. Use appropriate and up-to-date security software such as antivirus, anti-spam, and anti-spyware.

The signature list of this software is constantly updated. This strengthens the user's computer against attacks. While

anti-spam software can create bugs, it's better to flag suspicious emails and store them somewhere (locally) for quick review at

than simply deleting them. Keep the browser and

operating system software up-to-date with all updates and security updates. A security update is released when there is a critical vulnerability that an attacker could exploit.

3. Do not download free software from unknown sources as some free downloads are hidden or have built-in Trojans.
4. Use a strong firewall, many operating systems now have built-in firewalls.
5. Before entering personal information, look for the "https" protocol in the address bar at the bottom of your browser and the lock symbol in the status bar.
6. Be aware of internet scams and act accordingly.
7. The Anti-Phishing Toolbar works with Internet browsers to identify phishing sites and alert users if the site is suspicious during browsing.

Here are some steps companies can take to protect themselves against phishing:

- Train your employees and use simulated phishing scenarios for training.
- Viruses, spammers, etc. Activate the spam filters that detect it.
- Keep all systems up to date with the latest security features and updates.
- Install Antivirus, schedule signature updates and monitor antivirus status of all devices.
- Create security policies that include but are not limited to password expiration andcomplexity.
- Submit a web filter to block malicious websites.
- Encrypts all important company information.
- Convert HTML emails to plain text or disable HTML emails.
- Requires encryption from phone operators.

Tools to Prevent Phishing Attacks

Brand Shield Anti-Phishing

Brand Shield Anti-Phishing focuses on brand protection and trust. Its toolsmonitor social media and other contact information to identify phishing sites or fake brands (even to search for your company logo) and respond to requests. Please remove these malicious sites and add them to various anti-phishing blacklists.

RSA Fraud Action

RSA Fraud Action also detects and mitigates phishing sites that harm your business. While RSA scans for fake sites, it also uses its partner network to detect and disable fake sites through blocking and blacklists. RSA Fraud Action value based on attack volume (purchased in extraction pack).

Avanan

Avanan is one of many SaaS platforms that improves the security of Office 365, G Suite, and other software. Since Avanan is cloud-based and uses an API to connect to your Office 365 or G Suite for example, it is very useful to set up and also monitor for example user and platform settings, not just email. Document pairs in cloud storage. Avanan's anti-phishing suite starts at $4 per user per month, which includes email filtering, account takeover protection, and security settings.

Barracuda Sentinel

Barracuda Sentinel is another SaaS tool that is tightly integrated with Office 365 (G Suite is not supported). Barracuda monitors incoming email and identifies accounts that may have been compromised, fixes those accounts by identifying malicious emails sent to other internal users and removing, notifying people that they're accepting externally, closing accounts, and eve n calls are made by Inbox. There may be calls from the Inbox policies created. Malicious users Barracuda Sentinel is licensed per user or per active mailboxes.

Iron Scales

Iron Scales enhances your existing email security by combining AI-based authentication and human interaction (via notifications) to quickly respond to request attacks when the ban isn't a good thing. Administrators can also get intelligence about the nature and extent of threats, including how many mailboxes were targeted and how many users shared emails. IRONSCALES also provides tools for simulation/simulation and user training. Prices for IRONSCALES start at $5 per mailbox, with variable rates for all large businesses.

RESULTS AND EVALUATION

Email is one of the most important forms of communication. The increase in spam causes crashes, lost productivity, phishing is a big problem for the information world. Spam volume is increasing by per year. Therefore, spam filtering is an important, valuable and difficult problem. Due to the rapid spread of phishing attacks, many defenses have been developed.

Because the design of fake web pages is similar, it is sometimes difficultto distinguish between real and fake web pages.

An increasing number of email users are processing spam. Available server-side and client-side antispam filters are used to detect different types of spam. However, some good ideas have been created by adding spam content such as digital images, pdf's and word. This extension makes it so current

technology doesn't work.

Most of the operational strategies presented in this study offer ways to prevent spam based on data mining techniques to classify spam and phishing emails. The effectiveness of this process has been evaluated onmany systems.

CONCLUSION

In this article, we analyze various aspects of phishing attacks, both theoretically and practically. We briefly describe some of the attacks on business today and show some of the defenses has against these attacks. We also mention some new statistics to estimate the increasing phishing spam problem. We believe cybersecurity threats are nothing new, and since the dawn of e-commerce, businesses have had to deal with threats of all kinds. As the business world evolves to keep pace with new technological advancements, fraud is also used to present new technological opportunities.

Therefore, our article offers recommendations for preventing phishing, in the hope that with a better understanding of Internet fraud in general and phishing in particular, many of the dangers of the thief can be eliminated.

REFERENCES

[1]. https://www.tessian.com/blog/phishing-statistics-2020/
[2] . https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams
[3] . https://www.cybervie.com/blog/phishing-attack-using-kali-linux/
[4] . https://kalilinuxtutorials.com/shellphish-phishing-social-media/
[5] . https://www.akamai.com/us/en/products/security/enterprise-threat protector.jsp
[6]. https://www.csoonline.com/article/3575080/9-top-anti-phishing-tools-and-services.html
[7] . https://www.google.com/
[8] . https://www.youtube.com/
[9]. https://www.geeksforgeeks.org/
[10]. https://www.kali.Organization/
[11]. https://github.com/jaykali/shellphish
[12]. https://github.com/wifiphisher/wifiphisher
[13]. coresecurity.com/blog/how-phishing-has-evolved-and-thre-ways-preventattacks#:~:text=Geli şmeler%20are%20to,moment%20you% 20land%20on%20%20made%20.