INTERNATIONAL MULTIDISCIPLINARY JOURNAL FOR RESEARCH & DEVELOPMENT
SJIF 2019: 5.222 2020: 5.552 2021: 5.637 2022:5.479 2023:6.563 2024: 7,805
eISSN :2394-6334 https://www.ijmrd.in/index.php/imjrd Volume 11, issue 03 (2024)

MODERN PHISHING ATTACK PROTECTION RESEARCH OF METHODS

Turdimatov Mamirjon Mirzayevich

Associate Professor of the "Information Security" Department of the Fergana Branch of the Tashkent University of Information Technologies named after Muhammad al-Khorazmi

Otajonov Temurmalik Baxromjon o'g'li

Student of "Information security" department of Fergana branch of Tashkent University of Information Technologies named after Muhammad al-Khorazmi

ANNOTATION: This article is devoted to such questions as what are phishing attacks, who they are, their different forms and how to avoid them, which concern the whole world. As a solution to the problem, methods to bypass scammers, phishing techniques and characteristics that you need to know, and anti-phishing methods to use and eliminate phishing are recommended.

Keywords: Phishing, phishing attacks, anti-phishing methods, scammers, phishing methods, secure connection, itdefender, Norton anti-phishing, user-friendly interface.

Introduction, As we all know, is around the world these days attacks is becoming popular. Phishing on the Internet of fraud one type being his purpose of the user confidential using data (login/ password). opportunity have to be This is now wide spread out social engineering from schemes one is considered Phishing the most wide spread out example as of the victim electron to the mail sent official information bank in the form of or payment system fake message show can Such electron mail messages usually official to the website similar and personal information Demand who does in the form of to a fake web page the link own into takes

This is a phishing scheme according to user each how famous company by conducted in the lottery winner that it was about the message take can External on the other hand , this electron message of the company high official from employees one on behalf sent to looks like This phrase English " service " in the language for " service " . the meaning that is , social of engineering this in type hacker corporate network or electron mail through to the company appeal done increases . Most of the time hacker himself technical service pointer as introduced , technical of the employee the work in place problems eliminate " help " in achieving he says . Technician to " eliminate " the problem on time in target person commands to perform or of the victim to the computer different different programs to install encourage done is increased .

Come on, what's your business? You do not need to confirm your account information from your requesting bank sms message acceptance did you None when to him don't touch This Phishing is an attack .

Phishing password) - internet fraud type, his purpose - of users personal confidential information to the hand drop off is considered To this passwords, credit cards numbers, bank accounts and another confidential information stealing includes[1-3].

Phishing this banks, providers, payment from systems and another immediately personal to the recipient for any reason that comes in the mail from organizations from fake notices to deliver/update data consists of will be Various reasons display possible These are of information lost, in the system malfunctions and others it can.

Phisher attacks are becoming increasingly sophisticated, social engineering methods are being

used. But in any case, the client to scare she is own information disclosed to do for serious reasons thinking to find movement is being done. Usually, in messages popisas in the eye is held for example, if the user does not meet the requirements specified in the message it is said that it will be closed ("if you send your information for a week if you don't your your account closed will be placed"). Interesting side, most of the time user own confidential information disclosed to do need because of anti-phishing the system improve necessity they show ("if yourself from phishing If you want to protect yourself , check out this app and enter your login and password enter").

Phishing sites usually do not live long (on average - 5 days). To fishing because anti-filters learn information about new threats much faster phishers have to register new and new sites all the time. Theirs and their appearance remains unchanged - those scammers own their sites to forgery trying official in the site view remains.

The targets that attract the most attention of phishers are Ebay auctions and PayMi payment systems is considered Whole the world banks too harm sees Fishers attacks random and purposeful will be Random "at risk" of attacks done is increased. Ebay auction such as the most big and famous objects are attacked - because the random recipient has an account there very likely to be. In the second case, which bank is the recipient of fraudsters, the payment system, the provider, will find out that the site is used. This method phishers for much complicated and a lot time Demand enough but to the hook to hang possibilities bigger.

Problem The solution is from fraudsters keep methods .

Phishing technique and characteristic. Fisher's technologies improving is going For example, to phishing near has been - Farming concept appear is happening This too of users personal information to the hand to drop the goal by doing put, but not by mail, but directly through the official website to the hand dropper fraud. Farmers DNS on servers legit websites digital addresses fakes with they exchange As a result user are redirected to scam sites. This type of fraud is even more dangerous, because forgery almost knowing get possible it's not. Phishing own into as reliable seemed bank to questionnaires similar to from places sms message comes but the user confidential information intended for collection will be This done increase for them link will be and that's it through they are steals your information from the website. By this the user is reliable It thinks it's going to a website, but it ends up being a scam. The user takes the email to the website and the company has mastered the appearance collecting data get for food as uses

The most commonly used attack vector is a fake to the customer on behalf of the company email message sends and that's it through she is about all information to get succeeded.

From Phishing protection methods of the following consists of:

- possibility until your password often replace stand up;
- each always account in your number financial your money checking stand up;
- financial to your reports suspicious account visit when ordered alarm;
- procedure adding pour;
- if your account your number with suspicious account number connection happen if immediately suspicious account number close must

How do criminals work?

They register an e-mail address similar to the address of an online store, bank or other legal organization. For example, instead of the real address of the Supershop store, they use mail@supershop.ru mail@supersshope.ru . Sometimes fraudsters do not bother with such an address, because it is often hidden from the user's eyes. They just show the store name as the sender's name - the receiver will see it. It is easy to check the change, but everyone noticed that the usual design of such an online store has changed a little, but this did not worry him. It did not occur to him to carefully check the address bar of his browser [4, 5].

What to check when entering the site

Address. It is good to bookmark the addresses of banks, government offices, favorite online stores and other online services. You can enter the address manually, but you need to be careful - sometimes even a mistake in one character will lead you to a duplicate phishing site.

Always check your browser's address bar. Sometimes you can be on a phishing site even when you are browsing from one page of a portal that you know to another.

Connection security. If you want to enter personal data or card information or make a purchase through the site, its address must have https and a closed lock symbol in front of it . The letter S and the closed lock mean that the connection is secure: when you enter data on the site, it is automatically encrypted and cannot be intercepted.

A secure connection is a mandatory requirement, but not sufficient. Hackers cannot connect to such a site and find out your information. But this is no guarantee that the site itself was created by a legitimate company. Recently, criminals have also managed to obtain security certificates for their websites.

Criminals create online resources with the simple goal of collecting confidential information. Therefore, in most cases, they do not think about the structure and design of the site. Unstable layout, spelling mistakes, broken sections and links are clear signs of a fake.

Mistake №4: Paying through unsafe pages

The fake "online store" offered Nikolai to make a "test payment" by entering the code on the back of the card and the code in the SMS message directly on its website. Nikolai did not notice that he was not redirected to the payment system page to make the payment.

What you need to know

After entering your card information, the store's website should direct you to the gateway of your card's payment system. This is a separate, secure page; the online store cannot access the information you enter.

Payment gateways connect the cardholder with their bank when making a payment. The bank sends a one-time code to the customer via SMS to confirm the transaction. And only after the buyer enters it, the payment is made.

Do not tell anyone the secret codes of the bank - check that the SMS information matches the transaction details. If everything is in order, enter the code in the special field on the payment page. If not, call the bank.

Mistake №5: Using the same card for all payments

Nikolai paid in online stores with a salary card. Now he will have to order a new one. At the same time, the bank reissues it, he will only have access to the money balance in the account at the bank branch.

What to do

it is better to have a card . Before payment, you need to transfer money to him and deposit the amount you want to transfer.

Some banks and electronic payment systems (electronic wallets) offer virtual cards - they contain details, but they are not available in plastic form. Sometimes you can even create virtual cards that are valid for a single online purchase.

Phishing attacks can be a serious threat to your online security. Here are some effective ways to protect yourself from phishing:

Be careful with email: Phishing often happens via email. Be wary of unsolicited emails, especially those that ask for personal information or require urgent action. Avoid clicking on links or downloading attachments from suspicious or unknown senders.

Two factorial enable authentication (2FA) : possible Enable 2FA as long as possible . This is your password addition respectively mobile to your device sent unique code such as second confirmation shape Demand to do through addition safety level increases [6,7].

Qualification methods . yourself educate : the most latest phishing methods and common red flags about informed be Victims manipulation to do for attackers by applied social engineering tactics informed be yourself online of security the most good practices about regularly respectively teach

To fishing against from tools use : known phishing websites determination and blocking to do help giving authoritative antiphishing programs or browser extensions install it and use . This tools the internet seeing on the way out addition protection layer provide can

Get rid of it reach methods

Protect you from phishing attacks protection to do help giving one how much reputable anti-phishing software there is . Here it is one how many celebrities :

Bitdefender

Bitdefender cyber security according to wide comprehensive solutions , including phishing against features offer is enough It is different online from threats , including phishing attempts advanced protection provides .

Website : https://www.bitdefender.com/

Norton antiphishing

Norton AntiPhishing is NortonLifeLock product Phishing websites determination and blocking to do help will give . He is famous web browsers with unite and real time mode from phishing attempts protection does

Website : https://www.nortonlifelock.com/

McAfee WebAdvisor

McAfee WebAdvisor is a phishing and another online from threats protection doer browser extension . It websites suspicious actions for checks , harmful links blocks and potential Dangerous to sites visit when ordered warnings will give .

Website : https://www.mcafee.com/

Conclusion . User about message to give and feedback : Some anti-phishing software to users suspicious websites about message to give or they are face coming potential phishing attempts about thought notice enable will give . This report mechanism known phishing sites data base improve for user from the data use through software of supply accuracy and efficiency to increase help will give .

User for comfortable interface : To fishing against of programs most of them to users comfortable interfaces with created settings settings , warnings and warnings to see and addition to functions access makes it easier . Program protection level and to be determined need of phishing attacks types adaptation for setup options offer to do can That's it to emphasize ok , antiphishing software supply many phishing attempts determination and blocking in doing efficient to be possible , but be careful to be and safe to see methods compliance to do important Software supply regularly updated stand up and electron mail additions and from links caution to be such as good safety habits action from doing phishing attacks your protection more strengthens

REFERENCES

1. Practical Malware Analysis. Copyright © 2012 by Michael Sikorski and Andrew Honig .

2. Ganiyev SK, Karimov MM, Tashev KA " Information security ", "Science and technologies " publishing house , Tashkent 2016 .

3. Ganiyev SK, Karimov MM, Tashev KA Information safety . Information and communication systems safety . High students of the educational institution for intended . " Alokachi " 2008 .

4. SKGaniyev , AAGaniyev , ZTXhudoykulov . Cyber security basics : education manual . - T.: " Alokachi ", 2020 y.

5. Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code, First Edition (2010): Michael Ligh , Steven Adair, Blake Hartstein , and Matthew Richard. ISBN-10: 0470613033, ISBN-13: 978-0470613030. Wiley Publications.

6. Malware: Fighting Malicious Code: Ed Skoudis and Lenny Zeltser (2003). ISBN-10: 0131014056, ISBN-13: 978-0131014053. Prentice Hall Publications.

7. S.K. Ganiev, Z.T. Khudoykulov, N.B. Nasrullaev. Basic cyber security:

uchebnoe posobie, -T.: "Neighborhood and family publishing house", 2021. -240 p.