Research on Anti-phishing Strategy of Smart Phone

Lei Chen
China People’s Police University Langfang 065000, China
E-mail: chenlei4534 @163.com

Abstract: Phishing is a fraudulent method of online identity forgery. With the development of mobile Internet and the popularity of smart phones, many phishing methods and forms for smart phones appear. Mobile phone phishing has the characteristics, such as strong allure, chaotic information, clear target, short attack time and dynamic conversion of attack sources. It steals users’ privacy information and even endangers users’ fund security by creating fake networks, fake base station SMS phishing, sending phishing emails, malicious code attacks, malicious WiFi phishing attacks, etc. Some specific measures against mobile phone phishing are put forward in this paper, such as installing and updating mobile phone security software, using various anti-spam technologies, paying attention to personal information disclosure of social platforms, carefully linking WiFi, and preventing mobile payment traps.

1. Introduction
Phishing is a fraudulent method of online identity forgery. It often uses fake websites or fraudulent e-mails, uses malicious software and other technologies to obtain users’ confidential information, and conducts Internet fraud activities. Fraudsters usually disguise themselves as online banks, online retailers or credit card companies to deceive users.

With the development of mobile Internet and the popularization of smart phones, mobile phone surfing is very common. Phishing through mobile phones is increasing rapidly and in more diverse forms.

2. Characteristics of Mobile Phone Phishing

2.1 Strong allure
Phishing attackers often use words such as “winning a prize”, “free” and “cash gifts” to cheat users to fill out forms, so that they can steal users’ personal information and then cheat their money.

2.2 Chaotic information
Fake websites, fake emails and various information used by phishing attackers can mix fake information with real information, thus attracting many users. Phishing attackers often use virus technology to attack network servers, users’ computers and anti-spam filters to release their phishing information in order to obtain money.

2.3 Clear goal
Phishers are mainly aimed at financial online services, e-commerce and other industries, and usually carefully select some users as targets according to the stolen user information to improve the success rate of phishing as much as possible.
2.4 Short attack time
Phishing attacks are usually a relatively short period of time, only a few hours, a few minutes or even more than ten seconds. A short attack will make phishing difficult to detect in time.

2.5 Dynamic conversion of attack sources
To avoid detection, phishers often change the Web server they are using quickly. They also often use some vulnerabilities in the server to secretly install information on the server site. When fraud information is discovered and deleted, the attacker will go to other server sites.

3. Common Technical Means of Mobile Phone Phishing

3.1 Creating fake websites
Phishers often disguise themselves as online banks, online securities trading platforms, well-known e-commerce websites, etc. to induce users to enter account numbers, passwords and other information, and then transfer users' funds through the real online banking system and online trust system.

3.2 Sending phishing short messages with pseudo-base stations
Phishing attackers use fake base stations to copy the official service numbers of telecom operators or banks and other institutions, send phishing short messages to users, spread phishing websites, and lure users to be cheated by means of winning big prizes, bank arrears and other means, eventually revealing personal information.

3.3 Sending phishing mail
Phishing attacker lures or cheats the user to fill in the financial account and password by adding a phishing message to the sent mail and informing the user of the need to change some personal sensitive information in an official capacity, etc., so as to cheat the user's information and money.

3.4 Exploiting malicious code attacks
Vulnerabilities in mobile phone systems and APP will lead to phishing attacks on users. Most commonly, attackers implant Trojan horse programs into users' mobile phone systems. When a user makes an online transaction, the Trojan will record the account and password entered by the user and send it to the attacker.

3.5 Fishing with malicious WiFi
At present, many businesses or public places provide free WiFi to facilitate users to surf the Internet on the move. The simplest way for an attacker is to provide a free WiFi similar to that of a merchant. Once a mobile user accesses, the attacker will forward all the data packets on the Internet through hacker devices and steal their key information.

4. Anti-mobile Phishing Measures

4.1 Installing and updating software in a timely manner
There may be loopholes in the mobile phone system. Users should turn on the system to automatically detect and update settings, upgrade the system in time, repair loopholes and reduce risks. Install and update the security protection software in a safe environment, turn on the harassment interception function, effectively intercept spam and mobile phone viruses, turn on the financial protection and account protection functions, regularly check and kill viruses and clean up garbage.

4.2 Using various anti-spam technologies
At present, the mainstream anti-spam technologies mainly include filtering technology, SMTP-based improvement technology, and security management technology of mail servers. Don't randomly open mails and attachments of unknown origin, and don't randomly click on unknown links in mails.
4.3 Paying attention to the reliability of access
Do not visit websites of unknown origin. Download the official version of the APP from a regular APP store or official website to ensure that the downloaded app is safe and reliable. When installing applications, pay attention to the types of permissions that are open and not open to some unnecessary permissions that have nothing to do with the application, so as to prevent some illegal elements from bundling and installing some junk software and invading mobile phones through viruses or Trojan horse programs on the software.

4.4 Bewaring of personal information disclosure of social platform
Some users like to publish information and photos through social media such as WeChat, microblog, Facebook, etc. It is easy to expose personal preferences, social circle, location, economic status and other private information. It is easy for criminals to gain users' trust through such information, and to post or reply on these social platforms to lure users into phishing websites.

4.5 Being careful of connecting WiFi
When the mobile phone is automatically connected to WiFi, criminals may monitor all the operation behaviors of the user on the mobile phone through some technologies, thus stealing the user's account number, password and other information. Therefore, when accessing or using online banking or e-commerce applications with transaction nature, users should try their best to use the data provided by operators to access the Internet and avoid using public WiFi; When you do not use WiFi connection at ordinary times, you should close the mobile phone wireless network to avoid privacy disclosure. Do not connect to WiFi of unknown origin in public places, especially WiFi without password.

4.6 Bewaring of mobile payment trap
Now, it is very convenient and widely used to pay through mobile phone apps such as WeChat and Alipay. Phishers often steal their information when users pay through trojan horse invasion, which seriously affects the security of funds. Therefore, when paying by mobile phone, one should be alert to the payment environment and not make mobile payment at will when connecting to the public network. The mobile phone payment password should be set as complex as possible and changed regularly. Timely upgrade payment software to improve software performance and ensure timely plugging of software vulnerabilities.

4.7 Paying special attention to online transactions
Users must pay attention to the following points when conducting online transactions: check carefully to avoid errors when entering the business network address in the browser address bar. Do not click an unknown link to enter the website. The passwords used by commercial organizations to log on to websites should be more complicated and should be mixed with letters, numbers and special characters to avoid using the same passwords on different websites. Do a good job in transaction records, regularly check the history of transaction details, and regularly print statements. If an abnormal situation is found, the user should contact the commercial organization immediately. Correctly use digital certificates issued by commercial organizations and avoid using online trading systems on public computers. Use hardware equipment such as U-shield to ensure the security of network transactions. To enhance vigilance against abnormal dynamic changes, call the customer service hotline service mechanism immediately if risks are found, and modify the transaction password or report the loss of bank cards according to the suggestions of customer service personnel. When using related APP transactions, it is also important to pay attention to downloading ways and upgrading in time.

4.8 In-depth study and strict supervision
In order to effectively identify and defend phishing, we should conduct in-depth research on the source,
implementation approach, implementation process and results of phishing, so as to provide technical
basis for curbing and cracking down on phishing, and apply the research results to commercial
organizations in a timely manner to improve their safety level. As the functional department of
network security investigation and management, the public security organs should also improve the
level of information, perfect network standards and speed up the construction of new network
investigation technologies. We will step up penalties for phishing and urge relevant departments to
enact specific laws and regulations with operability according to the characteristics of phishing
violations. Do a good job in publicity, let the public understand the forms and harms of mobile phone
phishing, and mobilize the power of the masses to build a national regulatory environment, not to give
illegal elements a chance8.

5. Conclusion
With the development of mobile Internet and the popularity of smart phones, phishing platforms are
gradually developing to mobile clients. By analyzing the characteristics and main methods of mobile
phone phishing, some practical defense measures are put forward. In practical application, only by
using various technologies comprehensively can complementary advantages be realized and good
results be achieved. Nowadays, network security has become an international problem. Only by
continuously improving various technical means and strengthening supervision and management can
network security be guaranteed to the maximum extent.

Fund Project: National education information technology research topic “Research on virtual
simulation war room and teaching practice based on police big data”(No:186140038); Hebei
provincial higher education teaching reform research and practice project “Research on training mode
and teaching practice of police big data application specialty under the background of new engineering”
(No: 2018GJJG450); Hebei provincial key research and development program project “Research on
network anti-terrorism and crisis management mechanism based on social media” (No:18210706).

References
[1] Phishing https://baike.so.com/doc/5351713-5587171.html
[2] X.N. Wang and J.G. Han 2018 Research on security hidden danger and preventive measures of
smart phone in information age Information and Computer 14 pp 211-213
[3] X.C. Pan and M. Zhang 2017 Threat analysis of phishing attacks in dark mobile bank Information
Security Research 3 p 256
[4] Y.F. Chen 2017 Security risks of smart phone and preventive strategies Information Security
Research 13 pp158-160
[5] D.J. He 2015 Security risks and preventive measures of smart phone phishing Prospect of Science
and Technology 29 p14
[6] Y.R. Huang, G.S. Liu, K. Meng and N.S. Cai 2018 Research on multi-features phishing detection
algorithms Computer Applications and Software 5 pp 264-268
[7] H.D. Huang 2018 Security threat and countermeasure of smart phone on mobile Internet Digital
Communication World 11 p129
[8] M. Yang 2012 Analysis of phishing methods and research on countermeasures Network Security
Technology and Application 9 pp22-25