International Journal of Security and Its Applications
Vol.9, No.1 (2015), pp.1-10
http://dx.doi.org/10.14257/ijsia.2015.9.1.01

Phishing Sites and Prevention Measures[1]

Zhou Fu-an

(Beijing Technology and Business University)
netzfa@163.com

Abstract

With the growing number of Internet users in online transactions, the number of phishing sites is also increasing rapidly, the threat of malicious attack front is extended, the means are ever-changing, which gives great economic losses to China's Internet users and businesses, and caused a serious impediment to online financial services and the healthy development of e-business applications. Facing of the growing phishing epidemic, the initiative alone to enhance awareness of Internet users to avoid "phishing" is not enough. This paper analyzes phishing sites based on deception trick, focusing on the Internet user side, made several recommendations to strengthen their resistance to phishing sites.

Key words: *Phishing sites; prevention; measures*

Phishing sites scam is one kind of online fraud, refers to defraud behavior to get user accounts, property, and the file by false web site. "Interaction" is one of the features of phishing sites scams, firstly is the cheater tricking users to access web site, and then is the operations activity such as the user to view and access the web site, cheat by user filling form, get the user account, password, and other information. Without the user response, phishing site fraud will not be success. But in the situation of network users lacking basic safety consciousness and awareness, phishing site has a very large living space. As the technology development used by the phishing site, many internet users with many years online shopping experience are caught in a trap of phishing sites.

1. Phishing Site Overview

1.1. The Concept of Phishing Sites

So-called "phishing" is one kind of network fraud, refers to the criminals use of a variety of means, fake real website URL and page content, or use a loophole in the real web server program insert a dangerous HTML code in some of the web page in site, in order to defraud the user bank or credit card numbers, passwords and other private information.

1.2. The Classification of Phishing Sites

According to using different methods to entice users to visit phishing websites, phishing websites can be divided into passive access type phishing site (ordinary phishing site) and taking the initiative to attack phishing site (special phishing website).

1.2.1. Passive Access Type Phishing Site (Ordinary Phishing Site): Passive phishing access type refers to a phishing site after completion of the erection, first of all, let users

[1] This paper is supported by the scientific research fund project launched by the young teachers of Beijing Technology and Business University in 2102Project No. QNJJ2012-12
This paper is supported by students' scientific research and entrepreneurial action plan project of Beijing Technology and Business University in 2013

ISSN: 1738-9976 IJSIA

get links to sites and visit the web site by sending the user email, instant messaging, using a search engine, portal, phishing messages, and passively waiting for users to access. Only in the situation of users' trust of the information, there will be the visiting to phishing site. In phishing site, this type of site accounted for a significant proportion, and the using technology is relatively simple. In order to better illustrate phishing cheat principle and preventive measures of phishing site, this paper defines the phishing site for ordinary phishing sites.

1.2.2. Taking the Initiative to Attack Phishing Site (Special Phishing Website): Active attacking phishing website is to use the system vulnerabilities attacks of technology, Trojan horses technology, browser hijackers technology etc. forcing users to access phishing nets. This kind technology phishing websites used is complex, mainly divided into the following categories.

1.2.2.1. Browser Hijack Phishing Site: Browser hijacking is a malicious program which most important characteristic is to tamper the user's browser configuration, to force to guide the user's browser to the other sites. According to the phenomenon after the browser hijack, it could be divided into two kinds, dominant browser hijack and stealth hijack. Among them, the dominant hijacking means users can easily observe the browser changes after hijacked. For users, generally will not be cheat on dominant hijack.

Stealth hijacking is a browser hijack which user will not be easy to perceive. Stealth hijacking is often used in electronic commerce payment link, and fake page simulation is very high, inexperienced users will be easily deceived. When a user logs in online banking or use third-party payment platform to do account payment, the hijacked program will automatically judgment and will replacement the payment page, the consequence is that the user actually do the payment to the deceiver account, there is no doubt that will lose money.

1.2.2.2. Trojan Phishing Site: The type of Trojan phishing website is actually the combination of phishing website and the Trojans, program with each other, thus raising the cheat success probability. For cheaters, phishing site's advantage is able to get a user account, password, transaction password and dynamic password quickly; The disadvantage is easy to cause the user's suspicions. The disadvantage of using Trojans is that it is not very convenient to get the user's password; and the advantage is relatively easy to get the user's trust.

The type of Trojan phishing web site has several characteristics as below:

- Cheaters often set up shops in regular trading platform, but send phishing Trojan files to the users with a variety of reasons when users buy.
- Generally deceiver sent Trojan to the user with a zip file form.
- Commonly use the replacement browser hijack technology to steal the user money.
- The name of commodity users paid is often the name of commodity users bought, so it is very concealment.
- The Payment method are always modified to instant payment to the account

1.3. The Cheat Reasons and Fraudulent means of Phishing Site

Lure users to access the phishing web site is a liar premise to phishing success, in order to achieve this, the scammers are racking their brains, through read the user's psychological, invent all kinds of reasons let users move or have to do the action, encouraged people to visit a phishing website, such as the table 1 as below.

Table 1. The Deception Reasons Often used by Phishing Site

Cheating on thinking	Cheating reason
Using people fear psychological	Lied that the bank accounts involving criminal offence
	Lied that the abnormal false accounts, and that the large consumption
	Lied that the vulnerability of banking system, and e-commerce system
Utilizing people's getting profit psychological	Lied that the user winning a prize
	Lied that the ultra-low-cost goods selling, and the free gift to receive
	Lied that the consumer rebates
Make use of the people trust psychological to bank platform	Lied that the bill checking
	Lied that the need to guarantee for e-commerce transactions
	Lied that the users bought the goods
	Lied that the upgrade account password protection, upgrade the product

The common fraudulent means are using email to cheat, using real-time communication tools, using of search engine to cheat, using mobile phone short message, using 400 or 800 telephone fraud, *etc*.

1.4. Phishing Site Workflow

Phishing site working process is roughly divided into five steps, as shown in Figure 1.

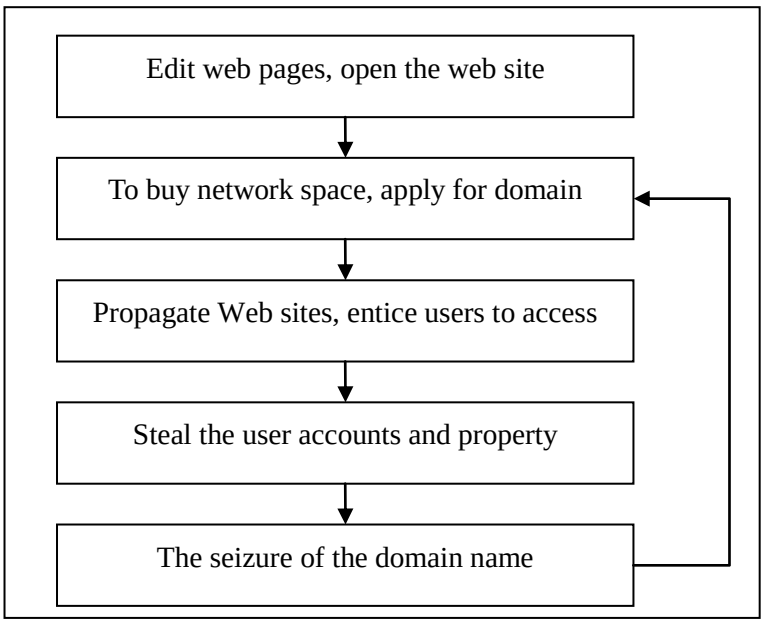

Figure 1. Phishing Site Working Process

1.5. Counterfeit Form of Phishing Sites

The counterfeit form of phishing website is mainly in two aspects of domain name and web page, no matter what kind of fake way is to reduce the doubt of users, so as to obtain the trust of the user.

1.5.1. Domain Name Confuse Cheating: Lenovo homepage is imitated by phishing site through the domain name confuse is the typical case of deception. With the development of e-commerce, more and more people have to look at such as taobao, the network bank, stock trading website and Zhifubao *etc.*, money direct related website. Then a variety of domain name confuse cheating cases appeared. According to the different domain name confusion method, domain name confuse cheating can be divided into the following categories:

1.5.1.1. Similar Characters Confusing: Named phishing website domain name by using similar or deceptive characters with formal website domain name characters, as shown in Table 1.

Table 1. Examples of Similar Characters Confusing

Web site name	Correct domain name	Phishing website domain name（Examples）
Taobao website	www.taobao.com	www.ta0bao.com
		www.taoba0.com
		www.taoobao.com
Microsoft's official website	www.microsoft.com	www.micr0soft.com
The industrial and commercial bank of China website	www.icbc.com	www.1cbc.com
Agricultural bank of China website	www.abchina.com	www.95599.com
China merchants bank website	www.cmbchina.com	www.cmb95555.com

1.5.1.2. Secondary/Tertiary Domain Name Confusion: Due to the top-level domain imitating is easy to be found, as a result, secondary/tertiary domain name confusion arises at the historic moment, as shown in Table 2.

Table 2. Examples of Secondary or Tertiary Domain Name Confusion

Website Name	The correct secondary domain name	Phishing site domain names (Examples)
Baidu website	image.baidu.com	image.baidu.xxx.com
Taobao website	fushi.taobao.com	fushi.taobao.xxx.com

1.5.1.3. Domain Name Encode Encoding Confusion: Encode coding is a kind of coding way, using that will confuse the form of domain name. For example, although the domain name in Table 3 is very different, but they are all pointing to the baidu website. If phishing website using this "look" domain name confusing is not website address, may be deceived.

Table 3. Different Forms of Domain Name in the Same Website

Baidu Website	The domain name
Form 1	http://www.baidu.com
Form 2	http://3546189924
Form 3	http:// 61.135.169.105
Form 4	http://0xd3.0x5e.0x90.0x64

1.5.1.4. Domain Name Jumping Technical Confusion: Domain name jumping technology refers to the technology jumping from A website to B website. Liars always use A website address to confuse users, and then use the domain name jumping technology, let users log on to the B website, namely the phishing website, as shown in Table 4.

Table 4. Domain Name Jumping

Normal taobao domain address	Website address of using taobao link address to jump
http://member1.taobao.com/member/loginByIm%2edo?&%65	http://member1.taobao.com/member/loginByIm%2edo?&%65rr url=hxxp://light.lz.taobao.com/?r=http://wxgww101.auvtoin.com %5CA.taobao.com/tb1.asp?IDC=1654

1.5.2. Fake Page: Fake phishing web site page technology is "make-up", make phishing website page especially “like" the homepage of real website.

1.5.2.1. Fake e-commerce Websites: Big, high-profile e-commerce websites is the object phishing site like to imitate. In many cases, phishing web site page copy can reach the level of spurious. According to statistics, only in April 2010, the complaint of faking Taobao phishing site is high as 1322, accounting for seventy percent of all phishing sites.

Bank payment platform is the main mock objects of the phishing site. In e-commerce, such as fake bank phishing sites cased the user money lost always occurred. Hackers usually send information to the user via E-mail, text messaging on mobile phones and lied

that the "your bank account is abnormal, please change the password"; Users click on the email address, and then is fake bank web site. After the user fills out the account password in the fake website, password leaked, bank capital will be possible stolen.

1.5.2.2. Counterfeit Client System Information: Counterfeit client system information is also a kind of common phishing site. Hackers will embed code in some bad website, imitation QQ voice of popup window, and then there will be a very high simulation of the QQ message alert window in the lower right corner. The user will be deceived when he clicks the window to login QQ, or to receive the prize. After Users fill in the account and password in the fake QQ website, the hacker will sell these numbers in private profit. In addition to QQ, Aliwangwang, and MSN client information is always the fake objects.

2. Prevention Methods of Phishing Sites

2.1. Prevention Methods of Passive Type Access Phishing Site (Ordinary Phishing Site)

Passive type access phishing site guard is very simple, as long as you do three points will not be cheated by phishing site: one point is making sure entering the correct websites address in manual, the second point is not logging in the strange link, the third point is to pay attention to check your browser's address. In addition, it is still could use some anti-phishing function software to prevent. In fact, in many cases preventing phishing web site attacks is the question of users' safety consciousness and habits, to be more vigilant and reduce the "greed", learn to prevent phishing site experience, is the most effective weapon against phishing site.

2.1.1. Manually Enter the Correct Url: Regardless of cheater using what kind of method to spread phishing site, as long as the user do not click, do not browse the phishing site, phishing site will not be succeed. Network users need to pay attention to the following points:

Make sure to remember clearly of the payment platform web sites such as banks, Zhifubao *etc*. If log in the payment platform directly, it is best to put the correct url in your browser, and then log in. For the process of shopping, in order to prevent online payment page jumping to phishing, the user must carefully identify the authenticity of the url.

For frequently accessed e-commerce sites, remember the url clearly, input manually.

For e-commerce sites need to access but don't know its address, the relatively safe method is to log in the web portal to research its web site in a large yellow pages.

2.1.2. Do not Access Unfamiliar Link:

- In any case, don't enter your user name and password in the email content page which sent by the other people.
- In any case, don't enter the user name and password in the non-account web site. For example: refuse to enter QQ user name and password in non-tencent official website (www.qq.com); Refuse to enter the bank account number and password of industrial and commercial bank of China in its none official website (www.icbc.com.cn) of any site, and so on.
- For strange website links send by strangers, default it as a phishing site, if you need to access, it should be careful screened, when necessary, it could be queried to distinguish its authenticity.

- Business services of funds change such as banks, stock funds will not notify the user of important information by email;
- All the sellers default to be the phishing site deceiver in e-commerce sites like taobao sell goods but let buyers purchase in other e-commerce sites.
- All the users' winning information, billing information, and the ultra-low-cost commodity information by the initiative sending will be default as the phishing site.
- All require the buyer to do e-commerce transactions on unknown guarantee platform by the sellers will be default as cheaters.
- All strange website links to mobile phone by short message will be default as the phishing site.

2.1.3. Pay Attention to Check your Browser's Address

- Review the main domain name

Primary domain mane is refers to the ending part of the domain name, means the two or three group of letter combinations before the first "Slash" of the web site. According to the main domain name it would judge whether this domain name is phishing website, as shown in Table 5.

Table 5 Real website domain name compared with false phishing website domain name.

Web site	URL	Main Domain name
Real web site	http://www.taobao.com/	taobao.com
	http://mail.taobao.com/	taobao.com
	http://news.taobao.com/	taobao.com
	http://jianghu.taobao.com/	taobao.com
	http://bbs.taobao.com/	taobao.com
	http://item.taobao.com/	taobao.com
	http://bbs.jianghu.mail.news.taobao.com/	taobao.com
Phishing site	http://item.taobao.com.taobaoo.com.cn/	taobaoo.com.cn
	http://auction1.taobao.com.taobaokeo.cn/	taobaokeo.cn
	http://fushi.taobao.auction.com/	auction.com
	http://taobao.123.com/	123.com
	http://item.taobao.com%2d%73%77%77%2eco.cc/	com%2d%73%77%77%2eco.cc

- Bank websites, stock trading website etc. that are relating to the financial websites, once entering into the page of user information, the related information are transferred through encrypted network protocol. So the bank website page of payment at the beginning must be based on “https://” rather than begin with "http://".
- Shopping sites typically show its identity in the browser. Phishing site is generally not so careful.
- After Bank website log in to the browser, there will be a lock safety sign on the right side.
- Some e-commerce sites, such as taobao, under the condition of the user login the client program (AliWangWang), the real taobao website may not require users to enter the password again.

2.2. Active Attacking Phishing Site (Special Phishing Site) Prevention Methods

The prevention method for phishing site which just use domain name and page deception is relatively simple. But for the special phishing site which are using browser hijackers and Trojan technology, its behavior are more concealed and the threatening is bigger, so the difficulty of the prevention is also increased a lot.

2.2.1. Prevent Method of the Browser Hijacks Phishing Site: For the preparedness of the dominant browser hijack, as long as pay attention to check the domain name will be fine. For prevent of the invisible browser hijack, if remember the following points that will not be cheated by the browse hijack:

- For successfully logged in the network bank that will not require entering your login name and password again when transfers.
- If entering the dynamic password correctly it could not have error for no apparent reason.
- If you login system successful, the system will record the user’s login state, may not require the user to enter the answer to the question of protection password.
- Banking services could not check the series of password of users one by one.
- For the banking system and the third party trading system could not display the system is down for maintenance after the user login.
- Pay attention to check the transaction amount, diddle amount of hijacking could not be the same as the amount of the users bought.
- Pay attention to check the name of commodity which is not be fake by hijack way.
- Pay attention to see the way of payment receiving, the way of instant payment receiving to account is a deceiver.

2.2.2. Prevention Methods of the Type of Trojan Phishing Site

- Check to see the way of payment receiving when pay.
- Be careful when the seller sends documents and it will be better not open.

References

[1] Phishing site threat to net bank safety. PC world, vol. 04, **(2011)**.
[2] F. Liu, "Cyber security strategy: How to quickly identify phishing site", Network & Information, vol. 09, **(2010)**.
[3] B. Cai and W. Zhao, "One of the most important threats to international Internet security: Bot net", Scientific and Technological Information, vol. (03), **(2010)**.
[4] L. Wang, "Introduction to computer network security and management", The China science and technology information, vol. 10, **(2009)**.
[5] Be careful of "phishing" around, Network security technology and application, vol. 10, **(2006)**.
[6] L. Wang, "Full disclosure of phishing diary", Computerize, vol. 7, **(2010)**.
[7] J. Jia, "Regulate phishing site also needs to take a long-term view", The Internet world, vol. 10, **(2010)**.
[8] J. Zhang, "Uncover "phishing" scam trap", Life and a partner (late Edition), vol. 08, **(2010)**.
[9] T. Li and Y. Mai, "Phishing crime technical analysis and countermeasure research", Information network security, vol. 04, **(2011)**.
[10] D. Chen, "Primary exploration of phishing status, way and protection", Network Security Technology & Application, vol. 07, **(2006)**.

Author

Zhou Fu-An, he received the B. education technology degree from Qu Fu Normal Universisty and the M. education technology degree from He Bei University in 2004 and 2007 respectively. He is currently researching on E-commerce Security and The Practice Teaching Methods.

