Overcoming Internet Fraud

By Yoram Nissenboim

When using the Internet, unless you are very inquisitive, skilled and have a lot of time, you know nothing about the site you visit other than the information displayed by the site. Scammers work very hard to mask themselves with Web sites that appear legitimate. Their intention is to tempt you to disclose your personal information. In fact, sites set up to steal personal information have become significant and widespread enough to warrant labels like "phishing" and "pharming."

Phishing usually employs e-mail messages or Web advertisements enticing you to go to a phony site. The incentives range from unbelievably tempting deals, like a $500 bonus card if you submit your personal details to messages like "There has been an unusually large purchase on your VISA card—please visit our site to validate." Some phishing messages, called "spear phishing," are personalized—an unsuspecting person receiving them cannot imagine that they are coming from scammers. For example, after you bid at an auction and do not win, you might receive a message telling you that you have been given a second chance to win at the price you offered. The scammers, pretending to belong to the auction site, take your money and you get nothing.

Pharming is an even more shifty approach. It uses DNS spoofing. This is a set of technical tricks, available on the Internet, which actually changes the destination of the URL that you see on your browser and directs you to an "undercover" site. In other words, you type www.mybank.com, you are sure you are accessing your bank, but you're actually entering a scam site.

There is a myth that the solution for phishing and pharming is tokens. These are small devices usually provided by banks or institutions who want their customers to connect to their web site. Some tokens can protect users from phishing, but most use a one-time password. In order to log into a site, the token is activated and the user is given a displayed password. The user must then type the password and login quickly because the password is valid for only a short time.

A phishing technology known as "man-in-the-middle" succeeds in accessing accounts of users protected by OTP tokens. The phishing site fools the user into thinking that it is the real site he or she has accessed before. This phishing site works during the login process as a proxy. It is connected to the real site and transparently transfers the data between the real site and the user, until the login process is complete. At that point, the phishing site disconnects the user. The operator of the phishing site has full access to the account of the unsuspecting user. If it is a bank account, financial transactions can be executed. If it is a corporate or government site, confidential information can be extracted. Several man-in-the-middle attacks were detected in 2005 causing banks to discontinue their online banking sites until the scam site was shut down.

Most users are aware of the risks caused by phishing. They receive frequent e-mails from banks where they have no account and recognize the problem. Subsequently, most users are afraid of becoming victims. They get numerous frightening warnings about the grave consequences of providing personal information to scammers. As a result, most users refrain from executing transactions through online banking. Instead, they only view their accounts online. Banks try to encourage users to execute transactions, but users rightfully demand protection against Internet fraud.

Although most users are aware of the risks in online banking, many of them are easy targets for unbelievable deals on the Internet. If they search for a new PC and find a half price offer from a company that has a name that looks familiar, they may choose to buy from that vendor and submit personal details, unaware of the fact that the site is bogus. Because of fear and uncertainty many e-commerce sites face a problem. Users that have bought goods and services on unfamiliar e-commerce sites have become more suspicious. Instead of looking for the best deal, they limit their search to large, well-known sites. Medium and small sites are the victims of this trend, and they are unable to influence users' behavior.

Many sites, especially large e-commerce and online banking sites, ask users to login in order to execute a transaction. The simple login process, utilizing user name and password makes it an ideal target for scammers.

The phishing and pharming scams discussed above tempt users to disclose their login parameters. But even if the user is well protected against phishing and pharming, a spyware – malicious software that may sneak into the user's machine – can detect the keystroke sequence or the sequence of mouse clicks and the associated screenshots used to login to a site, and send this sequence to an external source while the user remains unaware of the problem.

AVAILABLE SOLUTIONS

Education

Education is the key solution against Internet fraud. Banks warn customers about phishing, telling them not to trust messages asking them to log into their account and disclose information. Still, there are thousands daily who fall victim to Internet fraud attacks. Many of these people consider authorities—including banks—as an entity beyond any suspicion and, therefore, comply with scammers'

©2006 Technical Enterprises, Inc. Reproduction of this document without permission is prohibited.

requests. Others fall victim to sophisticated tricks, thinking they are doing the right thing. A popular scam offers an unbelievable deal. The opportunity to get this deal causes victims to ignore the basic rules of privacy protection.

E-mail filter

This solution tries to filter e-mail messages before the user receives them. It only protects against filtered messages. However, some scam messages bypass even the best e-mail filtering solutions and many new phishing techniques use advertising in web pages and other means to tempt victims.

Scam site block

The scam block solution is a service that protects the sites in which scammers try to phish. These solutions receive lists of known illegal sites and also monitor unusual activities used by scammers to duplicate an authorized site or add a plug-in to an authorized site. When an illegal site is detected, the scammer's access to the site is blocked. If the scammer has already established the phishing site, the mission is to take down the phishing site. This is done either by contacting the hosting service of the site or by attacking its server using denial-of-service attacks.

These solutions are considered a must for phishing prevention. However, the average time a phishing site is active is more than 100 hours, and during that time, many victims access it and provide information. On the other hand, many fraud sites that are trying to collect users' data for the exploitation of the collected information are not phishing sites and are, therefore, not blocked by the tools used for fighting phishing sites. The best example is a category of sites that use privacy protection services. This service lets site owners hide their identity and stay under cover. It was initially designed for non-commercial sites where the owners could publish their opinions free of civil rights limitations in specific countries. However, commercial sites that use this service should be avoided. If the user does not receive the goods or services he paid for, and the site does not acknowledge that he deserves compensation, he does not know whom to blame. More severe is a problem of abuse of users' identity details based on the information disclosed by the user. The user may find a new account opened in his name, his credit record will be destroyed and it may take a long time, and much embarrassment before such a problem may be resolved, usually after spending many weeks trying to prove that the identity was stolen.

Phishing site black list

This solution tries to protect the Internet user by employing a black list of phishing sites. When the user tries to access a phishing site, he or she receives a warning that the site is a phishing site and is advised to abort. This solution is already integrated into Netscape browsers. Internet Explorer and FireFox have it as a plug-in offered by several companies for free.

This is a good solution when the black list is up-to-date. However, more than 500 new phishing sites appear every day. Less than 50% of the new sites are added to the black lists within 24 hours from the moment they set out. Scammers take advantage of this and, in most cases, the messages sent by the scammers come in bursts, thus users can become victims before a site is added to the black list.

Browser-based white lists solutions

This is a relatively new approach that requires installation of a toolbar on the browser. Once installed, the user has good protection against Internet scam since he sees information about the site he visits. Examples of these solutions are CallingID for the Internet, Netcraft toolbar and TrustWatch. They analyze the site the user visits and provide the user with two types of information: a risk assessment and information about the destination of the data being submitted. The user can see if the data typed really goes to the intended site and whether there is any risk in sending the data. These solutions execute multiple verification tests and provide the user with the results. The user gets the information he or she needs in order to decide whether to proceed or abort. Among all Internet fraud solutions, these are the best. The main differences between these solutions are the quality of the verification of the site owner and the quality of the verification tests.

Strong authentication solutions

The strong authentication solutions protect users against Internet fraud problems when logging into their web account over the Internet. There are many strong authentication solutions. Most of them are based on either physical devices that users carry or use for authentication, or biometric characteristics of the user. The authentication solutions are categorized in three categories: something you know (password or PIN or a combination of both), something you have (usually a token the user carries, a smart card, mobile phone, etc.) and who you are (fingerprint, photo scan of the person, behavior characteristics, etc.) The main problems of these solutions are complexity (users must learn a new set of operations for authentication), costly new devices used for the authentication (like scanners or tokens) and accuracy (biometric solutions are not accurate—sometimes the real user fails in the authentication process; in other cases a scammer may access an account of a different person).

In the past year a few strong authentication solutions that simply use the user's name and password, yet provide a tool that overcomes spyware and phishing were introduced. The main solutions are Passmark Security platform and CallingID Safety Seal. Both solutions use sophisticated technologies that prevent even a scammer who has successfully detected the user's name and password from logging into the user's account, since there are other factors required. On the other hand, the user is not required to use new complex procedures in order to login.

REGULATIONS

2005 was the year that changed the way Internet fraud is regarded. The main change happened when the Federal Financial Institutions Examination Council (FFIEC) issued guidelines for Authentication in an Internet Banking Environment (October 2005), and the Federal Deposit Insurance Corporation (FDIC) issued two recommendations: June 2005 recommendation for a reliable form of authentication when customers access their account online, and July 2005 recommendation for protection of their customers against spyware. The recommendations can be found at

http://www.ffiec.gov/pdf/authentication_guidance.pdf
http://www.fdic.gov/news/news/financial/2005/fil6605.html
http://www.fdic.gov/consumers/consumer/idtheftstudysupp/idtheftsupp.pdf

The main change in these guidelines and recommendations is a requirement for strong authentication and the definition of the liability for the protection of users that login to their account over the Internet.

©2006 Technical Enterprises, Inc. Reproduction of this document without permission is prohibited.

The clear resolve that the financial institutions must protect their customers, forces banks to take action. The new solutions from companies like Passmark and CallingID, which keep the authentication process customers are used to unchanged, without adding an extra layer of complexity and inconvenience, help the banks in the transition to strong authentication solutions.

FUTURE CHALLENGES

Financial institutions will probably use strong authentication solutions because of regulations. There is a challenge to enforce e-commerce sites to use such solutions to protect themselves and their customers. An additional challenge is the education of users to employ the appropriate tools in order to protect themselves against Internet fraud. If this succeeds, both consumers and e-commerce suppliers will benefit.

NaSPA member Yoram Nissenboim is a networking and connectivity expert, and a veteran product provider, executive and entrepreneur. Nissenboim is the founder and CEO of CallingID. He holds a master's degree in computer science and a bachelor's degree in electrical engineering, both from the Technion Institute of Technology in Haifa, Israel.

NaSPA Network Supporting Servers and Desktop Environments SUPPORT™

©2006 Technical Enterprises, Inc. Reproduction of this document without permission is prohibited.