Cogn Comput (2010) 2:242–253
DOI 10.1007/s12559-010-9042-7

Experimental Case Studies for Investigating E-Banking Phishing Techniques and Attack Strategies

Maher Aburrous · M. A. Hossain · Keshav Dahal · Fadi Thabtah

Published online: 30 April 2010

Abstract Phishing is a form of electronic identity theft in which a combination of social engineering and Web site spoofing techniques is used to trick a user into revealing confidential information with economic value. The problem of social engineering attack is that there is no single solution to eliminate it completely, since it deals largely with the human factor. This is why implementing empirical experiments is very crucial in order to study and to analyze all malicious and deceiving phishing Web site attack techniques and strategies. In this paper, three different kinds of phishing experiment case studies have been conducted to shed some light into social engineering attacks, such as phone phishing and phishing Web site attacks for designing effective countermeasures and analyzing the efficiency of performing security awareness about phishing threats. Results and reactions to our experiments show the importance of conducting phishing training awareness for all users and doubling our efforts in developing phishing prevention techniques. Results also suggest that traditional standard security phishing factor indicators are not always effective for detecting phishing websites, and alternative intelligent phishing detection approaches are needed.

M. Aburrous (✉) · M. A. Hossain · K. Dahal
Department of Computing, University of Bradford, Bradford, England, UK
e-mail: mrmaburr@bradford.ac.uk

M. A. Hossain
e-mail: m.a.hossain1@bradford.ac.uk

K. Dahal
e-mail: k.p.dahal@bradford.ac.uk

F. Thabtah
MIS Department, Philadelphia University, Amman, Jordan
e-mail: ffayez@philadelphia.edu.jo

Keywords Phishing Web site · e-Banking · Social engineering · Malicious attack · Security awareness

Introduction

Online services simplify our lives. They allow us to access information ubiquitously and are also useful for service providers because they reduce the operational costs involved in offering a service. For example, online banking over the Web has become indispensable for customers as well as for banks. Unfortunately, interacting with an online service such as a banking Web application often requires a certain degree of technical sophistication that not all Internet users possess. For the last decade, such naive users have been increasingly targeted by phishing attacks that are launched by miscreants who are aiming to make an easy profit by means of illegal financial transactions. Phishing is a form of electronic identity theft in which a combination of social engineering and Web site spoofing techniques is employed to trick a user into revealing confidential information of economic value. Phishing techniques are continuously being updated, and there are always new variations appearing. Phishing attackers use various tactics to lure or hijack a browser into visiting bogus sites. Ordinary Internet users cannot become familiar with all these phishing techniques easily. Unfortunately, phishing attacks are growing, both in numbers and in complexity. Phishing websites are becoming increasingly sophisticated. They can capture e-banking website details automatically without any action on the part of the victim.

Phishing website attacks are growing at a torrid pace. The numbers of phishing attacks and reported phishing sites are increasing every year, even every month. Damage caused by phishing is severe. The APWG (Anti-Phishing

Working Group) is an industry association focused on eliminating identity theft and fraud that result from the growing problem of phishing and email spoofing. This voluntary-based organization provides a forum to discuss phishing issues, trials and evaluations of potential technology solutions and access to a centralized repository of reports on phishing attacks [39]. The number of unique phishing websites detected by this organization showed that there has been a huge increase in unique phishing sites all over the world. In December 2005, the forged phishing site alone exceeded 7,000 [5]. APWG has also recently released a new report containing statistics of phishing attacks during the first half of 2009. According to the APWG global phishing survey report [4], there were at least 55,698 phishing attacks, around 7% higher than the previous year. Those attacks occurred on 30,131 unique domain names. APWG identified that 4,382 were registered by phishers, representing about 14.5% of the domain names involved in phishing. In addition, phishing was detected on 3,563 unique IP addresses. The Gartner study [14] shows that phishing attacks escalated in 2007; more than $3 Billion was lost to these attacks. The survey found that 3.6 million adults lost money in phishing attacks in the 12 months ending in August 2007, when compared with the 2.3 million who did so the year before. And, in 2008, Gartner reported a 39.8% increase over the number of victims a year earlier. Media outlets have reported that phishing website-related scams have resulted in more than $5 billion in fraudulent bank and financial charges to date [25].

Internet Banking (E-banking)

Internet banking (e-banking) is defined as the automated delivery of new and traditional banking products and services directly to customers through interactive electronic communication channels. E-banking includes the systems that enable customers, individuals or businesses, to access accounts, transact business or obtain information on products and services through a public or private network, including the Internet [11]. Commercial banking is undergoing rapid changes, as the international economy expands and advances toward institutional and market completeness.

Phishing Websites

Phishing is a relatively new Internet crime in comparison with other forms, e.g., virus and hacking. More and more phishing Web pages have been found in recent years in an accelerative way [12]. Its impact is the breach of information security through the compromise of confidential data, and the victims may finally suffer losses of money or other kinds. A phishing website is a broadly launched social engineering attack that attempts to defraud people of their personal information including credit card number, bank account information, social security number and their personal credentials in order to use these details fraudulently against them [20]. Phishing has a huge negative impact on organizations' revenues, customer relationships, marketing efforts and overall corporate image. Phishing attacks can cost companies tens to hundreds of thousands of dollars per attack in fraud-related losses and personnel time. Even worse, costs associated with the damage to brand image and consumer confidence can run into the millions of dollars [5].

Phishing and the Trust of E-banking Business

Phishing websites can severely hurt Internet business, because people lose their trust in Internet transactions for fear that they will become victims of fraud. For example, many people believe that using online banking increases the likelihood that they will become victims of phishing websites and identity theft, even though online banking provides more secure identity protection than paper- and mail-based systems.

The most harmful effect is that it will create "trust crises". The trust will be eroded gradually without effective countermeasures to deal with the fraud, and everyone participating in network transactions will be harmed in the end. Trust is one of the most important determinants of successful e-banking [35]. Many researchers have argued that trust is essential for understanding interpersonal behavior and is relevant to e-banking. Trust is not merely a short-term issue, but also the most significant long-term barrier to realizing the potential of BtoC e-commerce [15]. Falling victim to phishing websites could steal a customer's proprietary information such as their account information and passwords, trade secrets or other intellectual assets. Theft of a customer's confidential information could have a disastrous effect on the companies or banks using electronic technology and could damage the trust between them and their clients.

Even in developed countries, many people are worried that their credit card details will be misused or hacked into and are concerned about online fraud, such as phishing websites that offer imaginary services or items.

Literature Review

Phishing websites are a recent problem. Nevertheless, due to their huge impact on the financial and online retailing sectors and since preventing such attacks is an important step toward defending against website phishing attacks, there are several promising approaches to this problem and a comprehensive collection of related works. In this section, we briefly survey existing anti-phishing solutions and a list of the related works. Dhamija and Tygar's [8] approach involves the use of a so-called dynamic security skin on the user's browser. This technique uses a shared secret image that allows a remote server to prove its identity to a user in a way that supports easy verification by humans but which is difficult for the phishers to spoof. The disadvantage of this approach is that it requires effort by the user. That is, the user needs to be aware of the phishing threat and check for signs that the site he/she is visiting is being spoofed. The proposal approach requires changes to the entire Web infrastructure (both servers and clients), so it can succeed only if the entire industry supports it. Also this technique does not provide security for situations where the user login is from a public terminal. More recently, Dhamija et al. [9] analyzed 200 phishing attacks from the Anti-Phishing Work Group database and identified several factors, ranging from pure lack of computer system knowledge, to visual deception tricks used by adversaries, due to which users fall for phishing attacks. They further conducted a usability study with 22 participants. The participants were asked to study 20 different websites to see if they could tell whether they were fraudulent or authentic. The result of this study showed that age, sex and computer habits did not make much difference. They even noticed that pop-up warnings of invalid signature of the sites and visual signs of SSL (Secure Sockets Layer), padlocks etc. were very inefficient and were overlooked. They found that 23% of the participants failed to look at security indicators warning about phishing attacks and, as a result, 40% of the time they were susceptible to a phishing attack. Based on their analysis, the authors suggest that it is important to re-think the design of security systems, particularly by taking usability issues into consideration. Wu et al. [37] proposed methods that require Web page creators to follow certain rules to create Web pages, by adding sensitive information location attributes to HTML code. However, it is difficult to persuade all Web page creators to follow the rules.

Liu et al. [24] analyzed and compared legitimate and phishing Web pages to define metrics that can be used to detect a phishing page on visual similarity (i.e., block level similarity, layout similarity and overall style similarity). A Web page is classified as a phishing page if its visual similarity value is above a pre-defined threshold. The phishing filter in IE8 is a toolbar approach with more features such as blocking the user's activity on a detected phishing site. The most popular and widely deployed techniques, however, are based on the use of blacklists of phishing domains that the browser refuses to visit. For example, Microsoft has recently integrated a blacklist-based anti-phishing solution into its Internet Explorer (IE8). The browser queries lists of blacklisted and white-listed domains from Microsoft servers and makes sure that the user is not accessing any phishing sites. Microsoft's solution is also known to use some heuristics to detect phishing symptoms in Web pages [32]. Obviously, to date, the company has not released any detailed public information on how its anti-phishing techniques function.

"The Phishing Guide" by Ollmann [26] gives a detailed understanding of the different techniques often included in phishing attacks. The phenomenon that started as simple emails persuading the receiver to reply with the information the attacker required has evolved into more advanced ways to deceive the victim. Links in email and false advertisements sends the victim to more and more advanced fraudulent websites designed to persuade the victim to type in the information the attacker wants, for example to log into the fraudulent site mimicking the company's original. Ollmann also presents different ways to check whether websites are fraudulent or not. Apart from inspecting whether the visited site really is secure through SSL (Secure Sockets Layer), the user should also check that the certificate added to the website really is from the company it claims to be from and it is signed by a trusted third party. Focusing more attention on the URL can also often reveal fraudulent sites. There are a number of ways for the attackers to manipulate the URL to look like the original, and if the users are aware of this, they can more easily check the authentication of the visited site. Watson et al. [36] describe in their *White Paper*, "Know your enemy: Phishing", different real-world phishing attacks collected in German and United Kingdom honeynets. Honeynets are open computer networks designed to collect information about different attacks out in the real world, for further forensic analysis. They noticed that phishing attacks using vulnerable Web servers as hosts for predesigned phishing sites are by far the most common, compared to using self-compiled servers. A compromised server is often host for several different phishing sites. These sites are often only active for a few hours or days after being downloaded to the server. PassMark [27] includes a personalized image in a Web page to indicate that the user has set up an account with the site. This approach places the burden on *users* to notice the visual differences between a good site and a phishing site and then to correctly infer that a phishing attack is underway. However, this requires user awareness and prior knowledge. Another approach is two-factor authentication, which ensures that the user not only knows a secret but also presents a security token [10]. However, this approach is a server-side solution. Phishing can still happen on sites that do not support two-factor authentication. Sensitive information that is not related to a specific site, e.g., credit card information and SSN, cannot be protected by this approach either. The PRIME project [28] helps users to manage their online identity in a more natural and intuitive way using three UI paradigms. It supports drag-and-drop actions for personal information submission. It does not specifically target the phishing problem, but its improved user interface could help users correctly manage their online information. One potential problem with the PRIME interface is its "Just-In-Time-Click-Through Agreements" (JITCTAs) that is used to generate "small agreements that are easier for the user to read and process". Users could still ignore the agreements by directly clicking through the "I Agree" button.

APWG provides a solution directory [2] which contains most of the major anti-phishing companies in the world. However, an automatic anti-phishing method is seldom reported. Cyveillance Fraud Management [22] uses proprietary Internet monitoring technology to identify phishing-related activity such as suspicious domain registrations, phishing lures, spoofed sites and the post-attack sale of compromised credentials. Others include Internet Identity's Domain Security Audit [24]. These approaches are mainly motivated to protect corporations' interests. Nonetheless, they do not directly defend against phishing attacks for users.

Gabber et al. [13] present a tool that tries to protect a client's identity and password information. They define client personality in terms of username, password and email address and introduce a function which provides clients with different personalities for the different servers they visit. Jakobsson introduced a new model, called a *phishing graph*, to visualize the flow of information in a phishing attack [18]. While this model is not, in essence, a defensive technique, it is the first step toward developing an abstract model for visualizing phishing. A phishing graph enhances the ability to analyze and understand the course of a phishing attack. TrustedBrowser [38] uses a synchronized random colored boundary to secure the path from users to their browser. The trusted status content is marked in the trusted window, whereas the server content is shown in the distrusted window. Anti-Phish [23] compares the domains for the same sensitive information in Web pages to the domains in the caches. That is, if it detects that confidential information such as a password is being entered into a form on a distrusted website, a warning is generated and the pending operation is canceled. PhishHook [34] converts a Web page to "normal form" through text, images and hyperlinks transformations.

PwdHash [31], in contrast, creates domain-specific passwords that are rendered useless if they are submitted to another domain (e.g., a password for www.gmail.com will be different if submitted to www.attacker.com).

The limitation of browser-based schemes is that they require prior knowledge of the target site, which is unfortunately not always available. More importantly, since phishing attackers are able to update the inducement techniques to get around those schemes, the effectiveness of these schemes is not convincing. In a proactive manner, a set of techniques are designed to capture phishing sites on the Internet.

One of the popular methods of detection is using add-in toolbars for the browser. Chou et al. introduced one such tool, SpoofGuard [7], that determines whether a Web page is legitimate based on a series of domain and URL-based tests. It uses domain names, URLs, links and images to measure the similarity between a given page and the pages in the caches or histories. It looks for phishing symptoms (e.g., obfuscated URLS) in Web pages and raises alerts. The technique examines the downloaded website using various stateful and stateless evaluations like checking for invalid links and URL obfuscation attempts. The major disadvantage with these approaches is that they are susceptible to attacks launched from the compromised legitimate website. Also, in many Web-hosting domains the attacker could create a user account with the name *login* and launch a successful phishing attack by hosting the masqueraded page in his domain space, which would typically appear as www.domain.com/login, thereby circumventing the aforementioned approaches. Herzberg and Gbara [16] proposed TrustBar, a third-party certification solution to phishing. The authors propose creating a trusted credentials area (TCA). The TCA controls a significant area, located at the top of every browser window and large enough to contain highly visible logos and other graphical icons for credentials identifying a legitimate page. While their solution does not rely on complex security factors, it does not prevent spoofing attacks. Specifically, since the logos of websites do not change, they can be used by an attacker to create a look-alike TCA in a distrusted Web page.

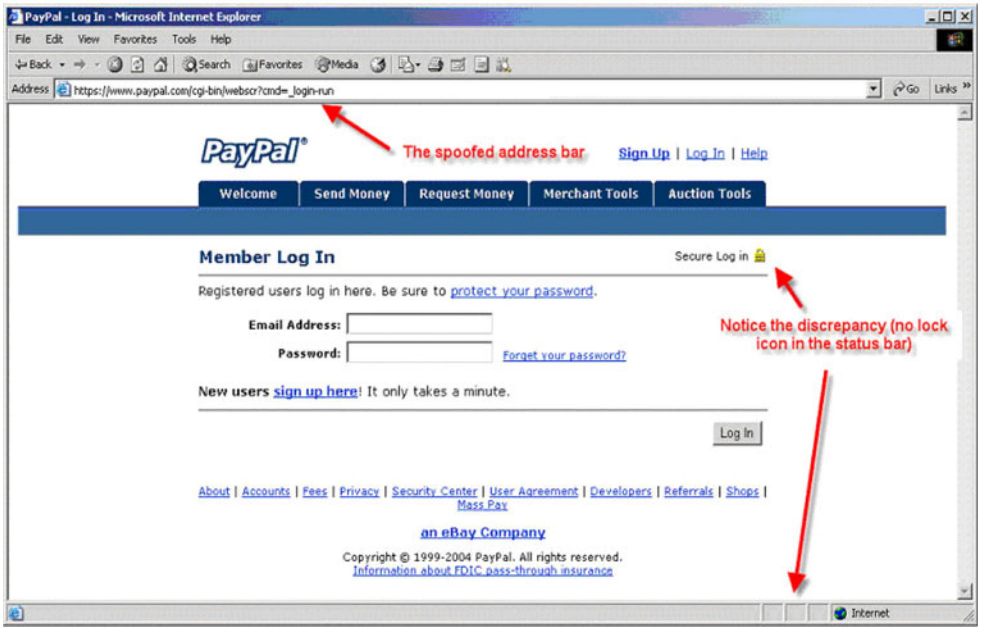
It should be emphasized that none of the above defense techniques—blacklist, spoofing detection, password-scrambling, anti-phishing toolbars or spam filters—will completely make phishing attacks impossible to perpetrate. Instead, they provide valuable but scattered roadblocks impeding the attacker.

Phishing Attack Strategies

Phishing Attack Using Internet Access

Most employees browse the Web for personal reasons, such as online shopping or research, at some time. Personal browsing may bring employees, and therefore the company

Fig. 1 Web page phishing hyperlink


PayPal - Log In - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://www.paypal.com/cgi-bin/webscr?cmd=_login-run
Go Links
PayPal
Sign Up | Log In | Help
Welcome
Send Money
Request Money
Merchant Tools
Auction Tools
Log In
Internet

The spoofed address bar

Member Log In

Secure Log in

Registered users log in here. Be sure to protect your password.

Email Address:

Password:

Forget your password?

New users sign up here! It only takes a minute.

About | Accounts | Fees | Privacy | Security Center | User Agreement | Developers | Referrals | Shops | Mass Pay

an eBay Company

Copyright © 1999-2004 PayPal. All rights reserved.
Information about FDIC pass-through insurance

Notice the discrepancy (no lock icon in the status bar)

computer systems, into contact with generic social engineers who will then use the staff in an effort to gain access to the company resources. The two most common methods of enticing a user to click a button inside a dialog box are by warning of a problem, such as displaying a realistic operating system or application error message, or by offering additional services.

Fig. 1 shows how a hyperlink appears to link to a secure PayPal website (https), while the status bar does not show anything that indicates for sure that it will take the user to a hacker's site. A hacker can suppress or reformat the status bar information.

Phishing Attack Using Phone Access

The telephone offers a unique attack vector for social engineering hackers. It is a familiar medium, but it is also impersonal, because the target cannot see the hacker. Phone phishing hacking is not considered to be a major threat. However, as more businesses embrace this technology, phone phishing is set to become as widespread as e-mail, and website phishing is now.

The most common approach is for the hacker to pretend to be the IT supervisor or outsource IT support engineer, requesting in a hurry all passwords and authenticated credentials to analyze and resolve the claimed problems reported to him, as shown in the following Fig. 2.

Requests for information or access over the telephone are a relatively risk-free form of attack. If the target becomes suspicious or refuses to comply with a request, the hacker can simply hang up. But it should be noted that such attacks are more sophisticated than a hacker simply calling a company and asking for a user ID and password. The hacker usually presents a scenario, asking for or offering help, before the request for personal or business information is made [6].

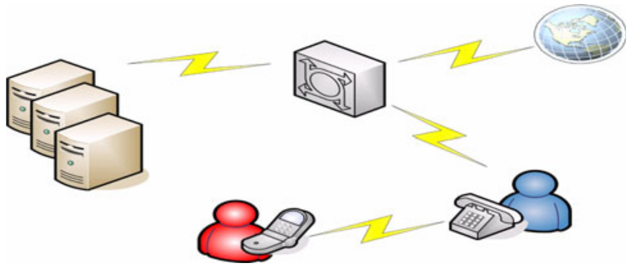


Fig. 2 Telephone phishing attacks

Phishing Experimental Case Studies

Conducting different kinds of phishing experiments can shed some light on social engineering attacks, such as phone phishing and phishing website attacks, and can also help us in designing effective countermeasures and analyzing the efficiency of performing training and security awareness about phishing threats [19]. The surprising percentages of victims who disclosed their credentials in our phishing experiments underscore the need to redouble our efforts in developing phishing prevention techniques.

Case Study 1: Phone Phishing Experiment

For our testing specimen, a group of 50 employees were contacted by female colleagues assigned to lure them into giving away their personal e-banking accounts, user names and passwords (through social and friendly conversations with a deceitful purpose in mind). The results were surprisingly beyond expectations; many of the employees fell for the trick. After conducting friendly conversations with them for some time, our team managed to seduce them into giving away their Internet banking credentials for fake reasons. Some of these lame reasons included checking their privileges and accessibility, or checking the account's integrity and connectivity with the Web server for maintenance purposes, account security and privacy assurance. To assure the authenticity of our request and to give it a social dimensional trend, our team had to contact them repeatedly, perhaps three or four times.

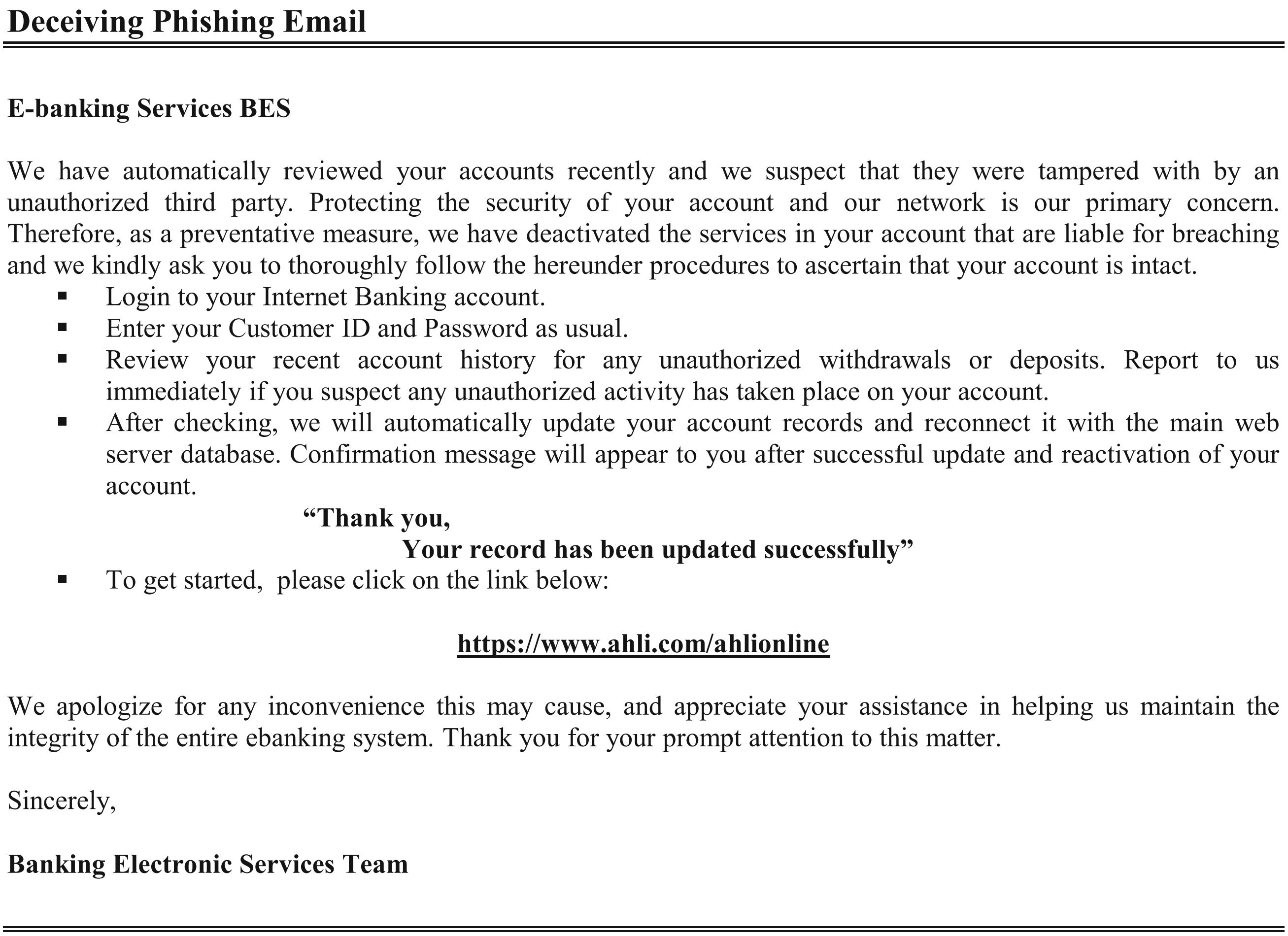
Our team managed to deceive 16 out of the 50 employees into giving away their full e-banking credentials (user name and password), which represented 32% of the sample. This percentage is considered a high one especially when we know that the victims were staff members of a bank, who are supposed to be highly educated with regard to the risks associated with electronic banking services. A total of eight employees (16%) agreed to give their user name only and refrained from giving away their passwords under any circumstances regardless of the excuse. The remaining 52% (26 employees) were very cautious and declined to reveal any information regarding their credentials over the phone, as shown in Table 1.

An overview of the results as shown in Fig. 3 reveals the high risk of the social engineering security factor. Social engineering constitutes a direct internal threat to e-banking Web services since it hacks directly and internally into the accounts of e-bank customers.

The results also show the dire need to increase the awareness of customers not to fall victims of this kind of threat which can have devastating results.

Case Study 2: Website Phishing Experiment

We engineered a website for phishing practice and study. The website was an exact replica of the original Jordan Ahli Bank website www.ahlionline.com.jo, designed to trap users and induce them by targeted phishing emails to submit their credentials (username and password). The specimen was inclusive of our colleagues at Jordan Ahli Bank after attaining the necessary authorizations from our management.



Deceiving Phishing Email

E-banking Services BES

We have automatically reviewed your accounts recently and we suspect that they were tampered with by an unauthorized third party. Protecting the security of your account and our network is our primary concern. Therefore, as a preventative measure, we have deactivated the services in your account that are liable for breaching and we kindly ask you to thoroughly follow the hereunder procedures to ascertain that your account is intact.

- Login to your Internet Banking account.
- Enter your Customer ID and Password as usual.
- Review your recent account history for any unauthorized withdrawals or deposits. Report to us immediately if you suspect any unauthorized activity has taken place on your account.
- After checking, we will automatically update your account records and reconnect it with the main web server database. Confirmation message will appear to you after successful update and reactivation of your account.

  "Thank you,
  Your record has been updated successfully"
- To get started, please click on the link below:

https://www.ahli.com/ahlionline

We apologize for any inconvenience this may cause, and appreciate your assistance in helping us maintain the integrity of the entire ebanking system. Thank you for your prompt attention to this matter.

Sincerely,

Banking Electronic Services Team

Table 1 Phone phishing experiment

Response to Phone Phishing Experiment	Number of employees
Giving away their full e-banking credentials(user name and password)	16
Giving away only their e-banking user name without password	8
Refused to reveal their credentials or any kind of information	26
Total	50

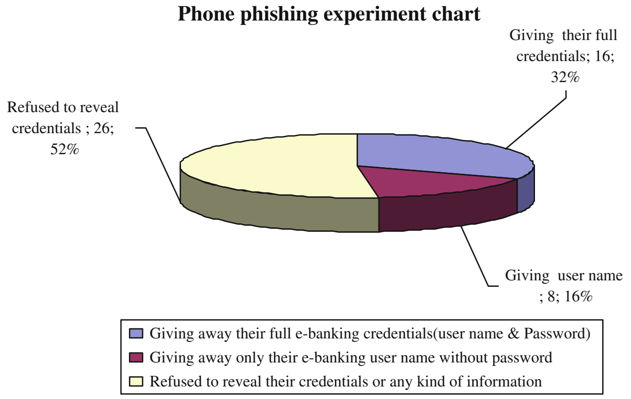


Fig. 3 Phone phishing response chart

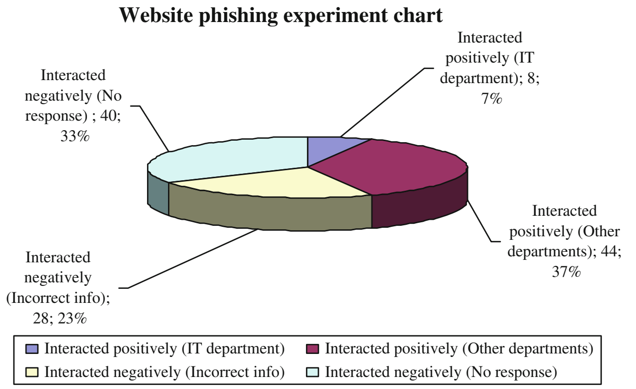


Fig. 4 Website phishing response chart

We targeted 120 employees with our deceptive phishing email, informing them that their e-banking accounts were at risk of being hacked and requesting them to log into their account through a fake link attached to our email using their usual customer ID and password to verify their balance and then log out normally.

The website successfully attracted 52 out of the 120 targeted employees, representing 44% who interacted positively by following the deceptive instructions and submitting their actual credentials (customer ID, Password).

Surprisingly, IT department employees and IT auditors constituted 8 out of the 120 victims representing 7%, which shocked me, since we expected them to be more alert than others. From other departments, 44 of the 120 targeted employee victims, representing 37%, fell into the trap and submitted their credentials without any hesitation.

The remaining 68 out of 120, representing 56%, were divided as follows: 28 employees (23%) supplied incorrect info, which seems to indicate a wary curiosity; and 40 employees, representing 33%, received the email but did not respond at all, as shown in Table 2.

Table 2 Phishing website experiment

Response to Phishing Experiment	Number of Employees
Interacted positively (IT Department)	8
Interacted positively (Other Departments)	44
Interacted negatively (Incorrect info)	28
Interacted negatively (No response)	40
Total	120

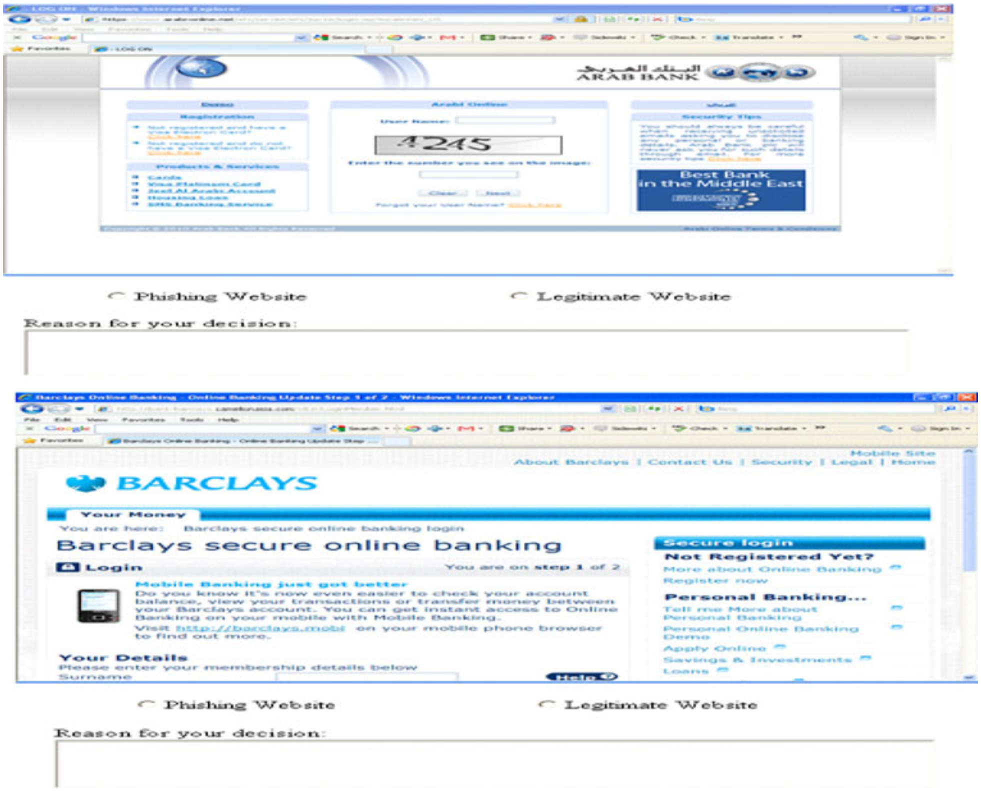
The results clearly indicate as shown in Fig. 4 that the target phishing factor is extremely dangerous since almost half of the employees who responded were victimized, particularly trained employees such as those of the IT Department and IT Auditors.

Increasing the awareness of all users of e-banking regarding this risk factor is highly recommended; this includes customers and employees alike.

Case Study 3: Phishing Website Survey Scenario Experiment

After the success of our previous phishing website empirical experiment which was conducted at our bank, targeting a specific number of its employees (120), the bank was really interested in studying the vulnerability of their employees toward spear phishing e-banking websites, since targeted spear phishing attacks have always been more successful than generic phishing attacks in conning people and causing financial damage to companies and individuals. We found this a good opportunity to perform a new usability study experiment to assess and to evaluate the accuracy and the precision of our 27 phishing website factors and features, previously collected and analyzed as a result of our cognitive walkthrough of phishing websites' patterns and clues.

This time, we decided to create two groups from our bank employees; each group consisting of 50 participants.



ARAB BANK

4245

Best Bank
in the Middle East

○ Phishing Website ○ Legitimate Website

Reason for your decision:

Barclays Online Banking - Online Banking Update Step 1 of 2 - Windows Internet Explorer

Mobile Site
About Barclays | Contact Us | Security | Legal | Home

BARCLAYS

Your Money

You are here: Barclays secure online banking login

Barclays secure online banking

Login

You are on step 1 of 2

Mobile Banking just got better

Do you know it's now even easier to check your account balance, view your transactions or transfer money between your Barclays account. You can get instant access to Online Banking on your mobile with Mobile Banking.

Visit http://barclays.mobi on your mobile phone browser to find out more.

Your Details

Please enter your membership details below

Surname

Help

Secure login

Not Registered Yet?

More about Online Banking

Register now

Personal Banking...

Tell me More about Personal Banking

Personal Online Banking Demo

Apply Online

Savings & Investments

Loans

○ Phishing Website ○ Legitimate Website

Reason for your decision:

Fig. 5 An example of phishing website scenario survey

In the first group, the employees were totally naïve about the phishing threat and did not have any previous experience or training in dealing with this kind of social engineering phishing attack. Regarding the second group, we decided to choose the 50 employees from our previous 120 employee specimen who had participated in our previous phishing website experiment case, in order to measure and evaluate the effectiveness and the efficiency of prior phishing website awareness training, and past experience of dealing with phishing attack hacking incidents. In total, our new specimen was 100 bank employees; half of them were untrained (First group) and the second half were trained (Second group).

We analyzed a set of phishing attacks and tricks to measure their effectiveness and influence and developed 50 phishing and legitimate website survey scenarios which were collected from the APWG's archive [3] and Phishtank archive [29]. The scenarios analyzed were carried out with the latest scenarios added to the archive by APWG and Phishtank experts. The scenarios were described and explained in detail in their archives. From these different scenarios, 30 out of the 50 were phishing websites, and the rest were legitimate.

We showed the two participating groups (trained and untrained) the 50 different website scenarios that appear to belong to decent financial institutions and reputable banks, as shown in Fig. 5, and asked them to determine which ones were fraudulent and which ones were legitimate and to give the reason for their decision and evaluation.

We showed the participants that the purpose of this experiment was to help them discover their knowledge and awareness of the new rising phenomenon of social engineering phishing website attack, and their capability to identify and to distinguish the legitimate genuine website from the phishing spoofed website.

For our part, the purposes of our experiment are to find the most common phishing clues and indicators that appear in the scenarios, to determine what aspects of a website effectively convey authenticity to our employees and to try to identify which malicious strategies and attack techniques are successful at deceiving general users and why [1].

From this experiment, we also tried to determine the effectiveness and the value of implementing some security training awareness and phishing courses or classes about phishing threats and detection expertise, and how this might reflect the determination of website legitimacy by the second, trained, group.

Our 27 phishing website factors and features were all deliberately distributed randomly across the 30 phishing website scenarios. One phishing factor could appear in many phishing scenarios, and one phishing scenario could have more than one factor. This is illustrated in Table 3.

As Table 3 presents, the phishing factor indicator ARUL "Abnormal Request URL" appeared in all 30 of the

Table 3 Phishing factor indicators

Phishing factor indicator	No. of appearance	Appearance percentage %
Using the IP address	14	46.66
Abnormal request URL	30	100
Abnormal URL of anchor	7	23.33
Abnormal DNS record	2	06.66
Abnormal URL	5	16.66
Using SSL certificate	17	56.66
Certification authority	4	13.33
Abnormal cookie	2	06.66
Distinguished Names Certificate (DN)	4	13.33
Redirect pages	3	10.00
Straddling attack	2	06.66
Pharming attack	4	13.33
Using on MouseOver to hide the link	6	20.00
Server Form Handler (SFH)	2	06.66
Spelling errors	24	80.00
Copying website	5	16.66
Using forms with "*Submit*" button	6	20.00
Using Pop-Ups windows	8	26.66
Disabling right click	2	06.66
Long URL address	22	73.33
Replacing similar characters for URL	16	53.33
Adding prefix or suffix	9	30.00
Using the @ symbol to confuse	6	20.00
Using hexadecimal character codes	8	26.66
Much emphasis on security and response	5	16.66
Public generic salutation	12	40.00
Buying time to access accounts	3	10.00

phishing scenarios. Furthermore, the phishing factor indicator, "Spelling Error", appeared in 80% of the phishing scenarios (24 appearances). In contrast, phishing factors such as "Abnormal DNS Record" and "Disabling Right Click" have the fewest appearances (6.66%, representing 2 appearances). We made sure that each phishing factor indicator had appeared at least once in the phishing website scenarios.

Table 4 The results of website legitimacy decisions for the first group (untrained group)

Decision website legitimacy	True	False
Positive	TP (11%) 275 Decision	FP (38%) 950 Decision
Negative	TN (17%) 425 Decision	FN (34%) 850 Decision

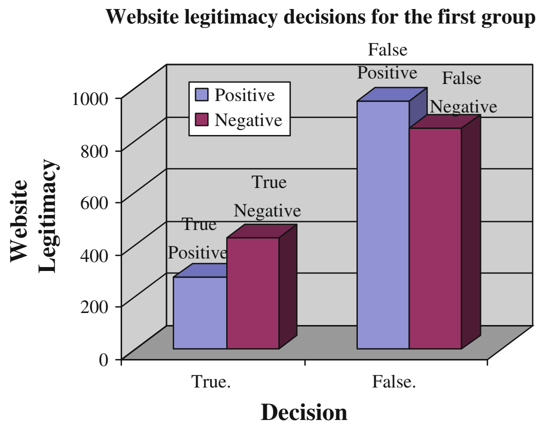


Fig. 6 Website legitimacy decisions chart for first group

The result from this experiment was very interesting. As shown in Table 4, in the first, untrained, group we found 72% of their decisions were wrong regarding the legitimacy of the websites presented to them in the experiment. These results were represented by either False Positive Case (FP, 38%), which happens when a legitimate website is considered as phishing by the participant, or by False Negative (FN, 34%), which happens when a phishing website is considered legitimate by the participant. Just 28% of their decisions were right regarding the legitimacy of the website, represented by either True Positive Case (TP, 11%), which happens when a legitimate website is considered legitimate by the participant, or by True Negative (TN, 17%), which happens when a phishing website is considered as phishing by the participant. Figure 6 represents the column chart for website legitimacy decisions for the first, untrained, group.

We found that most of these wrong decisions made by first, untrained, group arose from their lack of knowledge and awareness of the most common phishing website tricks and deceptions. Most of them did not pay attention at all to some very obvious phishing clues or indications like address bar contents, URL, domain name, page style, page contents and security indicators like SSL certificate or logos, leading to this high incorrect decision percentage. Most of their decisions and judgments concentrated on the look of the website and its fancy colors, pictures and animation style, thus supporting the arguments mentioned by Dhamija et al. [9].

Five decades of research [21, 33] demonstrates that the human brain processes visual imagery more reliably than text. Time and time again, it has been found that pictures are remembered better than words, because pictures are more likely than words to evoke both verbal and imagery codes. Furthermore, concepts presented in pictures rather than words are much more likely to be remembered.

The basis of the Picture Superiority Effect can be attributed to the greater sensory distinctiveness pictures have compared to words. Recognizing image categories

Table 5 The results of website legitimacy decisions for the second group (trained group)

Decision website legitimacy	True	False
Positive	TP (39%) 975 Decision	FP (12%) 300 Decision
Negative	TN (33%) 825 Decision	FN (16%) 400 Decision

minimizes the load on a user's memory by making options visible in plain sight. The user is not burdened or discouraged by trying to remember difficult, complex characters. Humans are capable of remembering between five and nine chunks of static information at a time.

However, in a dynamic environment such as the Web, a user's memory capacity is limited to roughly two or three chunks of information, thereby making the Web "an enemy of human memory" [30].

Regarding the second, trained, group, the results were totally different. Their previous experience of the phishing website experiment and the skills they gained from that were very obvious and played a big role in the total outcomes.

As shown in Table 5, from the second, trained, group we found 72% of their decisions were right regarding the legitimacy of the website, represented by either true positive case (TP, 39%) or by true negative (TN, 33%). Just 28% of their decisions were wrong, regarding the legitimacy of the websites presented to them in the experiment. These results were represented by either false positive case (FP, 12%) or by false negative (FN, 16%). Figure 7 represents the column chart for website legitimacy decisions by the second, trained, group.

We found that most of these correct decisions made by the second, trained, group resulted from their good experience, knowledge and awareness of the most common phishing website tricks and deception attacks that they had faced before. Most of them depended on their judgment and assessment of the website address bar, URL domain name and the different security indicators. They were not fooled by the design, style or fancy look of the website structure or animation, and their main concentration was focused on detecting all phishing website factor indicators, which led to this acceptable correct decision percentage. This of course suggests the importance of conducting phishing training awareness for all users.

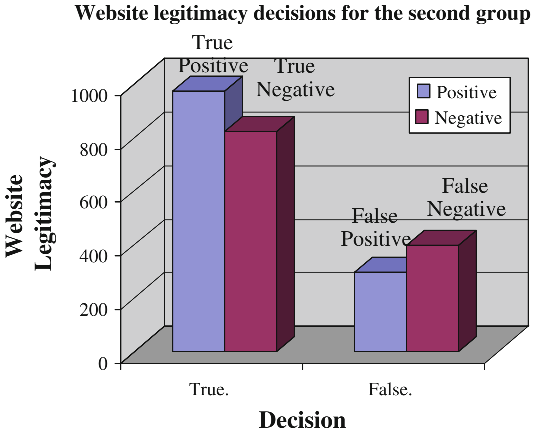


Fig. 7 Website legitimacy decisions chart for second group

Nevertheless, still some expert employees of the second trained group did not took the right decision for some of phishing or legitimate websites, and they were fooled for some visual deception phishing attacks. These results illustrate that traditional standard security phishing factor indicators are not effective enough for detecting phishing website and suggest that alternative intelligent approaches are needed.

Phishing Experiments Reaction Analysis

While some employees saw the learning value of the experience and appreciated the insights they had gained as a result of being part of the study, there were more employees who felt that the study had no value and felt violated at not having been asked permission before the experiment was performed.

Some of the employees called the experiment unethical, inappropriate, illegal and unprofessional. These reactions highlight that phishing has a significant psychological cost for victims. Many employees stated that they did not and would never fall for such an attack. This natural denial reaction suggests that we may find it hard to admit to our own vulnerability. As a consequence, many successful phishing attacks may go unreported, meaning that phishing success rates in surveys may be severely underestimated. Phishers know that most users do not know how to check the security and often assume that sites requesting sensitive information are secured. When users do not know how secure they are, they assume that they *are* secured, and it is not easy for them to see the difference between authentic security and mimicked security features. We found that security is often a secondary goal for most of our employees. They did not look at the address bar, status bar or certificate authority. They often focus on their major tasks and neglect all other security pointers or warning messages. Some employees were fooled by the presence of an SSL closed padlock icon appearing within the body of a Web page instead of looking for it in the right place. Many employees always looked for a certain type of content like the closed padlock icon when making their judgment, and they never mentioned the other security features like the characters and numbers shown in the address bar, the certificate authority or any other factors whatsoever. Some employees did not look for any SSL signs that can distinguish the secured encrypted website from the non-secured one, such as observing the "HTTPS" in the address bar. Some employees had some reservations when they saw an IP address instead of a domain name, and they were able to distinguish between them. On the other hand, many did not know what an IP address is!

Most of our employees did not check the certificate that was presented to their browser in our study since they do not know what it means; those that *do* know occasionally check them out. Some employees pointed out that the content details of the website and its fancy design and style were one of the main reasons for their opinion about the legitimacy of the website. They assumed that the site would be legitimate if it contained high-quality images and lots of animations. Many employees who clicked on the forged VeriSign logo that we created did not compare the URL displayed in the faked pop-up window, which shows the SSL certificate status of www.ahlionline.com.jo hosted at VeriSign, to the URL in the address bar to detect whether they are referring to the same website. Unfortunately, any site can provide a link to this pop-up page in order to gain credibility [17]. Some employees never paid any attention to the SSL padlock icon. Other employees did not know the meaning of the SSL padlock icon at all, and they could not give any justification for its existence. We found most of our employees do not know how to check or locate the self-signed certificate, and they have never checked a certificate before. We also found that some visual deception attacks can fool even the most sophisticated users.

As a conclusion, most of our employees made incorrect decisions about the legitimacy of the e-banking website because of their lack of knowledge and understanding of the phishing techniques and its malicious methods and indicators.

Conclusions and Future Work

It is being predicted that social engineering phishing attacks will be on the rise in the years to come. Billions of dollars are lost every year by corporations and Internet users to social engineering attacks, in the process making participants in e-commerce increasingly distrustful. The problem of social engineering attack is that there is no single solution to eliminate it completely, since it deals largely with the human factor. That is why implementing empirical experiments was very crucial in order to study and to analyze all malicious and deceiving strategies and attack techniques that were successful in confusing general users about their assessments of the authenticity and the legitimacy of websites. These experiments showed that there is no substitute for a good awareness campaign when implementing the social engineering elements of security policy.

Our experimental case studies point to the need for extensive educational campaigns about phishing and other security threats. People can become less vulnerable with a heightened awareness of the dangers of phishing. Our experimental case studies also suggest that a new approach is needed to design a usable model for detecting e-banking phishing websites, taking into consideration the user's knowledge, understanding, awareness and consideration of the phishing pointers located outside the user's center of consideration.

Results and reactions to our experiments show the importance of conducting phishing training awareness for all users. Nevertheless, these results illustrate that traditional standard security phishing factor indicators are not always effective enough for detecting phishing website and suggest that alternative intelligent approaches are needed.

Generally speaking, the primary advantage for criminals conducting phishing attacks is the public's lack of education and awareness of both the existence of financial crimes targeting Internet users and the policies and procedures of online sites for contacting their customers regarding account information and maintenance issues. Thus, public education and awareness are important factors to counter phishing. As awareness of phishing grows among consumers, the incidences of phishing will shrink to a certain extent.

However, getting rid of phishing through education alone will be very difficult. First of all, there are always new or technology-naive Internet users who do not have any experience and become victims of phishing. Another aspect is that phishers are getting better and better at mimicking genuine emails and websites; even the security expert may sometimes be fooled.

As a future work, we want to build an e-learning security awareness application regarding phishing attacks and scams; we will implement it to be used as a learning tool to increase the user awareness regarding phishing attacks and scams. We plan to demonstrate our decision justification extracted phishing features and their significance influence as summarized report. We also want to integrate phishing detection assessment user interface (example: short questionnaires, tests cases) to measure the effectiveness of our e-learning tools. To make the learning mechanism more effective and interactive, we are considering integrating concept of phishing games on the e-learning process. This ensures our package to be more dynamic and user friendly.

References

1. Alnajim A, Munro M. An evaluation of users' tips effectiveness for phishing websites detection, 978-1-4244-2917-2/08, IEEE; 2008. p. 63–68.
2. APWG. Phishing activity trends report. 2005. http://antiphishing.org/reports/apwg_report_DEC2005_FINAL.pdf. Accessed 12 Apr 2007.
3. APWG. Phishing activity trends report. 2008. http://antiphishing.org/reports/apwg_report_sep2008_final.pdf. Accessed 9 March 2009.
4. APWG. 2009. http://www.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2009.pdf. Accessed 8 Aug 2009.
5. Brooks J. Anti-phishing best practices: keys to aggressively and effectively protecting your organization from phishing attacks, White Paper, Cyveillance; 2006.
6. Business Security Guidance. How to protect insiders from social engineering threats. 2006. www.microsoft.com/technet/security/default.mspx. Accessed 8 Apr 2006.
7. Chou N, Ledesma R, Teraguchi Y, Boneh D, Mitchell J. Client side defense against web-based identity theft. In: Proceeding of the 11th annual Network and Distributed System Security Symposium (NDSS '04); 2004.
8. Dhamija R, Tygar J. The battle against phishing: dynamic security skins. In: Proceedings of ACM Symposium on Usable Security and Privacy (SOUPS 2005); 2005. p. 77–88.
9. Dhamija R, Tygar J, Marti H. Why phishing works. In: CHI '06: Proceedings of the SIGCHI conference on human factors in computing systems. ACM Press, New York; 2006. p. 581–590.
10. FDIC. Putting an end to account-hijacking identity theft, FDIC, Technical Report [Online]. 2004. Available: http://www.fdic.gov/consumers/consumer/idtheftstudy/identitytheft.pdf. Accessed 18 Apr 2007.
11. FFIEC. E-Banking Introduction, Federal Financial Institutions Examination Council, Information Technology Examination Handbook (IT Handbook InfoBase). 2003. Available Online: http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ebanking_00_intro_def.html. Accessed 15 June 2007.
12. Fu A, Wenyin L, Deng X. Detecting phishing web pages with visual similarity assessment based on Earth Mover's Distance (EMD). IEEE Trans Dependable Secur Comput. 2006;3(4):301–11.
13. Gabber E, Gibbons P, Kristol D, Matias Y, Mayer A. Consistent, yet anonymous, web access with LPWA. Commun ACM. 1999;42(2):42–7.
14. Gartner. 2007. (http://www.gartner.com/it/page.jsp?id=565125). Accessed 10 Sept 2007.
15. Gefen D. Reflections on the dimensions of trust and trustworthiness among online consumers. ACM SIGMIS Database. 2002;33(3):38–53.
16. Herzberg A, Gbara A. Protecting naive web users, Draft of July 18; 2004.
17. Jagatic T, Johnson N, Jakobsson M, Menczer F. Social phishing, community. ACM. 2007;50(10):94–100.
18. Jakobsson M. Modeling and preventing phishing attacks, School of Informatics Indiana University at Bloomington; 2005.
19. Jakobsson M, Tsow A, Shah A, Blevis E, Lim Y. What instills trust? A qualitative study of phishing. Bloomington: Indiana University; 2007. p. 356–61.
20. James L. Phishing exposed, Tech Target Article sponsored by: Sunbelt software. 2006. searchexchange.com.
21. Kinjo H, Snodgrass JG. Is there a picture superiority effect in perceptual implicit tasks? Eur J Cogn. 2000;12(2):145–64.
22. Kirda E, Kruegel C. Filching attack of on-line status. J Netw Secur Technol Appl. 2005;6(4):17–20.
23. Kirda E, Kruegel C Protecting users against phishing attacks with antiphishing. In: Proceedings of the 29th annual international Computer Software and Applications Conference (COMPSAC); 2005b. p. 517–524.
24. Liu W, Guanglin H, Liu X, Xiaotie D, Zhang M. Phishing webpage detection. In: Proceedings of the 2005 eight international conference on Document Analysis and Recognition (ICDAR'05), IEEE; 2005. p. 560–564.
25. Microsoft Corporation. Microsoft phishing filter: a new approach to building trust in E-Commerce Content, White Paper; 2008.
26. Ollmann G. The phishing guide, understanding and preventing phishing attacks (online available). 2004. http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf.
27. PassMark. Two-factor two-way authentication, PassMark Security. 2005. http://www.passmarksecurity.com.
28. Pettersson J, Fischer-Hübner S, Danielsson N, Nilsson J, Bergmann M, Clauss S, Kriegelstein T, Krasemann H. Making prime usable. In: Proceedings of SOUPS'05. ACM Press, Pittsburgh; 2005. p. 53–64.
29. Phishtank. 2008 http://www.phishtank.com/phish_archive.php. Accessed 14 Nov 2008.
30. Rhodes JS. Human memory limitations and web site usability. 1998. Moving WebWord from http://www.webword.com/moving/memory.html. Accessed 28 May 2008.
31. Ross B, Jackson C, Miyake N, Boneh D, Mitchell J. Stronger password authentication using browser extensions. In: Proceedings of the 14th Usenix Security Symposium; 2005.
32. Sharif T. Phishing filter in IE7. 2005. http://blogs.msdn.com/ie/archive/2005/09/09/463204.aspx. Accessed 6 Apr 2007.
33. Stenberg G. Conceptual and perceptual factors in the picture superiority effect. Eur J Cogn. 2006;18(6):813–47.
34. Stepp M. Phishhook: a tool to detect and prevent phishing attacks. In: DIMACS workshop on theft in E-Commerce: content, identity, and service; 2005.
35. Suh B, Han I. Effect of trust on customer acceptance of Internet banking. Electron Commer Res Appl. 2002;1(3):247–63.
36. Watson D, Holz T, Mueller S. Know your enemy: phishing, behind the scenes of phishing attacks, The Honeynet Project & Research Alliance; 2005.
37. Wu M, Miller R, Little G. Web wallet: preventing phishing attacks by revealing user intentions. MIT Computer Science and Artificial Intelligence Lab; 2006.
38. Ye Z, Smith S. Trusted paths for browsers. ACM Trans Inform Syst Secur. 2005;8(2):153–86.
39. Zin A, Yunos Z. How to make online banking secure, article published in The Star InTech; 2005.