Asian Journal of Information Technology 7 (9): 394-402, 2008
ISSN: 1682-3915

E-Commerce: Online Attacks and Protective Mechanisms

Veronica V.N. Akwukwuma and Annie O. Egwali
Department of Computer Science, University of Benin,
P.M.B. 1154, Benin City, Nigeria

Abstract: The convenience of online commerce has been embraced by consumers worldwide. However, criminals exploit the vulnerabilities existing in online systems to commit fraud. While, there has been good progress in identifying threats, educating institutional and individual users and identifying countermeasures, there has also been an increase in attack diversity and technical sophistication. Attack on consumer sensitive information has the adverse effect of decreasing consumer confidence in online commerce. Avoidance of security vulnerabilities in online systems requires awareness of typical risks, a good understanding of these vulnerabilities and the existing mechanisms to protect customer sensitive information.

Key words: E-commerce, customer sensitive information, fraud, security

INTRODUCTION

The birth of the internet has given rise to new innovations in technology and its usage has grown in our daily lives. It is now a medium for several types of professional activities. It has successfully, adopted itself as a device, which is used for a number of industry career ads and has emerged as the most successful promotion and commercial tools of the world (Brewer, 2001). Although, the world wide web was initially intended as a means to share distributed information amongst customers, it has now become the preferred environment for a multitude of e-services (Siau *et al*., 2001). It also offers many opportunities for service providers and financial institutions. Electronic Commerce (E-commerce), which is the exchange of business information using electronic formats, including electronic mail, electronic sensitive information interchange, electronic bulletin boards and electronic funds transfer (Adam *et al*., 1998), allows the online customer to survey business and online markets in a more efficient manner. E-commerce also enables online buying and selling of products (Brewer, 2001). Its numerous benefits has led to its wide spread acceptance. Unfortunately, a lot of security issues have also come up. It is not astonishing that wherever money is involved, criminals are always around trying to get at it. The same applies to online financial systems, which are a primary target for attacks for obvious reasons. An attacker or criminal in this context is someone who wrongfully obtains and uses another person's sensitive information in some way that involves fraud or deception, typically for economic gain and to carry out attacks on unsuspecting customers. These attacks include dumpster-diving, fraudulent attacks, in which customers are tricked by deceitful messages into giving out information to detestable applications that steal financial account information. These criminals target many kinds of confidential information, including customer names and passwords, social security numbers, credit card numbers, screen names, bank account numbers and personal information such as birthdates and mothers' maiden names (Aaron, 2005; Joakim, 2005).

This study, will discuss the methods of attacks used by criminals in an e-commerce environment, analyze their chances of successfully stealing sensitive information and discuss some of the defense techniques that have evolved to obviate their attacks.

STEPS IN ONLINE BUSINESS TRANSACTION

The following flow (Fig. 1) depicts the online business transaction process. Processing event and activities may differ slightly, depending on the type of business requirement, systems used, service provider and acquirer correlation.

Corresponding Author: Veronica V.N. Akwukwuma, Department of Computer Science, University of Benin, P.M.B. 1154, Benin City, Nigeria

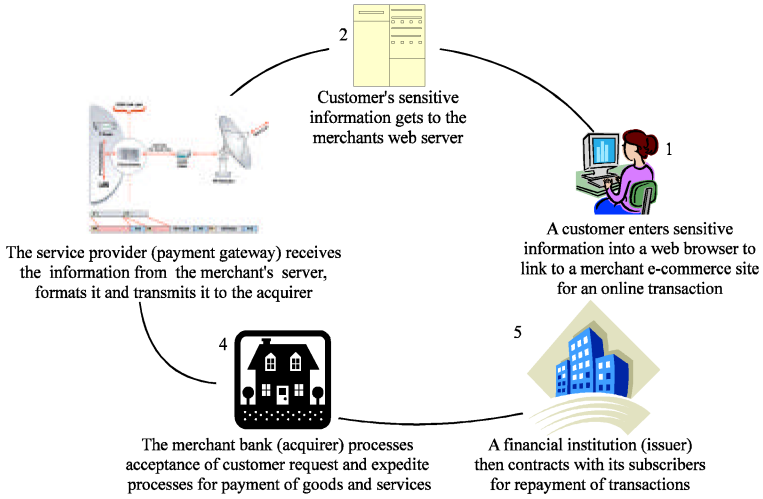

Fig. 1: Online business transaction process

TYPES OF E-COMMERCE ATTACKS

Deceptive e-mail: E-mails are the common tools for attacks. Most often, fraudulent emails claim to be from a trusted organization, such as a bank or an online retailer. In a typical scenario, a criminal sends deceptive email, in bulk; with a call to action that demands the recipient click on a link. Examples of a call to action include (Aaron, 2005):

- A statement that there is a problem with the recipient's account at a financial institution or other business. The email asks the recipient to visit a web site to correct the problem, using a deceptive link in the email.
- A statement that the recipient's account is at risk and offering to enroll the recipient in an anti-fraud program.
- A fictitious invoice for merchandise, often offensive merchandise, that the recipient did not order, with a link to cancel the fake order.
- A fraudulent notice of an undesirable change made to the customer's account, with a link to dispute the unauthorized change.
- A claim that a new service is being rolled out at a financial institution and offering the recipient, as a current member, a limited-time opportunity to get the service for free.

In a typical scenario, the criminal sets up a copy of the web site they want to impersonate on a server, they control. The criminal's site is usually designed to seem like the site of a reliable merchant company. This copy includes all the code from the original site including the set of used images, which the criminal would have accumulated during a previous legitimate session. This makes it hard to trace the imposter in the server logs as no suspicious access is made thus, the criminal then succeeds in convincing the customer to enter sensitive information. In some cases after the customer enters sensitive information, into the criminal's site, the criminal saves the information and redirects the customer to a fake error page or to the original web site. Many customers will think, they mistyped their password and do not necessarily suspect a fraud. According to Candid (2005), sometimes to disguise the actual server location particularly when HTML enabled emails are employed, the quartet of a standard IP address is translated into a dot-less decimal number i.e. http://3639551848(216.239.39.104). Most browsers support these decimal IP addresses, as well as web authentication strings in the form of customername: password@website.tld. To obfuscate the URL even more the criminal can add a fake web authentication string that looks like the impersonated domain name, such as http://mySecureBank.tld@ 3639551848. This corresponds to a customer-name of mySecureBank.tld with no password given on the decimal IP address representation of 216.239.39.104. This will trick many customers into believing that they are about to click on a link that leads to the mySecureBank.tld domain. After his success at tricking the customer, the criminals then impersonate the victim and relocate funds from the victim's account, purchase merchandise and do other damage. In many cases, the criminal does not directly cause the economic damage, but resells the illicitly obtained information on a secondary market. Criminals

participate in a variety of online brokering forums and chat channels where such information is bought and sold (Aaron, 2005).

DNS-based attacks (pharming): In pharming attacks, the focus is on the domain name system. This type of attack interferes with the integrity of the lookup process for a domain name, thus, the routing system of the internet is compromised. An example is when a customer types in a legitimate site such as www.clothsmerchant.org and gets diverted to a spoofed site without realizing it. It can also, be done with a system reconfiguration attack that changes the merchant's DNS server to a malicious server, by hacking a legitimate DNS server, or by polluting the cache of a misconfigured legitimate DNS server. Another form of DNS-based attacks involves polluting the customer's DNS cache with incorrect information that will be used to direct the customer to an incorrect location. If the customer, has a misconfigured DNS cache, this can be done directly. It also, involves hosts file poisoning (Aaron, 2005).

In March 2005, a large-scaled DNS cache poisoning attack (Haugsness, 2005; Candid, 2005) started to fill vulnerable DNS servers with false domain name-IP address pairs. As a result, machines relying on these poisoned DNS servers received a false IP address resolution for certain domains, which led them to malicious Web sites. Detailed analyses of aspects of DNS attacks can be found in the study from Ollmann (2005). In January 2005, the American ISP Panix experienced a social engineering attack (Cole and Tonkin, 2005). Due to lax domain change verification processes, someone was able to modify the registered details of the domain panix.com. The actual DNS records were moved to a company in the United Kingdom and Panix.com's mail was redirected to a company in Canada. Customers of the domain panix.com were redirected to false sites and could have fallen victims to fraudsters if a transaction site existed at this address (Candid, 2005).

Malware: Malware attacks refer to attacks that involve running malicious software on the customer's machine. It is spread mostly by downloadable software, traffic may be driven to a malicious web site via social engineering such as spam messages promising some appealing content at the site, or by injecting malicious content into a legitimate web site by exploiting a security weakness such as a cross-site scripting vulnerability on the site (Aaron, 2005) or by exploiting security vulnerability through the propagation of a worm or virus. In this type of attack, the problem is that the customer's computer is infected with spyware or other deceptive software. This software can get onto the customer's computer in a number of ways. For instance, it might be piggybacked onto legitimate software, the customer might accept it not knowing what it does, or the customer might use low security settings that accept it (www.nclnet.org). In a typical, social engineering attack a customer is convinced to open an email attachment or download a file from a misleading merchant site, often claiming the attachment has something to do with a beautiful and unresisting business proposal. A typical example as found in Joakim (2005) occurred in May 2003, only around 20 Trojans that target financial services were reported in the wild, most of them with basic functionality. Two and a half years later, the number of such malware has increased to nearly 2000 different variants. Web Trojans can also pop up over login screens to collect Sensitive information from the customer.

Session hijackers: Session hijacking refers to an attack in which a criminal may watch a session open on a network. Once authentication is complete, they may attack the client computer to disable it and use IP spoofing to claim to be the client who was just authenticated and steal the session. Session hijacking can be performed on a customer's local computer by malware, or can also be performed remotely as part of a man-in-the-middle attack. When performed locally by malware, session hijacking can look to the targeted site exactly like a legitimate customer interaction, being initiated from the customer's home computer.

Man-in-the-Middle attacks: Man-in-the-Middle (MITM) attack involves a criminal serving as a proxy between a customer and his genuine online commerce site. The criminal then saves valuable information, passes the messages to the merchant site and forwards the responses back to the customer. The criminals thus, have possession of a customer's sensitive information that can be used for session hijacking or DNS-based attacks. MITM attacks are usually difficult for a customer to detect, because the site will work properly and there may be no outer indication that anything is wrong (Milletary, 2007). In a normal SSL traffic, the handshake utilized by the SSL ensures that the session is established with the party named in the server's certificate and that a criminal cannot obtain the session key. The SSL traffic, which is encrypted using the session key cannot be decoded by an eavesdropper. Proxies have a provision for tunneling such encrypted traffic. However, a malware-based attack can modify a system configuration to install a new trusted certificate authority, in which case such a

man in the middle can create its own certificates for any SSL-protected site, decrypt the traffic and extract confidential information and re-encrypt the traffic to communicate with the other side (Aaron, 2005). In practice, man-in-the-middle attacks simply do not use SSL, since customers do not generally check for its presence.

Illegal card usage: Illegal card usage involves an attacker who illegally obtains an account number of a valid cardholder to purchase goods and services from a legitimate mail order/telephone order from an internet merchant. There are a number of ways, which criminals can get their hands on valid card account numbers. Some of the most common situations include internal compromises, discarded receipts, web site cloning scams, system hackings, account number generation software and deceptive solicitations.

Cross-site scripting attacks: A cross-site scripting vulnerability is a programming flaw involving content coming from an external source, such as a blog, a customer review of a product on an e-commerce site, an auction, a message in a discussion board, a search term or a web-based email (Aaron, 2005). A more common cross-site scripting attack that has been used involves the exploitation of vulnerable URL redirector programs. URL redirectors are often used by web sites to perform custom processing based on attributes such as web browser or authentication status or even just to display a message when clicking on a link to an external site. Thus, attackers are able to send attacks emails with URLs that use the vulnerable redirectors on the legitimate sites to trick people into visiting attacks sites (Milletary, 2007). Cross-site scripting is propagated through two different principal agents. In one vector, malicious content is injected into sensitive information stored on a legitimate web server, such as an auction listing, product review or web-based email. In the other vector, malicious content is embedded into a URL that the customer visits when he clicks on a link (Aaron, 2005).

Keyloggers: Keyloggers are devices that scrutinizes a customer's keyboard and mouse inputs in conjunction with scrutinizing the customer's activities or web browser programs that detect changes to the URL and logs information when a URL is at a designated credential collection site. They can install themselves into a customer's machine and scrutinize sensitive information being input and send relevant sensitive information to a criminal's server. When keyloggers are on a customer's machine, there is usually additional software to notify to the criminals whenever sensitive information is being entered (www.nclnet.org).

Password attacks: According to www.visa.com, criminals attack E-commerce merchants using weak or generic passwords. Once a password is compromised, the criminal then emulates the merchant and begins processing debits and credits, without the true merchant's knowledge. The fraud sales are usually similar in total to-and therefore-are offset by the credits deposited. This is done in an attempt to circumvent detection by deposit (volume monitoring).

Screenloggers: Screenloggers are software that scrutinize both the customer's inputs and his interface display input security measures. Screenloggers are able to capture images of what the customer sees, giving the criminals access to the information on the screen. Just as is the case with keylogger, there is also additional software to notify the criminals whenever sensitive information is being entered.

Hosts file poisoning: In hosts file poisoning the attacker redirects certain domains in the customer's predefined IP addresses. Navigation of the internet by customers relies heavily on the process of mapping domain names to IP addresses. By design, if a URL address is logged into the computer, the system translates that address into a numeric address before the site is visited. But during a host file poisoning, the attacker can modify the host file to look up host names before a DNS lookup is performed. After this modification, the unsuspecting customer may get to the wrong site unknowingly and enter sensitive information, which the attacker collates and utilizes later.

Search engine attack: In this case, the attacker creates a web page meant for fake products. According to Aaron (2005), the attacker gets the pages indexed by search engines and waits for customers to enter their confidential information as part of an order, sign-up, or balance transfer. Such pages typically offer products at a price too good to be true. Some attackers also create a page advertising an interest rate slightly higher than any real bank. Victims find the online bank via a search engine and enter their bank account credentials for a balance transfer to the new account.

The Man-in-the-Browser attack (MITB): MITB is the same approach as Man-in-the-Middle attack, but in this case a Trojan horse is used to intercept and manipulate calls between the main application's executable (i.e., the browser) and its security mechanisms or libraries on-the-fly. The most seen objective of this attack is to cause financial fraud through manipulating transactions of Internet Banking system, even when others authentication factors are in use. A previously installed

Trojan horse is used to act between the browser and the browser's security mechanism, sniffing or modifying transactions as they are formed on the browser, but still displaying back the customer's intended transaction.

The attackers objectives: The following are the main objectives of attackers as asserted by Thorsten and Raynal (2007):

- To gather information stored on the system.
- Prevent access to some resource on the system, resulting in a Denial-of-Service (DoS).
- Control the system, mount a Man-in-the-Middle attack and perhaps reuse it in a later Pharming attack.
- Use the target system as stepping stone to propagate the attack to neighboring systems.

The effect of online fraud theft on customers, merchants and credit providers: It is noteworthy to recognize the fact that the use of e-commerce creates new ways for both image and brands to be attacked. Customers, merchants, businesses and financial institutions alike are often affected by online fraud. The potential business implications of a security incident include the following (Joakim, 2005; www.businesslink.gov.uk):

- Online merchants bear direct financial losses and indirect costs (from repairing the damage), as a consequence of fraud or litigation.
- Subsequent loss as a result of unwelcome publicity.
- They also suffer blows to their reputations and credibility.
- Their images are ruined.
- They suffer the misfortune of being unjustly accused, arrested and detained, which can even result in discontinuing any future business transaction.
- They pay criminal charges if found to be in breach of the sensitive information protection or computer misuse acts, or other regulation on e-commerce.
- Loss of market share if customer confidence is affected by an attack.
- The images presented by a business, together with the brands under, which it trades, are valuable assets that are affected.
- Victims face significantly higher overall financial costs.
- These costs take several forms, including actual monetary loss (clean-up cost), credit score deterioration, foregone investments and sacrificed leisure time.

All of these risks can have a significant impact upon a business running an E-commerce service.

WHY CRIMINALS SUCCEED

Criminals targeting customer information are able to profit from the increased adoption of online banking and shopping activities. Customers of these services provide a target of opportunity in that they possess information of value. Along with an increase in the number of potential targets, there are three major factors that criminals have been able to take advantage of Milletary (2007).

Unawareness of threat: If customers are unaware that their personal information is actively being targeted by criminals, they may lack the perspective needed to identify criminals threats and may not take the proper precautions, when conducting online business activities.

Unawareness of policy: Criminals often rely on a victim's unawareness of organizational policies and procedures for contacting customers, particularly for issues relating to account maintenance and fraud investigation. Customers unaware of the policies of an online merchant are likely to be more susceptible to the social engineering aspect of an attack, regardless of technical sophistication.

Technical sophistication of the criminals: Criminals conducting attack scams are leveraging technology that has been successfully used for activities such as spam, Distributed Denial of Service (DDoS) and electronic surveillance. Even as customers are becoming aware of attacks, criminals have responded with technical tricks to make their attacks more deceptive and effective.

MECHANISMS TO PROTECT CUSTOMERS SENSITIVE INFORMATION

The exposure of a business to e-commerce vulnerability depends on the organization's business policies, prevention and detection tools, security controls, operational practices, counter attack tools and the type of goods and services provided. Customers and merchant organization should therefore have a thorough understanding of the risk associated with an internet transaction and should be acquainted with various existing risk management approaches (Brancheau *et al*., 1996).

Mutual authentication: A major mechanism for protecting customer sensitive information at this stage is a better

form of authentication different from the normal user id and password systems, which means better ways to establish someone's true identity. An authentication scheme that can monitor both the client and the server side should be employed. According to www.nclnet.org, it is perhaps even more important to develop new ways to authenticate web sites, so that ordinary users can tell a real site from a fake. The report suggests way to improve both user and site authentication, or what is sometimes called strong mutual authentication. Aaron (2005) asserted that a way to demonstrate to a user that a mutual authentication protocol will be used is to display a particular image in any window whose contents will be used for mutual authentication. Such an image is stored in client-side and kept secret from external parties. Another potential issue with a mutual authentication protocol is that both sides must have a matching credential.

Customer education: For most online attacks on customers and merchant sites, the attacker's advantage is due to the fact that both the customer and the merchant are unaware of the different techniques employed by attackers and financial organizations do not employ policies and procedures of online sites for contacting their customers regarding account information and maintenance issues. Customers, law enforcement agencies and financial organization awareness and education must continue to evolve to address the growing capabilities available to attackers.

All online commercial firms should see the need to enhanced customer education and awareness by:

- Sending regular alerts messages to customers email addresses and sites.
- Regularly reminding customers of commercial business policies regarding their accounts.
- Organizing seminars and workshops in collaboration with security enforcement organizations.

There should be awareness of the:

- Potential financial impact of installing malicious code on computer systems.
- Vulnerabilities inherent in clicking on links in an email
- Trend in attack methods.
- Different attack tools and their functionality.
- Fact that before authentication, transmission is through a secure socket layer.
- Fact that the domain name is accurate before entering sensitive information.

Points where educational information could be provided are:

- When a customer registers with a commercial organization.
- When a customer buys a software or hardware product.
- When a customer registers with an Internet service provider.

Financial institutions can foster such education by adhering to practices such as in Aaron (2005):

- Not telling customers they will never use clickable links, when in fact such links are a valuable form of marketing.
- Never using a call to action in email that warns of a negative consequence for failing to follow a link.
- Using email authentication technology.
- Using honestly named links, if links are used (e.g. not using deceptively named links).
- Always using the expected domain name for logging in.
- Always using SSL on the login page and all other pages.

Password hashing: Password hashing involves hashing password codes with the domain name assigned to it before transmission. While, the use of the common name, user id and password is vulnerable to attacks, hashing passwords increases the security level of the password codes. This is due to the fact that the transmitted password codes cannot be reused by an attacker in a different domain except at the same valid site. One way to prevent attackers from collecting useful passwords is to encode user passwords according to where, they are used and transmit only an encoded password to a web site. Thus, a user could type in the same password for multiple sites, but each site-including an attacks site-would receive a differently encoded version of the password. An implementation of this idea is called password hashing. Password hashing could ultimately be provided by a browser as a built-in mechanism that is automatically performed for password fields (Aaron, 2005). To prevent offline dictionary attacks, a site using password hashing should also enforce good password requirements.

Password hashing provides good protection and assurance that sites will not store plaintext password data and that the passwords cannot be reused on another site. Password hashing can also be combined with a mutual authentication protocol to obviate the need to store a mutually authenticated password in plaintext.

Conventional two-factor authentication: Two-factor authentication refers to utilizing any two of the three

factors for authenticating customers, which are what you are (biometric); what you have (a smartcard) and what you know (user name and password). What you know is very susceptible to attacks thus, an additional factor of authentication is needed, which is commonly referred to as second-factor authentication. It is needed to gain access to an account, or to execute a transaction.

One-time password: One-Time-Password (OTP) systems are not connected to the PC physically or electronically and they display codes that change either at regular intervals, or each time it is used. Using cryptographic algorithms, they are resistant to spy-wares because of the tokens usage. OTP tokens are either synchronous or asynchronous. For the synchronous ones, the tokens are synchronized with the host's authentication servers using the minute of current time or a sequence number, or both. For the asynchronous ones, they are simply calculators to compute a random number ('response') according to a given random number (challenge) by the host system. To demonstrate that a user has the device, the user is prompted to enter the current password, which is validated by a server that knows the sequence that is used and the current value. Some OTP tokens require the use of a PIN to unlock the tokens. Others involving Smart cards and USB dongles can perform onboard cryptographic processing and ensure that they are authenticating directly to an authorized party, in a manner that an eavesdropper would be unable to interpret.

Transaction confirmation: There is need for commercial firms to device mechanisms to always confirm transactions while, the transaction is still in progress. Such a system will help to assure customers that they are dealing with the right firm. In a situation, when such a confirmation is supposed to be forthcoming but did not appear, then the customer can take the necessary steps as prescribed by the commercial firm. Some transaction confirmations make use of phone calls; others make use of e-mail messages and SMS messages etc. to confirm transactions.

It is important that confirmation messages include details of the transaction itself.

Single-source authentication: Single-source authentication can be either by the issuance of an identifying PIN or code to the customer or the use of out-of-wallet data to further verify the customer's identity. The risk associated with an identifying PIN or code is that the thief also often steals this piece of data. Out-of-wallet databases use credit bureau data and specifically include information about the customer that typically cannot be discovered by stealing a person's wallet (Cheney, 2003), for example, the type of student loans the person holds. Credit providers can use such databases to ask customers more obscure questions on their credit applications that only they should know.

Two-factor authentication systems: Two-factor authentication systems ensure secure log on validation. One system that promises good user acceptance uses the user's registered mobile phone to receive an activation code. In this scenario, the users identify themselves to the bank with their account name (Candid, 2005). Next, the bank generates a random temporary password and sends it in a Short Text Message (SMS) to the user's mobile phone number. The user enters this challenge code into the browser and proves thus that he has access to the correct mobile phone. This two-factor authentication works fine and is quite convenient for most users.

Anti-attacks toolbars: Anti-attacks toolbars use a variety of technologies to determine that they are on an unsafe site, including a database of known attacks sites, analysis of the URLs on a site, analysis of the imagery on a site, analysis of text on a site and various heuristics to detect an attacks site. Browser toolbars are available that attempt to identify attacks sites and warn the user. These are available both as research projects and from technology suppliers. They typically display a visual indication such as a traffic light indicating the safety of a site, in which green indicates a known good site, yellow indicates an unknown site and red indicates a suspicious or known bad site. For example, eBay Account Guard and Stanford Spoof Guard (Aaron, 2005).

Virus, spyware and spam prevention: Solutions designed to protect users from viruses, trojans, spyware and spam play a role in protecting users from attacks scams. With the marked increase in attacks malware, products that detect and prevent the installation and execution of malicious code are an essential part of an environment for secure home computing. These products must be enabled and, in the case of anti-virus and anti-spyware products, must have up-to-date signatures. Spam prevention has also contributed to the fight against attacks. Attacks emails use the same distribution mechanism as spam and usually have many of the same characteristics. Email filtering based on content blacklisting, Bayesian filtering, blocking mail from known spamming/attacks relays, anti-forgery solutions such as Sender Policy Framework (SPF) and sender ID and other heuristics specific to attacks can help prevent a great many attacks emails from ever reaching potential victims in the first place. However,

spammers are continually evolving their tricks for bypassing filters (Schmidt, 2006) and the attackers can leverage this.

CONCLUSION

Vulnerabilities inherent in e-commerce technology are significant and growing problem, which threaten to impose increasing monetary losses on businesses and to shatter customer confidence in e-commerce. If the level of attacks continues to rise on the internet, numerous consumers may stop participating in online transactions. It is observed that attacks have the potential to become much more sophisticated, making user-based protection mechanisms fragile, given the user population of non-experts. Thus, all must admit that everyone individuals and businesses are threatened and potentially vulnerable to attacks. Despite the seriousness of current incidents and the increasing threat, some basic principles allow us to significantly reduce the risk. Awareness is the best defense. As asserted by Aaron (2005) and (www.nclnet.org), there exists no lone silver bullet technology that can really ward off attackers from conniving and inventing new mechanisms for attacking customers and businesses. Thus, a combination of good organization and practice, proper application of current technologies and improvements in security technology has the potential to drastically reduce the prevalence of attacks and the losses suffered from them.

RECOMMENDATIONS

To shield customers and businesses from the ambuscade of attackers, we propose the following that will not only reduce the customer's online transaction vulnerability but will also increase the cost and time for executing an attack on a legitimate site:

- Customers should not provide personal data on the phone or via mail. Clever identity thieves might pose as bank agents, phone companies and even government agencies.
- Caution is needed when opening email attachments-regardless of who sent them. If you download files, make sure your security software is enabled and pay close attention to any warnings.
- Never cut and paste the link from the message into your internet browser. Attackers can make links appear as if they go to one place, while actually sending you to a different site.
- Online accounts should be scrutinized regularly for any irregularities.
- Files should be permanently erased and burnt before disposal.
- Regularly apply official security patches and update the anti-virus, anti-spyware and anti-Trojan definition files on workstations and servers.
- Never discard a credit card, hard disk, credit card numbers, bank statements, charge receipts and credit card applications, old documents with sensitive information or ATM receipt in a public place without first burning them up or completely destroying them.
- At any point in time only the necessary documents containing sensitive information should be carried about.
- Avoid clicking on links in popup and e-mail messages without first verifying that they are from an authentic source.
- If necessary, contact an external consultant who can assess the security of your system and reconfigure, administer and modernize it.
- Review the web site's privacy policy. Trustworthy businesses will publish how they maintain the security of personal information collected by the site, how the information will be used and whether it will be provided to third parties.
- Controlling the circulation of information beyond electronic communication. Exchanges in public or private locations, presentations at conferences, seemingly personal solicitations, responses to questionnaires, invitations to tender and interviews are opportunities to expose information that should not be made public.
- While, designing and implementing online commerce sites, companies should be aware of when sensitive information is at risk. Also, it is necessary to realize the importance of authorization of transactions.
- Email addresses should not be shared indiscriminately. Addresses should not be posted on personal web sites, forums, or in chat rooms. If there is need to subscribe to a newsletter, a generic email address should be used that does not have a link to any of personal information.
- There should be a constant check for any indication that a site is secured.
- Install security software (anti-virus, anti-spyware, antispam and anti-Trojan) on all of the workstations as well as on any servers connected to the network.
- Take action to reduce risky behavior-downloading programs, accepting email without discretion, responding to email concerning confidential information-through education and by creating documents detailing the rules of hardware usage or listing user responsibilities.

- Maintain a single gateway to the Internet with a firewall and an intrusion detection/prevention system to detect and block suspicious data exchanges.

ACKNOWLEDGEMENT

We are grateful to Professor E. Onibere and O. Fajuyigbe for their invaluable support and encouragement.

REFERENCES

Adam, N.R. *et al.*, 1998. Electronic commerce: Technical, business and legal issues. Upper Saddle River, NJ: Prentice Hall. http://www.worldcat.org/oclc/40078180.

Aaron, E., 2005. Online identity theft: Phishing Technology, Chokepoints and Countermeasures. www.radixlabs.com.

A Call for Action Report from the National Consumers League Anti-Phishing Retreat National Consumers League, 2006. Washington, DC. www.nclnet.org.

Brancheau, J.C., B.D. Janz and J.C. Wetherbe, 1996. Key Issues in Information Systems Management: 1994-95 SIM Delphi Results. MIS Quart., 2 (20): 225-242. http://www.misq.org/archvist/vol/no20/issue2/vol20n2art5.html.

Brewer, B., 2001. Canada considers legalizing cell phone jamming systems. Computerworld. http://computerworld.com/cwi/story/0%2C1199%2CNAV47_STO58493_NLTmw%2C00.html.

Candid, W., 2005. Phishing. In: The middle of the stream today's threats to online banking. From the Proceedings of the AVAR, 2005 Conference. www.symantec.com.

Cheney, J.S., 2003. Identity Theft: A Pernicious and Costly Fraud. www.phil.frb.org.

Cole, T. and B. Tonkin, 2005. Email from Tim Cole to Bruce Tonkin (regarding the unauthorized transfer of panix.com domain). http://www.icann.org/correspondence/cole-to-tonkin 14mar05.htm.

Haugsness, K., 2005. DNS Poisoning Summary. http://isc.sans.org/presentations/dnspoisoning.php.

Joakim von Braun, 2005. Internal Study. Symantec Sweden. http://www.symantec.com/smallbiz/reseller_landing/pdf/Symantec_IT_Security_for_Small_Businesses_book.pdf.

Milletary, J., 2007. Technical Trends in Phishing Attacks. http://www.cert.org/archive/pdf/phishing_trends.pdf.

Ollmann, G., 2005. The Pharming Guide. http://www.ngssoftware.com/papers/ThePharmingGuide.pdf.

Schmidt, T.S., 2006. Flow Filtering Screens Out Spam. http://www.itstrategy.com/itworld/Threat/virus/how-filtering-screes/.

Siau, K., E. Lim and Z. Shen, 2001. Mobile Commerce: Promises, Challenges and Research Agenda. J. Database Manag., 12 (3): 4-13. http://www. informatik.uni-trier.de/~ley/db/journals/jdm/jdm12.html#SiauLS01.

Thorsten, H. and F. Raynal, 2007. Malicious Malware: Attacking the Criminals, Part 1. mailto:tt.holz@miscmag.com,%20f.raynal@miscmag.com.

Visa E-Commerce Merchant Guide to Risk Management. Tools and Best Practices for Building a Secure Internet Business, 2005. www.visa.com.