OCC 2005-24

OCC BULLETIN

Comptroller of the Currency
Administrator of National Banks

Subject: Threats from Fraudulent Bank Web Sites

Description: Risk Mitigation and Response Guidance for Web Site Spoofing Incidents

TO: Chief Executive Officers of All National Banks, Federal Branches and Agencies, Technology Service Providers, Department and Division Heads, and All Examining Personnel

PURPOSE

The purpose of this bulletin is to provide banks with guidance on how to respond to incidents of Web-site spoofing. The bulletin addresses procedures banks can implement to mitigate the risks to themselves and their customers by detecting and responding to Web-site spoofing. It also identifies the types of information banks can provide to law enforcement authorities to assist in investigating illegal activities. This bulletin expands on OCC Alert 2003-11, "Customer Identity Theft: E-mail-Related Fraud Threats," September 12, 2003.

BACKGROUND

Web-site spoofing is a method of creating fraudulent Web sites that look similar, if not identical, to an actual site, such as that of a bank. Customers are typically directed to these spoofed Web sites through phishing schemes[1] or pharming techniques.[2] Once at the spoofed Web site, the customers are enticed to enter information such as their Internet banking username and password, credit card information, or other information that could enable a criminal to use the customers' accounts to commit fraud or steal the customers' identities. Spoofing exposes a bank to strategic, operational, and reputational risks; jeopardizes the privacy of bank customers; and exposes banks and their customers to the risk of financial fraud.

PROCEDURES TO ADDRESS SPOOFING

Banks can mitigate the risks of Web-site spoofing by implementing the identification and response procedures discussed in this bulletin. A bank also can help minimize the impact of a spoofing incident by assigning certain bank employees responsibility for responding to such

[1]Phishing generally involves sending e-mails to a random or targeted list of consumers and directing them to provide their confidential information or to perform other tasks at a spoofed Web site.
[2]Pharming exploits vulnerabilities in the customers' computers or the Internet infrastructure to direct customers to a spoofed Web site instead of the actual site.

incidents and training them in the steps necessary to respond effectively. If a bank's Internet activities are outsourced, the bank can address spoofing risks by ensuring that its contracts with its technology service providers stipulate appropriate procedures for detecting and reporting spoofing incidents, and that the service provider's process for responding to such incidents is integrated with the bank's own internal procedures.

Banks can improve the effectiveness of their response procedures by establishing contacts with the Federal Bureau of Investigation (FBI) and local law enforcement authorities in advance of any spoofing incident. These contacts should involve the appropriate departments and officials responsible for investigating computer security incidents. Effective procedures should also include appropriate time frames to seek law enforcement involvement, taking note of the nature and type of information and resources that may be available to the bank, as well as the ability of law enforcement authorities to act rapidly to protect the bank and its customers.

Additionally, banks can use customer education programs to mitigate some of the risks associated with spoofing attacks. Education efforts can include statement stuffers and Web-site alerts explaining various Internet-related scams, including the use of fraudulent e-mails and Web-sites in phishing attacks. In addition, because the attacks can exploit vulnerabilities in Web browsers and/or operating systems, banks should consider reminding their customers of the importance of safe computing practices.

Detection and Information Gathering

Detection

Banks can improve their ability to detect spoofing by monitoring appropriate information available inside the bank and by searching the Internet for illegal or unauthorized use of bank names and trademarks. The following is a list of possible indicators of Web-site spoofing:

- E-mail messages returned to bank mail servers that were not originally sent by the bank. In some cases, these e-mails may contain links to spoofed Web sites;
- Reviews of Web-server logs can reveal links to suspect Web addresses indicating that the bank's Web site is being copied or that other malicious activity is taking place;
- An increase in customer calls to call centers or other bank personnel, or direct communications from consumer reporting spoofing activity.

Banks can also detect spoofing by searching the Internet for identifiers associated with the bank such as the name of a company or bank. Banks can use available search engines and other tools to monitor Web sites, bulletin boards, news reports, chat rooms, newsgroups, and other forums to identify usage of a specific company or bank name. The searches may uncover recent registrations of domain names similar to the bank's domain name before they are used to spoof the bank's Web site.[3] Banks can conduct this monitoring in-house or can contract with third parties who provide monitoring services.

Banks can encourage customers and consumers to assist in the identification process by providing prominent links on their Web pages or telephone contact numbers through which customers and consumers can report phishing or other fraudulent activities. Banks can also train customer-service personnel to identify and report customer calls that may stem from potential Web-site attacks.

[3] Refer to OCC Alert 2000-9, "Protecting Internet Addresses of National Banks" (July 19, 2000).

Information Gathering

After a bank has determined that it is the target of a spoofing incident, it should collect available information about the attack to enable an appropriate response. The information that is collected will help the bank identify and shut down the fraudulent Web site, determine whether customer information has been obtained, and assist law enforcement authorities with any investigation. Below is a list of useful information that a bank can collect. In some cases, banks will require the assistance of information technology specialists or their service providers to obtain this information.

- The means by which the bank became aware that it was the target of a spoofing incident (e.g., report received through Web site, fax, telephone, etc.);
- Copies of any e-mails or documentation regarding other forms of communication (e.g., telephone calls, faxes, etc.) that were used to direct customers to the spoofed Web sites;
- Internet Protocol (IP) addresses for the spoofed Web sites along with identification of the companies associated with the IP addresses;
- Web-site addresses (universal resource locator) and the registration of the associated domain names for the spoofed site;[4] and
- The geographic locations of the IP address (city, state, and country).

Spoofing Incident Response

To respond to spoofing incidents effectively, bank management should establish structured and consistent procedures. These procedures should be designed to close fraudulent Web sites, obtain identifying information from the spoofed Web site to protect customers, and preserve evidence that may be helpful in connection with any subsequent law enforcement investigations.

Banks can take the following steps to disable a spoofed Web site and recover customer information. Some of these steps will require the assistance of legal counsel.

- Communicate promptly, including through written communications, with the Internet service provider (ISP) responsible for hosting the fraudulent Web site and demand that the suspect Web site be shutdown;
- Contact the domain name registrars promptly, for any domain name involved in the scheme, and demand the disablement of the domain names;
- Obtain a subpoena from the clerk of a U.S. District Court directing the ISP to identify the owners of the spoofed Web site and to recover customer information in accordance with the Digital Millennium Copyright Act;[5]
- Work with law enforcement; and

[4]Domain Name Registrars are companies that allow firms to register domain names with such extensions as .biz, and .com. The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for regulating and certifying companies as domain name registrars. For a listing of all registered domain name registrars see (http://www.icann.org/registrars/accredited-list.html).

[5]The Digital Millennium Copyright Act of 1998 (17 USC 512(h) (2003)) allows firms to request the issuance, by a clerk of any U.S. district court, of an administrative subpoena to an ISP to compel it to disclose the identity of an ISP's subscriber who is allegedly infringing on the name or trademark of the firm. This procedure also allows banks to request confiscation of servers, which might contain illegally obtained customer account information.

- Use other existing mechanisms to report suspected spoofing activity.

The following are other actions and types of legal documents that banks can use to respond to a spoofing incident:

- Banks can write letters to domain name registrars demanding that the incorrect use of their names or trademarks cease immediately;
- If these demand letters are not effective, companies with registered Internet names can use the Uniform Domain Name Dispute Resolution Process (UDRP) to resolve disputes in which they suspect that their names or trademarks have been illegally infringed upon. This process allows banks to take action against domain name registrars to stop a spoofing incident. However, banks must bear in mind that the UDRP can be relatively time-consuming. For more details on this process see http://www.icann.org/udrp/udrp-policy-24oct99.htm; and
- Additional remedies may be available under the federal Anti-Cybersquatting Consumer Protection Act (ACCPA) allowing the bank to initiate immediate action in federal district court under section 43(d) of the Lanham Act, 15 USC 1125(d).[6] Specifically, the ACCPA can provide for rapid injunctive relief without the need to demonstrate a similarity or likelihood of confusion between the goods or services of the parties.

Contact the OCC and Law Enforcement Authorities

If a bank is the target of a spoofing incident, it should promptly notify its OCC supervisory office and report the incident to the FBI and appropriate state and local law enforcement authorities.[7] Banks can also file complaints with the Internet Fraud Complaint Center (see http://www.ifccfbi.gov/), a partnership of the FBI and the National White Collar Crime Center.

In order for law enforcement authorities to respond effectively to spoofing attacks, they must be provided with information necessary to identify and shut down the fraudulent Web site and to investigate and apprehend the persons responsible for the attack. The data discussed under the "Information Gathering" section should meet this need.

In addition to reporting to the bank's supervisory office and law enforcement authorities, there are other less formal mechanisms that a bank can use to report these incidents and help combat fraudulent activities. For example, banks can use "Digital Phishnet" (http://www.digitalphishnet.com/), which is a joint initiative of industry and law enforcement designed to support apprehension of perpetrators of phishing-related crimes, including spoofing. Members of Digital Phishnet include ISPs, online auction services, financial institutions, and financial service providers. The members work closely with the FBI, Secret Service, U.S. Postal Inspection Service, Federal Trade Commission (FTC), and several electronic crimes task forces around the country to assist in identifying persons involved in phishing-type crimes.

[6]Under the ACCPA, owners of trademarks can bring an action against anyone who, with bad faith or intent to profit, registers or uses a domain name that: (1) is identical or confusingly similar to a trademark that was distinctive when the domain name was registered; or (2) is identical or confusingly similar to or derivative of a trademark that was famous when the domain name was registered.

[7] National banks must file SARs in connection with computer intrusions and other computer crimes consistent with 12 CFR 21.11. See OCC Bulletin 2000-14, "Infrastructure Threats – Intrusion Risks" (May 15, 2000); Advisory Letter 97-9, "Reporting Computer Related Crimes" (November 19, 1997). (General guidance is still applicable, although instructions for a new SAR form were published in 65 FR 1229, 1230 (January 7, 2000).)

Finally, banks can forward suspicious e-mails to the FTC at spam@uce.gov. For more information on how the FTC can assist in combating phishing and spoofing, see http://www.consumer.gov/idtheft.

RESPONSIBLE OFFICE

Questions regarding this bulletin should be directed to the Bank Information Technology Division at (202) 874-4740 or to the Special Supervision Division at (202) 874-4450.

Mark L. O'Dell Deputy Comptroller for Operational Risk	John W. Quill Deputy Comptroller for Special Supervision