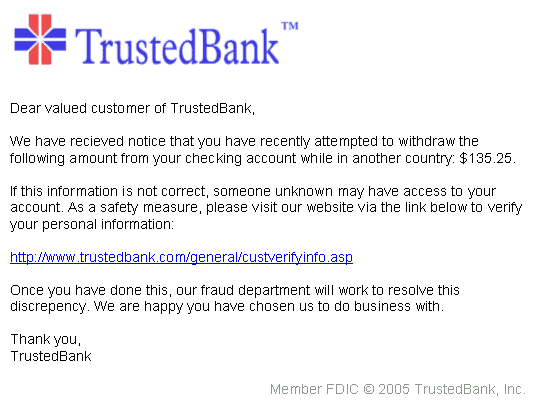
**Case Study Date: May 10, 2013**

**Identity Theft**

**Phishing**

Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.



*A phishing email*

Most people associate phishing with e-mail messages that spoof, or mimic, banks, credit card companies or other business like Amazon and eBay. These messages look authentic and attempt to get victims to reveal their personal information. But e-mail messages are only one small piece of a phishing scam.

**About Phishing**

The phishing process involves:

* Planning. Phishers decide which business to target and determine how to get e-mail addresses for the customers of that business. They often use the same mass-mailing and address collection techniques as spammers.
* Setup. Once they know which business to spoof and who their victims are, phishers create methods for delivering the message and collecting the data. Most often, this involves e-mail addresses and a Web page.
* Attack. This is the step people are most familiar with -- the phisher sends a phony message that appears to be from a reputable source.
* Collection. Phishers record the information victims enter into Web pages or popup windows.
* Identity Theft and Fraud. The phishers use the information they've gathered to make illegal purchases or otherwise commit fraud. As many as a fourth of the victims never fully recover.

If the phisher wants to coordinate another attack, he evaluates the successes and failures of the completed scam and begins the cycle again.

Phishing scams take advantages of software and security weaknesses on both the client and server sides. But even the most high-tech phishing scams work like old-fashioned con jobs, in which a hustler convinces his mark that they are reliable and trustworthy.

Since most people won't reveal their bank account, credit card number or password to just anyone, phishers have to take extra steps to trick their victims into giving up this information. This kind of deceptive attempt to get information is called social engineering.

Phishers often use real company logos and copy legitimate e-mail messages, replacing the links with ones that direct the victim to a fraudulent page. They use spoofed, or fake, e-mail addresses in the "From:" and "Reply-to" fields of the message, and they obfuscate links to make them look legitimate. But recreating the appearance of an official message is just part of the process.

Most phishing messages give the victim a reason to take immediate action, prompting him to act first and think later. Messages often threaten the victim with account cancellation if he doesn't reply promptly. Some thank the victim for making a purchase he never made. Since the victim doesn't want to lose money he didn't really spend, he follows the message's link and winds up giving the phishers exactly the sort of information he was afraid they had in the first place.

In addition, a lot of people trust automatic processes, believing them to be free from human error. That's why many messages claim that a computerized audit or other automated process has revealed that something is amiss with the victim's account. The victim is more likely to believe that someone has been trying to break into his account than believe that the computer doing the audit made a mistake.

The more complex a Web browser or e-mail client is, the more loopholes and weaknesses phishers can find. This means that phishers add to their bags of tricks as programs get more sophisticated. For example, as spam and phishing filters become more effective, phishers get better at sneaking past them.

**Phishing Methods**

The most common trick is address spoofing. Many e-mail programs allow users to enter their desired information into the "From" and "Reply-to" fields. While convenient for people who use multiple e-mail address, this makes it easy for phishers to create messages that look like they came from a legitimate source. Some e-mail servers also allow computers to connect to the simple mail transfer protocol (SMTP) port without the use of a password. This allows phishers to connect directly to the e-mail server and instruct it to send messages to victims.

Other tricks include:

Obfuscated links: These URLs look real but direct the victim to the phisher's Web site. Some obfuscation techniques include:

* Using misspelled versions of the spoofed company's URL or using international domain name (IDN) registration to re-create the target URL using characters from other alphabets. Including the targeted company's name within an URL that uses another domain name.
* Using alternate formats, like hexadecimal, to represent the URL.
* Incorporating instructions for redirection into an otherwise legitimate URL.
* Using HTML to present links deceptively. For example, the link below looks like it goes to a section of "GEC" that describes our college, but it really directs your browser to an entirely different article on zombies.

Graphics. By determining which e-mail client and browser the victim is using, the phisher can place images of address bars and security padlocks over the real status and address bars.

Popup windows and frames. Malicious popup windows can appear over the site, or invisible frames around it can contain malicious code.

HTML. Some phishing e-mails look like plain text but really include HTML markup containing invisible words and instructions that help the message bypass anti-spam software.

DNS cache poisoning. Also called pharming, this is when a phisher (often by speaking to customer service representatives) changes DNS server information. This causes everyone trying to reach the spoofed company's Web site to be directed to another site. Pharming can be hard to detect and can ensnare multiple victims at once.

Phishers can use proxy computers situated between the victim and the site to record victims' transactions. They can also take advantage of poor security at a company's Web page and insert malicious code into specific pages. Phishers who use these methods don't have to disguise their links because the victim is at a legitimate Web site when the theft of their information takes place.

Phishers also use malicious programs in their scams:

* Key loggers and screen capture Trojans record and report information to the phisher.
* Remote access Trojans turn victims' computers into zombies -- machines phishers can use to distribute more phishing e-mail or host phishing Web pages.
* Bots maintain fabricated conversations with victims in chat rooms or coordinate zombie networks.
* Spyware tracks and records users' online behavior, which can help phishers plan other attacks.

**Protection Against Phishing**

The steps you normally take to protect your computer, like using a firewall and anti-virus software, can help protect you from phishing. You can review Web sites' SSL certificates and your own bank and credit card statements for an extra measure of safety.

In addition, phishers tend to leave some telltale signs in their e-mail messages and Web pages. When you read your e-mail, you should be on the lookout for:

* Generic greetings, like "Dear Customer." If your bank sends you an official correspondence, it should have your full name on it. (Some phishers have moved on to spear phishing, which can include personalized information.)
* Threats to your account and requests for immediate action, such as "Please reply within five business days or we will cancel your account." Most companies want you as a customer and are not likely to be so quick to lose your business.
* Requests for personal information. Most businesses didn't ask for personal information by phone or through e-mail even before phishing became a widespread practice.
* Suspicious links. Links that are longer than normal, contain the @ symbol or are misspelled could be signs of phishing. It's safer to type the business's URL into your browser than to click on any link sent in e-mail.
* Misspellings and poor grammar.

Many Internet service providers (ISP) and software developers offer phishing toolbars that verify security certificates, tell you the location where the site you visit is registered and analyze links. They also provide tools for reporting phishing attempts. Other programs use visual cues to confirm that you've reached a legitimate site.

**Responding to Phishing**

If you get an e-mail that you believe is a phishing attempt, you should not reply to it, click on the links or provide your personal information. Instead, you should report the attempt to the business being spoofed. Use their Web site or phone number rather than following links in the suspect e-mail. You can also inform the National Fraud Information Center and the Anti-Phishing Working Group.

If you believe you may have given your personal information to a phisher, you should report the incident to:

* The company that was spoofed.
* Any bank, lending or credit institution for which you have disclosed your personal information.
* At least one of the three major credit reporting companies (Equifax, Experian and TransUnion).
* Your local police department.

You should also change your passwords for the site you believe was spoofed. If you use the same password at other sites, you should change your passwords there, too.