Abstract:

In computing, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from PayPal, eBay, YouTube or online banks are commonly used to lure the unsuspecting. Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a website. Phishing is an example of social engineering techniques used to fool users. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

A phishing technique was described in detail in 1987, and the first recorded use of the term "phishing" was made in 1996. The term is a variant of fishing, probably influenced by phreaking, and alludes to baits used to "catch" financial information and passwords.

Phishing is the practice of sending out fake emails, or spam, written to appear as if they have been sent by banks or other reputable organizations, with the intent of luring the recipient into revealing sensitive information such as usernames, passwords, account IDs, ATM PINs or credit card details. Typically, phishing attacks will direct the recipient to a web page designed to mimic a target organization’s own visual identity and to harvest the user's personal information, often leaving the victim unaware of the attack. Obtaining this type of personal data is attractive to blackhats because it allows an attacker to impersonate their victims and make fraudulent financial transactions. Victims often suffer significant financial losses or have their entire identity stolen, usually for criminal purposes.

The term phishing comes from the fact that Internet scammers are using increasingly sophisticated lures as they "fish" for users' financial information and password data. The most common ploy is to copy the Web page code from a major site — such as AOL — and use that code to set up a replica page that appears to be part of the company's site. (This is why phishing is also called brand spoofing.) A fake e-mail is sent out with a link to this page, which solicits the user's credit card data or password. When the form is submitted, it sends the data to the scammer while
leaving the user on the company's site so they don't suspect a thing.

Introduction:
Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well known and trustworthy Web sites. Web sites that are frequently spoofed by phishers include PayPal, eBay, MSN, Yahoo, Best Buy, and America Online. A phishing expedition, like the fishing expedition it's named for, is a speculative venture: the phisher puts the lure hoping to fool at least a few of the prey that encounter the bait.

Phishers use a number of different social engineering and e-mail spoofing ploys to try to trick their victims. In one fairly typical case before the Federal Trade Commission (FTC), a 17-year-old male sent out messages purporting to be from America Online that said there had been a billing problem with recipients' AOL accounts. The perpetrator's e-mail used AOL logos and contained legitimate links. If recipients clicked on the "AOL Billing Center" link, however, they were taken to a spoofed AOL Web page that asked for personal information, including credit card numbers, personal identification numbers (PINs), social security numbers, banking numbers, and passwords. This information was used for identity theft.

The FTC warns users to be suspicious of any official-looking e-mail message that asks for updates on personal or financial information and urges recipients to go directly to the organization's Web site to find out whether the request is legitimate. If we suspect we have been phished, we can forward the e-mail to uce@ftc.gov or call the FTC help line, 1-877-FTC-HELP.

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 he, is reliable and trustworthy.
History:

Phishing technique was described in detail in 1987, in a paper and presentation delivered to the International HP Users Group, Interex. The first recorded mention of the term "phishing" is on the alt.online-service. America-online Usenet newsgroup on January 2, 1996, although the term may have appeared earlier in the print edition of the hacker magazine 2600.

Early phishing on AOL

Phishing on AOL was closely associated with the warez community that exchanged pirated software. After AOL brought in measures in late 1995 to prevent using fake, algorithmically generated credit card numbers to open accounts, AOL crackers resorted to phishing for legitimate accounts.

A phisher might pose as an AOL staff member and send an instant message to a potential victim, asking him to reveal his password. In order to lure the victim into giving up sensitive information the message might include imperatives like "verify your account" or "confirm billing information". Once the victim had revealed the password, the attacker could access and use the victim's account for fraudulent purposes or spamming. Both phishing and warezing on AOL generally required custom-written programs, such as AOHell. Phishing became so prevalent on AOL that they added a line on all instant messages stating: "no one working at AOL will ask for your password or billing information".

After 1997, AOL's policy enforcement with respect to phishing and warez became stricter and forced pirated software off AOL servers. AOL simultaneously developed a system to promptly deactivate accounts involved in phishing, often before the victims could respond. The shutting down of the warez scene on AOL caused most phishers to leave the service, and many phishers—often young teens—grew out of the habit.
Transition from AOL to financial institutions

The capture of AOL account information may have led phishers to misuse credit card information, and to the realization that attacks against online payment systems were feasible. The first known direct attempt against a payment system affected E-gold in June 2001, which was followed up by a "post-911 id check" shortly after the September 11 attacks on the World Trade Center. Both were viewed at the time as failures, but can now be seen as early experiments towards more fruitful attacks against mainstream banks.

How phishing works?

Suppose we checked our e-mail one day and found this message in our inbox:

Phishing is a method of identity theft. We have an account with HSW Bank, and we've got an e-mail from them before. But this one seems suspicious, especially since it threatens to close our account if we don't reply immediately. What do we do?

This message and others like it are examples of phishing, a method of online identity theft. In addition to stealing personal and financial data, phishers can
infect computers with viruses and convince people to participate unwittingly in money laundering. In this paper, we'll examine the common traits of phishing schemes and the technological tricks that phishers use to deceive people and software.

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.

From beginning to end, the process involves:

1. **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.

2. **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.

3. **Attack.** This is the step people are most familiar with -- the phisher sends a phony message that appears to be from a reputable source.

4. **Collection.** Phishers record the information victims enter into web pages or popup windows.

5. **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

---

**Phishing Facts**

- 13,776 phishing attacks linked to 5,259 Web sites took place in August of 2005.
- They targeted 84 different businesses, but three businesses received 80 percent of the attacks.
- 85 percent of the attacks targeted banks and other financial institutions.
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 he is trustworthy.

Phishing and Establishing Trust
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.

Technical Trickery

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.

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:

  1. 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.
  2. Including the targeted company's name within an URL that uses another domain name.
  3. Using alternate formats, like hexadecimal, to represent the URL.
  4. Incorporating instructions for redirection into an otherwise legitimate URL.

- **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 turns 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.

**Protection from Phishers**
The steps we should normally take to protect our computer, like using a firewall and anti-virus software, can help protect us from phishing. We can review web sites' SSL certificates and our 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 we read our e-mail, we should be on the lookout for:

1. Generic greetings, like "Dear Customer." If our bank sends us an official correspondence, it should have our full name on it. (Some phishers have moved on to spear phishing, which can include personalized information.)
2. Threats to our account and requests for immediate action, such as "Please reply within five business days or we will cancel your account." Most companies want us as a customer and are not likely to be so quick to lose our business.
3. 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.
4. 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 our browser than to click on any link sent in e-mail.
5. Misspellings and poor grammar.
Fortunately, businesses and governments are fighting phishing. The United States government has instructed banks to start using two methods of security that include both passwords and physical objects, like tokens or biometric scanners, for online transactions by the end of 2006. 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 website 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 we have disclosed our personal information.
- At least one of the three major credit reporting companies (Equifax, Experian and TransUnion).
- Our local police department.
- The Federal Bureau of Investigation (FBI) via the Internet Crime Complaint Center.

We should also change our passwords for the site we believe was spoofed. If we use the same password at other sites, we should change our passwords there, too.
Conclusion:

In short, we can conclude that phishing (sometimes called carding or brand spoofing) uses e-mail messages that purport to come from legitimate businesses that one might have dealings with -- banks such as Citibank; online organizations such as eBay and PayPal; Internet service providers such as AOL, MSN, Yahoo and EarthLink; online retailers such as Best Buy; and insurance agencies. The messages may look quite authentic, featuring corporate logos and formats similar to the ones used for legitimate messages. Typically, they ask for verification of certain information, such as account numbers and passwords, allegedly for auditing purposes. And because these e-mails look so official, up to 20% of unsuspecting recipients may respond to them, resulting in financial losses, identity theft and other fraudulent activity against them.

Even before phishing became so prevalent, legitimate businesses and financial institutions would hardly ever ask for personal information via e-mail. If we receive such a request, we have to call the organization and ask if it's legitimate or check its legitimate Web site.

References:

www.howstuffworks.com
www.google.com

THANK YOU