



PHISHING ATTACKS

Reprinted with the Permission of SHAZAM Incorporated

Phishing Attacks

Phishing attacks use phony e-mails and fraudulent web sites designed to fool recipients into divulging personal financial data such as credit card numbers, account user names and passwords, and Social Security numbers. They often indicate that an account will be suspended or closed unless the consumer provides the requested information. By hijacking the trusted brands of well-known banks, online retailers, and credit card companies, phishers are able to convince up to five percent of recipients to respond to them. The phishers use this information to steal the recipient's identity and to either buy goods, obtain cash, or to sell the information to other fraudsters for money. Over the past year, phishing scams have become more sophisticated by using the following techniques:

- ♦ Embedding web site design into the e-mails, complete with stolen logos from the targeted company and fake return addresses that appear legitimate.
- ♦ Linking a legitimate web site in the background, with a fake login box placed in front of the real site. This looks convincing because the legitimate site and the pop-up appear to be from the same source.
- ♦ Providing consumer personal information and redirecting the victim to the real homepage of the company being targeted. Again, this trick is designed to make the victim feel that the request for information is legitimate.
- ♦ Altering the appearance of the victim's address bar by replacing the URL (web address) of the phishing site with that of the company being targeted.

- ♦ Including a virus in the phishing e-mail that runs when the consumer opens the e-mail. Even if the consumer is not fooled and does not respond to the phishing e-mail, the virus silently runs a script that can either record keystrokes made by the consumer (and obtain personal data); or when the consumer attempts to visit their bank's legitimate web site (during that or a future session) the malicious code redirects them to a fraudulent web site.
- ♦ Opening legitimate looking, but fake online sites (such as pharmacies, banks, or mortgage loan firms) with the intent of stealing the information that is provided to them. Online security company, Websense, reports that these advanced scans now outnumber the standard, original phishing e-mails.
- ♦ Using "second chance" scams – people who have lost out in an auction (such as e-Bay) are sent a phony e-mail offering them a second chance to buy the goods on which they bid, but when they click on the link in the fake e-mail, they are taken to a hacker's web site where their account details are stolen.

Test Your Knowledge of Phishing Scams

The Washington Post newspaper has a web site to test your phishing knowledge (<http://www.washingtonpost.com/wp-srv/technology/articles/phishingtest.html?referrer=email>). The web site has links to 10 e-mails – all are real, some are scams, some are not. Read the e-mails and then decide if the e-mail is a phishing scam or not. After you have read them all, click the VOTE button to see how you did.

(continued on next page)

Reporting Phishing Attacks

The Federal Trade Commission (FTC) has an ID Theft web site with information about what to do if you think your identity has been stolen (www.consumer.gov/idtheft). You can also call the FTC at 877-438-4338 for more information.

Report the receipt of a phishing e-mail to the Anti-Phishing Work Group at www.antiphishing.org/report_phishing.html. Instructions are provided on how to forward the suspect e-mail to keep pertinent information intact.

Phishing Tips

Here are some things to remember to help protect against becoming a victim of a phishing scam:

- ◆ Treat with caution any unsolicited e-mail that alleges to come from a trusted company.
- ◆ If you're suspicious about an e-mail, don't open it or click on any links. If you want to confirm the validity of the e-mail, open a new browser window and type the valid URL (web address) for the company itself.
- ◆ Be suspicious of e-mails that don't greet you by name. A message that says "Dear e-Bay Customer" is probably not from e-Bay.
- ◆ Ask yourself, "Why is the company writing to me about this?" If you have any doubts, call the company or go to its web site on your own.
- ◆ Don't click or open any attachments – they could contain viruses or spyware that records where you go online and captures any passwords or card numbers that you type online.
- ◆ Look for "https" in URLs displayed in your browser's address bar. The "S" stands for secure. If you don't see it, you're not in a secure web session and shouldn't enter any personal or financial data.
- ◆ If you see the @ symbol in the middle of the URL (web address), there's a good chance this is a phishing scam. Legitimate companies use the domain name in their web address (www.company.com) and don't have the @ symbol in their URL (web address).
- ◆ Maintain up-to-date firewalls and security patches.
- ◆ If your information is compromised, place a fraud alert on your credit report by contacting the fraud department of anyone of the three major credit bureaus.

Visit the Federal Trade Commission's ID Theft page for more information on how to protect yourself from identity theft (see link above).