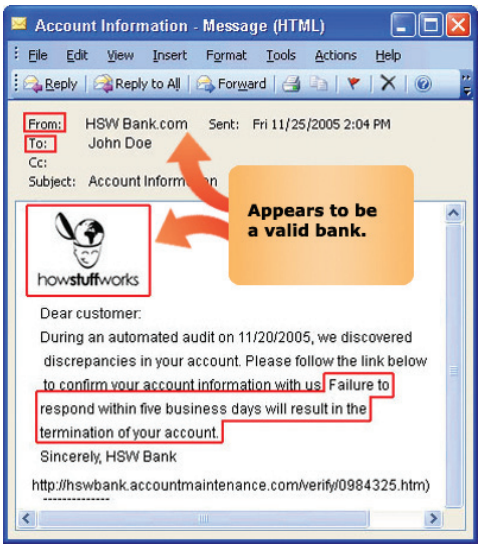
Phishing

What is "Phishing?"

Phishing is an attempt to fraudulently acquire sensitive information, such as usernames, passwords, credit card numbers and social security numbers, by masquerading as a trusted person or business in an electronic communication. Most commonly, phishing is attempted by e-mail or instant messaging (IM), often trying to trick users into entering their login details at a website that appears to be trusted, but in reality is controlled by the phisher, or by getting a user to click on a link in an e-mail or IM that executes malicious code on their machine.

For example, users of online banks are common targets: users may receive an e-mail claiming to be from their bank (see the e-mail in the example), asking them to follow a link provided in the e-mail. It will contain what appears to be a legitimate bank (maybe even your own) in both its logo and the "from" address. It will request that you log in to their online banking site. It is a scam that can cause phishers to remove funds from the victim's account. (Note that NO valid financial institution will ever ask you to do this!)



Phishing schemes can also be used to compromise login credentials of online applications such as NetSuite. Thus, we strongly encourage you to protect your financial and business data, and that of your customers by educating your employees about phishing: what it is, how to detect it; and how to avoid it.

Steps to Keep Your Personal Information Safe

All employees should be familiar with smart phishing-avoidance habits. Employee awareness is one of the most effective steps against any social engineering attack. The Anti-Phishing Working Group (http://www.antiphishing.org/) is a good resource for training materials and whitepapers.

1) First and Foremost

Never open suspicious e-mails. Do not ever click links in untrusted e-mail or emails from someone or a company you do not know. Often such links take you to a log-in page that could be bogus, and in logging in, you are surrendering your information. So if you click on a link in an email or an Instant Message, do not ever input any personal or account information—passwords, account numbers, etc., on any pages that then appear. To avoid fraudulent links, only access the sites you want to go to—your bank, for example—at its www address—never through any links sent within emails or IMs.

2) Protect Your Credentials

Always log in to NetSuite at https://system.netsuite.com/pages/customerlogin.jsp. Never follow a link to log in to NetSuite from within an e-mail or IM. Instead, bookmark the NetSuite login page.

3) Browse Wisely

Make sure your users are using the latest versions of Internet Explorer or Firefox as those web browsers include some built in protection against known phishing websites. These browsers use technology to compare visited sites against databases of discovered phishing sites.

4) Look Closely at URLs

Look for https://system.netsuite.com/pages/customerlogin.jsp in your browser every time you login and ensure that you get a secure lock icon. "https" + a lock means SSL is working. The "system.netsuite.com" domain is the secure login domain. The trailing slash "/" after the .com is important. It prevents an attacker from creating a malicious URL such as "https://system.netsuite.com.customerlogin.jsp.< malicious domain name>".

If you ever receive an "untrusted certificate" warning from NetSuite, do not accept the certificate. Instead, double-check the URL and ensure that you're really at NetSuite. If you have any doubt, contact NetSuite Support before logging in.

5) Harden Your Security

Enable IP address restrictions in your NetSuite account, especially for highly privileged accounts such as Administrator. With IP address restrictions in place, even compromised logins are useless to the phisher unless they can also gain access to the trusted network.

6) Know Your E-mail Originators

Block inbound messages at the perimeter that contain a "From" address with your own domain (as applicable). Make sure mail from known sources originates from those sources. For example, if you do a lot of business with a sister organization make sure e-mail from that organization originates from known SMTP servers.

7) Double up on spam defenses

Often times phishing messages originate from compromised computers or "botnets." Your anti-spam appliance may have already identified the source as a botnet—a compromised or rogue SMTP server. Having multiple devices, or services, verifying incoming mail ups the odds of detection.