

Safe Computing Initiative – Phishing Scams



Have you ever received an email message from your bank asking you to confirm your social security number or password? If so, you were the target of a "phishing" scam. Hopefully you didn't "take the bait."

Phishing is an online con game where thieves use fake email messages and websites to trick people into revealing sensitive personal information such as their social security number, credit card number, bank account information or personal passwords. They use this information to illegally purchase goods and/or commit identity theft.

Phishing most often occurs when an email message which looks authentic appears to come from a well respected company and asks you to confirm your account information. Many times the request is linked to a crisis such as the suspension of your account if you don't answer the questions. Should you click on a link in that email you are transported to a fraudulent website which looks very similar to that company's real website. Any personal information you enter at this point will be stolen.

Is Phishing successful? It is believed that 2-6% of phishing emails result in the end user revealing personal information. Remember, these email messages look legitimate and even have the company logo embedded in them.

How can you protect yourself?

1. Treat every email you receive with great caution. Legitimate companies will not send you an email asking you to provide account information, social security numbers.
2. Never click on links in an email that you suspect may be fraudulent. If you go to a financial website on your computer, go there directly by typing the web address yourself.
3. Protect your computer with excellent security software including retroviruses, , antispasmodic.
4. Don't panic, just delete these phishing messages.
5. Learn more about phishing and how to spot a phishing scam. Microsoft has an excellent article about phishing at:
<http://www.microsoft.com/protect/yourself/phishing/identify.msp>