

# Identity Theft: Can You Spot 'Phishing' Attempts?

by Chris Sivori, JSJ Productions, Inc.

There's a new type of email-based Internet scam called 'phishing' (pronounced 'fishing'). Internet scam artists 'fish' for your personal information by using carefully crafted methods to trick you into giving out your Social Security Number, credit card numbers, bank account numbers and other personal information they can use to steal your identity and defraud you. Once compromised, it could take years to clear your financial history and personal reputation. By understanding how these Internet thieves work, you can protect yourself from becoming a victim.

## How do these scammers get your information?

In many phishing scams, you will receive a realistic looking email from a company which you are familiar. You may even be a customer. The email will usually look legitimate and professional: it has the company logo, they address you by name, etc. Often, this email will warn you of some danger to your bank account or credit card and will tell you that you need to take action immediately to avoid serious consequences. There will be a link for you to click that indicates you will be taken to a website for account verification. If you click the link, you will see a website that looks exactly like the real company website. Next, you will be asked to 'verify' your account number, password or credit card information. If this happens, stop immediately! Do not fill in any personal information. Immediately close the web browser and delete the phony email that you received.

## How can you spot a 'phishing' email?

Look at the email. If you did not contact this company asking about your account



or for help with a problem, be suspicious. If you are not sure because the email looks so real and official, call the company by telephone. Use the phone number from your monthly statement, not from the email itself. If it is after hours and no one is there to take your call, wait until the next business hours when you can reach someone. Don't feel pressured that you have to take action immediately. 'Phishers' are hoping that you will fall for their scam by creating a sense of impending disaster. Don't let them trick you into clicking on their link and stealing your personal information.

## What steps can you take to avoid Identity Theft?

- Never give anyone your account information over the Internet or telephone when it is the result of an unsolicited request. Your credit card company and bank know who you are. They will never call or email to ask you to verify your password or credit card number. They can just look it up.

- Go over your monthly statements every month as soon as they arrive. Stay on the lookout for unfamiliar charges and check your credit report at least once a year. Recent legislation has mandated that the credit bureaus provide you with a free credit report once a year. Just visit [www.annualcreditreport.com](http://www.annualcreditreport.com) for more information on how to view your credit report online.
- If your bank or credit card statement is ever late in arriving in the mail, call and find out why.

Always ask questions and always follow your gut instinct that something is not right. By exercising a normal amount of caution you can avoid 'phishing' scams.

Christopher Sivori is Chief Web Designer for JSJ Productions, Inc. and Marketing Strategist for Duet Design ([www.duetdesign.com](http://www.duetdesign.com)). Problems, questions or comments? Email Chris at: [csivori@duetdesign.com](mailto:csivori@duetdesign.com).