



## Online Scams

In 2007, 90,008 fellow Americans reported that they were a victim of online fraud to the national Internet Crime Complaint Center ([www.ic3.gov](http://www.ic3.gov)). Of those 90,008 people 72,226 suffered a financial loss totaling \$239,000,000. Online fraud is a growing concern among many people and in this article we will examine the most popular online scams out there today and ways you can protect yourself.

Generally people falsely assume online scams originate from foreign countries such as Nigeria for instance, whom is actually ranked 3<sup>rd</sup> for computer crime suspects worldwide. The harsh reality is that the United States is the top originator of all worldwide online fraud crimes. This alarming statistic comes with the added information that the majority of online fraud victims are male, with the average age between 40-49 years old. Even more surprising is the fact that Oregonians rank #6 in the national standings for victims of online fraud in the United States.

All of these online scams have one common denominator; they use e-mail and/or a website to contact their victims. The largest scam method being actively used today is a method commonly referred to as Phishing. In addition to phishing other scam methods that are growing in popularity are pharming and vishing; please see the definitions below for more information.

*Phishing: The elicitation of information from people under false pretenses.*

*Pharming: A hacker's attack to redirect web traffic from a legitimate website to a bogus website.*

*Vishing: The use of social engineering and voice over IP telephone exploits to steal personal information by the telephone.*

If you've used e-mail for any length of time it is a safe bet you have received phishing e-mails. Most often these e-mails are sent purporting to be from a financial institution or a company such as eBay or PayPal. The goal of phishing e-mails are all the same – to collect personal information from you to use against you. When the recipient of a phishing e-mail enters in personal information such as name, address, account numbers, passwords, etc., it is all sent to a criminal who in turn uses that information to drain accounts, make fraudulent purchases, steal the recipient's identity, or sell the information to someone else.

There are many scams out in cyberspace right now, with the top scams involving the sale of pets, secret shopper employment and romance connections. While the content of the messages may differ, their methods are all very similar.

Several scams involve fraudulent checks and money orders. If you choose to sell goods on the Internet and a buyer pays you with a check or money order, ensure that they are legitimate and are cleared by a bank before you send the purchased items.

If you receive an e-mail that looks too good to be true, it probably is. Always remember that no financial institution is going to ask you to input your personal information into an e-mail. When in doubt, place a phone call to a business to inquire about the legitimacy of something, or do some researching on Google or Snopes ([www.snopes.com](http://www.snopes.com)). Often enough you can find a press releases or other information about a known scam just by pasting some of the body of an e-mail into a Google or Snopes search. If you do have a phishing e-mail the best thing to do is delete it, or forward it to the business it is claiming to be from and report it on the [www.ic3.gov](http://www.ic3.gov) website.

Written by Sergeant Josh Moulin

Southern Oregon High-Tech Crimes Task Force