



Protecting Yourself From Email Fraud

By Mark Bella

Email spam has grown exponentially over the last few years. Forty percent of all emails sent are considered spam, which equates to 12.4 billion spam email daily.ⁱ Besides spam, people are presented with another issue, fraudulent emails. An estimated 57 million American have received a phishing email.

Phishing is the most prevalent of all internet scams. Phishing is a technique used by criminals to have you disclose personal information. A phishing email pretends to be from a legitimate company such as a bank, credit-card company or website and often uses authentic letterhead and graphics to gain the trust of the recipient. The emails sent depict some type of urgency such as account validation and request usernames, passwords, address, phone numbers, bank account numbers, credit card numbers, and social security numbers. Any links provided in the email may display legitimate URLs, but when you click on them they lead you to a different address that spoofs the real URL. This is where your personal information is collected by the criminals. The information gathered is then used to access bank accounts, apply for credit cards, etc.

Each successful fraud nets an average of \$1,400 and is already a \$5 billion industry.ⁱⁱ The most common types of fraudulent emails are phishing, advanced fee and pyramid scheme. Identifying a fraudulent email is a key component in protecting yourself.

Here is a sample phishing email:

Subject: eBay Account Verification
Date: Fri, 20 Jun 2003 07:38:39 -0700
From: "eBay" accounts@ebay.com
Reply-To: accounts@ebay.com
To:

Dear eBay member,

As part of our continuing commitment to protect your account and to reduce the instance of fraud on our website, we are undertaking a period review of our member accounts.

You are requested to visit our site by following the link given below

<http://arribba.cgi3.ebay.com/aw-cgi/ebayISAPI.dll?UpdateInformationConfirm&bpuser=1>

Please fill in the required information.

This is required for us to continue to offer you a safe and risk free environment to send and receive money online, and maintain the eBay Experience.

Thank you



Accounts Management As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our Privacy Policy and [User Agreement](#) if you have any questions.

Copyright © 1995-2003 eBay Inc. All Rights Reserved.

Designated trademarks and brands are the property of their respective owners.

Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#) . iii

The Advanced fee fraud dates back to the 1920's. The advanced fee fraud tries to persuade people to advance small amounts of money and in return receive a larger sum. It has gone through much different iteration and comes through mail, fax and now e-mail. The messages themselves usually involve a person from a foreign country that needs to deposit money somewhere outside of their country and promise the email recipient a percentage of the money deposited. Following a reply, money is requested in order to cover transaction fees along with personal information such as a bank account number and social security number. In the end money is collected by the criminal or the email recipient's bank account is emptied and all further contact is lost.

The pyramid scheme is a scheme in which a hierarchy is created by people joining under others who joined previously with the expectation of being able to collect payments from those who join below. A chain-letter is sent to the email recipient with the request that an undisclosed amount of money be sent to the first person on the list along with additional names and to forward the letter. After payment is the sent to the first person on the list will, that name will be removed and the recipient's name added to the list. A new email will be sent out with the list of names provided by the email recipient and the process is repeated. The pyramid schemes are prohibited by US law and many other nations because it is consider outright fraud.

There are several key components you must lookout for in order to protect yourself. The first component is if an email requests personal information. Legitimate businesses do not request personal information via email. If you receive an email from your bank or creditor, call the number on the back of your credit or debit card and inquire about the information requested. Never click on the links within these emails. The second component is if the email requests money. Never send money. The third component is if any email addresses you with a general term such as "Valued Customer", this is a red flag that the email is sent in bulk to multiple people and the sender has no information about you. The forth component is fake URLs. This is harder to identify because the link provided is spoofing legitimate websites. You can usually identify fake URLs by examining the URL provided and highlighting the link. You will usually notice the link displayed on the lower left hand corner of your internet browser is different that URL displayed on the webpage. If you are still unsure, do not click the URL provided in the email message. Instead call your financial institution instead.

If you look for the components mentioned above, you can avoid becoming a victim of email fraud. However, if you believe you've fallen victim to fraud, there are a few steps you should immediately take.



First is to report the issue to your bank and creditors. They will freeze and monitor your accounts. The second is to file a police report. This will aid you in disputing fraudulent charges. The third is to report that you have become a fraud victim to the [Federal Trade Commission](#). They will assist you with contacting the proper law enforcement agencies.

ⁱ Don Evett - <http://spam-filter-review.toptenreviews.com/spam-statistics.html>

ⁱⁱ Gartner Group – <http://www.gartner.com>

ⁱⁱⁱ Privacy Rights – <http://www.privacyrights.org>