

# Increase your Understanding of Phishing Scams

## Sound Advice

### From Jeff York

As we become more and more reliant upon the internet, words like Malware, Spoofing, and Phishing are becoming part of our daily vernacular -- unfortunately, for all of the wrong reasons. These terms all are key components in identity theft. Understanding what they are and how they can compromise the confidentiality or integrity of your personal data is critical.

**Malware** is a shortened term for malicious software. It has everything to do with the intent of the software, which is to infiltrate a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software.

Software is considered malware based on the perceived intent of the creator rather than any particular features. Malware is not the same as defective software, that is, software that has a legitimate purpose but contains harmful bugs.

**Spoofing** is a term used to describe fraudulent e-mail activity in which the sender address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source. Simply put, you think an e-mail is coming from a legitimate source, but it instead is coming from someone with ill intentions. The goal is to acquire sensitive personal information, such as usernames, passwords, and even credit card details.

**Phishing** is a type of spoofing, luring unsuspected customers into providing sensitive personal information, or in some cases, downloading malware. The classic example of a phishing scam is an email that appears to be coming from a financial institution and includes a link to a fraudulent website. In order to access the link, you add sensitive password or account data, and the fraudulent site instantly and irreversibly captures your personal data. Phishing isn't just an email trap. You can fall victim through a text message (SmiShing), or through a phone call as well (Vishing).

Most people probably consider themselves as internet savvy, so why do phishing and spoofing scams work so often? Fraudsters are, in most cases, more savvy than you are. But, all is not lost. Here are some key tips to avoid becoming caught in the net of a phishing scam:

Be suspicious of any email with an urgent request for personal information. Phishers typically include emotional statements – both positive and negative – to get you to react immediately. Information requested often includes usernames, passwords, credit card numbers, even your social security numbers and date of birth. If you have the slightest

bit of suspicion, call your financial institution or your credit card company to verify the request before responding.

Do not use links in an email if you suspect the message might not be authentic or you do not recognize the sender. Instead, stop and verify. One phone call to the company whose card you are carrying can easily save the day for you.

You should regularly check your financial institution statements and credit card statements to make sure that all transactions are legitimate. If anything looks suspicious, contact your financial institution immediately.

It is important that you report any phishing scam immediately, and here are two links you can use: [reportphishing@antiphishing.org](mailto:reportphishing@antiphishing.org), or [spam@uce.gov](mailto:spam@uce.gov). Your email could prevent someone from taking the bait.