



PHISHING – knowing what to do...

What is Phishing and Pharming?

Phishing is the act of stealing consumers' personal identity data and financial account credentials. Spoofed e-mails are sent out to lead consumers to fake websites designed to look like the original websites to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers.

Phishers use well-known brand names of banks, e-retailers and credit card companies to convince recipients to respond. Some phishers plant crimeware onto PCs to steal credentials directly from the PCs using Trojan spyware.

SEO Solution believes that the only way to fully protect yourself from phishing is to understand and be able to identify the threats and ensure that any phishing emails are reported to the victimised directly. eCommerce businesses should understand the consequences of phishing and be able to deal with the issue. Communication on phishing issues should be communicated on their websites to assure customers that the business understands the risk and will take appropriate action.

How to identify a phishing email?

Read the subject lines carefully before opening an email. Emails with subject lines similar to the following are likely to contain spam or a virus:

- Notice: ****Last Warning****
- **SUSPENDED ACCOUNT**
- **Your Email Account is Suspended For Security Reasons**
- Notice:*****Your email account will be suspended*****
- **Your Email Account Has been Blocked**
- ***WARNING* Your email Account Will Be Closed**
- **Security measures**
- **Email Account Suspension**
- ***IMPORTANT* Please Validate Your Email Account**

In all reported cases, the email does not address you by name but it will address you in a generic way, such as "Dear member" or "Dear customer"

There is a threat that if you do not respond your account will be closed or suspended.

This document is proprietary and for use only by SEO Solution. This document cannot be distributed without the prior consent of SEO Solution.

What to do if you receive a phishing email?

Make it a habit to **carefully look at both the sender's email and subject line before opening any email messages**. This is especially important now as it has become common practice among spammers and virus programmers to send *spoofing* viruses which use email addresses that are similar to legitimate addresses, in order to increase the potential that the email carrying a virus will be opened and thereby spread.

You should contact the company or website owner either by telephone or by email (NOT by responding to the phishing email) immediately and inform them of the email. The company will normally ask you to send them a copy of the email and delete the phishing email immediately. The company should then get back to you to confirm whether it is a phishing email or otherwise. Please note that for small and medium-sized businesses they may not understand what phishing is about and therefore may fail to respond as appropriate.

You need to ensure that your anti-virus software is up-to-date. In some cases viruses are being attached to some of these messages. If you are concerned that you have contracted any viruses, run your anti virus programs and contact your anti-virus software provider if you need help to remove it.

If you would like more information about other current viruses, including how to check to see if your computer is infected, check the following sites

www.symantec.com
www.mcafee.com

To find out more about phishing, see www.antiphishing.org.

Prepared by Sally Fok
www.seosolution.co.uk