

## Something's a bit Phishy

7/12/2005

**Phishing is the latest internet fraud to hit businesses, governments and individuals alike. The WSI [Internet Consultants](#) marketing team outlines what it is and how to make sure you're not the next victim.**



Ron McArthur, president, WSI

Phishing, the practice of luring unsuspecting victims to disclose personal information online, has quickly become the fastest growing security threat to internet users. Governments, businesses and individuals worldwide are all being forced to take this threat seriously to avoid falling victim to this and other forms of online scams.

The objective of phishing is to collect sensitive information to commit identity theft and run up bills, empty bank accounts or commit crimes in the victim's name. Phishers accomplish this by sending emails or pop-up messages under the guise of a legitimate business: banks, online payment services, internet service providers and even government organizations. Recipients are solicited to submit personal information in order to 'validate' or 'update' their account information or face dire consequences.

Phishing is particularly insidious as it exploits internet-based technology to track the activities of internet users, identifying the businesses or organizations a particular target deals with, and thereby lending credibility to the scam and increasing the potential that the target will divulge the information desired. Phishers have been known to collect information using dummy sites developed to fool targeted individuals into believing these are legitimate sites of trusted businesses or organizations.

To avoid falling victim to this and other online scams, internet users must be cautious who they do business online with and make sure they never transmit sensitive information over email. Emails or pop-up messages that ask for personal information should be deleted, and users should never open attachments or click on links that seem suspicious or are sent from individuals or companies not known to them. Credit card statements should also be checked as soon as they are received and any dubious charges investigated through the provider. Anti-virus software and firewalls can also protect you from unintentionally accepting phishing emails or pop-ups which often also contain spyware or viruses.

**“ Phishers have been known to collect information using dummy sites developed to fool targeted individuals into believing these are legitimate sites of trusted businesses or organizations ”**

The FTC (Federal Trade Commission) is actively investigating the threat of phishing and internet service providers, led by AOL, are working towards preventing this activity online. These organizations continue to identify and limit the access of phishers to the online community, instigating legal action when appropriate.

### About [WSI](#)

[WSI ICE](#) is the world's largest network of [internet consultants](#) with offices serving over 1,000 local markets worldwide. Ranked the number one internet services business by Entrepreneur magazine, our proven systems are used to deliver thousands of economical e-business solutions to small and medium-sized businesses annually.