



ALLIANT ADVISORS

FIND DIRECTION



The Navigator

Important Markers To Guide Your Way

April 2006

Welcome to The Navigator's April update. Alliant advisors is here to emphasize the passion we have for working in close alliance with our clients to Find Direction for their business and personal goals. With the continuing promise to share dialogue with you, we will be sending you bits of helpful and useful information through e-mail to keep you up to date on any current changes, due date reminders, or other information that may be relevant to your specific needs.

We hope you will enjoy and value this information. If you do not wish to receive this information by email please respond to this message and we will remove you from the list. For more information about any aspect of our services, visit www.alliant-advisors.com or call your local office.

The Alliant Team

Suspicious e-Mails and Identity Theft

The Internal Revenue Service has issued several recent consumer warnings on the Use of the IRS name or logo by scamsters trying to gain access to consumers' financial information in order to steal their identity and assets. When identity theft takes place over the Internet, it is called "phishing."

Phishing (as in "fishing for information" and "hooking" victims) is a scam where the Internet fraudsters send e-mail messages to trick unsuspecting victims into revealing personal and financial information that can be used to steal the victims' identity.

Current scams include phony e-mails which claim to come from the IRS and which lure the victims into the scam by telling them that they are due a tax refund.

When the IRS learns about the schemes, they try to alert both consumers and authorities so that they can shut down the scheme, if possible. Here is one of the most recent schemes:

E-mails claiming to come from tax-refunds@irs.gov, admin@irs.gov and similar variations told the recipients that they were eligible to receive a tax refund for a given amount. It directed recipients to claim the refund by using a link contained in the e-mail which sent the recipient to a Web site. The site, a copy of the IRS Web site, displayed an interactive page similar to a genuine IRS one; however, it had been modified to ask for personal and financial information that the genuine IRS interactive page does not require.

The Treasury Inspector General for Tax Administration has found numerous separate Web sites in at least 20 different countries hosting variations on this scheme.

For more information on the various schemes, see the following:

[IR-2005-136, IRS Warns of e-Mail Scam about Tax Refunds](#)
[IR-2006-25, IRS Announces 2006 Dirty Dozen Tax Scams](#)

* Above information obtained from <http://www.irs.gov>

.