



Helping Employees Make the Most of Their 401(k)/403(b) Plans

Don't Be Phish Bait

Avoid Phishing Scams

With newspapers, magazines, television, and the Internet full of warnings about phishing scams, it's astonishing that so many people continue to fall victim to the many variations of this high tech scam that tricks you into providing private information for the purpose of stealing your identity. Phishing scams use a variety of ways to convince you to give up one or more of the following pieces of personal information:

- your credit card number
- bank account information
- social security number
- passwords
- other personal information

Falling for a phishing scam by providing this personal information can have disastrous consequences for you financially.

Protect yourself from becoming phish bait with a little information and a big dose of skepticism.

Phishing usually occurs when you receive an e-mail or pop-up message that claims to be from a legitimate business with which you have a relationship: your credit card company, bank, Internet Service Provider, or an online service like Ebay or PayPal. You're told that it's critical for you to update or validate your personal information in order to avoid dire consequences to your account. If you take the bait, you'll be directed to a Web site that looks legitimate but isn't.

Chas. P. Smith & Associates, PA, CPA's
1509 South Florida Avenue, Lakeland, FL 33803
Telephone (863) 688-1725; Fax (863) 688-0692
www.my401kpilot.com
email pgolotko@my401kpilot.com

Once at the site, you'll be asked to provide personal information. Don't do it! Legitimate businesses will not approach you in this manner. If you have a question after receiving such an e-mail or pop-up message, call the organization and ask if the message was legitimate; Chances are it wasn't.

Common phishing come-ons include statements such as:

- Verify your account...
- Dear Valued Customer...
- If you don't respond within 48 hours, your account will be closed...
- Click the link below to gain access to your account..

To protect yourself from phishing scams the Federal Trade Commission offers the following advice:

- Never respond to the type of e-mail or pop-ups mentioned above.
- Keep your virus protection software up-to-date.
- Don't send personal or financial information in emails. E-mail is insecure.
- When entering personal information on a Web site with which you initiate a transaction, make sure the "http" in the address bar changes to "https" and the padlock icon appears in your browser window, indicating that the site is secure.
- Check your credit card statements carefully and report any charges that look suspicious.
- If you have broadband Internet access, consider adding a firewall to protect your computer.
- Be very cautious when opening any e-mail attachments.
- Don't download files you receive in e-mail.

Call for a free half-hour analysis of your retirement account.

Chas. P. Smith & Associates, PA, CPA's
1509 South Florida Avenue, Lakeland, FL 33803
Telephone (863) 688-1725; Fax (863) 688-0692
www.my401kpilot.com
email pgolotko@my401kpilot.com