progressive strategies
FINANCIAL GROUP

THE WHITE PAPER

Your Guide to Life Planning

February 2016

Tori Patrick
President
Progressive Strategies Financial Group
27201 Puerta Real Suite 300
Mission Viejo, CA 92691
949.204.3800 702.893.1500
Fax: 702.549.1900
Tori@psfgwealth.com
www.psfgwealth.com
CA Insurance Lic# OJ13973

Surf Safely: Protect Yourself From Online Scams

Online criminals continuously change their operating methods. That's why it is crucial that Internet users keep up on the latest scams and the steps to take to protect their personal and financial information when online.

Here is an overview of two of the most widespread techniques being used to commit online fraud, as well as some practical tips to protect your personal security.

Phishing: This is one of the most popular methods of online fraud. Phishing, or "spoofing," is a scheme whereby users are sent fake emails that claim to be from a legitimate source. The email directs the user to a counterfeit website where they are asked to update personal information, such as passwords and user names or credit card, Social Security, and bank account numbers. By hijacking brand names of banks, online retailers, and credit card companies, phishers often convince recipients to respond.

Crimeware: This is a class of computer programs designed exclusively to facilitate online identity theft. Cyber thieves use a variety of techniques to steal confidential data through crimeware, including:

- Secretly planting keystroke loggers onto a user's computer to collect sensitive data -- such as login and password information for online bank accounts -- and reporting the data back to the thief.
- Redirecting a user's browser to a counterfeit website controlled by the thief even when the user types the website's proper address in the address bar.
- Stealing passwords cached on a user's system.

This type of scam received national attention several years ago when it was revealed that business executives at major U.S. firms were the targets. The "bait" used to lure the recipient was an official-looking subpoena from the U.S. District Court in San Diego. When recipients clicked on the document to view it, software designed to collect keystroke data was secretly installed on their computers. It was estimated that thousands of people fell victim to this scam.

Play It Safe

The Federal Bureau of Investigation estimates that online scams were responsible for approximately $782 million in losses in 2013.[1] With the number and sophistication of online scams increasing, there are some basic recommendations you can follow to help avoid becoming a victim.

- **Don't recognize it? Don't open it.** Do not open any email, email attachment, or website link from suspicious or unknown senders.
- **Don't give out your info.** Be wary of any e-mail that asks for personal information such as passwords or account numbers. Similarly, avoid any email that promises a prize or gift in exchange for completing a survey or answering questions online.
- **Blast those pop-ups.** These small windows typically appear on or behind the window that you are currently viewing. While many are harmless advertisements, some may contain viruses or software that can monitor your Web activity.
- **Be sure sensitive data is encrypted.** Always ensure that you are using a secure website -- one that employs state-of-the-art encryption technology -- when submitting credit card data or other sensitive personal information.
- **Check your accounts.** Regularly log in to your online accounts and check your bank, credit, and debit card statements to ensure all transactions are legitimate.
- **Keep your system up-to-date.** If your computer's operating system is more than five years old it may not offer the same degree of protection as newer models. Most system manufacturers issue updates and security patches on their websites or automatically through your Internet provider. Similarly, be sure to use the latest Web browser and anti-virus software.

Finally, if you think you've fallen victim to a scam, report it. The FBI has a Cyber Operations unit devoted to fighting cyber crime. Their Internet Crime Complaint Center is at www.ic3.gov.

[1]*Federal Bureau of Investigation, Internet Crime Complaint Center, 2013 (most recent available).*

Compliance Tracking #517633
This article was prepared by Standard & Poor's Financial Communications