NOYES CAPITAL MANAGEMENT, LLC

Personal Financial Planning & Prudent Investment Management
www.NoyesCapital.com
(973) 267-8120

February 9, 2011

Protect Yourself from Internet Theft and Fraud
By Scott P. Noyes, CFA® CFP® and Claudia E. Mott

Internet identity theft and fraud is on the rise and is becoming increasingly more sophisticated. One of our clients was recently "phished" through his bank account and over $60,000 was removed. I am aware of another case, where the crooks phished a man's brokerage account and used the information to open a second brokerage account which could be accessed with the thief's fraudulent signature. Over $200,000 was transferred on a like-name basis. Fortunately, in both cases the victims received full recoveries – they were lucky. Retirees with less computer sophistication and more money seem to be prime targets. I am writing this today because I believe you should take action now to protect yourself.

The word fishing used to evoke images of leisurely time spent near a quiet lake or stream with a rod in hand. Today "phishing" refers to the activities of Internet hackers who use sophisticated techniques to steal private information from individuals such as account numbers, account ids and passwords. Fake bank or brokerage websites are a standard ploy. Providing your credit card number to a phony charity or relative is another. These tricks are known as identity theft and affected over 11 million Americans in 2009 at a cost of $54 billion. You should take a few simple steps to protect yourself and avoid the risk of falling prey to these criminals.

Easy Steps to Protect Yourself

Avoid getting caught. Most phishing is done by sending an official looking email from a bank, credit card agency, or even a charity, asking you to provide personal information because there is a problem with your account. The message provides a link to a website that may look exactly like your banks', but is designed to capture your account or social security number, along with other personal information. Never open an email requesting this information. If in doubt, log in to the bank website from your own safe link. If there is a problem with your account, most banks and credit card companies will call you directly.

Beware of phone scams. Be suspicious of any request for personal information from someone representing a bank, credit card company, charity or other organization. The caller may try to convince you that you must provide either your account number, social security number or both. A legitimate call from a bank or credit card company will require you to answer very specific security questions before they will discuss the reason for the phone call. If you are wary about a caller's intentions, hang up and call the Customer Service number on your statement.

Keep your personal information private. The rise in popularity of social networking sites like Facebook has opened a new door for hackers to find personal information. Recently, a teenage

girl's Facebook account was hacked by someone who not only started sending inappropriate messages to her friends, but changed the passwords on the email, instant messaging and blog accounts she had linked to her profile. By taking control of her account, this individual also had access to all of the information on her friends' profile pages. After numerous emails to Facebook, the password was reset and she was able to regain control of her account. The lesson from this is to be mindful of what you post to your profile. Listing your high school, former employers and interests are good for reconnecting with old friends, but your phone number, email address and home address should not be entered on the contact page.

Create unique passwords. A good password should contain a combination of letters, numbers and symbols and should not contain your birth date, social security number, name or initials. It is recommended that you change your passwords periodically.

Use secure email. Do not send important personal information in unencrypted e-mails or via fax machines. An ordinary email can be intercepted and read by more than the intended recipient once it has been sent. This is a growth industry in Russia! Encryption is a process of protecting an email and its contents from identity thieves who may be looking for account numbers, passwords, social security numbers or other personal information. Both Hotmail and Gmail allow users to use secure email by modifying your profile setting to automatically use an "https" prefix.

Monitor your bank and credit card charges online. It is easy to log on to your bank website or credit card website and review your recent charges. Reviewing a monthly statement can be too late. Fraudulent or questionable charges should be reported immediately. Ten minutes of weekly review is an important step to maintain control of your finances.

Close unused bank, brokerage and credit card accounts. They do not die on their own. Even if you have a zero balance, banks and brokerage accounts will leave your accounts open and may even charge a fee. It takes about two minutes to draft, print and mail your closing account letter.

Subscribe to a credit monitoring service. Subscribing to a credit monitoring service for as little as $10 per month helps you control unauthorized new accounts and manage your credit score. While your bank may offer a similar type of service, the features are not as comprehensive as the independent providers. These services will notify you of new account applications or any changes to your credit profile. Basic services are about $10 a month, while a full package of coverage can cost up to $18 per month. While not a panacea, they are a first round of defense. We strongly recommend you subscribe to a credit monitoring service for you, your spouse and possibly your parents or children. (see recommendations in Attachment 1)

Consider freezing your credit. A "security freeze" on your credit file means it cannot be accessed by a new creditor. This is another tool to aid in preventing identity theft, but can be a time consuming process. Each of the three credit bureaus requires notification by certified mail that you wish to freeze your credit. Once you receive your identification PIN, you may temporarily authorize the release of your credit information for a specified time period or for a specific creditor. If you intend to use a credit freeze, we recommend using TrustedID.

Information regarding a security freeze for each of the three credit bureaus can be located on their websites at:
Equifax: (www.equifax.com)
Experian (www.experian.com)
Trans Union (www.transunion.com)

Keep important documents safe. Documents such as social security cards, passports, birth certificates, and other valuables should be safely locked away in a bank safe deposit box. You can also scan important documents such as Wills and tax records and save them on a secure disc. It is recommended that you take pictures of your valuables and the contents of your house, copy them to a disc, and add them to your safe deposit box.

Purchase a shredder. Any document that you receive which contains an account number or other personal information should be destroyed. An inexpensive paper shredder will allow you to dispose of old documents, credit card applications, account statements and bills safely and securely.

Shop online using secure websites. Shopping online is safe -- when you use secure web pages. Check the bottom of your browser and look for a locked graphic, or look for "ht*tp*s" in the address bar. This means you are on a secure web page and your data is encrypted. Without a secure connection, hackers can eavesdrop on your transaction and grab your private data.

Enroll in the National Do Not Call Registry. If you want to stop bothersome phone solicitations go to https://www.donotcall.gov/ or call 1-888-382-1222 and enroll both your home phone and cell phone.

Opt out of credit card offers. Tired of annoying "pre-approved" credit card offers? I sure am. According to the Fair Credit Reporting Act (FCRA) of 1970 as amended in 1996, the three major credit bureaus have the right to sell your information to companies that want to offer you a credit card. Fortunately, the amendment also stipulated that credit bureaus must provide a way for consumers to have their names excluded from pre-approval lists. You can call 1-888-567-8688 or visit https://www.optoutprescreen.com to notify the credit bureaus not to sell your history to credit card companies.

Attachment 1

Recommended Identity Theft Monitoring Services

We have reviewed multiple identity theft and credit monitoring services and make the following recommendations:

For Families and those with Established Credit: TrustedID (www.TrustedID.com) TrustedID offers a family plan which can include children regardless of age and other family members living at the same address. The cost is $125 per individual or $240/year per family and includes credit report monitoring for two adults, tracking of social security, credit card and bank account numbers, junk mail reduction, lost wallet protection and fraud alerts. An additional service provided by TrustedID is the ability to easily add and lift credit freezes at each of the three credit bureaus for a nominal fee.

Incapacitated or Custodial Care Family Members: Lifelock (www.lifelock.com)

Lifelock will allow an account to be set up for an incapacitated or special needs individual. A Power of Attorney or Custodial Care document on behalf of the incapacitated individual must be provided. The Lifelock Credit Score Manager service is $165/year and offers daily credit monitoring, scanning for fraudulent use of all personal information on the internet, lost wallet protection and threat alerts.

Young Adults Just Starting Out: Identity Guard (www.identityguard.com) 800-452-2541

For individuals and young couples who need to start tracking their credit reports, credit scores and have their social security and account numbers monitored, Identity Guard provides a comprehensive array of credit and internet surveillance. In addition to quarterly credit reports and credit scores, the service provides daily public record monitoring, lost wallet assistance and suspicious activity alerts. Identity Guard also provides anti-virus, anti-spyware and anti-keylogging programs. The annual fee for the Total Protection package is $180 per person.

Scott P. Noyes, CFA®, CFP® is the President of Noyes Capital Management, LLC, an independent fee-only wealth management firm based in New Vernon, New Jersey. www.noyescapital.com

---