Protect Your Financial Identity

Every year, thousands of unsuspecting individuals are targeted for fraud and identity theft in a number of ways via mail, telephone, the internet, conversations—even sifting through victims' trash. We've all heard the horror stories resulting from these scams. Hopefully, the gruesome details convinced you to heed warnings from financial institutions, credit card companies and government agencies to take basic necessary precautions for protecting your good name and credit. But are you doing enough to keep your identity secure? Storing personal records in a safe place, shredding financial documents, protecting passwords and not opening suspect computer files or email from unknown sources are a good start. But there are also less obvious suggestions you may want to consider to safeguard your personal information.

Have your full name and birth information removed from professional directories. These biographical dictionaries, such as "Who's Who" listings, typically include: full name, contact address, occupation, date and place of birth, family background, education summary, career profiles, memberships, awards, military service, religion, political activities and other information. Most content is public in nature. However, listing your full name and date of birth is considered risky. Contact the source to remove sensitive information.

Monitor credit history, inquiries and changes by ordering a free credit report once a year. With the passage of the Fair and Accurate Credit Transactions Act (FACT) in December 2003, you are entitled to receive one free copy of your credit report from each credit reporting agency (Equifax, Experian, TransUnion) during any 12-month period. Order your free annual credit report online at www.annualcreditreport.com, by calling 877-322-8228 or by completing the Annual Credit Report Request Form and mailing it to: Annual Credit Report Request Service, P.O. Box 105283, Atlanta, GA 30348-5283.

Destroy hard drives or memory cards with personal information before disposing or donating personal electronic equipment or devices. Wireless devices such as PDAs and cell phones should have the internal memory reset to ensure that all personal data is removed (most devices of this nature have a reset button—simply removing a battery from devices does not always delete the information). Be sure to check with your waste management service/recycling company to follow proper environmentally safe guidelines for disposing of this type of equipment.

Examine your supply of checks to determine if any have been stolen. If your home or office is burglarized, look closely at your supply of checks. Often thieves will take one or two checks from the middle or back of a book of checks, making it more difficult to discover they are missing. Immediately reporting lost or stolen checks to your financial institution may decrease potential losses. Another tip: never leave your checkbook in your vehicle.

When you are on your computer, seek out secure web sites. Look for signs of a secure website such as a web address that begins with "https" instead of "http" and the display of a "closed lock" in the status bar at the bottom of the screen. In most cases, these will indicate that your information is secure during transmission. However, malicious software can actually make a site look secure even when it is not, so it is always best to type in a website address whenever possible instead of clicking on links in emails or being directed from other web sites.

Be cautious and limit your access to your personal and confidential information on public computers. Malicious software may be installed to obtain your account number and sign-on information, leaving you vulnerable to fraud. And whether you are on a computer at home, work or in a public facility, always remember to log out of online sessions that require you to use a password or login process and close out the browser. Unauthorized transactions and activity can occur if you leave your online session accessible to other people. Whenever possible, particularly in public facilities, reboot the computer to clear out any additional traces of your information that might be in memory.

Assistance to victims of identity theft. Contact your financial institution immediately if you suspect that someone has had unauthorized access to your account(s) or access to your personal identifying information such as your Social Security number or credit card information. In addition, you should also report the crime to your local law enforcement agency and to the Federal Trade Commission (FTC). To speak with a trained FTC telephone counselor, call toll-free at 877-IDTHEFT (438-4338). To enter information about your complaint into a secure FTC online database, sign onto www.ftc.gov/idtheft. The site also provides links to numerous consumer education materials.

For more information or suggestions on how to protect your personal data and financial records, contact your financial advisor today.

This article was written by Wells Fargo Advisors ©2014 and provided courtesy of Greg Patterson, Financial Advisor in Morehead City at 726-1114.

These suggestions are not all-inclusive and should not be considered nor interpreted as legal, accounting, financial or technical advice. You may wish to consult your attorney, accountant or other advisor for specific advice, guidance or recommendations concerning these topics.