Tips to Prevent Identity Theft

It's scary how easy it is for criminals to get to our personal information – as technology improves, so do the skills of fraudsters. In fact, I find myself being what some think is paranoid – triple checking for the http**s** in online shop URLs, and shredding almost everything with my name on it. I mean look what happened to Sandra Bullock in ***The Net*** – if that could happen in the 90's just think of what's possible now!

Here are some key tips to help prevent identity theft.

1. **Check your credit card statements regularly**, and consider paying for credit monitoring. Credit card and account statements, which typically arrive and can be checked monthly, are a great indicator of whether or not your account is being used fraudulently. A credit monitoring service can be a valuable tool in fighting and detecting identity theft, helping alert you when any new accounts are opened in your name.

2. **Get used to shredding documents**, which can help ensure that papers with personal information are properly disposed of and do not fall into the wrong hands. Anything that has your name and address on it should be shredded in a cross-cut shredder to be safe, including credit card offers, bills and financial statements.

3. **Protect your computer** by enabling all security features and keeping anti-virus and spyware protection up-to-date. Research shows that the most common reaction to a person finding out they were a victim of identity theft is installing anti- virus protection on their computer. Don't wait for this simple step. Install and activate a pop-up "blocker."

4. **Destroy all sensitive data on your hard drive** prior to selling, donating or discarding an old computer.

5. While it can be difficult to remember so many different passwords, it is essential to **create "strong" passwords.** A strong password is one that is not easy to guess and it should include both numbers and capital letters, and possibly characters as well. Also, it's helpful to utilize a password locking system on your computer if it is left on while you are not sitting in front of it. Keep your passwords hidden, even in your own home. Keep your user IDs, passwords and any other information used to access your financial accounts secret and be aware of anyone else who has access to your personal information.

6. **Don't take the bait. Beware of phishing scams.** Phishing scams include emails that appear to be from legitimate organizations asking the recipient to update their personal information – with the sender intending to steal their identity to commit fraud. One key giveaway for this type of scam is that it will typically ask you for some sort of personal information (perhaps as verification). When you receive something like this, call the institution directly, and ask them if this email is legitimate.

7. **Regularly monitor your accounts online.**

8. **Be cautious about opening emails from unknown senders** and don't ever download a file or click a link from an email from an unknown sender.

9. **Use only one credit card for personal expenses and one card for business expenses** and monitor accounts online weekly.

10. **Always send or receive mail only through secure and locked mail boxes.**

11. Never give out any sensitive information (SSN, Acct #, Pin #, Password, etc.) via an email solicitation. **Always type in and visit the website directly.**

12. **On all credit cards, in addition to signing your name, write "Please ASK for ID!"**

13. **Never give out your Social Security Number, Drivers License Number or Date of Birth** unless the person or firm has just cause and really needs it.

Post written by *Kirstin* Hemsteger, Marketing Manager, NAFCU Services Corp.