How to protect yourself from identity theft

September 04, 2014 - Northern New England

Identity theft is the fastest-growing crime in the U.S., affecting more than 13 million people every year, at a cost of over five billion dollars.

Recent high-profile cases of identity theft, involving millions of stolen credit and debit card numbers have increased awareness and raised troubling questions for consumers. With clever scammers (some as far away as China) breaking into databases with seeming impunity, protecting our identity is definitely more challenging than ever. And it's worth taking the time to protect yourself. Experts estimate that resolving an identity theft problem takes about 330 hours.

Here are some basic steps you can take to reduce your chances of becoming a victim of fraud.

Keep your Social Security
number to yourself

We all carry a lot of cards around with us. But one card you should never carry with you is your Social Security card. With this one number, a thief can create bank and credit card accounts in your name everywhere - and clean out your savings. Keep this card at home, in a safe place - and only give out the number when it is absolutely necessary, and only to a person or company that you fully trust.

Don't use easy passwords - and don't keep them in your wallet

You might be shocked at how easy it is for thieves to guess passwords. But consider this: millions of Americans use the password "1234" or "ABCD" for their personal accounts - or they use easy-to-guess terms like their nicknames. Remember, if you picked an easy or obvious password so you wouldn't forget it, it won't take long for a smart thief to figure it out.

Some identity theft experts advise choosing difficult, meaningless passwords, and then changing them regularly. This is good advice, but in the real world, it can lead to chaos. If you choose just one complex password, at least 8 characters long, including at least one capital letter, numbers and a symbol, that will at least ensure that your password won't be easily guessable.

If security is paramount for you, you may want to investigate software programs that will generate new passwords regularly and remember them for you.

Monitor your credit card
and bank accounts

Over 70% of identity theft involves credit or debit cards, so it is important to monitor your accounts. Check expenses and payments item by item, and do it every month.

Shred the evidence

You might be surprised how much identity theft starts with a discarded bill or statement. Be safe; shred it.

Shop only on
"verified secure" websites

Remember, you should never have to give your Social Security number to shop online. If you are asked for personal information, such as a bank account or credit card number, make sure the site address has an "s" after the "http" in the browser window, and that somewhere on the site there is an SSL certificate seal, such as (Verisign, GeoTrust, SSL.com, etc.) These seals are designed to be difficult for thieves and scammers to duplicate.

Leave no "cookie crumbs"

If you use a public computer, or share a computer with others, be sure to erase your browser history, clear all cookies and log out when you are finished.

Keep copies of vital

documents in a safe place

If your wallet is stolen, you'll need copies of your birth certificate and driver's license to begin the process of rebuilding your identity. Keep credit card and bank account information secure as well.

Beware of email and

phone "phishing" scams

Never give out any personal information over the phone or Internet unless you are 100% sure that you know and trust the person you are talking to.

Email scammers are getting very, very good these days, with official-looking logos and language that sounds genuine. Remember, reputable companies NEVER use email for security issues. If your credit card company or bank contacts you by phone, they should already know your account number and personal information; if a caller asks for this information, chances are you are talking to a con artist engaged in "phishing"

If you suspect identity

theft, act immediately

If you suspect that identity theft has occurred, your first step should be to call your bank and credit card issuers. It can also be helpful to call one of the leading credit regulating bureaus and place a fraud alert on your name to prevent new accounts from being opened.

Ask for a copy of your credit report as well to check for any new accounts that you have not opened.

You can find a wealth of information about identity theft on the consumer side of the Federal Trade Commission website at www.consumer.ftc.gov. Use the search term "identity theft."

Ron Magoon is executive vice president and chief operating officer at Franklin Savings Bank, Franklin, N.H.