PROTECT YOURSELF IN THE REAL WORLD....

DON’T CARRY YOUR SOCIAL SECURITY CARD WITH YOU
Memorize your number and don’t share it unless absolutely necessary. Store the card in a safe, secure place.

KNOW YOUR WALLET
Keep track of what’s in your wallet.
If your wallet is lost or stolen: 1) Notify your banks and cancel your credit cards ASAP! The longer you wait the more money you could lose. If you wait more than 60 days to report a lost debit card, your bank is not responsible for returning any of the money that might have been stolen using your card! 2) File a police report. You may not get your wallet back, but having proof of the theft could be important down the road.

SECURE YOUR MAIL
Make sure your identity-sensitive mail is sent where it can only be accessed by you. Consider having the documents sent electronically. Don’t forget to update your address when you move. Don’t just toss your mail – shred it first! This includes unwanted credit card applications.

LOCK YOUR PHONE AND LAPTOP
Make sure all of your personal electronics are password protected and that those passwords are not easily guessed.

AVOID USING PUBLIC COMPUTERS TO ACCESS FINANCIAL ACCOUNTS
Don’t leave behind information you never intended to be public.

KNOW YOUR BANK ACCOUNTS AND YOUR CREDIT HISTORY
Check your bank and credit card statements monthly, and check your credit report periodically. Access your free credit report through AnnualCreditReport.com.
PROTECT YOURSELF IN THE VIRTUAL WORLD....

MAINTAIN UPDATED SOFTWARE
Make sure your computer has up-to-date antivirus and spyware software.

USE SECURE WEB SITES
When you access financial accounts or shop online, make sure the Web site is secure and steer clear of paying bills or shopping online when connected to the web through an unsecured or unknown network.

BE CAREFUL WHEN USING PUBLIC WI-FI
These can be susceptible to hackers. When you shop online, always log off and close the browser after making a purchase.

AVOID STORING PASSWORDS IN LAPTOPS AND MOBILE PHONE DEVICES
Don’t allow your computer and phone to remember your passwords. Do not use your banking password as a password for other online accounts.

QUESTION LINKS IMBEDDED IN EMAILS OR TEXT MESSAGES, EVEN IF IT LOOKS LEGITIMATE
Before you click an link, roll your cursor over it – does it match the site you think you will be visiting? It is highly unlikely your bank will ask for your account information by email. Call or visit your account online before you provide anything.

LIMIT SHARING PERSONAL ONLINE
Keep the following in mind:
• Each piece of information you post online maybe harmless on its own, but when strung together this information could be the key to your identity.
• Never post your full birth date or exact place of birth.
• Never post your address, phone number, or primary email address.
• Limit information about your activities.
• Be careful about revealing seemingly unimportant information like your car color and your pet’s name.
• Be wary of quizzes. A survey, like “10 Things Others Don’t Know About You”, may be designed to harvest your data.
• Control who can see your personal information. Manage privacy settings for social networking sites, and make sure you restrict your page to your real friends, not friends or friends.
• Make each post knowing that the information could be public and is permanent.