So how do you keep your personal information secure in the midst of all these threats?

Ten smart steps to take are:

1. Don't leave your wallet or credit card statements lying around—even at home. The Federal Trade Commission (FTC) estimates that one in four victims knows the identity thief.

2. Sign new credit cards as soon as you receive them, cut up and discard expired cards, and shred or tear up unwanted "pre-approved" credit card applications.

3. When you sign receipts, draw a line through any blank spaces above the total. Save your receipts until you reconcile them with your statement, then either rip them up or keep them and any carbon copies in a safe place.

4. Never give your credit card number or Social Security number to anyone over the phone unless you initiate a call to a business to discuss your account. And never send these numbers by E-mail—it is rarely secure.

5. Always keep PINs for your credit and debit cards completely confidential. Don't write PINs on your cards or carry them with you.

6. Review all of your monthly statements carefully, and report unauthorized charges and other activity immediately.

7. When it's time to clean out your financial files, shred anything that has your Social Security number or credit card numbers on it.

8. On your computer, install and use firewall, anti-virus, and anti-spyware software, and learn how to keep them all up to date.

9. Don't fall for phishing or pretexting scams. Legitimate businesses that contact you should not have to ask for your account number or Social Security number. If you think there really might be an issue with an account, get a customer service number from your statement, and call the business back.

10. When you buy something on the Internet, check that the page is secure before entering your credit card number. You should either see an icon of a closed padlock  or unbroken key  in the bottom browser bar or that the site's address begins with "https" (notice the "s") to show it's secure.