



# TIPS TO PROTECT YOURSELF

## DO'S

1. Guard your social security number. It is the key to your credit history, your employment history and your financial life.
2. If you can't remember your social security number, disguise it as part of a phone number in your address book.
3. Carry your health insurance provider card and Medicare card only when utilizing health care services. They contain your social security number. (Carry only copy of cards with social security number blanked out.)
4. Review all credit card and bank statements carefully and promptly.
5. Keep a calendar for expected or regular monthly bills.
6. Request your credit reports regularly. (Free reports begin in June 2005.)
7. Do call to cancel any credit card or store credit accounts you no longer wish to use. (Just having them sit there with no activity on your part is an invitation for thieves.)
8. Drop outgoing mail into a secure postal service mailbox instead of leaving it to be picked up at your home. For incoming mail, purchase a mailbox that can be locked.
9. When creating passwords and PINs, use a random mix of letters and numbers.
10. Consider using other security passwords for financial accounts rather than common identifiers such as mother's maiden name and birthdate.
11. Ask your financial institution to add extra security protection to your account(s).
12. Designate one credit card to use for over-the-phone orders or transactions.
13. Use a cross-shredder or carefully destroy old checks, credit-card statements and financial records by hand.
14. Ink out credit card information or checking account numbers and information on copies of receipts that you send in for rebates, returns, warranties or reimbursement.
15. Remove the label (with key code and/or customer number) from magazines and catalogs before donating or disposing of them.
16. Shield the keypad with your body when using an ATM or when punching in your PIN number.
17. Consider insurance, but know that most identity-theft policies just cover out-of-pocket expenses and lost wages.





## DON'TS

1. Don't return your room "key" after hotel stay. (These are often imprinted with name, credit card account, etc.)
2. Do not preprint social security number, driver's license number or phone number on checks.
3. Don't give your social security number or credit card numbers to people who have called or e-mailed you.
4. Don't give PIN numbers and/or account numbers to friends.
5. Don't use the same PIN number for all your accounts.
6. When creating passwords and PINs, do not use the last four digits of your social security number, your birthdate, middle name, mother's maiden name, pet's name, address, consecutive numbers or any information that may be easily discovered by identity thieves.
7. Don't give or write your name and address in conjunction with a credit card sale.
8. Don't have checks delivered in the mail. Use direct deposit.
9. Don't store old financial records and tax returns in a box in your unlocked garage.
10. Never provide personal information in chat rooms or via e-mail.
11. Don't conduct personal business on PCs at internet cafés, libraries, or other public places.
12. Don't give your outdated computer to friends, relatives or a charity without having a professional wipe the hard drive clean of all information first.

Prepared by:  
Brenda C. Williams, Ed.D.  
FCS Agent III  
Alachua County Extension/IFAS



Upon request, this fact sheet is available in alternate formats for persons with print-related disabilities. This information may be shared or duplicated for educational purposes, however it is expected that credit be given to both the author and the Alachua County Extension Service, phone (352)955-2402. Funding for the duplication of this publication is provided in part by the Alachua County Board of County Commissioners.