

# HOW THIEVES GET YOUR IDENTITY:

- **DUMPSTER DIVING**—Going through your trash.
- **SKIMMING**—Storing your credit card number in a special storage device when processing your card.
- **PHISHING**—Pretending to be a financial institution and sending scam alerts to get your personal information.
- **CHANGING YOUR ADDRESS**—Completing a change of address form to get your mail and personal statements.
- **STEALING**—Taking your purse, wallet, mail, pre-approved credit cards, new checks, personnel files from work, or tax information.

# TIPS TO AVOID IDENTITY THEFT:

(See Page 2 for definitions & details)

1. Shred Financial Documents
2. Never Click on Links in Unsolicited E-mails
3. Do Not Use Obvious Passwords
4. Do Not Give Out Personal Information
5. Protect Your Social Security Number
6. Keep Your Personal Information in a Secure Place
7. Be Alert to Bills that Do Not Arrive when They Should
8. Be Proactive about Unexpected Credit Cards or Account Statements
9. Be Alert for Credit Being Denied Unexpectedly
10. Respond Immediately to Calls or Letters about Purchases You Never Made
11. Check Your Credit Report
12. Regularly Review Your Financial Statements
13. Close Any Accounts that have been Tampered With or Established Fraudulently
14. Go Paperless
15. Store Your Financial and Personal Information in a Storage Box by Year
16. Be Alert when Responding to E-mails
17. When Contacted by an Institution by Phone, Tell Them You will Call Them Right Back
18. Opt Out of Pre-Approved Credit Offers
19. Get a Locking Mailbox
20. Copy All of Your Credit Cards and Save Them in a File at Home
21. Carry Only One or Two Cards at a Time

# TIPS TO AVOID IDENTITY THEFT:

## 1. SHRED FINANCIAL

**DOCUMENTS:** Any paperwork with personal information should be put through a shredder before being thrown away.

## 2. NEVER CLICK ON LINKS IN

**UNSOLICITED E-MAILS:** Since “phishing” is becoming a common problem, use up-to-date firewalls, anti-spyware, and anti-virus software to protect your home computer. Good anti-spam software is a must. Plus, never click on links in e-mails. Instead, open a new window and go to the website address you know in order to enter information. (Fake PayPal e-mails are becoming more common, so be extra wary when dealing with these.) You might also want to avoid e-mail archiving in the event that someone hacks into your account.

## 3. DO NOT USE OBVIOUS

**PASSWORDS:** These include your birth date, mother’s maiden name, or the last four digits of your Social Security number.

## 4. DO NOT GIVE OUT PERSONAL

**INFORMATION:** Whether over the phone, through the mail, or over the Internet, don’t share your information unless you know who you are dealing with.

## 5. PROTECT YOUR SOCIAL

**SECURITY NUMBER:** Never carry your social security number in your wallet or write your social security number on a check.

## 6. KEEP YOUR PERSONAL INFORMATION IN A SECURE PLACE:

This is especially important with roommates, outside help, or if you are having work done in your home.

## 7. BE ALERT TO BILLS THAT DO NOT ARRIVE WHEN THEY SHOULD:

If they do not arrive, they may have been routed somewhere else.

## 8. BE PROACTIVE ABOUT UNEXPECTED CREDIT CARDS OR ACCOUNT STATEMENTS:

If an account or credit card arrives that you did not open/activate, someone else did. Call the company immediately and have it closed/canceled.

## 9. BE ALERT FOR CREDIT BEING DENIED UNEXPECTEDLY:

Credit is

often denied for a variety of reasons, one of which is when too much credit is opened in a short period of time. Being denied credit may mean that someone else has opened accounts in your name.

## 10. RESPOND IMMEDIATELY TO CALLS OR LETTERS ABOUT PURCHASES MADE:

Credit card companies create a profile of their clients detailing out the most common places a customer shops and the items that they frequently buy. If something is purchased that does not suit your profile, they will contact you for verification. Respond to the notice right away to head off potential theft and damage to your credit.

## 11. CHECK YOUR CREDIT

**REPORT:** Any credit opened in your name will show up on your credit report. By staying on top of this, you will be able to stop identity theft before too much damage occurs.

## 12. REGULARLY REVIEW YOUR

**FINANCIAL STATEMENTS:** Look for any charges that you did not make. Also not that consumers usually have only 30 days to dispute items they did not authorize.

## 13. CLOSE ANY ACCOUNTS THAT HAVE BEEN TAMPERED WITH OR ESTABLISHED FRAUDULENTLY:

Get a new card with a new number and close the old card, since this alone may stop a thief in possession of your information.

## 14. GO PAPERLESS:

You can receive many of your bills through your e-mail/online banking instead of having them mailed. By requesting this benefit, you keep account numbers and personal information private. You are also able to save hard copies directly to your hard drive, which allows you to find the information quickly and easily when needed.

## 15. STORE YOUR FINANCIAL AND PERSONAL INFORMATION IN A STORAGE BOX BY YEAR:

This is especially important when dealing with taxes since the IRS can demand to see evidential proof of deductions for as long as eleven years after you file. By keeping it in a storage box, you can shred the contents when the time period is up. Note: this does not include social security numbers.

## 16. BE ALERT WHEN RESPONDING

**TO E-MAILS:** E-mails are now commonly used to steal or “phish” information out of consumers by making the e-mail look as if

it came directly from a financial institution. If you respond to the e-mail, you encourage them to continue trying to get personal information from you. Simply add the address to your spam list to keep them from contacting you in the future. Visit the addresses you know if you are concerned the notice is valid.

## 17. WHEN CONTACTED BY AN INSTITUTION BY PHONE, TELL THEM YOU WILL CALL THEM RIGHT BACK:

Let them give you their name and number, but do not call that number back. Instead, call the number on the back of your card and ask to speak to a representative about your account. Let them know that you were contacted and ask them to verify any problems. All account managers have access to the same information, so they will be able to see if there is a problem with your account or not.

## 18. OPT OUT OF PRE-APPROVED

**CREDIT OFFERS:** Although I do not personally believe that people can get your identity through pre-approved credit card applications without your social security information, it never hurts to opt-out of credit card offers. By doing so, you lessen the amount of mail that comes to your mailbox, and you will still be able to apply for credit online. Check out the FTC’s Consumer Alert webpage to see all the ways you can opt out.

## 19. GET A LOCKING MAILBOX:

This is an especially good idea for anyone in a nice area. The nicer the area you live in, the more ideal a target you make to an identity thief because they assume you have more money for them to steal.

## 20. COPY ALL OF YOUR CREDIT CARDS AND SAVE THEM IN A FILE AT HOME:

By having a copy of the card (front and back) in a locked filing cabinet or other safe place, you will be able to quickly and easily contact your creditors should your purse or wallet ever be stolen.

## 21. CARRY ONLY ONE OR TWO

**CARDS AT A TIME:** Lock away all the other cards in a safe place and carry as few cards as possible. This way, if someone ever gets into your wallet or purse, you will notice immediately if a card is stolen and be able to report it right away.

