

Is Your Identity Safe?

During the holiday season we are all more likely to be in stores purchasing gifts with our credit cards, to be asked to make contributions to charitable organizations via mail campaigns sent to us or via unsolicited phone calls, some of us will be using the internet to make purchases and most of us will get and send more mail. All of these instances increase the likelihood of what is called *identity theft*.

Identity theft is a very common serious crime and according to the Federal Trade Commission it is one of the most prevalent types of consumer fraud. Although exact statistics are not known (some are too embarrassed to report it and others may not even know they are victims), it is estimated that over 10 million Americans are victims annually by at least one of the three main forms of identity theft which are financial identity, criminal identity and identity cloning.

Financial identity theft involves the criminal using your personal information such as your Social Security number, driver's license number, birth date, etc. to get credit cards, loans, or to lease apartments. Criminal identity theft is when the criminal gives another person's personal identity to a law enforcement officer or to a government agency so they won't be charged with a traffic violation or other crime. Identity cloning is when the criminal uses your identity to establish a new life as they may be an undocumented immigrant, be trying to avoid a warrant for arrest or just want to avoid being tracked by an agency or court for such things as child support payments, etc. The most common form that affects those of us 50+ in age is financial identity theft.

According to the Federal Trade Commission skilled identity thieves use a variety of methods to steal your personal information including:

- **Dumpster Diving:** they rummage through your personal trash looking for bills/invoices, offers of new preapproved credit cards, medical records or other paper with elements of your personal information
- **Skimming:** they steal credit/debit card numbers by using a special storage device when processing your card
- **Phishing:** they pretend to be financial institutions or companies and send spam or pop-up messages to your computer to get you to reveal your personal information
- **Changing Your Address:** they divert your billing statements to another location by completing a "change of address" form...therefore, you do not receive your monthly statement and unless you notice this you may have charges on your credit card for a few months
- **"Old Fashioned" Stealing:** they steal wallets and purses; mail, including bank and credit card statements; preapproved credit and loan offers; and new checks or tax information. They steal personnel records from their employers, or bribe employees who have access to your personnel records.

In order to limit your chances of being a victim of identity theft and to protect your identity and your assets, the following are a few suggestions for you:

- Keep your Social Security card in a safe place in your residence (never carry it in your wallet). Memorize your number so you do not need your card. If you think someone else may have used your Social Security number without your authorization, call the Social Security Administration fraud phone line 1-800-269-0271.
- If you pay your credit card monthly balance with a personal check, write only the last four digits of your account number in the check memo line.

- Do not put your signature on the back of your credit cards. Instead write the following statement on the card back *“Ask for photo ID”*.
- Do not have your Social Security number, driver’s license number, date of birth or home phone number printed on your personal checks. If a clerk asks for your Social Security number when using a personal check at a gas station, store or restaurant refuse to give it.
- Shred or burn any documents or credit card offers or any other mail that contains personal identity information (you are advised to purchase a cross cut, not a strip shredder).
- Ask to opt out of direct mail credit offers because these are often the targets. Call 1-888-567-8688.
- If your mail is delivered to your home, take it out of the mailbox as soon as you can or if you are often gone be sure to stop your mail or have someone pick it up daily. Many law enforcement personnel recommend you only use a post office box. And, always take outgoing mail to a post office or drop box instead of letting it sit in your curb-side home mailbox as thieves love to steal mail.
- Be very cautious about caregivers, acquaintances, or family members asking you for financial or personal information. Keep your bank, credit card, Medicare statements and other personal documents locked up. A significant portion of identity theft is actually done by people that are known to the victim. Also keep in a lock box a list of all credit card, debit, and ATM numbers and their toll-free contact phone numbers so in case they are missing you can contact them.
- If you use a computer be sure to update your virus protection software regularly and certainly don’t click on e-mails or download any files from people you don’t know.
- Only give personal information on an internet site if it is using a secure URL which should begin with *https://* You should also look for a “lock” icon in your browser.
- Use only your first and middle name initials with your last name on your imprinted personal checks but sign your bank’s signature card and your checks with your full name. Your bank will know how you sign your checks but a criminal will not.
- Never write your PIN on the back of your credit or ATM or debit card or carry it in your wallet/purse. When choosing a PIN do not use a portion of your Social Security number, your birth date, phone number or any set of numbers that is part of your identity.

If your wallet/purse is stolen, immediately file a police report, close all accounts for missing credit cards, notify your bank or credit union, and contact one of the three national credit reporting organizations to have a fraud alert placed on your name and Social Security number. Your law enforcement agency and bank can provide you with contact information.

Give yourself a gift this holiday season...protect your identity!

Sue Montesi
 Dean of Learning Centers and Innovative Programs
 Delta College