As new and returning students head off to college, they're usually concerned with such things as where to live, where classes are located on campus, how to stretch a tight budget, financial aid, buying books, and a host of other factors important to their day to day life. What most students aren't concerned about is identity theft. Most students think this is an issue which won't affect them; after all, students don't usually have much money or credit, so they think, "Why would anyone want to steal my identity?"

The truth is that identity theft is not just about stealing someone's money or assets – it's about stealing their name and reputation. Identity theft is the fastest-growing crime in the United States, costing Americans over $50 billion in fraudulent charges and affecting some 8 million people annually. Unfortunately, college students are a prime target due to lax habits and a rather surprising indifference.

What is Identity Theft and How Does It Occur?

Identity theft is the act of someone else taking information which personally identifies someone else - a social security number, driver's license, birth certificate, etc. The thief then uses this information to establish credit accounts, loans, apply for jobs, or commit other fraudulent acts in the victim’s name, or to use the victim’s currently established accounts to buy merchandise or services. Unfortunately, the person responsible for these charges is the victim himself and it can often take years to clear up the resulting problems.

The consequences of identity theft are dire. In most cases, the victim is left with a large amount of debt and may be denied a job, loans for a house or car, and have their credit rating damaged irreparably. This is not a good way to start what should be the beginning of a new life after receiving a college education.

Why College Students are Particularly Vulnerable

In order for a thief to steal someone’s identity, they must first obtain the necessary information which allows them to “become” someone else, at least in the eyes of lending institutions and other financial companies. How easy this task is depends on how vigilant a person is about protecting their personal information.
More than half of all college students receive multiple pre-approved credit offers monthly. Those mass-mailed forms, usually partially filled out with the recipient’s information such as name, address, and other personal data is fantastic opportunity to steal a person’s identity.

If the recipient is not interested in the offer and simply throws away the form, it is one of the most common documents used by identity thieves. By picking the offer out of the trash can, the thief can then fill in the rest of the blanks and send it in or simply call the toll free phone number provided on the form, allowing them near instant access to one aspect of the victim’s identity.

Another manner in which identity theft occurs is when thieves get their hands on personal banking account information, such as a checking or savings account statement. Anyone who does not balance their account is at risk of incurring fraudulent charges, simply because they do not keep track of what charges are legitimate. Oftentimes, the thief steals by withdrawing money in small increments – not enough to stand out as a glaring error to the casual observer but enough to build up to a large amount over time.

Another danger to college students is their Social Security Number. Many college courses require a student to use their Social Security Number to log in to websites used to post homework assignments and other course communications. The university may also use that number as an identifying number in the administration office.

It is very easy to forget to exercise caution when using a Social Security Number, particularly when it is used so often. Lax computer security or even something as simple as a criminal watching a student enter the number, allows a thief can quickly and easily gain access to the Social Security Number, which is the key to obtaining additional information about an individual.

Computers and laptops also pose a threat that many students don't think about. Many students use a laptop every day in class to take notes and organize coursework documents. But what if that computer is stolen? What would a thief find inside?

Most students in today’s world use their computers to access online banking, pay bills, order merchandise, and communicate in just about every other aspect of their lives, too. If personal and account information is stored on the hard drive, the thief has instant access to very information that makes it possible for them to assume the student's identity.

Of course, students also shouldn't overlook one of the most common ways to steal someone’s identity - stealing a wallet, purse, or backpack. This can even occur in the student's dorm room, particularly if parties or unfamiliar guests are common, and they usually are in college dorms. Students should exercise the same security at home as in any unfamiliar environment.

**How to Stay Safe from Identity Theft**

The best way to deal with the prospect of identity theft is to avoid it by employing safe practices in everyday life. Here are some tips and best practices to prevent identity theft:
Shred all important documents, such as bank statements, credit card offers, and any pieces of paper which contain an account number or social security number. Remember prescription drug containers, too, as they usually have an account number and other personal information printed on the label.

Don't let mail pile up and lay around where anyone could gain access to it. Be sure that anything which goes in the trash bin does not contain any usable information – shred or tear documents into small pieces if necessary.

Always ensure your web browser does not save log in and password information associated with sensitive sites.

Never store personal information or username and password combinations on your computer’s hard drive. If you must write them down somewhere, make sure the document is stored in a safe location, such as lock box. But it’s best to memorize them no written record that could be compromised.

Use secure passwords which are not composed of obvious numbers such as date of birth, phone numbers, anniversaries, or addresses. Using a long string of numbers and letters in a random combination is best to avoid hacking.

Ensure that the web sites you use for buying merchandise or services are secure. Oftentimes, the URL will be preceded by https:// and it will bear the logo indicating a Secure Sockets Layer (SSL) certificate.

Be wary of emails which are “phishing” for information, or trying to get you to respond to what looks like a legitimate site but redirects you to a thief’s site where your personal information will be recorded. Learn how to spot these phishing emails.

Be very careful in giving out your social security number. There are few instances when it is the only number you can use to access or open an account (even at the university). Use a driver’s license to prove identity and do not carry your social security card with you; instead keep it in a safe place. The same applies to a student ID card, particularly if it contains your social security number.

What to Do If You Suspect You Have Become a Victim of Identity Theft

Not just an inconvenience or a detriment to your credit rating, identity theft is classified as a federal crime. According to the Identity Theft and Assumption Deterrence Act of 1998, it is a federal crime if someone "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of the Federal law, or that constitutes a felony under any applicable State or local law."

If you suspect that you’re identity has been compromised, the first step is to notify all your financial institutions that may have been affected. Ensure that all accounts are closed immediately and ask that any new accounts be flagged for possible fraudulent charges in the future.

Next, notify your local law enforcement office of the crime. They will be able to advise you of further steps as well as begin an investigation.

Also contact the three credit reporting bureaus and notify them of the theft of your identity. They can put a fraud alert in your file with a date so that charges occurring after this date will not negatively affect your credit rating.

The time spent going to college is, for most students, one of the best and most memorable periods in their life. Make sure it is not memorable, however, because of the trauma and suffering which result
from the theft of your identity. Be vigilant about protecting your information and never assume that such a crime cannot happen to you. Chances are, there is already someone you know who has had it happen to them.