By Carolyn Lee
The Imperial Republican

Someone steals your identity. It costs you money and time to fix the problem. It costs law enforcement agencies time. It costs credit card companies, employers, the government and other agencies time and money.

And, it's growing.

Ryan Sothan, outreach coordinator for the Nebraska Department of Justice, Office of the Attorney General of Nebraska, Consumer Protection and Anti-Trust Department, was in Imperial Tuesday and Wednesday to address the issue with a variety of people.

He spoke at Mid-Plains Community College, Imperial Rotary, to residents and their families and staff at Imperial Manor, to students at Chase County Schools and to their parents.

Last year identity theft was the leading consumer complaint, with 11.6 million new victims, Sothan said. That's up 13 percent over 2011.

With 225 million adults in the United States, it's a good bet that "identity theft will come up in a family once in every generation," he pointed out.

The average victim loses $4,607, and spends an additional $631 to clear his record. It takes about 33 hours to clear the record.

Identity theft occurs when someone obtains a person's personal identification, such as name, date of birth, Social Security number, drivers' license number, bank and credit card numbers. The most important number is that Social Security one.

Sothan said the prime reason identity theft occurs is to receive government benefits, followed by obtaining new credit cards and new phone and utility records to establish new households.

Identity theft can be financial, such as when a Social Security number is used to establish new lines of credit to purchase items with no intention of paying the bills when they come due.

Identity theft can be criminal, when information is "borrowed" to obtain a drivers' license or when a person is caught in a criminal act.

Sothan said, for instance, that a pharmacist in Omaha learned that her identity had been stolen when it was used in a criminal traffic violation. She is no longer practicing pharmacy because she couldn't renew her license.

It can also be an identity assumption, when a thief uses an identity for a financial, criminal or governmental purpose. Sothan said thieves target children's Social Security numbers, because it will be years before the theft is noticed. Youths typically don't need to use a Social Security number until after age 16.

The number one thief is a family member or friend. Next is a stranger outside the workplace, followed by a friend, neighbor or in-home employee.

Someone at a company with access to your information is next, followed by someone at work.

"Keep your information in a secure place," Sothan admonished.

Not paying attention to what you're doing aids a thief in obtaining information about you, Sothan said. It occurs when you're posting mail, writing a check at the store, making a purchase on a credit card, talking on a cell phone, or using a computer at free public Wi-Fi places such as coffee shops, restaurants, libraries or bookstores. Thieves can break into your systems in public.

"Linkedin, Twitter and Facebook users have the highest incidence of fraud," Sothan noted. "Those with public profiles are the most likely to expose personal information. We're unaware that information thieves are trolling these areas to gather information to use against us."

On these public sites, 68 percent of users share their birthdays; 63 percent share their high school name; 18 percent share their phone number; 12 percent share their pet's name.

Any of these pieces of information can open the door to a thief bent on finding out more about you or accessing your passwords and PIN numbers.

How identity thieves steal

Interestingly enough, with all of the ways a thief can use technology to steal your identity, "Plain old fashioned stealing is still the number one cause," Sothan noted.

Stealing wallets, purses and mail; changing your address at the post office; fraudulently obtaining your credit report; viewing unsecured Internet transactions and dumpster diving are some ways theft occurs.

Another is phishing, which is an e-mail scam. Fraudsters pretend to be a legitimate business. They send you an e-mail saying you're shut off until you give certain information, which then goes to an illegitimate site.

Sothan stressed, "Call the company. Don't hit 'reply' or respond at all."

Another form of theft is smishing. This uses a text message to deliver a "bait" message designed to get you to divulge personal information. It can also attach a virus to the text that tracks your visits to web sites, then obtains your information.

Another form of theft is skimming, involving credit cards.

You're at a nice restaurant and pay with a credit card, which is tucked into a leather folder. You lose sight of your card.

In the meantime, the waiter is running the card through a tiny, unnoticeable skimming device that collects your information. The waiter receives $50 per card for information collected and given to a thief.

Pretexting obtains your information under a false pretence, such as a "survey" over the telephone. The pretexters sell your information to people who use it to get more information to get credit in your name.

Detecting fraud

Sothan said most identity theft occurs within 48 hours of your loss, such as the loss of your wallet.

You may notice many odd, small charges on your credit card. You may receive credit cards you didn't apply for. There is an increase in the number of pre-approved credit cards and insurance offers received. The thief is applying for as many cards as he can before he gets caught.

There's a noticeable decrease in your mail and you don't receive bills. That's because the thief has changed your mailing address so he receives the bills and you don't notice the theft.

There may be a change in your utility bills. You may be being charged for properties you don't own.

You receive calls from debt collectors for things you didn't buy.

There is a high number of new inquiries on your credit report. Most people only receive between 12 and 24 inquiries per year from companies to which you've applied for credit cards.

You are denied credit.

Defending yourself

What do you do the moment you suspect identity theft, or the theft of information? Take immediate action and contact your local police department. File a report and get a copy of that report. That protects you later from having to make restitution.

Contact, by telephone, all your existing accounts and get new ones with new PINs and passwords. Follow that up with a written letter to the companies.

Place a fraud alert on your credit reports. Those are Experian, TransUnion and Equifax. Then review and monitor your credit reports through AnnualCreditReport.com.

Fighting back

Sothan said Facebook is frightening. "It takes all of your personal information and shares it with the public if you don't use security settings." He noted that even with security settings, thieves may get through.

He suggests applying the top 10 Facebook privacy settings for social media. "Fix your Facebook accounts and you'll go a long way for peace of mind. But, you need to check them occasionally."

Sothan manages his mail, such as catalogues and magazines, through the Direct Marketing Association's DMAchoice.org. At that website you can choose which mail you wish to receive, "to remove yourself from the grid so you're eventually hard to find." He said that although legitimate marketers belong to DMA, they can legally sell your information to other marketers.

You may also delete e-mail marketers at this site.

Under the Fair Credit Reporting Act, Americans have rights to be protected as victims. In Nebraska, the Fair Credit Reporting Act protects you further, Sothan said.

He said the Consumer Protection Division of the Nebraska Attorney General's Office "has a successful track record on mediated claims and recovering money."

Last year there were over 5,000 claims of identity theft made in Nebraska, with $3.7 million dollars recovered.

"Every click, every website, every move we make in cyberspace makes a footprint," Sothan stated, "that can be used to steal your identity."

The Consumer Protection Division may be reached at (800) 727-6432, or go to www.ago.ne.gov.