

Publish Date: 3/7/2009

Safe and Secure: Businesses learn to limit ID theft

By Shelley Widhalm
Loveland Reporter-Herald

Loveland business owner Kendall Payne shreds documents and locks client files to protect her customers from identity theft.

“We shred anything with any names, addresses, policy numbers — anything with information that may identify someone,” said Payne, owner of Payne & Associates, a Loveland insurance company.

Though Payne already has several security measures in place, including staff passwords and log-ons for client files, she wants to learn more about protecting her business from fraud and identity theft, which involves someone pretending to be someone else in order to steal.

She was one of about a dozen businesspeople who attended a two-hour Business InSights workshop Wednesday afternoon hosted by the Loveland Chamber of Commerce.

Three speakers led the workshop, including a private investigator, a police detective and a computer security expert, to provide tips for businesses and individuals on preventing identity theft, fraud and Internet crimes.

“Make yourself a hard target,” said private investigator Brian Brooks, owner of Brooks Investigations and Fugitive Recovery in Loveland.

Brooks recommended shredding all documents with personal information and avoiding giving out information while using a cell phone in public places.

Why?

“‘Dumpster diving’ is more common than you believe,” Brooks said.

Dumpster diving involves sorting through trash and removing papers with any personal information, while “shoulder surfing,” or listening in on phone conversations, is another method for obtaining information.

Brooks used the acronym SCAM to point out ways to protect personal identity:

- S: Be stingy about giving information out to others.
- C: Check financial information regularly and look for anything out of the ordinary.



Reporter-Herald/Jenny Sparks
Kendall Payne of Payne & Associates, a Farmers Insurance agency, dumps shredded documents from her shredder Friday in preparation for recycling them.

Must do's for safe computing

- Back up all important data
- Use and update virus protections
- Install spyware protection and keep it updated
- Scan computer for viruses and spyware
- Install a firewall
- Run Windows updates regularly
- Use extreme caution when opening e-mail attachments
- Don't download free offers
- Use passwords

— Source: Del Hunter,
president of CMIT Solutions

“As a business, you need to do checks and balances,” Brooks said. “There should be a system in place where the responsibility goes from one person to another.”

- A: Ask periodically for a copy of credit reports.
- M: Maintain careful records of financial accounts.

“If you become a victim of identity theft, act immediately to minimize damage to personal funds,” said Brooks, who recommended a report to the Federal Trade Commission.

Detective Chuck Sutterfield of the Loveland Police Department said victims involved in more serious cases of identity theft can spend hundreds of hours repairing their credit and proving their innocence.

“The largest source of identity theft is corrupt individuals on the inside,” Sutterfield said.

Identities can be lifted from a variety of sources, such as trash cans, wallets and purses, the Internet and places of business, including automobile dealerships, health care facilities, travel accommodations and credit bureaus, Sutterfield said. The identity information is used to open credit card and bank accounts, fill out loan applications and write checks, he said.

In Loveland, the crime is growing, with 249 identity theft and felony fraud cases reported in 2006, and 355 in 2007.

“We’re slowly catching up to what the bad guys have been doing for years,” Sutterfield said.

Del Hunter, president of CMIT Solutions in Loveland, discussed identity theft in terms of cyber crime.

About 70 percent of malicious computer software attacks are seeking confidential information, Hunter said.

And 95 percent of attacks target home-based and small businesses, which are less likely than large corporations to have comprehensive security systems in place, he said.

“In general, the goal is to make money through the information they can get off your computer or that you type into your computer,” Hunter said.

These attackers are looking for credit card numbers, passwords, account information, Social Security numbers and medical information, he said.

Hunter outlined the different forms of computer attacks, including Trojan horses, the most popular form right now, worms, viruses, spyware and phishing.

Hunter recommended that businesses install and regularly update anti-virus and anti-spyware programs, install a software firewall, and use computer passwords to help prevent attacks.

“For the typical individual, the cyber side of identity theft is only about 10 to 12 percent of identity theft,” Hunter said.