

Computer expert tells what crimes are on horizon

**By Daniel LeBlanc**  
**Olean Times Herald**

OLEAN - Credit card number theft, computer hackers, viruses, compromised Web sites, real estate scams, malicious e-mail - these were among the topics addressed by author and computer security expert David Stelzl Wednesday.

Databranch hosted the event at the Bartlett Country Club and offered several seminars throughout the morning on various computer issues.

With all types of cybercrimes being committed, companies are still at risk despite advances in technology.

One of the most common crimes is credit card and personal information theft, Mr. Stelzl said. Among the most targeted entities are financial institutions and universities.

Citing statistics from the Web site [www.idtheftcenter.com](http://www.idtheftcenter.com), Mr. Stelzl said anywhere from half to two-thirds of those in the U.S. may have had their personal information accessed by a computer hacker. In some cases, millions of files with personal information or credit card numbers have been stolen.

Even if an individual has not been the victim of credit card or information theft, it is possible the information just may not have been used yet, he said.

Organized crime has been among the leaders of this information theft, he said. In comparison, information theft is often much simpler than dealing drugs, he said. Estimated state that as much as \$105 billion may have been stolen last year alone.

“It’s estimated that it will grow 20 times within the next year,” he added.

Mr. Stelzl said he traveled to South Africa once and came back to find someone had copied his credit card number and used it to purchase \$25,000 worth of merchandise.

“I never lost my credit card,” he said. His financial institution contacted him to ask if he had authorized the purchase.

The company used his credit card history to flag the unauthorized purchase.

That is why hackers target universities and colleges because many of the students attending have little or no credit history, making it hard to determine spending habits, he said.

So, how does this information get accessed?

So, how does this information get accessed?

Mr. Stelzl said it can be as simple as opening a suspicious e-mail and clicking on a Web link. Doing this may download malicious software to a computer, thus bypassing firewall protection or a virus program.

“Hackers don’t break through a firewall anymore,” he said. Once the unwanted software is embedded, it can be used to access information or to be used as part of a network to launch a virus attack.

Security at companies is often compromised by a hacker easily gaining information about the company’s hardware and software.

Current employees looking for another job often have “resumes online with enough information to get into systems,” he said.

Hackers also use deception by calling a company and just asking for passwords to computer systems.

“Hacked companies often have insiders,” Mr. Stelzl said. Some hackers will pay an “insider” to provide information on the company’s computer system.

Another danger is employees using personal computers or remote networks to access company files. These computers are often easy targets for hackers.

In order to combat these scenarios, Mr. Stelzl said companies should see security as a protocol that needs to be enforced.

“Detection is the issue, not protection,” he said. Since no system is completely safe, companies need to monitor their systems to quickly detect when an unauthorized person accesses information.

“How comfortable are you with your ability to detect and respond?” he asked.

“It’s hard to test your own system.”

Companies should also limit access to key information and limit unnecessary user access.

“Have the mindset that people are already in your system,” he said. “Measure the likelihood of it and take action.”

“I feel we have an opportunity and obligation to educate businesses,” Databranch president David Prince said after the seminar. “We need to get people thinking about security.”

When asked if local companies have been targeted by hackers, Mr. Prince said “we see it all the time. We have had clients experience intrusion attempts.”

He cited e-mail spam as one of the “primary vehicles for these kind of attacks.”

(Contact reporter Dan LeBlanc at [dleblanc@oleantimesherald.com](mailto:dleblanc@oleantimesherald.com))