Businesses fall prey to cyberthieves' cunning

April 4 2011, By Steve Johnson

Among the growing ranks of consumers, business owners and others being lured by the convenience of online banking are legions of cybercrooks who have found the technology a convenient way to steal from unsuspecting victims.

More than 72 million households now manage their money online - up from about 12 million a decade ago, according to the financial services firm Fiserv. It's unclear how many of them have been targeted by crooks, but the FBI and a consortium of other government agencies reported in October that "thousands of businesses, small and large, have reportedly fallen victims to this type of fraud" with municipalities and nonprofit organizations increasingly coming under attack. And unlike individuals, they lack legal protections for their losses.

Ann Talbot learned of the danger four years ago when nearly $21,000 was taken from the bank account of her general contracting firm, Golden State Bridge. Then in May last year, cybercrooks struck her Martinez, Calif., company again, making off with about $100,000 from another account.

By then, Golden State had taken out an online-theft insurance policy, which limited its liability to about $10,000, according to Talbot, the company's chief financial officer. Even so, she is wary of the outlaws preying increasingly on those who bank via the Web.

"It's a huge problem," she said, adding that many people "have no idea of the threat out there."

It's just not lay people, either. FBI Director Robert Mueller told the Commonwealth Club of California in 2009 that he stopped online banking after getting an email that appeared to be from his bank, but that he realized was bogus after answering a couple of its questions.

After that, Mueller said, his wife told him, "no more Internet banking for you."

The cyberthieves aren't fussy about whom they target.

-In September last year, federal prosecutors in New York announced criminal charges against 37 people in a global online scheme that allegedly netted the crooks more than $3 million, including $130,000 from an unidentified hospital's California bank account.

-In October 2009, lawbreakers tried to abscond with $87,000 from a Danville, Calif., church, according to the Washington Post. Luckily, the transfers were blocked by the church's bank. Last August, the Catholic Diocese in Des Moines, Iowa lost several hundred thousand dollars in an online banking breach.

-In April last year, Aleksey Volynskiy was sentenced to 37 months in prison for plotting with hackers in the U.S. and Russia to loot individual Charles Schwab brokerage accounts.

Sarah Bulgatz, a spokeswoman for Charles Schwab, said the accounts were accessed through the victims' computers and not those of her company, adding that Schwab reimburses individuals for such losses. Under the federal Electronic Fund Transfers law, the liability of consumers who report an online bank loss within two days of discovering it is limited to $50 and only after 60 days are they liable for the entire amount.

But the law doesn't protect commercial, governmental or nonprofit enterprises. And the sizable sums those entities often maintain in their financial accounts make them attractive quarry for criminals. Of 504 small and medium-size businesses recently surveyed by Guardian Analytics, which helps banks and credit unions prevent theft, 32 percent said they had experienced an online-banking scam during the previous year.

While some banks have taken steps to prevent such larceny, many others have left themselves easy prey to hackers, who are becoming highly organized and using increasingly sophisticated tactics, said Guardian CEO Terry Austin. With more and more people banking online, he added, "the banking industry in general needs to step up to provide a higher level of security."

Some people - including Talbot of Golden State Bridge - also are urging lawmakers to give commercial ventures the same reimbursements afforded individuals. They have formed an online organization - Cyber Looting Awareness & Security Project - to lobby for the change.

That worries the American Bankers Association. It fears that if a company was shielded from liability the way a consumer is, "the business would be less inclined to take the protection measures necessary to protect their online accounts," which might prompt banks to stop offering online services, said the group's spokesman Doug Johnson.

He added that banks are working with law enforcement authorities to try to limit such crimes but that the problem is increasing because more people are banking online.

Still, many others are reluctant to send their financial information across the Internet. Of the more than 3,000 respondents to a survey by German security software firm Avira in November, 31 percent - nearly one out

of three - said they avoid online banking entirely for fear of being ripped off.

Even a security expert can get hoodwinked, said Larry Ponemon of the Ponemon Institute, a data-protection research outfit in Michigan. After recently receiving an email that seemed to be from his bank, "I came really close to doing something silly" that might have compromised his finances, he said. "The bad guys are getting really smart."

One of the crooks' methods is to send a person a "spear phishing" email containing a malicious attachment. Once the person opens it, their computer is infected with malware that snaps up their bank-account login information, allowing the thief to masquerade as the person and steal their money.

Another common scam is to create websites that look just like those of real banks. When people mistakenly give the sites their financial information, criminals use it to make withdrawals.

The increasing numbers of people who bank via their cell phones face another threat, according to a report in November by viaForensics, a Chicago information security firm. It discovered that some phones stored the owner's financial data, making the information vulnerable if the phone is lost. Bogus banking applications for phones also have been designed to steal money from anyone using them.

Although banks are working to fix some of the phone vulnerabilities, "it's still pretty bad out there," said Andrew Hoag, viaForensics' chief investigative officer.

Unfortunately, by the time many people realize their savings have been hijacked, there's little they can do to get it back, said David Johnston, whose Modesto, Calif., electric sign business, Sign Designs, lost about

$20,000 two years ago when thieves broke into its online account and transferred the money overseas.

"I was very angry," he said. "Your money should be safe in the bank."