

LOCAL

Cyber crime keylogging:
Don't become a victim
— A3



Keyloggers snatch information

Officials warn of new scam involving keystroke copying

BY MARK HORNICKEL
mhornickel@kenoshanews.com

An estimated 61 million people shopped online Monday, the so-called "Cyber Monday," during which consumers try to take advantage of holiday deals online. That means millions of consumers also were entering their credit card and bank account numbers into Web sites they think are secure.

But one malicious keylogger could shatter that sense of secu-

rity with just a few keystrokes, however.

According to a New York Times report published earlier this year, keylogging is on the rise, and U.S. computer security companies have reported theft through keylogging programs increased dramatically in 2005. Other reports noted a Brazilian ring stole roughly \$4.7 million from 200 bank accounts in less than a year, and Russian keyloggers took more

than \$1 million. A recent report from a security group known as CERT, states that 80 percent of the malicious keylogging programs go undetected by anti-virus software.

than \$1 million.

A recent report from a security group known as CERT, states that 80 percent of the malicious keylogging programs go undetected by anti-virus software.

Stop keylogging

Keylogging is the latest cyber crime in which thieves record a person's computer keystrokes to determine passwords and bank account information. To avoid keylogging:

- Don't open an e-mail or link that looks odd or you don't know the sender.
- Never give out personal account information unless you initiate it, and the recipient is a trusted, secure source.
- If you do need to send information to a credit card company or banking account, type the Web address yourself rather than connecting to it from an e-mailed link.

This fall, Wisconsin banks have tried educating their customers about the danger.

"It's really gained momentum in the last few months I think," said Peggy Theisen, a security officer for North Shore

Bank. "A lot of people don't know what this is all about."

While consumers have begun catching on to the phishing scams — fraudulent e-mails or Web sites designed to look exactly like one from your credit company — keylogging has emerged as a simpler, more direct type of fraud, experts say. It involves criminals stealing online banking passwords, account numbers and credit card numbers by using software programs that monitor and copy the letters or numbers you type into your keyboard.

The software usually infects computers through viruses at-

KEYLOGGING: Be smart using the Internet

From Page A3

tached to e-mails or downloads, and most of the time, victims don't realize it's there.

"By clicking on links in e-mails, it infects your computer and it logs every keystroke that you make," Thiesen said. "And the person on the other end, is now tracking every keystroke. So it sees that you're typing in northshorebank.com, and it types in your password and everything else and your account numbers."

Thiesen said she was aware of at least one customer this year who nearly fell victim to a keylogger.

"Because we caught it so

soon, she didn't take a loss," Thiesen said. "We were able to jump on it right away. She called us and said there was something weird going on and we knew. I could tell right away that it was keylogging."

The best prevention, law enforcement and security officers say, is to be smart about your Internet usage. Don't open an e-mail or link that looks odd or you don't know the sender. Also, never give out personal account information unless you initiate it and the recipient is a trusted, secure source. If you do need to send information to a credit card company or banking account, experts say it's better to type the Web

address yourself rather than connect to it from an e-mailed link.

"We try to get people to just be educated about it so that they don't open e-mails that they don't know and they don't download things that are from unfamiliar sources," Thiesen said. "Any kind of e-mail that you're not expecting or if you get an e-mail from Bank of America and you don't have an account there and it's got an urgent message like 'your account's been compromised,' don't even open that. Just delete it immediately and make sure you have the most updated virus protection."