LAMORINDA WEEKLY
Wednesday, December 26, 2007 ▪ Volume 01; Issue 23 ▪ www.lamorindaweekly.com

The Treacherous Information Highway

By Jennifer Wake

Recent advances in software and technology have enabled users to browse the Internet from remote locations (including their cell phones) and meet new friends via the Web on social networking sites. At the same time, more doors have opened for the cyber criminal.

In the past few years, Orinda Police Detective Nate McCormack has seen a large increase in local identity thefts. "Some are through the mail, but more are through the Internet," he said.

According to a report by the National Cyber Security Alliance (NCSA), more than 70 million people use social networking sites such as MySpace and Facebook, and the numbers are increasing daily. Of those adults who "social network," 83 percent expose themselves to hackers and thieves by downloading unknown files potentially opening up their PCs to attacks, and 74 percent have given out some sort of personal information such as their e-mail address, name, and birthday – even social security numbers.

"Providing this type of information can provide enough ammunition for criminals to hack into financial records and compromise users' personal information," the report noted.

Although not a "social networker," Lafayette resident Ginna Bowles says she gets about two dozen spam e-mails a day on her home computer. "Some e-mails say, 'You only need to click here to get $2,400.' I just delete them," she said.

Many of these e-mails can include links that send victims to bogus Web sites that look legitimate. Requests for users to reenter passwords or provide personal information can look safe, but often the information is either sold to scammers or used by identity theft criminals.

Unfortunately, the number of identity thefts in this area is difficult to nail down because they are often classified in different categories, such as petty theft or grand theft, McCormack explained. "It's hard to get exact numbers," he said. "It's even harder to catch the online perpetrators because they're often operating out of state or out of the country."

The Federal Trade Commission (FTC) states that only 39 percent of identity theft victims notify a police department after being scammed, so the actual numbers are likely much higher than reported.

Although Bowles is very careful about not opening any e-mails from anyone she does not know, she still fell victim to a scam.

Last month, while reviewing her bank statement, Bowles came across a strange copy of a check for $29.99. The writing on the check was nearly impossible to read and the check's date was Nov. 27, the same day she and her husband had taken a long flight and were not writing any checks.

"I went to the bank and told them I didn't know what this was," she said. "They made an enlarged copy and with a magnifying glass we could make out 'Market Billing' on the check. The person at the bank googled the name and found six pages of people caught in this national scam. They had an electronic signature of mine on file and had all my bank information." Although Bowles never places outgoing mail in her mail box, somehow a criminal got one of her checks.

In addition to changing her bank account, Bowles had to change a number of documents and financial accounts linked to the checking account. "It was a nightmare," she said. "We now don't pay by check and pay by computer, but that opens another can of worms."

According to the FTC, in 2005 Consumer Sentinel – the complaint database developed and maintained by the FTC – received over 685,000 consumer fraud and identity theft complaints: 63 percent were fraud, 37 percent were identity theft.

Last week at a seminar on how to avoid financial exploitation hosted by Lafayette Senior Services, Shirley Krohn, senior assembly member for Contra Costa County and elder abuse prevention advocate, passed around copies of dozens of e-mails she had received in just one day – all of which were potential scams. One e-mail even stated it was from the Internal Revenue Service, asking to click on a link regarding a $240.34 refund.

"It's doubtful the IRS would be sending e-mails to people so they could get their refund," she said. "It's hard enough to get money out of the IRS. Never click on a link inside an e-mail or give out personal information."

"Many elders are too trusting and are easily duped by official looking (or sounding) communications such as e-mails," said Jenefer Duane, CEO and executive director of Elder Financial Protection Network. "Also, elders who are more isolated may respond to an e-mail without asking around or checking out a bogus request for account (or other) personal financial information."

The best defense is awareness and education.

"I generally tell people to always be sure you know who you're talking to," Detective McCormack said. "You should have the most updated software, have firewalls, spam filters, all the latest features."

For information on how to protect yourself from cyber criminals, visit On Guard Online, hosted by the FTC, at http://onguardonline.gov.

If you think that your personal information has been stolen, visit the Federal Trade Commission's Identity Theft Resource Center at www.consumer.gov/idtheft/index.html for information on how to file a complaint and control the damage.

Shirley Krohn, senior assembly member for Contra Costa County and elder abuse prevention advocate, addresses a group of seniors about financial abuse at the Lafayette Community Center Photo Jennifer Wake