

## Cyber security focus at Safety Conference

Earlier this month, a Clark County couple brought an apparently fraudulent "mystery shopping assignment" to the attention of a county employee. Enclosed were what looked like two \$933 postal money orders bearing the woman's name and address.

Also this month, a man reported to the Vancouver Police Department that his relative had been the victim of a \$10,000 scam involving someone posing as a law enforcement officer.

These incidents illustrate the kinds of threats FBI Supervisory Senior Resident Agent Michael D. Rollins discussed during a personal security talk at the county's Sept. 10 Safety Conference.

For example, last year, nine million Americans were victims of identity theft, with a loss of at least \$5 billion, Rollins said.

If you are a victim of ID theft, he said, you should:

- Close accounts that were tampered with or fraudulently set up.
- Contact the fraud departments of your credit card companies.
- Review a current copy of your credit report and place a fraud alert on it.
- File a police report.
- Put your phone number on the telemarketing Do Not Call Registry at [www.donotcall.gov](http://www.donotcall.gov) or 1-888-382-1222.
- Opt out of pre-approved credit offers to limit unsolicited mail and email by calling 1-888-5OPTOUT, or 1-888-567-8688.

To prevent online identity theft, you should:

- Not click on unsolicited emails. Type in the web address yourself.
- Not store personal or financial information on websites.
- Keep computer operating systems, software, virus scanners and plugins updated and patched.
- Use two-factor authentication when you can.
- Set Facebook to be notified when your account is accessed from a mobile device or unfamiliar computer
- Require personal information to reset your Twitter password.
- Consider options at <http://www.avg.com/us-en/for-mobile> for protecting Androids and iPhones.
- Change your router's default password.