

Lessons Learned At Identity Theft Seminar

Those attending the informative March 28, 2006 program at the Sandcastle presented by Kiawah's Director of Security, Joe Croughwell, gained important information about how to protect themselves from fraud and scams associated with this fast-growing crime. Following his presentation, Joe answered questions and allowed the audience to share their own experiences and concerns.

He explained that some of the most common means of identity theft include:

- Sending false e-mail messages to obtain bank or credit card information
- Intercepting financial data
- Creating bogus websites
- Hacking into computer systems and accessing personal data
- "Skimming" - retail establishment employees using a small electronic machine to record information on your credit card's magnetic stripe
- "Dumpster diving" for credit cards, loan applications, bank statements, insurance forms, etc.
- "Phishing" - pretending to be someone from a business you deal with asking to update billing information

He also advised how to protect yourself from these schemes. General rules include:

- Don't give your personal information out over the phone, through the mail or over the Internet unless you're certain with whom you're dealing.
- Resist providing your Social Security number, and don't carry your Social Security card.
- Secure personal information in your home, especially if you are having work done in your house.
- Shred documents with personal information before throwing them away.
- Deposit outgoing mail with personal information in post office collection boxes rather than an unsecured mailbox.
- Monitor billing statements and credit reports
- Cancel all unused credit card accounts.
- Be wary of promotional scams asking for personal information for "billing purposes."

For Internet users, his advice was:

- Do not download files or click on hyperlinks sent by strangers. Opening them could expose your system to a virus that hijacks your modem - allowing access to stored information.
- Update your virus protection software regularly.
- Use a firewall program to prohibit uninvited guests from accessing your computer.
- Look for the "lock" icon on the browser's status bar to indicate your information is secure during transmission.
- Do not use automatic login features that save your user name and password and always log off when you're finished with an online transaction.

- Exclude personal information from family websites.
- If you are discarding an old computer, use a “wipe” utility program that overwrites the hard drive to make any personal files unrecoverable.
- If you receive an e-mail with little or no notice, that your account will be shut down unless you confirm your billing information, do not reply or click on the e-mail. Instead, contact the company using a phone number you know to be legitimate

If you suspect you are a victim of Identity Theft, you can receive help by calling the FTC number: 877-438-4338 or by logging on to www.consumer.gov/idtheft.