



Avoiding Cyber Scams in the Age of Technology

By Audrey Cortes

[Share](#) |

« Back to Issue



On Jan. 17, the Older Americans of the Bay Area hosted an event featuring Suzana Gal, Director of the Consumer Mediation Unit of the Santa Clara District Attorney's Office at St. Mark's Episcopal Church. The seminar "Scams, Spams, and Other Lies: How to Avoid Scams and Be a Savvy Consumer," covered a wide range of schemes from telephone marketing to email hacking and ransomware.

Gal discussed the importance of informing consumers about the problems that exist, since these crimes are on the rise, and can often be easily avoided. Gone are the days when scammers would have to send their pleas for cash through the mail—now they can reach an infinite number of potential victims with the click of a button.

Bay Area Older Adults says that in 2014, 47 percent of American adults had their personal information stolen by hackers. "Increasingly, criminals are exploiting the speed, convenience, and anonymity of the Internet to commit a diverse range of crimes including scams, identity theft, and tax refund fraud."

Accusations about Russian interference in the November election have brought cyber crime to the forefront of American political discourse in recent months. Regardless of

political preference, many people are worried that if our government can't protect itself from hacking, then individuals have little hope of warding off the vast amount of cyber crime that has cropped up.

One issue raised by Dr. Anne Ferguson, Executive Director of Bay Area Older Adults, is that, "The majority of seniors are now online which means they have become the primary target of online crimes." Dr. Ferguson said she felt it was necessary to hold this event because older adults are increasingly susceptible to these types of crime.

The seminar, an example of the group's efforts to ensure the well-being of older adults in Santa Clara County, drew an active crowd, eager to discuss ways of protecting themselves online.

Director Gal says she is now dealing with people who sent money to the infamous telephone scam in which people in India called Americans posing as IRS agents, threatening them with jail time. While there is no clear data on how many people were affected, the numbers indicate that close to \$100 million was lost by victims of this group alone.

Possibly an even more damaging type of cyber crime is called ransomware. Through a variety of means, the criminal will find a way into the victim's computer, either by sending a link that automatically downloads the malicious software or by claiming to be from a reputable tech company calling to let the customer know they found an issue with their machine.

If the customer follows a few simple instructions, the fake tech support agent can gain remote access to the victim's computer. This allows them to control the files or photos on that computer and then demand a very large sum of money, or ransom, in order to gain the files back. Many large businesses like law firms, major companies and even hospitals have fallen victim to this and many choose to pay for the sensitive information to avoid devastating loss.

Gal advised wary consumers to check banking statements and credit reports carefully and in a timely manner. She reminded participants that everyone is eligible for a free yearly credit check at annualcreditreport.com. It can also be helpful, especially for older people who aren't planning on large purchases like a home or auto loan, to freeze their credit to avoid potential fraud. In the state of California, seniors can do this for free.

Here are Gal's top tips for avoiding the most popular scams:

1. Take a deep breath before taking any action. Stop. Think. Verify.
2. Never send money to strangers. Scammers will often pressure you to respond right away. It can always wait if it's a legitimate request.
3. Never respond to requests for personal information, whether it through phone, email, or advertising.
4. Do not open attachments or click on links in emails from anyone you don't personally know.
5. Use passwords that combine uppercase letters, lowercase letters, numbers and symbols to reduce the risk of having your accounts hacked.

While it can be very difficult to track down these criminals after the fact, it's important to report cyber crime so the information can be tracked. If you think you may have been a victim or the target of a scam, call the Santa Clara District Attorney's Office, Consumer Mediation Unit at (408) 792-2880.