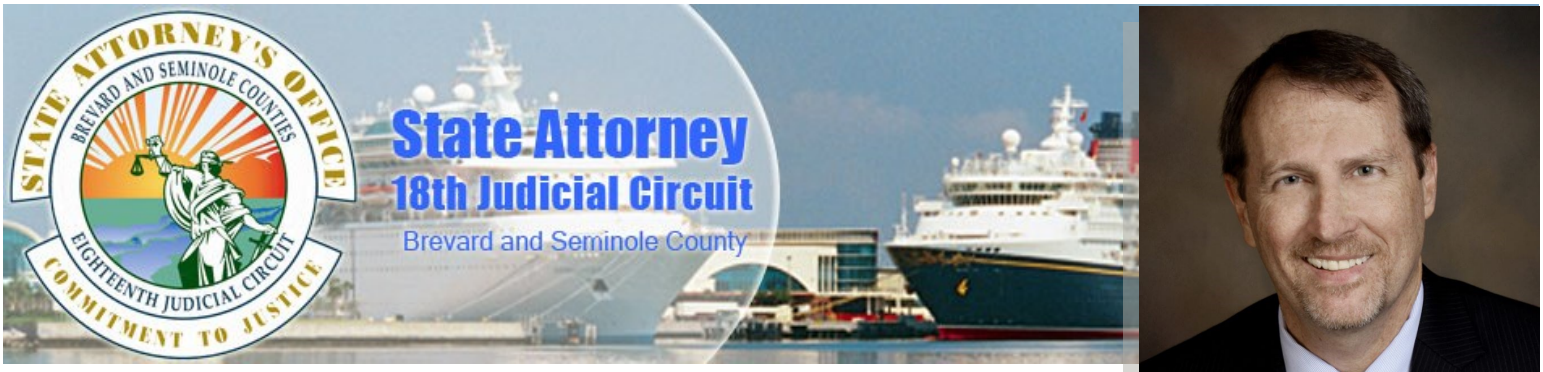

The Monthly Brief

Volume 7 Issue 2 February 2019

Investment Fraud

Investment fraud can take many forms, but all prey on the desire to make money without much risk. It can sometimes take years to realize you've been scammed. Even savvy investors fall for investment scams.

In basic versions of the con, the scammer convinces you to "invest" in a project, company, loan, or other initiative. You may be shown reports that the project is producing great returns. But when you try to withdraw your money, it turns out the investment never existed.

Another common investment fraud is a pyramid scheme or Ponzi scheme. You buy in not based on sales of a product, but on bringing in more people to invest. Unable to sustain returns, the pyramid collapses.

- Be wary of terms like "guaranteed" to do well, or that offers low or no risk with a high return.
- Investments are regulated by the SEC or other investment industry regulators. Check licensing for the sellers.
- High-pressure sales tactics, opportunity meetings, success stories, and selling to a shared connection like ethnicity, church, profession, are all warning signs.
- Chain letters or emails that ask you to send money or other items in the mail with a promise of a return gift or payment are illegal in the US and Canada.

Learn more about investment fraud with tips and info directly from the BBB

Follow Us On Facebook

Subscribe: philarcher@sa18.org

Romance Scams

Beware Valentines Love Scams! Scammers are relentless and with Valentines Day approaching they've got those looking for love clearly in their sites. IBM and the FBI say the threat is real and victims can expect everything from extortion attempts and computer take overs to identity theft and malware attacks. Scammers are also using personal info from dating site and social media to target their victims.

Popular Scams and Romance Cons

The Foreign Love Scam - An email or social media contact says that the writer is new in the US or wants to move there. They found your online pictures so compelling they had to write. Essentially a catfish scam designed to gain the victim's trust; the people behind the campaign ask for revealing photos, seek money for a supposed visit or infect computers with malware. Check out tips in this dating scam video from the FTC

The Military Love Scam - In this variation the scammer claims to be a member of the U.S. Army, usually stationed overseas. They claim to quickly fall in love and then ask for money needed for medical, travel or other expenses.

The Flower Scam - People who ordered flowers online receive an email explaining their bouquets can't be delivered unless credit card information is reentered online. By following a link to a fake website, the credit card numbers are stolen and used for purchases.

The Valentines Message Scam - Emails announce that someone has sent you a Valentine's greeting and directs people to a fake website mimicking popular greeting card sites. Clicking on the link triggers a malware dump onto the machine, making its owner a target for more spam and future phishing attacks.

The best way to avoid these scams is to be aware, ignore free offers, romantic advances from unknown people, keep your security software updated and never provide personal information or money to anyone contacting you by phone or email that you didn't contact first. Learn more about Imposter Scams of all kinds with tips from the FTC

Phishing Quiz

Can you spot a phishing email? We thought we could but Google's Jigsaw has a new quiz that tests you with the cleaver ways scammers use to trick us. We admit it wasn't easy, but very informative. Some are examples of an innocent email, while others have all been inspired by real phishing emails that Google has come across.

TAKE THE QUIZ HERE

This quiz will not only tell you if you were right or wrong, it'll also point out the details you can use to spot phishing emails in the future. Pass or not, you'll be harder to trick!