State Attorney
18th Judicial Circuit
Brevard and Seminole County

The Monthly Brief

Volume 5 Issue 10 October 2017

Craigslist Corner

Property Rental Scams

Crooks posing as property owners or agents will post photos of real homes in desirable areas at very attractive monthly rental rates. By offering both pet and child friendly options, these ads target a wide range of potential victims.

The crooks then use high demand pressure tactics to convince victims to immediately wire a deposit or credit check fee to hold the property. Some even go so far as to send lease agreements to sign and asking for application fees or 1st months rent.

Of course the property isn't theirs and a quick internet search of the address often produces the actual listing by a licensed real estate agent. Potential renters should also check out the address on the local property appraiser's website or contact a licensed rental agent to check it out.

Another twist on this scam is out of area vacation rentals. Operating in much the same way, victims send advance rental fees only to find out when arriving for vacation the listing was a scam. Attempt to find out the address of any vacation rental and then conduct an internet search for the property. It's most likely already listed on a local vacation rental site.

Avoid these rental scams by doing your homework online and asking for a personal inspection of the property before paying any fees.

Find out more by visiting Craigslist Scams Information Page

Follow Us On Facebook

Subscribe: philarcher@sa18.org

Credit Bureau Data Breach

Equifax, a national credit reporting bureau, has suffered one of the largest data breaches in history and has revealed the sensitive data of as many as 143 million people. Unidentified criminal hackers are expected to begin exploiting the information immediately with various scams targeting consumers.

Included were full names, birthdates, social security numbers, addresses, and in some cases driver's license numbers of consumers. All information used by lenders to confirm a consumer's identity. Also lost were emails, passwords and more than 200,000 credit card numbers.

The FTC reports that consumers should be alert for any calls from someone claiming to be from Equifax and attempting to verify or obtain information. You should also watch your credit accounts, mail and banking information carefully for anything suspicious.

Some additional steps include using a Credit Freeze, Change Passwords & Usernames, check your Credit Report and consider obtaining a Credit Monitoring Service.

Equifax is offering a free credit monitoring service and a website page to verify if your information has been revealed. Transunion is also offering a free credit service called TrueIdentity. However both have terms and conditions you should read very carefully.

My Social Security Account

With the Equifax breach the Social Security Administration is urging everyone to either create or add security to their My Social Security Account. This account is your gateway to many SSA online services. Creating your account today will take away the risk of someone else trying to create one in your name, even if they obtain your Social Security number.

Here's an instruction Video from the SSA on how to open a My Social Security Account OR Click Here to visit the My Social Security account home page and click on the green tab that says "Sign-In or Create an Account." You will need some very specific info to verify your identity so make sure your personal financial and tax records are available to use. The questions can be tricky, if you get some wrong, your electronic access will be suspended for 24 hours. If your account gets suspended, you can call 1-800-772-1213 and ask for the Help Desk for assistance with your account.

Consider adding second layer verification using your phone or email to receive access codes before each use. Using two ways to identify you when you sign on will help protect your account from unauthorized use and potential identity theft. If you suspect identity theft, report it to the Office of the Inspector General and visit identitytheft.gov.

*Source Material Komando.com