



State Attorney  
18th Judicial Circuit  
Brevard and Seminole County



# The Monthly Brief

Volume 6 Issue 2

February 2018

## ONLINE SHOPPING SCAMS

A jersey from a fan's favorite team is very popular during this time of year, but beware of online stores that offer "official" merchandise at unbelievably low prices.

Scam websites are conning people out of their money. Here's how the scam works:

You're looking for an item online, and you come across a site (often on social media) that promises great deals and fast shipping.

The store isn't one you've heard of but has great photos and very cheap prices. After placing your order, your account is charged and you receive confirmation emails. All seems normal... until weeks pass and the product never arrives.

It's called an [Online Purchase Scam](#) and they target all kinds of popular products, not just sports jerseys. Here's what to look out for:

- A low price significantly less than other well-known retailers' charge.
- Limited or missing contact info; terms of use; privacy, return and refund policies.
- Phones answered by an individual
- Located overseas or out of the U.S.
- Limited payment options; won't accept secure payment services like PayPal; and the site is not secured (https & lock icon).

Before buying online with an unfamiliar seller, research the company with a web search for established positive reviews. Also check the address, phone numbers and if it's listed on [BBB.org](#) or [BBB Scam Tracker](#)

\* BBB.org

**Follow Us On Facebook**

Subscribe: [philarcher@sa18.org](mailto:philarcher@sa18.org)

## IRS Tax Scams

The IRS is reporting a dramatic increase in the number and type of tax related scams targeting Americans this year. Experts point to the 2017 Equifax data breach that exposed the personal info of more than 145 million people to hackers as a major contributor. We've reported on several scams on our Facebook page, including The [Top 6 Tax Scams of 2018](#), the [W-2 Tax Scam](#), and [IRS Imposter Scam Calls](#).



However the problem is becoming so wide spread that scammers are now targeting tax professionals, payroll directors, and even the [disabled](#). They pose as tax preparation professionals, tax advocacy groups, law enforcement officers and IRS collection agents.

To combat the problem the [IRS has published a page on their website](#) dedicated to identifying these scams. It also includes links on how to report the scams and what to do if you've become a victim of tax fraud or identify theft (<https://goo.gl/o1JulK>).

Unfortunately many tax payers had their social security numbers exposed in the Equifax breach and scammers can file fraudulent income tax returns using just a name, address and social security number. If you're notified by the IRS that a suspicious or previous federal return has been filed in your name, find out what to do by [downloading this IRS guide](#) or visiting the [IRS Tax Payer Guide to Identity Theft](#) for more information. \*IRS.gov

## AIRBNB SCAM TARGETS TRAVELERS



Booking through Airbnb is so popular the company reached more than \$1 billion in revenue in 2017. Unfortunately, that also makes it a target for scammers. In this con, scam artists spoof the Airbnb website and fool victims out of thousands of dollars with no hope of reimbursement.

The scam starts when a consumer visits the Airbnb website and finds an apartment or house to rent. The host requests that questions be directed to an email address instead of through the site. When the consumer emails, the scammer replies that the property is not available for the stated dates. Instead, they offer a link to a similar property.

The link points to a spoofed Airbnb site that looks almost identical to the real one. The "About" page even links to the real site's "About us" page. There also a live chat option, which is not offered on the official site. If the consumer decides to rent the property, they are prompted to wire money and are never contacted again.

**TIPS:** 1. Never wire money outside of the Airbnb platform. 2. Watch out for lookalike URLs 3. Look for a Superhost listing.

For more info on how this scam works check out [The Online Citizen](#) and read an article written by a victim of the scam published in the [Huffington Post](#).

\*BBB.org