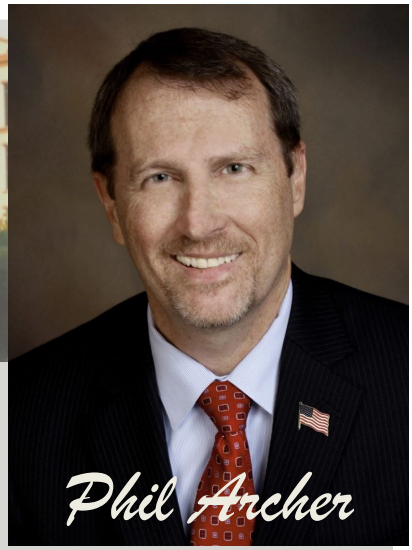

The Monthly Brief

Volume 8 Issue 3 March 2020

Tax ID Theft

The United States' tax season is here, and so are the scammers. Con artists are using the Social Security numbers of unsuspecting Americans to file phony tax returns and steal their refunds. **How the Scam Works:**

You file your taxes as normal but you get a legitimate IRS notice that more than one tax return was filed using your Social Security number.

So what happened? Scammers used your stolen personal information and filed your tax return early. They got a refund and left you to explain it all to the IRS. Tax ID theft is clever because victims don't know they've been targeted until they file their real tax return.

Crooks can steal your personal info using Phishing/Smishing scams, social media ads, malware, data breaches, fake websites, or employees of corrupt tax prep services and other companies with your personal info.

How to avoid Tax ID Theft: File as soon as possible each year, before crooks can do so. Also don't give out your SSN# unless absolutely required like applying for a loan. Watch for red flags like notices from the IRS that don't apply to you, or an employer you never worked for. If you've been the victim of ID theft, consider getting an Identity Protection PIN from the IRS.

Immediately report Tax ID theft to the IRS at 800-908-4490, then to the FTC online or by calling 1-877-FTC-HELP. The FTC also offers a personalized identity theft recovery plan at identitytheft.gov.

*Sources BBB .com, FTC .gov

Follow Us On Facebook

Subscribe: philarcher@sa18.org

Data Breach Payment Scam

There have been a lot of data breaches in the past few years, in fact so many it's hard to remember them all. Consumers had their personal information exposed and often weren't compensated for damages caused by crooks who used it for identity theft.

Now Russian scammers are posing as US government officials with a fake website offering data breach victims payments similar to those offered in the Equifax case. This attempt was uncovered by researchers at Kaspersky Labs who found a site offering financial compensation for "leakage of personal data." and identifying itself as the US Trading Commission (not a real agency). The website leads to numerous forms where users are asked to provide personal information like first and last name, credit card number and SSN to verify identity. If you don't have an SSN or aren't a U.S. resident, the site conveniently sells you a temporary one. Researchers found there are several mis-spellings and grammar mistakes, but less tech-savvy or senior users could be fooled.

Avoid fake websites: Be suspicious! Use caution with sites pushing for ID or payment info. Always run a Google search about the site first. Consider using Google Chrome Safe Browsing or software that will alert you before visiting suspicious sites. While not proof positive, look for the "s" in https before the site address, indicating it's secure.

To learn more about spotting fake or phishing websites, download or read these helpful tips from Dell Computer.

*Sources Komando .com, Kepersky Labs, Google, Dell

Government Services Rip-Off

The Federal Trade Commission filed a complaint against a group of websites that were claiming to offer government services (including Florida) for a fee. They would charge for things like registering your car, applying for a fishing license or renewing your driver's license. Some sites had no ability to perform the service, while others were charging for documents that are freely available to the public from official government websites. Some of the sites encouraged people to sign up for Section 8 housing and services like food stamps or unemployment. Potentially more bad news is what happened to the information customers were handing over, like birth dates, employment status, health insurance data and phone numbers. With paid ads on internet search engines, these scam sites are often shown first in a key word search.

The FTC was successful in its complaint and a federal judge has ordered the companies to stop making claims they can't back up. The court order said that while visiting these sites, customers "were not clearly informed that they could not obtain the government service they were misled to believe was available." Sadly many others still exist.

A few companies behind the sketchy sites named in the FTC complaint include On Point, Dragon Global, Eagle Media, Skylar Media and many more. You can learn more about these sites or get help by reading the FTC press release.

To read more of the Federal Trade Commission's consumer scam alerts or to sign up for email updates, visit them at https://www.consumer.ftc.gov/features/scam-alerts.

* Sources FTC, Komando .com