https://www.nhregister.com/opinion/article/Today-s-Business-If-it-seems-too-good-to-be-16641021.php

## New Haven Register

https://www.middletownpress.com/opinion/article/Today-s-Business-If-it-seems-too-good-to-be-16641021.php

#### **The Middletown Press**

https://www.registercitizen.com/opinion/article/Today-s-Business-If-it-seems-too-good-to-be-16641021.php

#### THE REGISTER CITIZEN

https://www.ctpost.com/opinion/article/Today-s-Business-If-it-seems-too-good-to-be-16641021.php

### CONNECTICUT POST

https://www.thehour.com/opinion/article/Today-s-Business-If-it-seems-too-good-to-be-16641021.php

The Hour

https://www.stamfordadvocate.com/opinion/article/Today-s-Business-If-it-seems-too-good-to-be-16641021.php



https://www.greenwichtime.com/opinion/article/Today-s-Business-If-it-seems-too-good-to-be-16641021.php



https://www.newstimes.com/opinion/article/Today-s-Business-If-it-seems-too-good-to-be-16641021.php

newstimes.com

# Today's Business: If it seems too good to be true — beware identity theft

Christine M. Tenore
On the Internet on Nov. 26 and in print on Nov. 28, 2021



Christine M. Tenore Contributed photo

At this time of year, we are doing more shopping online, looking for bargains, searching for the deal of all deals. The item we're looking for pops up, like magic, at a very reduced price and we are tempted to order it "right now" because there are only a few remaining at that price.

Beware! If something seems too good to be true, there is a strong probability that someone is trying to steal your identity — and your money.

The statistics are alarming. There was a 250 percent increase in identity fraud reported to the Federal Trade Commission from 2016 to 2021 — from 400,000 reported cases in 2016 to 1.3 million in 2020. Individuals of any age, gender, marital status, education and economic status are vulnerable. Resolution can take months or even years.

Why the increase? First of all, more of us working from home. We take phone calls from home. We do more shopping and searching online, especially since the pandemic. There are more opportunities for us to become victims.

The goal of an identity thief is to obtain victim's Social Security number and, if possible, a full name, address and date of birth.

How do you know whether you've been a victim? Here are few ways:

- You see an unfamiliar loan or credit account on your credit report.
- You have an unexpected drop in your credit score.
- You receive an unexpected notice from your health insurance reflecting that you've reached your benefit limit.
- You don't receive expected U.S. mail.
- You try to file your tax return online only to have the IRS reject it, saying a return connected to your Social Security number already has been filed.

Telephone scams often target seniors. The caller pretends to be a person in authority and employs a sense of urgency that prompts the victim to move quickly — with no time to think about responses. Seniors tend to have more time and may be more trusting. And they often have more money than younger people and often have good credit reports. They may not report identity theft because they don't want to be seen as not being able to manage.

Internet scams are another source.

Online con artists often "phish" for personal data through email, seemingly legitimate requests, claiming information is needed by the victim's bank, credit card or mortgage company. The criminals ask the victim to verify their financial information by clicking a link, which then could either hijack the victim's information or infect the victim's computer. In addition, victims of online scams say they did not receive goods purchased — usually a "deal" online or a "bait and switch" scheme with high international shipping charges.

Protect yourself. Only shop directly with online reputable retailers. Avoid typing the name of the retailer into your browser bar — type in the website address to

avoid being diverted to a fake website that looks similar. Vet new-to-you businesses by looking for online reviews and search the Better Business Bureau website for complaints. Check the "contact us" page on the website for a U.S. address and phone number and then call the business to verify. And pay with a credit card — not your bank debit card.

Don't browse on public Wi-Fi because information can be shared unknowingly. Especially avoid online shopping in a public place where sensitive information may be grabbed by a thief. If you do, use a virtual private network (VPN) which creates an encrypted tunnel between your computer and the server. And always choose strong passwords.

Protect yourself from "IRS" scam identity theft. The IRS does not send emails about tax refunds or sensitive financial information. If you receive an email from what seems like an IRS site, delete it. Never clink the links. Safeguard your Social Security number and other personal information. Don't give information via email or over the telephone. There is a new IRS identity protection tool, Identity Protection Personal Identification Number (IP PIN), that can be found at www.IRS.gov. This is a unique six-digit number for your correspondence with the IRS. An identity thief would have to know not only your basic personal information but also this number.

If you suspect that you've been a victim of identity theft, you can place a fraud alert with one of the credit bureaus: Equifax (800-525-6285), Experian (888-397-3742) or TransUnion (800-680-7289).

If you have been the victim of tax-related identity theft, you can complete IRS Form 14039, Identity Theft Affidavit, and send it to the IRS with your proper paper tax return.

Identity theft can happen to anyone.

Change your habits to protect yourself from becoming a victim. Be more aware of what you do and how you do it on the telephone and online, monitoring your bank and credit card statements for fraudulent activity, and not giving personal information over the telephone or Internet until you verify that the request is valid. It will save you time, anxiety, money and the information that defines you.

Attorney Christine M. Tenore is a partner at the Fairfield-based law firm, Eliovson & Tenore. She can be reached at www.connecticutelderlaw.com or 203-336-2566. The firm is dedicated to helping clients face a host of issues related to aging, including those related to finances, health and special needs.