Three Tips for Protecting Against Online Identity Theft

Here are some suggestions for thwarting fraudsters when digitally communicating personal information.

The amount of personal information available online these days is leading to new levels of digital theft. In fact, eCommerce fraud cases increased by 50% in 2020 alone, according to a recent estimate by security consulting firm Sift.

At the same time, the average value of fraud attempts involving online retail purchases increased some 69% from the previous year, the company noted in its late 2021 report "Digital Trust and Safety Index: Navigating the New Normal of Digital Fraud and Disputes."

"The global disruption caused by the pandemic gave fraudsters fluctuating online transaction volumes to hide behind, more data to steal and a growing number of accounts to take over, leading to the proliferation of online abuse," Sift's analysts observed.

Online security professionals are urging anyone who shops online — or anyone who has reason to conduct business over the Internet involving the exchange of personal information — to take appropriate precautions.

Along those lines, below are three tips offered by security experts in the field.

#1 — Password Protection: The First Line of Defense

This might seem a bit obvious, but the rule-of-thumb is to use a unique phrase that you can remember and doesn't duplicate passwords utilized in other accounts.

Instead of typing in something generic and short, many security software professionals suggest thinking of a complete sentence or phrase. Oftentimes, they'll even recommend a password manager with strong encryption security features to store all of your passwords in the same place.

In these cases, as well as others, it's probably a good idea to enable multi-factor authentication on all of your accounts and devices.

Another big no-no in the security world is sharing personal information through social media accounts. Users of such services — whether it's Twitter, Meta or Instagram — might be well-advised to review any such provider's privacy and security policies, along with any internal settings that can guide your interactions online.

Three Tips for Protecting Against Online Identity Theft

#2 — Stay Vigilant Against Phishing Scams

A common method for scammers to nab your personal information is by sending you an email or text with a fake link or malicious file. These are known as phishing scams and are intended by hackers to steal your online identity.

It might sound pretty straightforward, but phishing can be quite convincing if you're not careful.

A basic rule of engagement is to make sure and check closely any sender's email to make sure it's someone you know and can verify. Even then, security experts point out that a fraudster might be able to come very close to tricking you into thinking it's a person worthy of your trust.

Things like misspelled words and broken phrases can turn into good clues that an email or text isn't coming from a legitimate source.

With all of the technological innovations and sophisticated software tools available to hackers, how do you really know what email or text could be dangerous? An overriding tip made by industry veterans is to be very skeptical about any online message that asks you to take action.

The bottom line: If you don't take time to fully vet your communications online, you're taking a chance of giving criminals access to your personal information. In other words, if you're asked to click on a link or reply to a text, stop and think first.

#3 — Communicate Through Secure Networks

You can take all the operational precautions possible, but if the Internet network your computers and/or mobile devices are connected to isn't secure, then other security measures can very well go for naught.

A major red flag is trying to work from an unsecured Wi-Fi network. This includes any network that isn't designed to provide encryption between communication endpoints connecting your computers and/or mobile devices.

Potential issues have cropped up when using so-called public Wi-FI networks, which are often offered at restaurants, hotels and other highly trafficked public gathering spots and businesses. A safety tip when you must connect through a public Wi-Fi spot is to stay away from opening a bank account or any other online account with a financial institution.

That applies to other services in which sensitive personal information is delivered online — especially when accessing your employer's computer systems or databases remotely for work-related purposes.

Three Tips for Protecting Against Online Identity Theft

Even though you should never try to access sensitive personal and professional data through an unsecured network, for generic purposes a helpful precaution is to add software to create a Virtual Private Network. Such a program or app, commonly referred to as a VPN, automatically encrypts your digital communications to help create a more secure environment.

When setting up a secured Wi-Fi network at home, it's still advised that you implement many of the same safety practices as those recommended for working with individual apps and social media services. In other words, you need to pay attention to creating and maintaining network passwords, keeping on your toes for phishing scams and software updates.

Specialized security programs, such as antivirus and firewall software, adds an important layer of protection to help you guard against fraudsters — even for those using a secured network in their own homes.

Developing a consistent and secure process to communicate over the Internet is considered as critical to leveling the playing field, so to speak.

While it might seem a bit overwhelming at first, taking such steps as setting up and maintaining secure passwords as well as being mindful of phishing scams can help you to establish a line of defense in protecting against online identity theft.