

# Fast Facts on Identity Theft

Identity theft, like virtually all forms of cybercrime, has seen a resurgence during the COVID-19 crisis. And while everybody knows about the harm ID theft can cause, many computer users fail to address the basics. Here are some things to be aware of:



## Identity theft is the fastest growing crime in America

On average, each victim spends 100 to 200 hours over a six-month period trying to resolve an identity fraud issue. While the common conception is that identity thieves are online scammers, evidence indicates that up to 50% of all reported cases involve theft committed by a neighbor, co-worker, or family member. Most cases can be resolved with minimal long-term impacts if they are caught early.

## What's considered personal information

- ✘ Social Security number
- ✘ Driver's license number
- ✘ Credit card numbers
- ✘ Bank account numbers
- ✘ Birth certificate
- ✘ Tax information
- ✘ Employee Identification number

## Common types of ID theft

- ✘ Financial
- ✘ Insurance
- ✘ Medical
- ✘ Criminal
- ✘ Social Security
- ✘ Synthetic (in which thieves "create" a consumer using details stolen from others)
- ✘ Child

## Prevention tips

- ✘ Create a unique password for each of your accounts and devices to limit the risk of having multiple accounts compromised at once.
- ✘ Change your login passwords on a regular basis, and don't store them in your email or cloud storage services, which a hacker can potentially access. However, many experts do recommend using a digital password manager.
- ✘ Avoid sharing sensitive information such as credit card or Social Security numbers through texts, emails, or chats.
- ✘ Never use public networks to conduct online financial transactions. Remember to log out of personal accounts opened on public devices.
- ✘ To keep your personal devices up to date, install the latest versions of the operating system and antivirus software.