Consumer Education 101 Document

2021

Communications Fraud Control Association

Version 1.0

Collaboration by CFCA and SpyCloud

CFCA
Communications Fraud Control Association

What Is Identity Theft?

Identity theft means that your personal and confidential information has been stolen and is being used without your permission to apply for lines of credit, make purchases, and commit other types of fraud.

There were 4.8 million identity theft and fraud reports received by the Federal Trade Commission in 2020, up 45 percent from 2019. Identity theft accounts for 33% of fraud attacks experienced by Europeans.

Are You a Target?

Yes. While it's true that cybercriminals often go after "high-value" targets (think: CEOs and public figures), everyone's personal data is worth something to fraudsters. On average, Americans have $22,751 in available credit across all credit cards, which can be drained by criminals in minutes.

If you are not proactive about protecting your information, you are far more likely to become a victim. Too many of us willingly make our personal information available online and on social media while doing the bare minimum to keep it secure. To a cybercriminal, our lack of cyber-awareness is like leaving your wallet on your dashboard or your house keys in your front door lock – it's easy to steal from you.

How Does It Happen?

Identity thieves look for important pieces of information, such as your Social Security number, address, account numbers, medical information, etc. If cybercriminals can obtain one of your user account passwords, which happens frequently, countless doors for fraud can be opened.

Once criminals obtain this information, they can impersonate you as a consumer by virtually taking over your account and causing serious damage. Among other things, they can reroute your paycheck to an untraceable account, purchase gift cards, open new lines of credit in your name, file a tax return and divert the refund, steal your unemployment benefits, and much more.

How Do They Get Your Information?

Cybercriminals use so many tactics that even security professionals can't keep up. But among the most common to watch out for are:

Data Breaches

A data breach is when someone gets unauthorized access to a company's data. Breaches affect businesses of all industries and sizes, from social media platforms to streaming services to hospitals, for example, customer names, email addresses, passwords, Social Insurance or similar numbers, credit card data, and phone numbers are among the most common information stolen.

Social Engineering
Social engineering attacks rely on human interaction aimed at manipulating people into giving up information.

Phishing is common: you might get an email that looks like it is from your bank, and within it is a link that takes you to a website that looks almost exactly like your bank's website but is in fact fraudulent. If you enter any information on that website, such as your username or password, it could end up in the hands of bad actors.

Similarly, mobile device users should be aware of "voice phishing" (aka **"vishing"**), where scammers call and pretend to be from your credit card company or a government agency, and "SMS phishing" (aka **"smishing"**), where the goal is to get you to click a link in a text message. Both types of scams are designed to collect personal information that can be used for fraudulent purposes.

Malware
Malware is malicious software designed to corrupt your computer or mobile device (such as your smartphone) once it is installed. Cybercriminals can use it to steal your data, tracking your every move online. There are a variety of ways malware can be installed, but primarily it happens through email, when you click on a suspicious link and unknowingly download a malicious attachment. This is called a **Payload.**

Unsecure Wi-Fi
Whenever you use public Wi-Fi at airports or coffee shops, be careful what sort of personal business you conduct – bad actors also use those networks. By entering any information into a website while on a public WiFi network, a bad actor may be able to intercept it.

Dark Web Marketplaces
Stolen information often ends up for sale on the dark web. The dark web is a haven for cybercriminals as it is a concealed network of websites that the average person can't access without special software to mask their identity and activities. Your stolen information may be listed on a dark web marketplace, packaged up with other people's data and sold for a very low price.

Tips for Reducing Your Risk of Identity Theft

This will sound scary, but it's the truth: someone, somewhere, is trying to steal from you online. The best way to protect yourself is to be vigilant, continuously monitor your financial accounts, and ensure you have access to services to minimize the impact when something happens.

Things to Do	Things Not to Do
Use Unique Passwords Too many of us are guilty of using the same or similar passwords for multiple accounts. If a criminal obtains the password you use for your TV streaming service, they can assume you use the same or similar password for other accounts, such as email or online banking.	**Don't Talk to Strangers** Never respond to unsolicited phone calls or emails requesting personal information – even if the emails appear to be from a legitimate source such as a bank or financial institution. It could be a phishing scam.

	You can always call your bank's trusted phone number to verify the ask.
Protect Your Cell Phone and your computer Prevent criminals from having access to your cell phone or phone number. This could be a critical step in bypassing multi-factor authentication. (Intercepting the codes some websites and financial institutions send you before letting you login) and committing fraud.	**Don't Take the Bait** Avoid participating in questionnaires on social media designed to get you to share personal information. These are the "killer clowns" of identity theft – they look like fun, but they have malicious intent. When asked for "your first car," "your favorite color," "your first pet," or "your favorite movie," be aware that fraudsters can harvest these answers to bypass security questions and log into your sensitive accounts. This is sometimes called pharming.
Check Your Statements Monitor your credit card and banking accounts regularly. Check carefully for any unauthorized charges or withdrawals and contact your financial institution to report them immediately.	**Don't Go Unprotected** While using personal devices to access work accounts, make sure to use a secure connection whenever possible. Your personal device is more susceptible to hacking than your work device.
Additional Tips Clear your cache and cookies frequently. User virus protection. Utilize security tools offered by your online accounts. Use secure networks; Avoid public Wi-Fi. Secure your computer when you're not there. Think about using a password manager. Regularly update your computer and apps.	**Also Remember** Don't write your password down anywhere. Don't plug in unfamiliar devices (USBs). Don't reuse password across accounts.

Can Identity Theft Be Prevented?

Yes, with some basic knowledge, planning, and awareness (like the tips above). The best protection against identity theft is to remain diligent and cautious, to monitor how much you share online, and think before clicking links or answering calls from unknown sources. This might sound overwhelming, but this guidance is as practical as remembering to lock your doors and windows when you're away. In addition, some mobile operator offers consumer protection services, Customers can leverage one of the many mobile device security solutions that are available in iOS or Android from their respective app store.

About Communications Fraud

Communications fraud is the use of telecommunications products or services with no intention of payment. Fraud negatively impacts everyone, including residential and commercial customers. The losses increase the communications carriers' operating costs. Although communications operators have increased measures to minimize fraud and reduce their losses, criminals continue to abuse communications networks and services. Therefore, communications operators tend to keep their actual loss figures and their plans for corrective measures confidential. Due to the sensitive nature of this topic, CFCA used a confidential opinion survey of global communications operators to support the global fraud loss study.

About CFCA

CFCA is a not-for-profit global educational association that is working to combat communications fraud. The mission of the CFCA is to be the premier international association for revenue assurance, loss prevention and fraud control through education and information. By promoting a close association among telecommunications fraud security personnel, CFCA serves as a forum and clearinghouse of information pertaining to the fraudulent use of communications services. For more information, visit CFCA at www.CFCA.org.

Correspondence should be sent to fraud@cfca.org

About SpyCloud

SpyCloud is the leader in account takeover (ATO) prevention, protecting more than 2 billion consumer and employee accounts worldwide. Our award-winning solutions proactively defeat fraud attempts and disrupt the criminals' ability to profit from stolen information.

We're the trusted ATO prevention partner for B2B organizations and consumer brands — including 4 of the Fortune 10. Our solutions are backed by the most comprehensive and actionable repository of recovered stolen credentials and PII, with over 135B assets and counting. SpyCloud is active in GSMA, ETSI, & the CFCA. For more information or to Check Your Exposure visit spycloud.com.

Disclaimer of Liability

The material and information contained in this document is for general information purposes only. You should not rely upon the material or information in this document as a basis for making any business, legal or any other decisions.

Whilst we endeavor to provide correct information, CFCA makes no representations or warranties of any kind, express or implied about the completeness, accuracy, reliability, suitability or availability with respect to the information and graphics contained in this document for any purpose. Any reliance you place on such material is therefore strictly at your own risk.

CFCA will not be liable for any false, inaccurate, inappropriate or incomplete information presented in this document.

To the extent not prohibited by law, in no circumstances shall CFCA be liable to you or any other third parties for any loss or damage (including, without limitation, damage for loss of business or loss of profits) arising directly or indirectly from your use of information contained in this document.