UNION BANK

June 2024

How common is identity theft in 2024? 24 identity theft statistics

Identity Theft Statistics

There were at least 27,922 victims of ID theft in 2022.

Source: FBI

12% of people over 16 learned that an entity with their personal information experienced a data breach.

Source: Bureau of Justice Statistics

People aged 30 – 39 are most likely to have their identities stolen.

Source: Consumer Sentinel Network

US victims of identity theft lost at least $189,205,793 in 2022.

Source: FBI

Understanding identity theft statistics can help you avoid becoming one. Read on to learn how common identity theft is and about the consequences.

Identity theft facts

The statistics on identity theft cases and other online fraud can be staggering. If you haven't done everything to prevent your identity from falling into the hands of cybercriminals—and you aren't regularly monitoring your credit reports—you might not even know if someone is using your identity.

Look at the statistics below to see how widespread this type of fraud is:

1. The FBI reported 27,922 victims of identity theft in 2022.[1]
2. The Federal Trade Commission (FTC) received 231,724 reports of identity theft in Q4 2023 alone.[2]
3. Data breaches involving personally identifiable information had one of the highest victim counts compared to other crimes in 2022, according to the Internet Crime Complaint Center.[1]
4. AI-driven identity theft scams will likely increase in 2024.
5. The Bureau of Justice Statistics found that 12% of people over 16 learned that an entity with their personal information experienced a data breach in 2021.[3]

Most common types of identity theft

Identity theft isn't as simple as someone taking your credit card or driver's license. What might start as a social engineering scam could end up with a stranger (or even a family member) using pieces of your identity to commit synthetic identity theft, Medicare scams, or other identity crimes.

Here are some statistics about common identity theft types:

Continued on Page 2

EQUAL HOUSING LENDER

Member FDIC

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

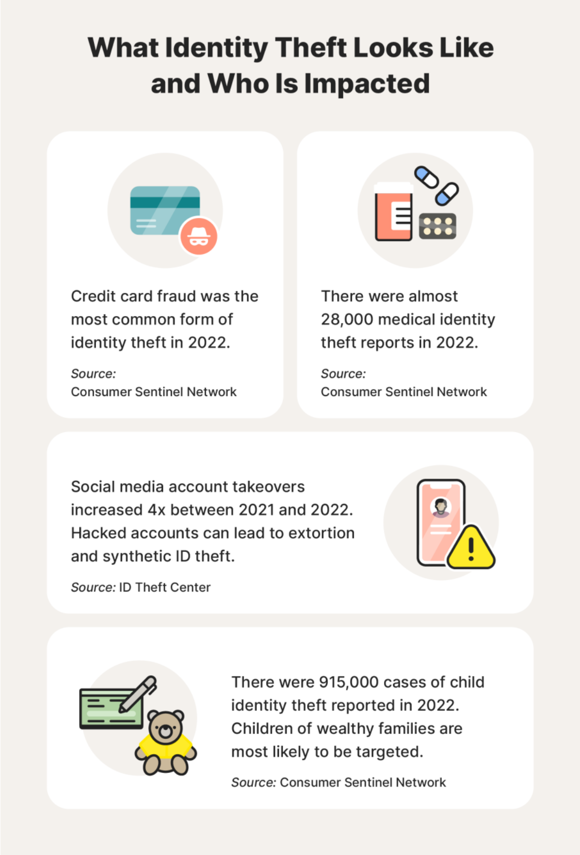
Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
By Appointment Only

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967


What Identity Theft Looks Like and Who Is Impacted
Credit card fraud was the most common form of identity theft in 2022.
Source: Consumer Sentinel Network
There were almost 28,000 medical identity theft reports in 2022.
Source: Consumer Sentinel Network
Social media account takeovers increased 4x between 2021 and 2022. Hacked accounts can lead to extortion and synthetic ID theft.
Source: ID Theft Center
There were 915,000 cases of child identity theft reported in 2022. Children of wealthy families are most likely to be targeted.
Source: Consumer Sentinel Network

1. Credit card fraud was the most common type of identity theft reported in 2022, with 441,882 cases reported to the FTC.[4]
2. Phishing, a tactic commonly used to steal personally identifiable information, was the most common type of cybercrime in 2022.[1]
3. The FTC received 37,924 reports of military ID theft in 2022.[4]
4. In 2022, the Identity Theft Resource Center received four times the number of inquiries related to social media account takeovers than in 2021. Cybercriminals can use hijacked accounts to extort money from the account owner, friends, and family members.[5]
5. There were 27,820 reports of identity theft relating to medical services in 2022, according to data from the Consumer Sentinel Network.[4]
6. In 2023, the FTC received 89,465 reports related to tax-related or employment identity fraud in 2023.[6]

Does identity theft ever go away?

You can limit the damage done after identity theft by taking appropriate actions: First, freeze or lock your credit and dispute any charges or accounts you didn't open. Then, monitor your credit report and bank and credit card accounts for fraud. If you don't dispute accounts or charges, it can take years for those accounts to disappear from your credit report after they're closed.

How do I clear my name after identity theft?

The best way to clear your name after identity theft is to take steps to prevent it from happening again. Lock your credit unless you're actively applying for new accounts, place a fraud alert on your reports with the credit bureaus, protect your Social Security number, and dispute all charges and accounts the thief created. You may need to file a police report to prove you didn't open those accounts and have false criminal records expunged.

What are some warning signs you have had your identity stolen?

There are several warning signs that somebody stole your identity, including:

- Calls from creditors regarding accounts you didn't open
- Bills in the mail
- Charges on credit cards you didn't make
- Your name appearing in criminal records searches
- Being denied credit you should qualify for
- Not receiving government benefits you're entitled to

1. "2022 Internet Crime Report," Federal Bureau of Investigation Internet Crime Complaint Center, Mar. 14, 2023.
2. "Sentinel Report Categories," Federal Trade Commission Sentinel Network, Nov. 1, 2023.
3. "Data Breach Notifications and Identity Theft, 2021," Bureau of Justice Statistics, Jan. 2024.
4. "Consumer Sentinel Network Data Book 2022," Federal Trade Commission, Feb. 1, 2023.
5. "The Weekly Breach Breakdown: Hacked and Furious – The Rise in Social Media Account Takeovers," Identity Theft Resource Center, Mar. 17, 2023.
6. "Sentinel Compare Identity Theft Report Types," Federal Trade Commission Sentinel Network, Nov. 1, 2023.

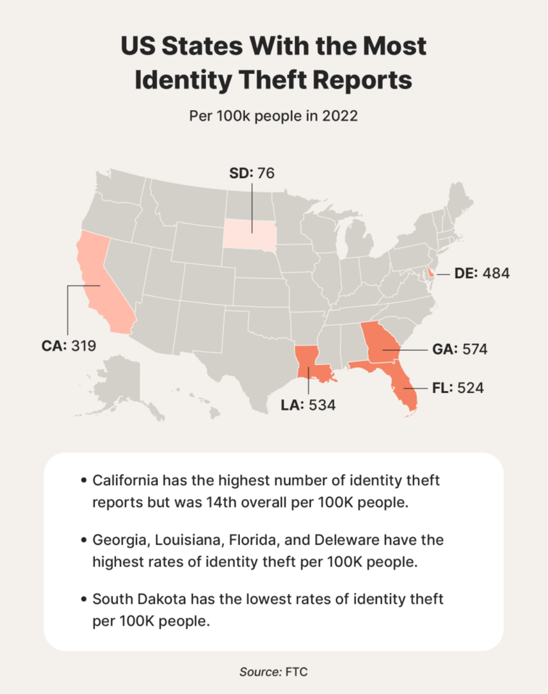
Sources/Credit:

Article:

Clare Stouffer, Staff Writer, LifeLock by Norton, April 08, 2024

Images:

How common is identity theft in 2024? 24 identity theft statistics, LifeLock by Norton, April 08, 2024


US States With the Most Identity Theft Reports
Per 100k people in 2022
SD: 76
DE: 484
CA: 319
GA: 574
FL: 524
LA: 534
• California has the highest number of identity theft reports but was 14th overall per 100K people.
• Georgia, Louisiana, Florida, and Deleware have the highest rates of identity theft per 100K people.
• South Dakota has the lowest rates of identity theft per 100K people.
Source: FTC

What is a Keylogger?

Keyloggers: What They Are and How They Work

Securing your internet is of paramount importance in today's digital world. In an age where personal information and financial data are often stored online, the need to understand different cybersecurity threats and how to protect against them cannot be overstated. One particular threat is a keylogger, a malicious program designed to track and record every keystroke on a computer or mobile device, thereby gaining unauthorized access to personal data. This guide aims to provide you with an in-depth understanding of what a keylogger is, how they work, and the various ways you can protect yourself from this insidious threat.

Overview of Keyloggers

A keylogger, short for keystroke logger, is a type of cyber threat that records the keys struck on a keyboard, typically covertly, so the person using the keyboard is unaware that their actions are being monitored. This enables attackers to gain unauthorized access to confidential information, such as passwords, credit card numbers, and other sensitive data, which can then be used for identity theft, financial fraud, and other forms of cybercrime.

Keyloggers can be hardware-based or software-based. Hardware keyloggers are devices that are physically connected to the computer's keyboard or installed inside it. While these are effective, their physical presence makes them easier to detect. On the other hand, software keyloggers are more commonly used as they can be easily installed remotely as part of a Trojan or virus, making them harder to locate and remove.

How Keyloggers Work

Just as their name suggests, keyloggers work by secretly recording every keystroke that is made on a computer or a mobile device. Once installed, they operate in the background, collecting data without the user's knowledge. They can capture virtually every type of information entered through a keyboard; this includes but is not limited to email correspondence, instant messages, documents, and web forms.

Software keyloggers, the more prevalent type, work by functioning at the kernel level of an Operating System (OS). This means they intercept signals sent from the keyboard to the OS, capturing all information typed on the keyboard. The recorded data is then sent back to the cybercriminal, who can extract personal and financial details for their nefarious purposes.

Hardware Keyloggers

Hardware keyloggers, while less common, are equally as damaging. They function by being manually connected to the computer, either between the keyboard's plug and the PC's keyboard port, or installed inside the keyboard itself. Once installed, they begin capturing keystrokes directly, storing them in their internal memory. This data can then be accessed by the cybercriminal either by physically retrieving the device or via wireless methods if the device has such capabilities.

Because hardware keyloggers require physical access to the computer, they are often used in targeted attacks where the criminal has some access to the victim's premises, for example, in office spaces. Although their physical nature makes them easier to detect, they are often disguised to appear as regular parts of the computer, making detection without a thorough inspection difficult.

Keylogger Detection and Removal

Detection and removal of keyloggers can be a challenging task due to their covert nature, but it's not impossible. Regular system scans with a reliable antivirus or anti-malware software can often detect keylogging software. For hardware keyloggers, a physical inspection of your computer system is required, which includes checking the back of the computer and keyboard for any unfamiliar devices. Keeping your operating system and security software up-to-date also enhances your defenses against these threats as patches for known vulnerabilities are often included in updates.

Furthermore, using firewall protection can also deter keyloggers as they can block unauthorized access to your computer. So, it's important to keep your firewall enabled and properly configured. For online protection, consider using a secure browser and a virtual private network (VPN), especially when connecting to public Wi-Fi. This helps to encrypt your online activities, making it harder for keyloggers to capture your data.

Preventing Keyloggers

Prevention is always better than cure, especially when dealing with cybersecurity threats like keyloggers. One of the most effective ways to prevent keyloggers is through practicing safe online habits. This includes not opening suspicious emails or links, downloading software from trusted sources only, and refraining from clicking on pop-up ads. It is also beneficial to change passwords regularly and use complex combinations of letters, numbers, and symbols to make them harder to guess or decode.

Another proactive measure is using two-factor authentication (2FA) whenever available. 2FA adds an extra layer of security by requiring the user to provide two forms of identification before accessing an account. This means, even if a keylogger captures your password, the attacker would still need the second form of verification to access your account.

As we rely more heavily on digital platforms for various aspects of our lives, understanding cybersecurity threats like keyloggers becomes increasingly crucial. Keyloggers, whether hardware or software, pose a significant risk, collecting personal and sensitive data without the user's knowledge or consent. Detecting them can be challenging, but with the right security tools like McAfee and safe online practices, you can protect your data and maintain your digital privacy.

Remember, always keep your OS and security software updated, practice safe browsing habits, and use the layers of security measures available to you. Cyber threats like keyloggers are persistent, but with vigilance and proactive protection, your personal data can remain safe.

Sources/Credit:
Article:
McAfee
Images:
Thomas Breher from Pixabay, Attribution: Pixabay, Pixabay Content License Summary