First Bank & Trust Company

The Bank That Puts You First

Member FDIC

Member FDIC

EQUAL HOUSING LENDER

June 2023

Identity Theft Statistics to Keep in Mind

It seems like only yesterday the word "theft" brought to mind visions of home breaches or street muggings. While these weren't exactly harmless, they were at least evils we could see. With ID theft the new big thing, similar risks are largely out of sight.

Here's the deal:
As a quick look at the latest identity theft stats reveals, breaches can now come from all angles, and controlling them isn't as easy as installing CCTV. As we share ever more data online, we're all increasingly at risk of third-parties.

Now:
While identity theft statistics may be enough to put the fear in you, they're crucial to consider. Understanding the numbers behind crimes like these is, after all, our best chance at staying safe!

ID theft occurs when someone steals another person's sensitive personal information. It's slightly different from ID fraud, which involves the actual use of someone else's sensitive information in a fraudulent or deceptive way.

To get a thorough look at identity theft patterns over the last year, we analyzed recent relevant data from the Federal Trade Commission and other government agencies that deal with theft and fraud. We've outlined these insights in a more digestible format below.

Key insights

- Recorded instances of identity theft have soared by 584% over the last 20 years. In the last decade, Louisiana, Delaware and Pennsylvania saw the largest increase in identity theft reports per 100,000 people.
- Thirty-somethings reported identity theft more frequently than any other age group in 2022, accounting for almost 26% of all reported cases in 2022.
- Georgia had the highest number of reported identity theft cases per capita in 2022.

There were 441,822 cases of credit card fraud reported over the past year, making it the most common type of ID theft in 2022.

ID Theft By State
According to The Federal Trade Commission's "2022 Consumer Sentinel Network Data Book," Georgia saw the highest number of ID theft reports per capita in 2022. There were 574 reported cases per 100,000 residents in Georgia last year; Louisiana, second on the list, had 534 per 100,000 residents, and Florida, third, had 524 per 100,000 people.

1. Georgia
2. Louisiana
3. Florida
4. Delaware
5. Nevada
6. Texas

Continued on page 2

Virginia Bank Locations
Abingdon, Virginia, East
276-628-3838
Abingdon, Virginia, West
276-628-9558
Blacksburg, Virginia -
540-951-1656
Bridgewater, Virginia
540-266-0003
Bristol, Virginia, East
276-466-9222
Bristol, Virginia, West
276-669-1122
Christiansburg, Virginia
540-260-9060
Fairlawn, Virginia
540-633-3793
Hanover, Virginia
804-550-5700
Harrisonburg, Virginia
540-434-0671
Lebanon, Virginia East
276-889-3401
Lebanon, Virginia West
276-889-4622
Lynchburg Virginia
434-455-0888
Norton, Virginia
276-679-7401
Staunton, Virginia
540-885-8000
Verona, Virginia
540-248-7700
Waynesboro, Virginia
540-943-5020
Wise, Virginia
276-328-3439
Woodstock, Virginia
540-459-7228
Wytheville, Virginia
276-228-1125
Operations Center
276-623-2265

Tennessee Bank Locations
Bristol, Tennessee
Volunteer Pkwy
423-652-2022
Gray, Tennessee
423-467-9966
Johnson City Tennessee
423-975-9900
Kingsport, Tennessee
423-246-3700

First Bank & Trust Loan Production Offices
Bedford, Virginia
540-583-5458
Daleville, Virginia
540-966-7006
Hanover, Virginia
804-550-5700
Lynchburg, Virginia
434-509-0444
Mount Airy, North Carolina
743-212-2013
Red Oak, North Carolina
252-220-4208
Roanoke, Virginia
540-774-0269
Rocky Mount, Virginia
540-484-0338
Winchester, Virginia
540-545-8110
Wytheville Annex

First Bank & Trust Mortgage Lending Division
Bristol, Virginia
276 -644-9900

7. Pennsylvania
8. Alabama
9. South Carolina
10. Mississippi

Who's Most Vulnerable to ID Theft?

Of the 1,108,609 total identity theft reports in 2022, 30- to 39-year-olds made up 25.9% of victims in the U.S. This group reported more cases of every type of ID theft (with credit card theft topping the charts, followed by "other" ID theft and loan or lease fraud) than any other group.

It's worth noting, however, that 30- to 39-year-olds made up the largest percentage of Americans in 2021, with 30-somethings accounting for almost 13.7% of the U.S. population that year. Still, on a per-capita basis, 30- to 39-year-olds reported ID theft at a higher rate than any other age group (0.6%). Those in their 40s reported ID theft at the second-highest rate (0.5%).

One distinction to remember is the difference between ID theft and ID fraud. ID theft is stealing someone's sensitive information, and ID fraud is the act of using that information to steal money or commit other crimes. In 2022, 30- to 39-year-olds reported higher instances of both ID theft and fraud than any other age group. In terms of money stolen due to ID fraud, however, 40- to 49-year-olds experienced the biggest total dollar loss ($840 million).

Most Common Types of ID Theft in 2022

Credit card fraud was the most common type of ID theft in 2022, with 441,822 reported cases in 2022.This type of fraud, which accounted for about 40% of more than 1.1 million ID theft reports in 2022, involves thieves using your personal information to either steal from an existing credit card account or to open a new one in your name.

"Other" identity theft made up about 29% of all reports in 2022. This category includes fraud related to online shopping, payment accounts, emails and social media, medical services, insurance and more.

People in their 30s reported the most of each type of fraud. Americans 80 and over reported the fewest cases in almost all categories, though those 19 and younger reported the fewest instances of bank and credit card fraud.

There were also 14,501 credit card fraud reports from military consumers in 2022. Credit card fraud was the most common type of identity theft reported by military consumers, followed by bank fraud.

How do identity thieves get our information?

Phishing and ransomware were among the most common categories of cyberattacks leading to data breaches in 2022, the Identity Theft Resource Center's annual report states. Cybercriminals in 2022 seemed to focus their energy on resetting passwords, modifying authentication processes and attacking identities rather than deactivating antivirus and firewall technologies and log-tampering efforts, according to CrowdStrike's 2023 Global Threat Report.

How to prevent ID theft

Most people operating in today's financial world are vulnerable to identity theft in some way, unfortunately. Once someone has hold of your Social Security number, for instance, they might have enough information to access your bank accounts.

Over the last year, among fraud reports with a contact method identified, text messaging was most common, accounting for 22% of total reports, the FTC report says. Fraud through phone calls (20%) and email (19%) was also common.

Whether you're texting, calling, emailing or just browsing the internet, make sure to be vigilant in protecting your privacy — and your identity. The FTC recommends employing two-factor authentication and unique passwords, especially for email and online bank accounts.

You can freeze your credit with Experian, Equifax and TransUnion so no one can use your credit to their advantage. There are also services that let you monitor your credit and alert you to any suspicious activity.

It's also important to keep track of your wallet and cards and to keep any PIN information to yourself. When you're online, use secure websites (these start with "https") and keep your private information off public servers and computers.

Are solutions coming?

In March 2023, the White House proposed spending $600 million on fraud and identity theft prevention measures and $400 million to help victims of identity theft. It also announced an executive order that will aid federal agencies in preventing identity theft, calling for $300 million toward improving identity verification systems.

The American Rescue Plan Act, which President Joe Biden signed into law in 2021, includes $1.6 billion in funds to help prevent fraud and identity fraud that will be available to states by June 2023.

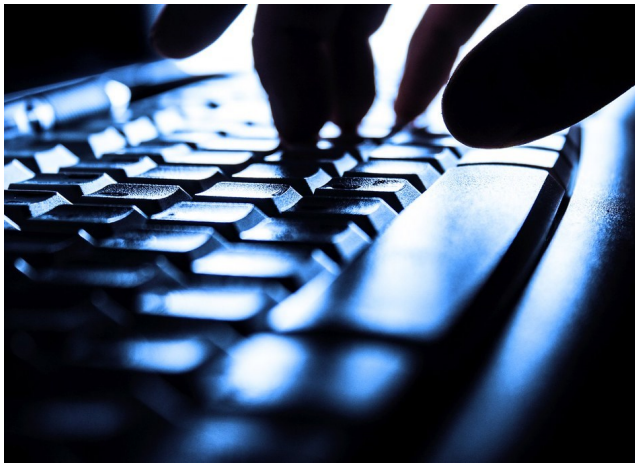
Sources:

Article: Jenifer Kuadli, March 30, 2023, LegalJobs

ConsumerAffairs

Images: The Blue Diamond Gallery, Title: Identity Theft, License: Creative Commons 3, Required Attribution: Alpha Stock Images, Original Author: Nick Youngson, No changes have been made to the original image

What Is a Keylogger? Definition, Prevention, and Removal



A keystroke logger, also known as a keylogger, is a software program or hardware device that logs and records every keystroke input on a computer. Bad actors can use it to steal sensitive data like passwords, financial information, and other confidential information. Keyloggers can also be used legitimately by parents to monitor their kids' online activities, and employers can use them to track employees' computer usage.

Keyloggers can be broken down into two distinct definitions:

Keystroke logging: The process of recording and storing every key that's pressed on a keyboard.

Keylogger tools: Devices or programs designed to log a user's keystrokes.

In addition to recording keystrokes, keylogger software can also collect user data through other methods, such as capturing screenshots, recording web searches and visits, and monitoring clipboard activity.

2 types of keyloggers

Keyloggers are either hardware-based or software-based.

Hardware-based keyloggers

Hardware keyloggers are physical devices used to monitor and record a user's activity on a computer. These devices are plugged into the back of a computer keyboard and have their own internal memory. The data is recorded directly to the device's memory and can be retrieved later by the attacker.

Hardware keyloggers are more difficult to detect than software keyloggers, as they are hardly visible on the computer's system. To prevent hardware keyloggers from being installed, physically inspect your computer's ports and cables periodically for any suspicious devices that may have been installed without your knowledge.

Software-based keyloggers

A software keylogger is a type of monitoring and tracking software that logs keystrokes from a computer keyboard. These keystrokes are recorded and stored in an encrypted log file that the attacker can access remotely.

Software keyloggers can be disseminated when you click on malicious links, download malware, visit a website with dangerous code, or open files that have been infected with malware. Although more easily detectable than hardware keyloggers, software-based keyloggers can be installed remotely, without needing physical access to your system.

How do keyloggers work?

Hardware-based and software-based keyloggers work differently. Generally, both types of keyloggers track and record every keystroke made on a computer based on a predefined command. These commands include:

- Length of the key press
- Number of keystrokes
- Key sequence
- Time of keypress
- Clipboard content

In the case of hardware keyloggers, a physical device is plugged into a computer's keyboard connection and records every keystroke that is entered into the keyboard. These keyloggers require physical access to a computer in order to be installed and are usually undetectable because computer users rarely pay attention to devices plugged into the backside of the computer.

On the other hand, software keyloggers are programs installed on the user's computer and run invisibly in the background. They include two files that are installed in the same directory: a dynamic link library (DLL) and an executable file. The DLL file will monitor the system and record keystrokes into a file, while the executable file is responsible for launching the keylogger when the computer is turned on.

4 best practices to prevent keylogging

1. Avoid clicking on suspicious links
2. Update software and OS regularly
3. Enable firewalls and antivirus protection
4. Use strong passwords

How to detect and remove keyloggers in 6 steps

If you find or suspect that a keylogger has compromised your system, here are the steps you can follow to detect and remove it.

1. **Use an anti-malware program:** An anti-malware program can scan your computer for malware, including keyloggers. Install a reputable anti-malware program and run a full scan of your system.
2. **Check task manager**: Open your task manager and look for any unfamiliar or suspicious processes running on your system. Keyloggers often run in the background and can be difficult to detect, but you might notice a process with a strange name or high CPU usage. Research them online to determine whether they're legitimate or malicious.
3. **Check your startup programs**: Keyloggers may start automatically with your computer. Check your startup programs and look for any suspicious entries. You can use the Windows system configuration tool or a third-party program to manage your startup programs.
4. **Change your passwords**: If you suspect that your computer has been compromised by a keylogger, change your passwords for all your accounts immediately. Use a strong, unique password for each account.
5. **Inspect your system for hidden devices**: Check your computer for any unusual hardware that can be used to capture keystrokes. This may include USB drives, external hard drives, or other connected hardware.
6. **Reinstall your operating system**: If all else fails, the best way to remove a keylogger is to reinstall your operating system. This will erase all programs and data on your computer, including any software keyloggers that might be present.

Sources: ***Article:*** *Aminu Abdullahi, March 14, 2023, Enterprise Networking Planet*

Image: Creator: *Christoph Scholz, Creative Commons License*