First Bank & Trust Company
The Bank That Puts You First
Member FDIC



June 2022

# 20 Worrying Identity Theft Statistics for 2022

***Not so long ago, when we thought about theft, we imagined a house being robbed or someone getting mugged in the street. These crimes are far from harmless, but the devil was at least visible. The problem with identity theft is that you don't know you're in danger until the crime has already been committed.***

***As tech advances to keep people safe, criminals evolve in parallel, becoming more adept at stealing data. While far from pleasant, this is something you need to be aware of: Here are the latest identity theft stats to keep you vigilant.***

**1. Identity theft cost people in the US $56 billion in 2020.**
Well over 49 million people were victims of identity theft in 2020. This resulted in $13 billion in damages from "traditional" identity theft, i.e., people losing their info through data breaches and similar attacks. On the other hand, one of the strangest statistics is that the majority of the losses ($43 billion) stemmed from direct-interaction scams, such as phishing emails. In other words, bad actors are getting bolder and are willing to target people directly.

**2. 2.2 Million fraud reports were filed with the FTC in 2020.**
Consumers have also stated that they lost $3.3 billion in fraud in the same year. That's nearly double the money lost the same way in 2019 - $1.8 million. When you look at the statistics released by the FTC, you will soon see that imposter scams were the most common type of fraud; as mentioned, this is one of the most shocking ID theft stats.

**3. Someone becomes the victim of identity fraud every 14 seconds.**
Studies have also shown that every 14 seconds, someone becomes a victim of identity theft in the US. In light of the sharp rise in attacks we've seen in recent years, more and more people are calling for online data to be better protected.

**4. Identity theft affected around 0.6% of the US population in 2020.**
Identity theft also disproportionately affects the older population. One explanation for this is that the elderly aren't always tech-savvy and often cannot tell the difference between a legitimate site or email and those that are fake.

**5. 33% of Americans have been the victim of identity theft.**
ID theft statistics show that 33% of Americans have been the victim of identity theft at some point in their lives. This is three times higher than the numbers from Germany or even France. It is also double the world average. US respondents leave their social media more open than worldwide users, making them vulnerable by exposing their information to cyber thieves.

**6. Credit card fraud is the most common kind of identity theft.**

*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

The FTC has found that credit card theft was the most common type of identity fraud in 2020 and 2021. The FTC has received nearly 18,000 reports from various individuals who have stated that their information has been used to gain access to their credit card accounts illegally.

**7. People active on social media are more likely to have their details stolen.**
People who are active on social media are 30% more likely to have their details stolen when compared to other people. These are the main channels where attackers seek out targets. Identity theft statistics also show that Facebook, Snapchat, and Instagram are exposed to an even higher level of risk, which propels the statistic to 46%.

**8. Most stolen identities were used to apply for government documents and benefits in 2020.**
The second most common target of stolen ID use is credit card fraud. Following that, you have bank fraud and utility fraud. The millions of people who have been affected by these crimes often experience considerable financial, psychological, and reputational damage.

**9. 15 million US citizens experience identity theft every year.**
15 million people in the US experience identity theft every single year. This results in $50 billion in financial losses. This equates to 4.5% of all US residents, with an average loss of $3,500.

**10. 2.5 million identities are stolen every year.**
Identity theft statistics also show that the dead can become victims of cybercrime. There have been over 800,000 incidents where criminals have exploited the identities of the deceased to open credit cards or even get a cell phone plan. Studies have also shown that twice as many thieves used a fake Social Security number belonging to those who have passed away.

**11. One out of five people in the EU have experienced identity theft**
When you look at the latest cybercrime statistics for Europe, you will soon find that more than half of Europeans (56%) have been the victim of cyber-crime at least once in the last two years. Identity theft is the second-most common type of cyber-attack, with one-third of the 56% mentioned above being victims. The UK is the most vulnerable, with 53% of respondents from this country having reported some kind of ID theft. Ireland has a rate of 50%, and France comes in third, at 45%.

**12. Californians are the main target for identity theft.**
The FTC has found that Californians are the primary target for identity theft, with recent statistics showing that 147,382 complaints were filed from this state alone. This makes the state one of the top targets for cybercrime. If you look at the statistics for the top five worst US states by identity theft, you will see that Illinois comes in second with 135,038 cases, Texas has 134,788 cases, Florida is at 101,367 cases, and Georgia comes last at 69,487 cases.

**13. Millennials account for around 35% of fraud cases in the US.**
The FTC received 2.2 million reports of fraud in 2020. People between the ages of 20 and 40 account for 35% of those reports. On the other hand, people over 70 only accounted for 8% of reports. However, the average financial losses experienced by the older population were much higher compared to the younger generations, despite the totals being bigger for Millenials.

**14. The 60 to 69 age group lost the most in fraud-induced expenses.**
Baby Boomers lost the most to identity theft in 2020 and 2021. However, identity theft statistics for 2021 also show that they are in fourth place in terms of report numbers. This means scams are particularly costly per person for this age group.

**15. Over 1.3 million children have fallen victim to identity theft.**
Over 1.3 million young children become the victims of identity theft every year. Studies have also shown that 50% of those youngsters are the age of six or younger, and that the average age is decreasing.

**16. Families are expected to pay $540 million out of pocket to account for fraud damage from scammed children.**
Data from 2017 shows that $2.6 billion in damages may be attributed to cybercrime involving children. Only 7% of adults know the person responsible for identity theft. However, when you look at children, you will see that this percentage skyrockets to 60%. More often than not, crimes involving children are perpetrated by someone who knows them.

**17. 3% to 10% of the annual health budget in the US is lost to fraud.**
While that number is alarming in itself, it's worsened by the fact that medical identity theft accounts for 2 million cases of fraud to date. Considering the price of health insurance in the US, this is a life-threatening figure for many.

**18. 113,593 employment and tax-related fraud cases were reported in 2020.**
According to online fraud statistics, this type of fraud was the fifth most commonly reported in 2020. It had the most significant spike in the second quarter of 2020 - when the pandemic first hit - and has been on a slow decline since.

**19. Credit card account fraud accounted for 48% of all fraud complaints in the UK in 2019.**
The same percentage represents the annual increase from 2018 to 2019 in personal losses incurred by police and bank impersonation scams. The sheer number of cases increased by 112% in the same period.

**20. Gross losses from gift card fraud in 2021 exceed $148 million.**
Unfortunately, cybercrime statistics account for the dark side of gift-giving too. Gross losses from fraudulent gift card redeeming saw a sharp uptick in the first three quarters of 2021, already surpassing the numbers for all of 2020. This can be traced back to over 40,000 consumers who used gift cards to pay criminals.

***Source:** Fortunly, Julija A., February 17, 2022*

# Keyloggers Explained: How Attackers Record Computer Inputs

***While sometimes keyloggers can be used legally, generally they're used to snoop on you for illicit purposes.***

***What is a keylogger?***

A keylogger is a tool that can record and report on a computer user's activity as they interact with a computer. The name is a short version of keystroke logger, and one of the main ways keyloggers keep track of you is by recording what you type as you type it. But as you'll see, there are different kind of keyloggers, and some record a broader range of inputs.

Someone watching everything you do may sound creepy, and keyloggers are often installed by malicious hackers for nefarious purposes. But there are legitimate, or at least legal, uses for keyloggers as well, as parents can use them to keep track of kids online and employers can similarly monitor their workers.

***What does a keylogger do?***

The basic functionality of a keylogger is that it records what you type and, in one way or another, reports that information back to whoever installed it on your computer. Since much of your interactions with your computer—and with the people you communicate with via your computer—are mediated through your keyboard, the range of potential information the snooper can acquire by this method is truly vast, from passwords and banking information to private correspondence.

Some keyloggers go beyond just logging keystrokes and recording text and snoop in a number of other ways as well. It's possible for advanced keyloggers to:

- Log clipboard text, recording information that you cut and paste from other documents
- Track activity like opening folders, documents, and applications
- Take and record randomly timed screenshots
- Request the text value of certain on-screen controls, which can be useful for grabbing passwords

***How does a keylogger get on your system?***

A physical keylogger has to be physically plugged into a computer, and so requires direct access, which is a tricky business often executed via social engineering techniques or a compromised insider.

But the most common type of illicit keylogger is the software variety, and that can best be described as keylogger malware. In fact, keyloggers, because they can harvest such lucrative data, are one of the most common malware payloads delivered by worms, viruses, and Trojans.

Thus, the way a keylogger gets onto your system is the same way any other type of malware gets onto your system, and that means that if you exercise good cybersecurity hygiene, you should be able to keep keylogger software at bay. To do that, you should:

- [Watch] out for phishing emails, and don't open or download attachments if you're not absolutely certain where they came from
- Similarly, don't download or install applications unless they come from a trusted source. That includes browser navbars, which are a common malware vector.
- Keep your computer safe with updated antivirus software.

***How to detect a keylogger***

How can you know if there's a keylogger on your system? For a hardware keylogger, of course, you should check for the hardware. If there's a thumb drive or something that looks unfamiliar plugged into your computer, investigate it. If you work on a corporate desktop, check the back panel once in a while to see if something new and strange has popped up.

With software keyloggers, there are some signs that you might be able to pick up on yourself. Keyloggers can sometime degrade web performance, spawn unusual error messages, and interfere with loading web pages. These are all features of malware generally; sometimes you can just tell that something is "off" with your computer. Keylogger-specific signs could include lags in your mouse movement or keystrokes, where what you type doesn't appear on screen as quickly as it should. On a smartphone, you might notice that screenshots are degraded. (Yes, keyloggers can be installed on smartphones, just like any other kind of malware.)

***Source:*** ***CSO, Josh Fruhlinger, Contributing writer, May 17, 2022***