idwatchdog®
from Equifax

Identity Theft Affects Every Generation

No single age group is immune to identity theft.

Approximately 49 million Americans were victims of identity fraud in 2020, costing a total of $56 billion.[1] Although the exact age ranges of each generation can vary, each group tends to have habits that savvy cybercriminals know how to exploit.

Infants and Children — Identity Theft Can Go Undetected for Years

Imagine a young adult applying for a college loan and discovering that their credit score is already damaged as a result of thousands of dollars in fraudulent debt from an identity that was stolen when they were a child.

Child identity fraud affects one out of every 50 children and costs US families almost $1 billion annually to resolve.[2] Each victimized family loses more than $1,100 per incident on average.

Unfortunately, children are particularly at risk for identity theft because they have a clean credit history[3] and because the crime can go undetected for years[4]—often until a child turns 18 and applies for an apartment, student loan, or credit card.[3] Further, since child identity fraud can be difficult to detect, it is also more time consuming to resolve than identity fraud impacting adults.[2]

In some cases, child identity theft may lead to a child being the victim of blackmail, grooming, or bullying.[5] The perpetrator of child identity theft could even be a family member or close friend.[6] Seventy-three percent of child identity fraud victims personally know the perpetrator, according to a study by Javelin Strategy & Research.[2]

A child's personally identifiable information (PII) can be compromised through the theft of legal documents or a data breach.[6] Both adults and children are at risk from having their information misused online. The difference is that a child likely doesn't understand what information is safe to share publicly, and they may be unaware of proper privacy settings or the myriad of scams that are pervasive on the internet.[7]

Child identity fraud affects one out of every 50 children and costs US families almost

$1 billion

annually to resolve.[2]

Gen Z — The Least Cybersecure Generation May Be Gen Z

According to one survey, Gen Z may be the least cybersecure generation.[8] They are the most likely to readily admit to reusing passwords, with one in four repeatedly doing so. The younger generations are also those most likely to say that they don't update their passwords in an attempt to keep their data safe.

Though this generation is new to the workforce, Gen Zers are already being targeted for scams. According to the Better Business Bureau (BBB), the three riskiest scams for adults ages 18 to 24 were online purchases, fake check or money orders, and employment scams.[9] Experts say that younger people may be more susceptible to fake check scams because they are less knowledgeable about how checks work. Young consumers may be caught in a fake check scam because they believe a check is legitimate once it "clears" at the bank—not understanding that it may take weeks for the bank to realize a check is fake.

23%

of Millennials admitted to sharing their online credentials with someone outside of their family.

Millenials — A False Sense of Online Security Can Drive Increased Risk of Theft

While Millennials are often considered the most tech-savvy generation, that level of comfort with technology carries risk as well.

Millennials are generally believed to be more knowledgeable about technology, and in turn, people assume they have good cybersecurity habits.[10] However, experts say the opposite is true. Millennials are more likely to engage in risky password behaviors that could compromise their online security. For example, one study reported that 23 percent of Millennials admitted to sharing their online credentials with someone outside of their family.

Though older people are typically thought of as the stereotypical fraud victims, experts say that younger adults are more likely to lose money to fraudsters.[11] The Federal Trade Commission (FTC) states that 44 percent of people ages 20 to 29 (a group that includes both Gen Z and Millennials) reported losing money to fraud, which is more than double the 20 percent of people ages 70 to 79 who reported losses.[12]

Generation X — Gen Xers Are the Most Likely to Experience Identity Theft

According to reports, Generation X tops the list of the most at-risk generation for identity theft.[13] The FTC states that 44 percent of identity theft reports in 2020 were committed against victims ages 40 to 59.[14]

In addition, Gen Xers have the highest consumer spending and the most debt of any generation,[15] which could put them at increased risk for the financial consequences of identity theft. According to identity theft victims who spoke with the Identity Theft Resource Center, these consequences could include the need to borrow money from family and friends.[16]

Not surprisingly given their spending, experts report that Gen X also has more credit card debt on average than any other generation.[17] Both of these factors are likely caused by Gen X being sandwiched in the generational crunch of financially supporting both children and aging parents.[15]

Finally, add to the equation that many Gen Xers regularly use social media.[18] Social media encourages sharing personal information, but reckless oversharing can endanger a person's financial records as well as their personal safety.[19] The FBI warns users of social media to be wary of sharing certain types of personal information that can be mined by hackers and used to access password-protected accounts or sold on internet marketplaces.[20]

Gen Xers have the highest consumer spending and the most debt of any generation[15] which could put them at increased risk for the financial consequences of identity theft.

Baby Boomers — Retirement Accounts Can Be Attractive to Thieves

Baby Boomers can make a prime target for cybercriminals because they often have—or are believed to have—a substantial amount of wealth in their retirement accounts.[21]

Experts say that cybercriminals are more frequently targeting retirement accounts,[22] and some of those accounts may have fewer fraud protections than traditional banks.[21] To access the victim's account, hackers may impersonate the investment firm to get login credentials, and then change the contact information and transfer funds to a different account.[22] By the time the crime is discovered, it may be too late for the victim to recoup losses.

According to the BBB, individuals could find themselves susceptible to Social Security scams or romance scams. Social Security scams were the most common type of impersonation scam in 2020, which may affect Boomers as they attempt to seek their benefits.[9] Scammers may pretend to be a government employee and claim that there is a problem with their Social Security number, demand payment of outstanding debt, or threaten the victim with arrest.[23]

The riskiest scam for Boomers ages 55 to 64 in 2020 was the romance scam.[9] Romance scams occur when a criminal uses a fake online identity to connect with a victim and gain their trust, only to later ask the victim for money.[24]

Seniors — Elderly Americans Are Frequent Targets for Impersonation Scams

It is unthinkable that a vulnerable population would be a frequent target for financial fraud and identity theft, yet sadly, the rate of financial exploitation of seniors is high.

According to the Internet Crime Complaint Center (IC3), every year millions of elderly Americans become victims of some type of financial fraud or internet scam.[24] In 2020, 28 percent of total fraud losses reported to the IC3—approximately $1 billion—were from victims over the age of 60. And though a larger number of younger adults reported fraud loss to the FTC, the reported median loss for victims over the age of 70 was much higher.[12]

Experts say that seniors are frequent targets for phishing scams, in which a fraudster poses as a trustworthy person or company, often through email or other electronic communication.[25] Scammers may pretend to be someone interested in companionship or romance, a grandchild or other family member in need of financial help, a government agency, a charity, or even a technical support representative.[26] Cybercriminals can even spoof calls to falsely identify incoming calls as another person or organization.[27]

Common Impersonations used in Scams

Trustworthy Company

Romantic Interest

Family Member

Government Agency

Charity

Technical Support Representative

To make matters worse, elderly victims are less likely to report a financial crime because they don't know how, they are ashamed that they fell prey to a scam, or they are unable to gather detailed information about the crime.[28] Some victims even fear confiding in a family member, who may question the victim's ability to live independently.

Unfortunately, **Identity Theft** can be one of the consequences of the modern, interconnected world, but there are steps individuals can take to help better protect themselves. For more information on identity theft protection services, visit **www.idwatchdog.com**.

Sources Cited

[1] CNBC make it, “Consumers lost $56 billion to identity fraud last year—here’s what to look out for” (https://www.cnbc.com/2021/03/23/consumers-lost-56-billion-dollars-to-identity-fraud-last-year.html)

[2] Javelin, “Child Identity Fraud: A Web of Deception and Loss” (https://www.javelinstrategy.com/coverage-area/child-identity-theft-fraud)

[3] Florida Department of Agriculture and Consumer Services, “Child Identity Theft” (https://www.fdacs.gov/Consumer-Resources/Scams-and-Fraud/Identity-Theft/Child-Identity-Theft)

[4] Identity Theft Resource Center, “How to Fight Child Identity Theft” (https://www.idtheftcenter.org/wp-content/uploads/2020/09/ITRC-SAS_How2FightChildIDTheft.pdf)

[5] Internet Matters, “Learn about ID theft & data” (https://www.internetmatters.org/issues/privacy-identity/learn-about-privacy-and-identity-theft/)

[6] Identity Theft Resource Center, “What You Need to Know About Child Identity Theft?” (https://helpcenter.idtheftcenter.org/s/article/What-You-Need-to-Know-About-Child-Identity-Theft)

[7] Internet Matters, “Privacy & Identity theft advice hub” (https://www.internetmatters.org/issues/privacy-identity/)

[8] Cybernews, “Gen Z are the least cybersecure generation” (https://cybernews.com/security/gen-z-are-the-least-cybersecure-generation/)

[9] Better Business Bureau, “BBB Risk Report: Adults 18-24 were highest scam risk in 2020” (https://www.bbb.org/article/news-releases/23820-adults-18-24-report-highest-scam-risk-in-2020)

[10] Infosecurity Group, “The Great Authentication Gap: How Password Habits Differ Across Generations” (https://www.infosecurity-magazine.com/next-gen-infosec/password-habits-differ-generations/)

[11] The New York Times, “The Young Fall for Scams More Than Seniors Do. Time for a Warning ” (https://www.nytimes.com/2021/06/25/your-money/young-seniors-scams-warning.html)

[12] Tableau, “Consumer Sentinel Network Data Book 2020” (https://public.tableau.com/app/profile/federal.trade.commission/viz/ConsumerSentinel/Infographic)

[13] Security World, "Millennials and Gen Zers are Most Likely to Fall for Phishing Emails, Study Finds" (https://security.world/millennials-and-gen-zers-are-most-likely-to-fall-for-phishing-emails-study-finds/)

[14] Federal Trade Commission, “Consumer Sentinel Network Annual Data Book 2020” (https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf)

[15] Insider, “Meet the typical Gen Xer, America's 'forgotten middle child' who earns more than everyone else but has the most debt at $136,000” (https://www.businessinsider.com/typical-gen-x-debt-net-worth-income-earnings-caregiving-stress-2021-8)

[16] Identity Theft Resource Center, “Identity Theft: The Aftermath Study” (https://www.idtheftcenter.org/identity-theft-aftermath-study/)

[17] NerdWallet, “How Gen X Can Start Tackling Its Credit Card Debt” (https://www.nerdwallet.com/article/credit-cards/pay-off-gen-x-credit-card-burden)

[18] The Drum, “Social media: the generation gap brands can exploit” (https://www.thedrum.com/profile/whatagraph/news/social-media-the-generation-gap-brands-can-exploit)

[19] Business News Daily, “Privacy on Social Media Guards Against Identity Theft” (https://www.businessnewsdaily.com/4194-social-media-security-tips.html)

[20] Pittsburgh Post-Gazette, “FBI warning: Cyberthieves mining social media for personal data to hack accounts” (https://www.post-gazette.com/business/tech-news/2020/04/24/FBI-warns-sharing-personal-information-could-lead-to-password-problems-hackers/stories/202004240098)

[21] NBC Chicago, “Sleeping Giant:' Thieves Target Retirement Accounts” (https://www.nbcchicago.com/consumer/sleeping-giant-thieves-target-retirement-accounts/2518741/)

[22] Forbes, “Is Your Retirement Plan Protected From Fraud?” (https://www.forbes.com/sites/forbesfinancecouncil/2021/07/01/is-your-retirement-plan-protected-from-fraud/?sh=3554b0107f69)

[23] Social Security Administration, “Protect Yourself from Social Security Scams” (https://www.ssa.gov/scam/)

[24] F.B.I., “Elder Fraud Report 2020” (https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3ElderFraudReport.pdf)

[25] seniorliving.org, “Identity Theft Protection for Seniors” (https://www.seniorliving.org/identity-theft-protection/)

[26] OVC, “Common Scams and Warning Signs” (https://ovc.ojp.gov/program/stop-elder-fraud/common-scams-and-warning-signs#7dguy)

[27] ABC News, “Coronavirus scams: guard against fraud cures and other cons” (https://abcnews.go.com/Business/wireStory/coronavirus-scams-guard-fraud-cures-cons-70038967)

[28] F.B.I., “Elder Fraud” (https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/elder-fraud)