The McAfee Safety Series

Tax Season Security Guide

Tax Season is Upon Us

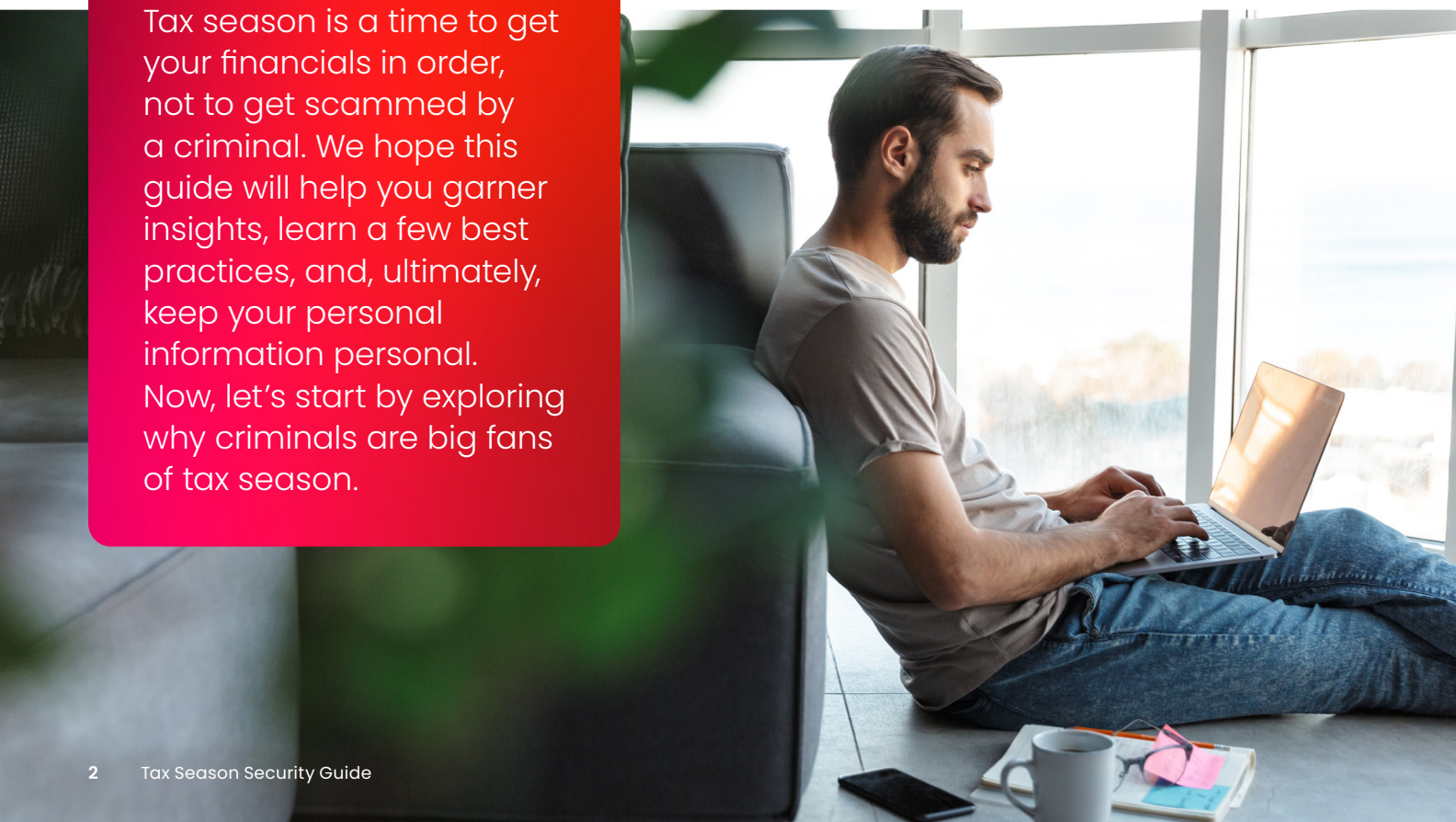
While responsible taxpayers gather their W-2 and 1099 forms in preparation for the tax filing due date, which typically occurs in April, criminals seize this opportunity to scam these people and go after their personal and financial information. These scams come in many shapes and sizes and can be tricky to identify—which is precisely why we've created this guide, to help you stop these scams in their tracks and fight back against fraudsters.

In this definitive guide, we will:

- Take a closer look at the sneakiest tax season scams, including the Dirty Dozen
- Provide security best practices for filing taxes
- Discuss how to determine if you've been impacted by a tax scam
- Offer insights on what to do if you're a victim
- Explore identity theft as it impacts consumers at different life stages

Many consumers assume that filing taxes is a make or break situation, a fear that criminals are eager to prey upon.

Tax season is a time to get your financials in order, not to get scammed by a criminal. We hope this guide will help you garner insights, learn a few best practices, and, ultimately, keep your personal information personal. Now, let's start by exploring why criminals are big fans of tax season.



Why Tax Season?

There's a lot at stake as a consumer when it comes to filing your taxes. As a result, many people have a deep fear of the Internal Revenue Service (IRS). Much of this fear stems from the IRS[1] being an incredibly powerful entity, combined with the fact that taxes can be quite complicated to file on your own. Contrary to popular belief, filing your taxes is not a matter of being good at math or accounting. Rather, it's entirely based on knowing what can be deducted and how. The U.S. tax code is also complex in nature, so a statement like "read the statute" doesn't just mean that—it means "read the statute, and the case law, and develop a sense of how IRS agents are likely to interpret this during an audit." Most people who aren't tax professionals simply don't have the time to delve into these complexities, as they're busy earning a living in their own careers.

While the intricacy of the tax code is ultimately why we receive tax deductions and credits, its complex nature instills pervasive fears around the government and tax season.[2] One common fear? The IRS will come after you if you make a mistake. In reality, if you make an honest mistake on your return, the IRS will usually work with you to address the error without serious repercussions. Taxpayers are also scared of being audited. However, less than 2% of individual returns are audited,[3] and most cases involving deficiency don't require a full-blown audit. Finally, many people fear correspondence from the IRS. Consumers usually think the worst when they see a letter from the IRS, although it's usually not as bad as they think. Often, it's just an informational letter, a notice of adjustment, or a notice of deficiency—all of which can be fixed if they are addressed quickly.

Thousands of people fall victim to IRS scams every year as a result of fear tactics used by criminals, losing millions of dollars in the process. The schemes are typically all based in IRS-related trouble, as scammers know consumers' fear may cause them to not question the legitimacy of the interaction. Criminals also know they can get the most bang for their buck during tax season when it comes to harvesting data. From Social Security numbers to marital status to income amount, tax documents provide hackers with the data they need to pursue identity theft and other attacks.

Hackers & IRS Scammers

There are various degrees of scams that criminals use to exploit taxpayers. From common threats like phishing to more creative schemes like creating fake charities, scammers will go to great lengths to benefit from tax season at the expense of innocent civilians. Stay informed on the Dirty Dozen list and find more resources for filing your taxes properly by visiting the official IRS website.[4]

Deep Dive on the Dirty Dozen

Many of the schemes tax scammers invoke go beyond the basic security threats we hear about daily. Thankfully, the IRS outlines these schemes in an annual list called the Dirty Dozen, highlighting twelve scams consumers should beware of approaching the filing date. Let's take a look at the most recently available list.[5]

Phishing

Before responding to an email claiming to be from the IRS regarding your tax return, know that phishing is a very common tactic used to bait and hook innocent users into giving up their financial data. Phishing,[6] an attack vector used to trick users into giving up their private information or money, is a common strategy used by criminals as it can be executed in multiple ways. In fact, the IRS reported a steady stream of fake emails, text messages, websites, and social media attempts to steal personal information from taxpayers in recent years.

Fake Charities

Taxpayers should be on the lookout for con artists disguised as charitable organizations looking to make a profit on donations from unsuspecting contributors. Many schemers pose as charities or organizations that are familiar to trick consumers looking to receive a tax deduction for donating. Per the IRS, the people behind these scams "normally start with unsolicited contact by telephone, text, social media, e-mail or in-person using a variety of tactics. Bogus websites use names similar to legitimate charities to trick people to send money or provide personal financial information."

EIP and Refund Theft

Whether scammers have their eyes on funds from an Economic Impact Payment (EIP) or a tax refund, this ongoing form of fraud involves rerouting payments from their intended recipient. It's another case where criminals file a false tax return or provide the IRS with incorrect information to send funds either to the wrong address or bank account—one that's in the hands of the scammer.

Senior Fraud

According to the IRS, elder adults are more likely to be victimized by scammers than other segments of society. Whether this happens online or via a phone call,[7] scams linked to Covid-19 have been a major threat as have imposters posing as IRS agents or officials. Seniors need to be alert for a continuing surge of fake emails, text messages, websites, and social media attempts to steal personal information.

According to the Treasury Inspector General for Tax Administration, phone scams have cost 14,700 victims a total of more than $72 million between 2013 and 2020.[8]

More on the Dirty Dozen

Threatening Impersonator Phone Calls

These scams typically involve a criminal impersonating the IRS via phone and threatening arrest, deportation, or license revocation if the victim doesn't pay a bogus tax bill. If the victim doesn't answer the call, the scam artists will typically leave voicemails urging the victim to call back and shell out cash via wire transfer, prepaid debit card, or gift card. Sometimes, scammers will even trick victims into disclosing personal information, which they can then use for identity theft.

Social Media Fraud

In a social media attack, scammers harvest information from social media profiles and turn it against their victims. Per the IRS, because "[s]ocial media enables anyone to share information with anyone else on the Internet, scammers use that information as ammunition for a wide variety of scams. These include emails where scammers impersonate someone's family, friends, or co-workers." From there, scammers will send phony links, ask for personal information, promote bogus charities, or flat-out ask for money or gift cards to "help them out" at tax time.

Fraud Targeting non-English Speakers

Scammers will prey on non-native speakers, particularly if they are recent immigrants to the U.S. Usually by way of a robocall or an in-person call, a con artist will pose as the IRS and threaten the non-native speaker with deportation, denial of their driver's license, or even jail time—all of which can be avoided if they make an immediate form of payment. Given that the IRS does not levy such threats, especially threats of these measures, any such call or contact is most certainly a scam. Victims should hang up and simply not engage, says the IRS.

Unscrupulous Return Preparers

Accountant fraud, a practice sometimes known as ghost preparers,[9] involves bogus preparers tricking clients by perpetrating refund fraud, identity theft, and other malicious scams. According to the IRS, these criminals typically prey on older Americans, low-income taxpayers, and non-English speakers. And while most tax professionals provide honest, high-quality service, it's important for consumers to exercise caution and choose tax preparers wisely.

According to the Federal Trade Commission, nearly 90,000 consumers reported tax-related fraud in 2020—a 225% increase over 2019.[10]

More on the Dirty Dozen

"Offer in Compromise" Mills

An Offer in Compromise, or OIC, is a means for taxpayers to resolve tax debt with the IRS, providing they qualify. To give you some idea of how often people apply and are accepted, in the 2019 tax year, 54,000 OICs submitted to the IRS and 18,000 of them were accepted. In this climate, several "OIC mills" have cropped up that, for a pricey fee, will create an OIC application even though the people applying for them won't likely qualify. The IRS reminds taxpayers that they can use the free online Offer in Compromise Pre-Qualifier tool to see if they qualify.

Fake Payments with Repayment Demands

This is a another rather involved, yet increasingly common scam. As described by the IRS, "A con artist steals or obtains a taxpayer's personal data including Social Security number or Individual Taxpayer Identification Number (ITIN) and bank account information. The scammer files a bogus tax return and has the refund deposited into the taxpayer's checking or savings account. Once the direct deposit hits the taxpayer's bank account, the fraudster places a call to them, posing as an IRS employee. The taxpayer is told that there's been an error and that the IRS needs the money returned immediately or penalties and interest will result."

Payroll and HR Scams

In these scams, crooks pose as a business reaching out to its employees to gain sensitive personal information, such as what is contained on a W-2 form. Other versions include imposter schemes where a scammer poses as the company and requests the payment of fake invoices, or where the scammer poses as the victim and asks the company to re-route their direct deposit checks to a new (scammer-owned) account. In some cases, the scammer will use phony IRS documents to make the request look more legitimate.

Ransomware

Ransomware, where a scammer holds the files and information on a victim's computer hostage for a price, has increased in recent years, thanks in part to criminals demanding payment in difficult-to-trace cryptocurrency. The IRS reports that "cybercriminals might use a phishing email to trick a potential victim into opening a link or attachment containing the ransomware. These may include email solicitations to support a fake COVID-19 charity."

In 2019, 54,000 debt-reducing Offers in Compromise were submitted to the IRS. Only 18,000 of them were accepted.[11]

Signs That You May Be a Victim

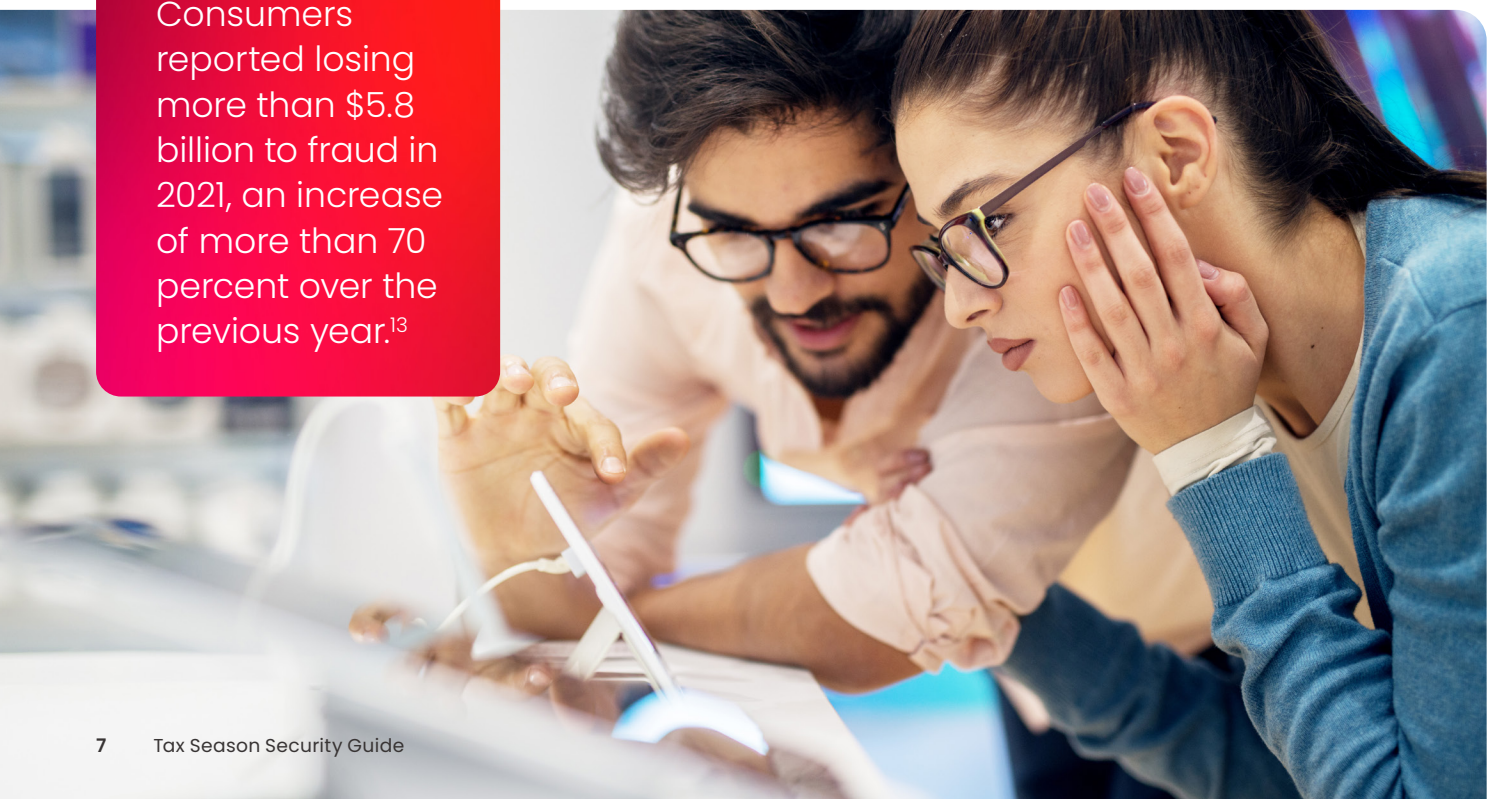
Recognizing the signs[12] that you may be a victim of an IRS scam could greatly suppress the repercussions. Look out for these indications that you've been the victim of tax-related identity theft:

- Your tax return is rejected when you file it. This could occur if a criminal has already filed a fake return using your Social Security number to claim a fraudulent return in your name.
- You receive a letter from the IRS. If the IRS sends you a letter inquiring whether you sent a tax return containing your name and Social Security number, this could indicate that someone has tried filing a return with your information.
- You receive a W-2 or 1099 form from an employer that you haven't worked for. If you do receive one of these forms from a company you're unfamiliar with, look up the company's name online. This will help determine whether the name you know the company by is different from its official name, which is what appears on tax documents.

It's precisely why this season is so enticing for criminals—a little fear can go a long way.

- You receive a tax refund for a refund you didn't file for. While this might appear to be a pleasant surprise at first, know that the IRS isn't just handing out free money and that this could point to tax-related fraud.
- You receive a tax transcript by mail that you never requested. Tax transcripts show most of the line items from your originally filed tax return. However, they don't show any changes you may have made after you filed the return.

Consumers reported losing more than $5.8 billion to fraud in 2021, an increase of more than 70 percent over the previous year.[13]



Protecting Your Identity & Personal Data

It doesn't matter what stage of life you're at—your personal identity is incredibly valuable. It is used for everything from applying for federal loans to getting a driver's license. But because personal identities hold so much value, they are consequently always a prime target for thieves. Here's how identity theft varies at different stages of life and what you can do to stay vigilant against threats at all ages:

18 and under[14] Underage consumers usually have a Social Security number and clean or nonexistent credit, which is ideal for identity thieves. This "blank slate" allows a criminal to open new lines of credit before the individual is old enough to catch on. Parents/guardians can help prevent childhood identity theft by keeping the child's data out of circulation, locking down sensitive documents, freezing the child's credit, and looking out for red flags like jury summons and collection calls addressed to the child.

20s[15] Consumers in their 20s are dealing with a flurry of new life experiences. With so much going on, it can be easy for people in their early 20s to lose sight of their identities. That's why staying educated on common identity theft schemes like phishing emails and social engineering scams designed to compromise user data should be made a top priority.

30s–40s[16] With kids, mortgages, and car payments, there is even more at stake when it comes to identity theft. Because users in their 30s and 40s have a more established income, they must be vigilant when it comes to monitoring and protecting their online and financial accounts.

50s[17] According to one study, the majority of 50-somethings say they have little confidence that what they do online remains private. Add to this that this is the time when many have children in college, a maturing investment portfolio, and perhaps a fair share of old records from the days much was still done on paper, their risk for identity theft can increase. In addition to looking after their online protection, people in their 50s will want to secure the old paper documents wish to keep and securely dispose of the ones they don't.

60s and up[18] Many consumers begin to think about retiring in their 60s. Additionally, many elderly people spend time in hospitals or nursing homes, where their personal information is passed between many hands regularly. But these are years to be cherished, not to be spent dealing with identity theft. These people should practice proper security hygiene by recognizing phishing attacks and operating safely online.

According to its "Consumer Sentinel Network Data Book 2021," the FTC fielded reports of identity theft from 141,494 victims between the ages of 20 and 29.[19]

Fight Back Against Fraudsters

While recognizing the signs of tax-related fraud helps ease the burdens associated with these schemes, there are multiple steps users can take to prevent becoming a victim of IRS scams in the first place. Here's what you can do to fight back against tax schemes:

- One way to protect yourself from an identity thief from claiming a return in your name is to file yours before they do. In fact, many victims of identity theft find out they've been scammed when they receive an IRS notification that their tax claim has already been filed. Simply put, file early.
- Tell the Treasury Inspector General for Tax Administration (TIGTA). Report IRS scams online[20] or call TIGTA at 1-800-366-4484.
- Forward email messages that claim to be from the IRS to phishing@irs.gov.
- Tell the Federal Trade Commission via the FTC Complaint Assistant on FTC.gov.[21] Include "IRS scam" in the notes.
- Report Social Security Administration phone impostor scams. Use the form on the Social Security Administration's website.[22]
- If scammers appear to be impersonating a state tax authority rather than the IRS, contact your state Attorney General's office.

Whether you're 25 or 55, identity theft can have a significant impact on your life. It's important to stay educated on the various tax schemes designed to harvest this information.

Staying Secure Now and in the Future

By following the tips in this guide, you can not only be better prepared to ward off IRS scams and tax-related identity theft, but also be acclimated to head off future advanced threats that may emerge out of the digital age. With so much riding on your personal and financial data, being prepared and educated, you can live your online life with ease and connect with confidence.

About McAfee

McAfee is a global leader in online protection for consumers. Focused on protecting people, not just devices, McAfee consumer solutions adapt to users' needs in an always online world, empowering them to live securely through integrated, intuitive solutions that protect their families and communities with the right security at the right moment.

www.mcafee.com

Appendix

1. McArdle, Megan. "Why We Fear the IRS." Bloomberg.com, Bloomberg, 4 Jan. 2016, www.bloomberg.com/opinion/articles/2016-01-04/why-we-fear-the-irs.

2. Erb, Kelly Phillips. "5 Things Taxpayers Are Irrationally Afraid Of - And Shouldn't Be." Forbes, Forbes Magazine, 13 Apr. 2015, www.forbes.com/sites/kellyphillipserb/2015/04/12/5-things-taxpayers-are-irrationally-afraid-of-and-shouldnt-be/?sh=4113fed92954.

3. Ibid.

4. "Home: Internal Revenue Service." Internal Revenue Service | An Official Website of the United States Government, IRS, www.irs.gov/.

5. "IRS Concludes 'Dirty Dozen' List of Tax Scams for 2019: Agency Encourages Taxpayers to Remain Vigilant Year-Round." Internal Revenue Service, IRS, 28 June 2019, www.irs.gov/newsroom/irs-concludes-dirty-dozen-list-of-tax-scams-for-2019-agency-encourages-taxpayers-to-remain-vigilant-year-round.

6. "Phishing Email Examples: How to Recognize a Phishing Email." McAfee Blogs, McAfee, 15 Mar. 2021, www.mcafee.com/blogs/internet-security/phishing-email-examples-how-to-recognize-a-phishing-email/.

7. "Taxpayers Beware: Tax Season Is Prime Time for Phone Scams." IRS, Tax Tip, 27 Jan. 2022, www.irs.gov/newsroom/taxpayers-beware-tax-season-is-prime-time-for-phone-scams.

8. Iacurci, Greg. "Tax Scams Are in Full Swing. Here's How to Protect Yourself." CNBC, CNBC, 18 Feb. 2020, www.cnbc.com/2020/02/18/how-to-protect-yourself-from-tax-scams-this-filing-season.html.

9. "Beware of 'Ghost' Preparers Who Don't Sign Tax Returns." IRS, 5 Feb. 2021, www.irs.gov/newsroom/beware-of-ghost-preparers-who-dont-sign-tax-returns.

10. Iacurci, Greg. "Tax Scams Are in Full Swing. Here's How to Protect Yourself." CNBC, CNBC, 18 Feb. 2020, 4.

11. "IRS Unveils 'Dirty Dozen' List of Tax Scams for 2020: Americans Urged to be Vigilant to these Threats During the Pandemic and its Aftermath.", Internal Revenue Service, IRS, 16 Jul. 2020, www.irs.gov/newsroom/irs-unveils-dirty-dozen-list-of-tax-scams-for-2020-americans-urged-to-be-vigilant-to-these-threats-during-the-pandemic-and-its-aftermath.

12. Fontinelle, Amy. "Know the Sneakiest IRS Scams." Investopedia, Investopedia, 5 Feb. 2020, www.investopedia.com/taxes/know-latest-irs-scams/.

13. "New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021.", 22 Feb. 2022, www.ftc.gov/news-events/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers.

14. Grant, Kelli B. "Identity Theft Isn't Just an Adult Problem. Kids Are Victims, Too." CNBC, CNBC, 24 Apr. 2018, www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html.

15. Bisson, David. "Millennials Reported More Cases of Identity Theft Than Senior Citizens in 2017." Security Intelligence, Security Intelligence, 8 Mar. 2018, securityintelligence.com/news/millennials-reported-more-cases-of-identity-theft-than-senior-citizens-in-2017/.

16. Maxfield, Natalie. "Top Signs of Identity Theft." McAfee, 13 Oct. 2021, www.mcafee.com/blogs/consumer-cyber-awareness/top-signs-of-identity-theft/.

17. Baig, Ed. "Older Adults Wary About Their Privacy Online." AARP, 13 Apr. 2021, www.aarp.org/home-family/personal-technology/info-2021/companies-address-online-privacy-concerns.html.

18. "How Seniors Can Protect Themselves from Identity Theft." SeniorLiving.com, www.seniorliving.com/article/how-seniors-can-protect-themselves-identity-theft.

19. "Consumer Sentinel Network Data Book 2020." Federal Trade Commission, Feb. 2021, www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf.

20. "Home: Treasury Inspector General for Tax Administration." U.S. Treasury Inspector General for Tax Administration (TIGTA), 18 May 2004, www.treasury.gov/tigta/.

21. "Federal Trade Commission." Federal Trade Commission, 3 Mar. 2020, www.ftc.gov/.

22. "Office of the Inspector General, SSA." Office of the Inspector General, SSA | Social Security Administration, SSA, 13 Feb. 2020, oig.ssa.gov/.

6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com