ΛURΛ

America's $10 Billion Cyber Crisis

The cost of cybercrime now outpaces that of home burglaries.[1] As American families lose billions of dollars a year to hackers, scammers, identity thieves and government imposters, Aura wants to work with our nation's leaders to help inform, support and scale solutions that put money back in Americans' pockets, restore trust in government programs and convey to bad actors that their time is up.

aura.com

Table of Contents

The Problem

Americans lost **$10.3 billion** to cybercrime in 2022, according to the FBI's 2022 IC3 Report[2] — nearly double the amount lost the prior year.[3] In fact, the cost of digital crime **now outpaces the estimated cost of home burglaries** ($1.6 billion estimated loss in 2022).[4] Yet, while we lock our doors and invest in home security systems, many of us continue to leave our digital lives unguarded.

While difficult to measure given under-detection and under-reporting, most attribute the growing number, type and cost of internet attacks to the increasing sophistication of hackers, scammers and cybercriminals who leverage news and trends as crimes of opportunity. Whether it's tax return fraud in filing season, medicare fraud during open enrollment season or submitting fraudulent unemployment claims amid mass layoffs, scammers are paying attention to the same things we are and using them to make money.

With the amount of time we spend online and how much of our lives take place digitally, the risk of cybercrime will only increase. The average American household has 25 connected devices,[5] and each of us has an average of 150+ online accounts.[6] As such, criminals have created a lucrative market for our data, which they often obtain by tricking victims. The hacker or scammer may then sell that data on the dark web, buy our account logins to commit identity theft or use our information to gain access to our accounts and finances.

And while this is a billion-dollar problem in the United States and Americans experience identity theft 3X more often than the rest of the world population,[7] we're not the only ones paying the price of preventable cybercrime.

Americans experience identity theft 3X more often than the rest of the world population.

The global annual cost of cybercrime is predicted to reach $8 trillion annually in 2023.[8] If cybercrime were measured as a country, it would be the world's third-largest economy after the U.S. and China, according to the Cybersecurity Ventures 2022 Official Cybercrime report.[9] That same report predicts the global cybercrime damage costs in 2023 will be:

$8 Trillion	USD a year
$667 Billion	USD a month
$154 Billion	USD a week
$21.9 Billion	USD a day
$913 Million	USD a hour
$15.2 Million	USD a minute
$255,000	USD a second

Cybercrime To Cost The World 8 Trillion Annually In 2023 - October 17, 2022, | Cybersecurity Ventures

More Than a Monetary Threat

Sometimes criminals target individuals directly, but they often go for the bigger prize – a massive collection of personal data from a government organization or corporation. While 34% of Americans have stopped paying attention to them because they happen so often,[11] data breaches are a major cause of identity theft and fraud, often serving as the initial source of leaked personal information – like names, emails, passwords, Social Security numbers (SSNs), addresses, bank account numbers, insurance information and more. In 2021, for example, there were 4,145 publicly disclosed breaches exposing over 22 billion records.[12]

Corporate Data Leaks

In the past decade, there have been major data breaches across nearly every industry, costing an average of **$9.44 million**.[13] We've seen leaks affecting telecom companies like AT&T and T-Mobile, social media platforms like Twitter and Facebook, financial institutions like Equifax and Capital One, as well as insurance companies and healthcare providers. Insurance and healthcare breaches are especially worrisome as they have the potential to result in medical identity theft, which can leave a victim without access to the proper care, ultimately meaning the difference between life and death.

Breach in Government Trust

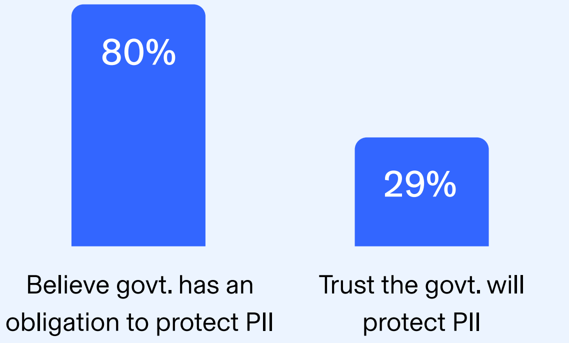
Government agencies have been the target of some of the most widespread, news-driving and damaging data breaches yet. The 2015 Office of Personnel Management (OPM) data breaches,[14] for example, impacted the personal data of more than 20 million individuals, including federal government employees, contractors and prospects. The breach not only leaked their sensitive personal information, but that of those close to them — including personality assessments, drug use and travel history. Other examples include the 2018 U.S. Postal Service data breach of 50 million records[15] and the Consumer Financial Protection Bureau's employee-driven leak of 250,000 consumers' names and account numbers.[16] According to Comparitech, across all levels of government, there have been 822 data breaches, affecting nearly 175 million records from 2014 to 2022.[17] The total cost of these government breaches is an estimated $26 billion.

Not only are data breaches costly to the government, to businesses and to consumers, but they also erode the public's already decreasing trust in the government.[18] According to a September 2021 Aura and Harris Poll survey, Americans are actively worried about the future of cybercrime, perceiving it to be a greater threat than climate change (77%) and COVID-19 (81%). An alarming 82% of those ages 18-34 feel cybercrime will be a threat to the safety and well-being of the next generation. But perhaps most importantly, a whopping 80% of U.S. adults think the government has an obligation to protect consumers' personal information, while only 29% currently trust the government to actually protect it.[19]

The total cost of government data breaches is an estimated $26 billion.

Did You Know?

80% of U.S. adults think the government has an obligation to protect consumers' personal information, while only 29% currently trust the government to actually protect it.



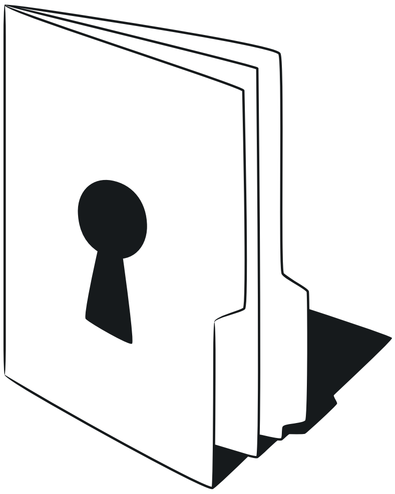
Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents - January 13, 2022 | U.S. Government Accountability Office

Foreign Threats

While the cost of government data breaches and the number of those impacted is stark, perhaps most unsettling is the potential for foreign governments to use cybercrime as a way to wage war on Americans. This was the case in January 2019, when a hacker from the Russian Foreign Intelligence Service breached computing networks at SolarWinds,[20] which provided the government with software that monitored network activity and managed devices on federal systems. As a result, several federal agencies' networks were breached. In 2021, while the response and investigation into the SolarWinds breach was still ongoing, Microsoft reported that malicious cyber actors affiliated with the People's Republic of China were able to gain access to a Microsoft Exchange server. Ultimately, account privileges were escalated and enabled ongoing, persistent malicious operations even after the vulnerabilities were patched. The OPM breach has also been linked to China.[21]

Infrastructure Attacks

As if foreign infiltrators weren't threatening enough to national security, the largely privately-owned infrastructure systems that provide Americans with water, energy and transportation are also threatened by cybercrime. The ransomware attack that targeted the Colonial Pipeline Company[22] in May 2021 is one example of this, caused by just one stolen password used to access the company's legacy Virtual Private Network (VPN).[23] The attack, which shut down the pipeline for several days, resulted in a spike in fuel prices and localized shortages, caused by panic buying. Had it gone on for longer, mass transit and trucking would have had to limit operations due to a lack of fuel.[24]



While the cost of government data breaches and the number of those impacted is stark, perhaps most unsettling is the potential for foreign governments to use cybercrime as a way to wage war on Americans.

Mental Health Implications

There is no doubt that corporations, government institutions and infrastructure providers can be severely affected by data breaches and ransomware attacks. Many now have cyber incident insurance and plans in place to mitigate these crises. On the other hand, individuals and families dealing with identity theft and fraud on their own are fighting a time-intensive, stressful and frustrating uphill battle.

The risk of immediate financial loss is evident, but it's more difficult to measure the impact to one's mental health, as well as the long-term and potentially generational effects of monetary loss and ongoing family strain. Some victims, for example, begin having thoughts of suicide they did not have before (8%), cannot get a job (13%), trust people less (37%) and feel violated (54%) and stressed (54%).[25]

To further understand the more difficult to measure mental health implications, Aura worked with Ipsos to publish research illustrating cybercrimes' impact on a family's well-being.[26]

By the Numbers

54%	of people experience moderate to extreme feelings of anxiety or stress following a scam incident
1 in 5	of those who have fallen victim to an online scam say they struggled to focus after the incident (23%) or experienced financial strain (20%)
64%	of those with income under $50K per year report moderate to extremely high stress after a scam incident
42%	of parents who have fallen victim to a scam worry their children will also be a victim

Aura Online Scams and Mental Health Impact Survey Reveals Staggering Effects of "Scam Economy" on American Mental Health and Well-Being - October 2022 | Aura

Who's at Risk

Cybercrime, identity theft and fraud do not discriminate. It is no longer a question of if you'll be targeted by a scam, but when. As scammers and hackers become more sophisticated, all Americans are at growing risk of cybercrime. And while technology has the power to support proactive and preventative consumer cybersecurity, it cannot protect them entirely on its own — yet.

Whether young or aging, tech-savvy or technophobic, wealthy or low-income, we are all at risk. For example, older adults tend to lose greater amounts of money, while younger people report losing money more often.[27] In fact, Aura found that while nearly half of adults aged 50-64 are targeted once a week, targets are getting younger.[28] In fact, people ages 20-29 reported losing money to fraud more often (43%) than older people 70-79 (23%) – but those over the age of 70 had a much higher median loss to fraud.[29] And while scammers may prefer to target older Americans because of their higher net worth (and potentially lower level of comfort with technology), lower-income individuals have access to government benefit programs that are the target of scams, too.[30]

Highly Vulnerable Communities

While no family is safe from today's evolving digital threats, some are especially vulnerable. As a mission-driven company, Aura has invested in efforts to help reverse cybercrimes' disproportionate impact among certain, higher-risk communities, including:

☆ Military & Veterans

Aging Adults

Children & Foster Youth

☆ Military & Veterans

American heroes and their families have made great sacrifices to protect our freedoms and civil liberties. In return, we must do more to protect them. Not from enemy fire or foreign threats to our democracy, but from the hundreds of thousands of fraud and identity theft cases they report every year.[31] Unfortunately, active-duty service members and their families are up to three times more frequently victims of digital theft than other U.S. adults,[32] costing them $414 million in 2022.[33] And with cybercrime being the fastest-growing crime in America, there are no signs of a slowdown.[34]

For service members, the consequences of fraud extend beyond financial ruin or damage to mental health — they can be catastrophic,[35] putting a military career in jeopardy by compromising security clearances that often depend on strong credit histories.

Military families' higher-than-average vulnerability to digital crime can be attributed to the nature of military life. Frequent changes of station risk important records being sent to old addresses. Deployment and boot camps limit account and credit monitoring abilities. Communal WiFi used on bases can mean less secure transfers of information. Military families' personal data has also been affected in government leaks, including the previously mentioned Office of Personnel Management (OPM)'s 2015 data breach.[36]

As military quality of life declines and enlistment rates slow, a hero's choice to dedicate his or her life to protecting our country should not come with the burden of digital danger. While some effort has been made to address this community's vulnerability to cyber threats, recent years' rate of increase indicates that more must be done.

It is no longer a question of *if* you'll be targeted by a scam, but *when.*

Unfortunately, active-duty service members and their families are up to three times more frequently victims of digital theft than other U.S. adults, costing them $414 million in 2022.

By the Numbers

Our Veterans agree, according to Aura research from April 2023:[37]

1 in 4	Veterans say they worry about their sensitive PII being compromised online every day (24%)
9 in 10	Veterans say they worry about their sensitive information being compromised at least once a year (89%)
1 in 5	Veterans say their identity has been compromised in the past 5 years (19%), while one in seven vets are not sure if their identity has been compromised (14%)

Aging Adults

Older Americans are another group frequently targeted by cybercriminals. With many having saved and invested over the course of their lives, they tend to have higher net worth, potentially a lower level of comfort with technology and may be more likely to trust than younger generations.[38]

Facts

In 2021, older adults reported nearly 100,000 fraud complaints to the FBI's Internet Crime Complaint Center, costing them $1.7 billion — a 74% increase since 2020. Their median losses are up to 16 times those of other age groups, with victims losing an average of nearly $20,000 and many losing more than $100,000.[40]

2021 Internet Crime Report | Federal Bureau of Investigation

Children & Foster Youth

Children's safety online, especially on social media, has been a key focus of the national consumer privacy conversation in recent years, and with good reason. One in five children[41] report they have been solicited or contacted each year by one of the more than 500,000[42] predators online.

A lesser-known, but equally alarming threat is child identity theft. With their clean and often unmonitored credit histories, children are an extremely easy target for identity thieves and fraudsters. According to research from Javelin Strategy, nearly 1 million children were victims of identity fraud in 2022, costing $688 million.[43] However, because many victims of child identity theft only discover they've been affected by these crimes when they reach adulthood and attempt to use their credit for the first time, these cases — like most cybercrime — are severely underreported.

Anyone with damaged credit might want to use a child's identity to start over — get a job, open a new credit card, apply for a loan or even avoid criminal prosecution. While it's illegal for anyone under the age of 16 to apply for a loan, few companies actually verify ages before issuing credit cards or lines of credit.

While plenty of criminals are buying and selling children's SSNs on the dark web, it is tragically more likely that the fraud is committed by a family member, friend or guardian who has easy access to their sensitive information. Over 70% of child identity theft victims know the perpetrator — which explains why foster youth are especially vulnerable to these crimes.[44] California, for example, discovered that 50% of the children in state's foster care — 84,000 total — have had their identities stolen, with an average debt of more than $12,000.[45] As they move homes and foster families, an increasing number of adults and digital databases gain access to foster youths' sensitive personal information. Many only discover their SSN has been stolen and fraudulently used after they turn 18 and become one of the 23,000 young adults who age out of the foster care system each year.[46] Unfortunately, the consequences of these crimes can be especially debilitating to former foster youth, leaving them unable to obtain a credit card, employment or housing.

Stories of Real Impact

While data is helpful in understanding cybercrime's immense scale and impact, nothing brings this issue to life like the stories we hear everyday. Below are just a few examples of the experiences we help prevent and resolve at Aura. Of note, in many of these stories, the victims have chosen to be anonymous, highlighting the feelings of shame, vulnerability and embarrassment that many feel after being affected by cybercrime.

First Foster Homes, Now Night Trains

Lenique Carter was 16 when she and her younger sister were placed in foster care. Carter, now 24, was working at T.J. Maxx, did not have a credit card, had not taken out loans and used a pay-as-you-go cell phone. She was doing everything she could to avoid becoming one of the 33% of foster youth who end up without housing.[47] That's why Carter was confused when three rental companies rejected her apartment applications in the same year, claiming she had bad credit. She was in good health and lived frugally, but according to her credit report, someone had racked up more than $5,000 in hospital bills and purchased nearly $500 of jewelry on her credit. The identity thief, who Carter suspected stole her information while she was in a group home before turning 18, used her SSN to apply for a job because she had a clean criminal record that would pass background checks. As a result, Carter's bank froze her checking account and California began garnishing her wages from T.J. Maxx to pay back taxes the identity thief owed. As Carter works with a pro bono law firm and youth advocacy group to resolve the credit fraud, she still has no permanent place to live and spends nights on the Blue Line train.[48]

Grandparents to the Rescue

A Maryland couple got a frantic call from their granddaughter, proclaiming that she had been in a serious car accident, three people were hurt and she was at the police station, where her phone was taken and her car was impounded. Like many grandchildren, she begged the couple not to tell her parents. And like many grandparents, they calmed her down, told her they loved her and that they would do anything they could to help. They assured her not to worry and spoke with her lawyer, who said a gag order imposed by a judge meant no one else could find out. The lawyer urged them to send $38,000 to help their granddaughter, and they did. For three days they worried — they didn't sleep or eat. A few days later the grandfather realized he had been scammed after texting with his real granddaughter. They felt embarrassed, ashamed and gullible for falling for the scam and never recovered the money.[49]

Tricked by Love

In 2017, an 87-year-old Holocaust survivor seeking companionship met a woman named Alice on a dating website. After wooing the survivor and escalating their relationship, Alice told him that she desperately needed money. She had gotten a settlement from a lawsuit, but to receive it, first needed to pay her lawyer. The unsuspecting man thought he could help. And he did, for four years, as Alice consistently claimed she needed more money or her bank accounts would be frozen and he'd never get his money back. Alice made a fake email account to impersonate a TD Bank employee to assure her victim he would be repaid if he continued to fill her account. She sent him fake invoices that he could show his own bank after they became suspicious about the amount of money — usually $50,000 checks each month — he was transferring to Alice. As his bank balance dwindled, the victim told his son what was going on. He had given away his life savings and lost his apartment. But Alice, who was in fact a woman named Peaches Stergo, was now rich, spending her $2.8 million dollars on luxury items including designer watches, jewelry, handbags, a home, condo, boat, vacations, cars and more.[50]

A Victim, Even in Death

Alexis was just four years old when she died from a brain tumor in 2012. As her parents were grieving, someone else was ready to take advantage of an opportunity to profit from the child's death. When her parents filed their taxes later that year, they learned that someone else had already submitted a return using their late daughter's SSN and claiming her as a dependent. They learned that they were not alone, that at least 14 other families had lost their children to illnesses at a young age, and that their SSNs had also been stolen. Apparently, the government published a public Master Death List containing the birthdays, full names and SSNs of more than 80 million death records in the country. While the publicly available database was intended for banks and credit agencies to prevent identity theft, it's been abused by scammers for the opposite purpose. As they were grieving, Alexis's parents had to work for over a year to prove to the IRS that she was, in fact, their child.[51]

Informing Action

To begin tackling the billion-dollar (and growing) cyber crisis, we must first understand how these breaches have occurred, our history of incident response and what we can learn from previous tactics to inform a productive discussion and enactment of effective solutions.

Threat Drivers

While each individual instance of identity theft and fraud have differing causes, the largest driver of these crimes is likely massive data breaches that leak names, account logins, addresses, Social Security numbers and other information that criminals use to steal someone's identity, money or both. The Identity Theft Research Center reported 1,802 data compromises in 2022, impacting at least 422 million individuals (more than the U.S. population).[52]

Employee error is unfortunately a common thread in data breaches and infrastructure attacks. Stanford University and IBM research estimate that 88-95% of breaches are caused by individual employee actions,[53] like using easy-to-guess passwords, connecting to unsecured WiFi or not updating software on devices. SolarWinds, for example, was infiltrated by hackers guessing passwords, according to the Cybersecurity and Infrastructure Security Agency (CISA).[54]

In just the first six months of the year, 1,393 data breaches leaked private and personal data from over 156 million Americans.[55] In one of the worst examples, the MOVEit data transfer breach gave hackers access to private healthcare data from millions of patients in Missouri, Oregon, and more.[56]

The Identity Theft Research Center reported 1,802 data compromises in 2022, impacting at least 422 million individuals (more than the U.S. population).

Keeping your personal and private information safe is a critical part of online safety. The more personal details scammers and fraudsters have about you, the easier it is for them to hack your accounts, steal your identity, and scam you.

While it's getting harder to live a "private life" online, it's not impossible. With a few steps and additional security measures, you can learn how to protect your privacy, fend off identity thieves and hackers, and take back control of your personal data.

How To Protect Your Privacy and Personal Information Online

1. Share less information with apps and services
2. Use strong and unique passwords with 2FA
3. Tighten privacy settings on your social media accounts
4. Delete unused accounts, apps, and browser extensions
5. Stop search engines from tracking you
6. Use a VPN to hide your browsing history
7. Don't ignore software or operating system updates
8. Use a Privacy Assistant to block ad and data tracking
9. Use encryption to hide your data from prying eyes
10. Revoke unnecessary third-party app connections
11. Request that data brokers remove your personal information
12. Monitor your sensitive information with identity theft protection

Follow these 12 steps if you're concerned about how much personal information is available about you online.

1 Share less information with apps and services

The best step you can take to protect your information from people trying to scam you online is to share less of it. The best place to start is with social networks — but you should also be aware of the data collection policies for any app or service you use.

All social media platforms and apps collect data about who you are, your interests, and what you do online. All of these shares and data points make up your online footprint (which scammers can use to get access to your sensitive information).

Unfortunately, they're rarely as careful with your data as you'd like. Some recent examples include when Zoom connected its user accounts to LinkedIn profiles,[57] revealing names and professions (even for "anonymous" users); or when Facebook kept hundreds of millions of account passwords in a searchable, employee-accessible database — and didn't notice for seven years.[58] How to remove your personal information from social media:

- Share less on your profiles. Share as little as possible and skip any "optional" information, like a middle name or phone number.

- Create a throwaway email address. Email lists are often sold or rented on the Dark Web and can fall into unsafe hands. Consider making a throwaway email just for subscriptions. With Aura, you can use email aliases to protect your primary email address from scammers.

- Limit collaborative folders, albums, or playlists. The more people who have access to your data, the more likely it could be leaked or hacked.

2 Use strong and unique passwords with 2FA

Strong passwords are the most important — and sometimes the only — protection we have against identity theft and hackers. Just think about how much personal information could be found in your email account — such as bank account details, home addresses, or even your Social Security number (SSN).

If you don't already have passwords or passcodes for all your devices (including guest accounts), add them now.

- Store passwords in a secure password manager. Make sure that you're using strong and unique passwords on your online accounts. Since you probably have dozens of accounts, a password manager is an easier way to keep the information secure.

- Enable two-factor authentication(2FA). This is secondary secure measure that can even protect you if you've shared your password with hackers in a phishing scam. If you've ever needed to type in a code sent to you via text message, you've used two-factor authentication before.

- Set devices to automatically lock when not using them. Hackers can evade even a strong password if your device doesn't automatically lock. For devices that use fast biometric authentication like fingerprint scanning or facial recognition instead of a code, the best setting is "30 seconds" or "immediately."

3 Tighten privacy settings on your social media accounts

You don't have to delete your social media accounts to improve online privacy. Instead, it can be enough to simply review the privacy settings on the online accounts you use regularly.

Companies make billions off collecting your personal information. In general, their default settings skew towards collecting more over protecting your data.

The best settings for you depend on what you want to share and what you want to protect. But there are a few areas where you should pay careful attention.

Pay special attention to these factors:

- Location tracking. Consider turning off automatic geolocation data on your social media posts, photos, and comments.

- Public information. Think carefully about what information should be public, hidden, or somewhere in-between. There are typically three levels of data: profile data, your content, and your interactions with other content.

- Likes, shares, and comments. We usually think about limiting what we share, but your "likes" and comments on other posts are usually public as well. Profile pictures, names, and comments on other posts often show up in search results, even for "private" accounts.

4 Remove unused mobile apps and browser extensions

Apps and browser extensions can change their security and privacy policies at any moment. If you're not actively using a tool, it's best to delete or remove it.

For example, Unroll.me is a free app that summarizes newsletters and subscription emails. But after an FTC investigation, their revenue model became clear: they scanned emails and sold the contents.[59]

If you don't understand how an app makes money, user data might be the answer.
Here's what to do:

- Only download apps and extensions from reputable app stores. Scammers and hackers create free apps and tools that hide malware or tracking software. To stay safe, stick with official app stores that are more likely to only approve legitimate apps.

- Only download apps and extensions from reputable app stores. Scammers and hackers create free apps and tools that hide malware or tracking software. To stay safe, stick with official app stores that are more likely to only approve legitimate apps.

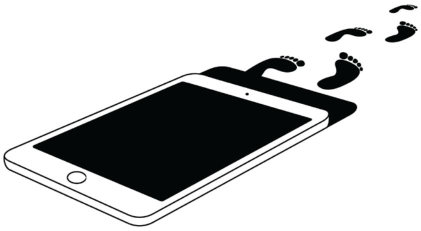
- Be suspicious of every app. Your device should warn you about the permissions an app or tool is asking for before you install it. Read through these carefully and make sure the tool isn't asking for more than it needs.

- Remove extensions from your browser. Eight popular Chrome and Firefox extensions turned out to include code that tracked all browser activity.[60] The data included tax returns, medical data (which could lead to medical identity theft), and secret developments at companies like Tesla and Apple.

Pro Tip

If you use Chrome, you can see all extensions by typing chrome://extensions/ in your search bar. It's good to delete — not just disable — any extensions that you're not using.

5 Stop search engines from tracking you



Your search engine collects a huge amount of personal data about you. And for 92% of us, that search engine is Google.[61]

The owners of the two largest search engines — Google and Bing — also operate the popular browsers Chrome and Edge, respectively. (So, they track a lot of data.)

The first step to improving search engine privacy is deleting your data.

For Google: Go to the My Activity dashboard and delete everything.

For Microsoft: You'll need to clear data separately from Microsoft Edge and Bing.

For Yahoo: You can delete data from search history management.

Unfortunately, there's no way to eliminate all tracking on Google. An alternative is to switch to an online privacy-focused search engine like DuckDuckGo.

6 Use a VPN to hide your browsing history

Your internet service provider (ISP) and web browser — like Google Chrome, Firefox, or Safari — may also collect data on your online activities. This can be used by advertisers, sold to scammers, or even shared with the government (or your work), even if you're using private or incognito mode.

A virtual private network (VPN) encrypts your internet traffic so that no one can track what you do or see where you've been. Using a VPN can also protect you from hackers when using public Wi-Fi networks.

Here's how you can protect your privacy while browsing online:

- Use a VPN when off of your home network. Scammers can intercept your data over public Wi-Fi networks (such as at a coffee shop or airport). Be especially cautious when online shopping and submitting credit card or banking details to websites.

- Use Safe Browsing tools to warn you of fake websites. Some websites are made to steal your personal information. Aura's Safe Browsing tools will warn you if you're on a lookalike or fake website.

- Protect your Wi-Fi password. Your router handles plenty of sensitive information, from passwords to financial information. Anyone with your Wi-Fi password and nefarious intent could try to steal your information.

7 Don't ignore software or operating system updates

Most privacy hacks don't come about from newly-discovered bugs. Instead, they take advantage of known vulnerabilities that have already been fixed — on computers that haven't installed the fix. The owners of the two largest search engines — Google and Bing — also operate the popular browsers Chrome and Edge, respectively. (So, they track a lot of data.)

A 2021 report by Bitdefender showed that unpatched vulnerabilities were among the top reasons why Windows systems were prone to attacks [*].

The first and most crucial step is to set your operating system to install updates automatically. Here's how to set-up autoupdates on:

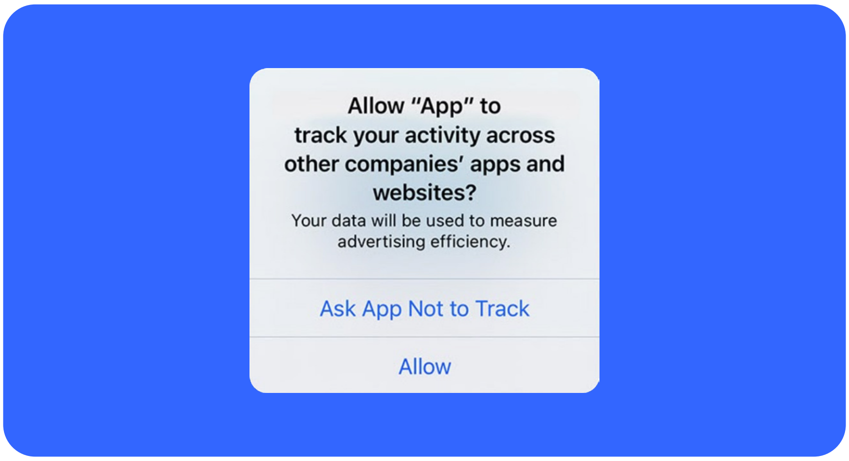
Microsoft Windows   Apple Mac OS   Google ChromeOS

Pro Tip

You can also download antivirus software to protect against malware like spyware, which collects data like credit card information in the background.

8 Use a Privacy Assistant to block ad and data tracking

Most of your personal data collected online isn't for scams or data breaches — it's for marketing. With a few simple steps, you can disable many of these trackers. First, when pop-ups ask if you want to share data, say no.



Allow "App" to track your activity across other companies' apps and websites?

Your data will be used to measure advertising efficiency.

Source: Apple

Whenever possible, decline cookies on websites. If you use an iPhone or other Apple mobile device, iOS versions 14.5+ let you disable cross-app tracking.[62]

Finally, you can disable ad customization across the apps you use, including Google search, other Google services, Apple, Facebook ad settings, third parties that use Facebook data, Twitter (X), Microsoft, and Amazon.

Thousands of other websites use tracking as well, but disabling these larger companies will eliminate the biggest offenders.

9 Use encryption to keep data from prying eyes

You might think computer data, texts, and emails are safe. But you could be wrong. Encryption "scrambles" your data unless you enter a decryption key or password. Encryption can protect your data in case cybercriminals steal your hard drive, intercept your text messages, or trick you into entering information into a fake website.

Here's what to do:

- Encrypt the data on your computer. All modern Apple and Android mobile devices use encryption by default. You can also set up encryption on Windows[63] and Mac[64] so the data will be meaningless to anyone without your password.

- Use messaging apps with end-to-end encryption. WhatsApp, Telegram, or Signal, are the safest messaging options (though WhatsApp still has other privacy concerns).[65] Other methods without encryption, including texts and Facebook's Messenger app, have "back doors" which allow third parties to read what you send. You can add extra privacy protection against email hackers by disabling "smart features and personalization" in Gmail and other Google Apps.

- Protect your Wi-Fi password. Your router handles plenty of sensitive information, from passwords to financial information. Anyone with your Wi-Fi password and nefarious intent could try to steal your information.

- Wipe devices before you sell or recycle them. Delete everything and restore your devices to their factory settings before giving them away.

Pro Tip

Protect your privacy on devices when in public by disabling message previews on your lock screen. If previews show up on your phone's lock screen, a thief can learn who's contacting you and even use two-factor authentication without needing your passcode.

10 Revoke unnecessary third-party app connections

Many modern apps ask to connect to other services to share data or work together. For example, any time you "sign in with Google/Facebook" you allow that tool access to certain data that Google or Facebook has about you.

For both your online privacy and security, it's a good idea to limit the number of third-party app connections you have in place.

Here's how to see which third-party apps are connected to:

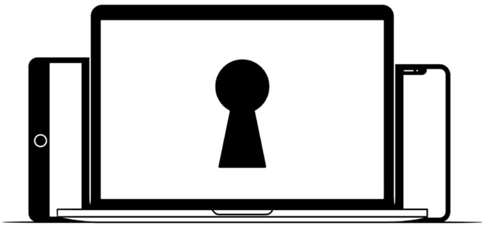
Google

Facebook

Apple (select "Sign in with Apple")

Microsoft

Slack



11 Request that data brokers remove your personal information

Data brokers are services that scrape the internet and public records for your personal information — and then sell it to advertisers, marketers, or even scammers.

While you can request that data brokers remove your information, the honest truth is that there are hundreds of data brokers in the U.S. alone, each with their own process for requesting a data removal. Even worse, sometimes requesting a removal can mean providing even more personal data to these companies.

To remove your personal data from data brokers you have two options:

1. Contact each data broker individually. PrivacyRights.org has a list of data brokers with instructions on how to request that they remove your data.[66] You can go through the list and contact each company separately.

2. Use Aura to automatically remove your data. Aura will scan data broker databases and request that they remove your personal data on your behalf.

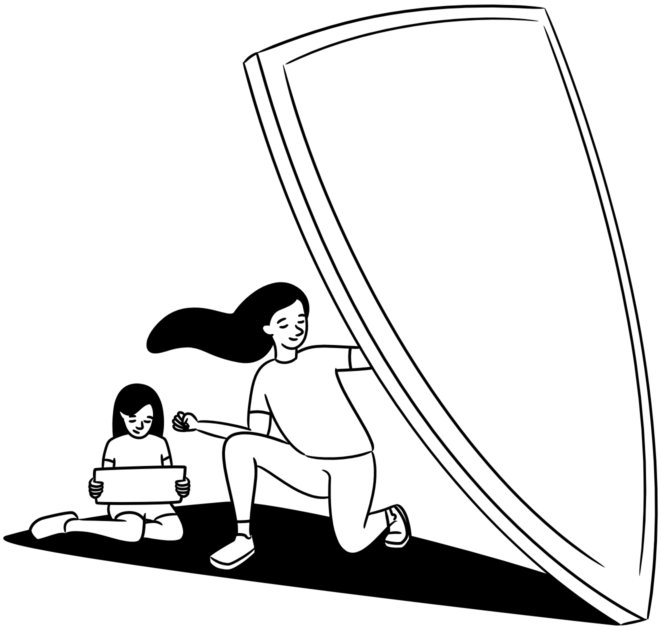
12 Monitor your sensitive information with identity theft protection

No matter how much information you remove from the internet, data leaks happen. When your personal data is available, it puts you at risk of scams, hacking, identity theft, or simply more spam.

If your personal information is leaked or being used fraudulently by scammers, Aura will warn you in near-real time and give you the support and help you need to shut fraudsters down.

Aura's all-in-one identity theft protection solution combines powerful digital security software that protects your devices and data with 24/7 identity, account, and financial monitoring.

Our goal is a world where people have peace of mind that they are protected from scammers, and our mission is to create a safer internet for everyone. Learn more at aura.com.



Sources

[1] Estimated using the latest FBI data on the average cost of home burglary from FBI 2019 Crime in the United States multiplied by 607,415 reports cited in Council on Criminal Justice Year-End 2022 Update Report, cost of Cybercrime from FBI 2022 IC3 Report

[2] Internet Crime Report 2022 - March 22, 2023 | Federal Bureau of Investigations

[3] Internet Crime Report 2021 - March 22, 2022 | Federal Bureau of Investigations

[4] Estimated using the latest FBI data on the average cost of home burglary from FBI 2019 Crime in the United States multiplied by 607,415 reports cited in Council on Criminal Justice Year-End 2022 Update Report, cost of Cybercrime from FBI 2022 IC3 Report

[5] 2022 Connectivity and mobile trends - August 3, 2023 | Deloitte Insights

[6] World Password Day: How to Improve Your Passwords - May 11, 2018 | Dashlane

[7] 2023 ID Theft Crime Statistics and Sentencing

[8] Cybercrime To Cost The World 8 Trillion Annually In 2023 - October 17, 2022, | Cybersecurity Ventures

[9] Cybercrime To Cost The World 8 Trillion Annually In 2023 - October 17, 2022, | Cybersecurity Ventures

[10] Cybercrime To Cost The World 8 Trillion Annually In 2023 - October 17, 2022, | Cybersecurity Ventures

[11] More Americans See Cybercrime as Threat to Future than Global Warming and COVID-19 - Sep 23, 2021 | Aura

[12] Over 22 billion records exposed in 2021 - February 10, 2022 | Security Magazine

[13] Cost of a data breach 2022 | IBM

[14] Cybersecurity Incidents | U.S. Office of Personnel Management

[15] USPS Site Exposed Data on 60 Million Users - November 21, 2018 | Krebs on Security

[16] CFPB Says Staffer Sent 250,000 Consumers' Data to Personal Account - April 19, 2023 | Wall Street Journal
Government breaches - can you trust the U.S. Government with your data? - November 29, 2022 | Comparitech

[17] Government breaches - can you trust the U.S. Government with your data? - November 29, 2022 | Comparitech

[18] 2022 Edelman Trust Barometer

[19] More Americans See Cybercrime as Threat to Future than Global Warming and COVID-19 - September 23, 2021 | Aura

[20] Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents - January 13, 2022 | U.S. Government Accountability Office

[21] China's Hacking Spree Will Have a Decades-Long Fallout - February 2020 | WIRED

[22] Colonial Pipeline Cyber Incident | May 2021 | Energy.gov

[23] One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators - June 8, 2021 | Reuters

[24] Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity - May 14, 2021 | New York Time

[25] 2021 Consumer Aftermath Report, Identity Theft Resource Center

[26] Aura Online Scams and Mental Health Impact Survey Reveals Staggering Effects of "Scam Economy" on American Mental Health and Well-Being - October 2022 | Aura

[27] Consumer Sentinel Databook 2022 | Federal Trade Commission

[28] Aura Online Scams and Mental Health Impact Survey Reveals Staggering Effects of "Scam Economy" on American Mental Health and Well-Being - October 2022 | Aura

[29] Consumer Sentinel Databook 2022 | Federal Trade Commission

[30] SNAP Fraud Alerts - 2023 | U.S. Department of Agriculture Food and Nutrition Service

[31] Consumer Sentinel Network Databook 2022 - February 2023 | Federal Trade Commission

[32] Identity theft causing outsized harm to our troops - May 21, 2022 | Federal Trade Commission

[33] Consumer Sentinel Network Databook 2022 - February 2023 | Federal Trade Commission

[34] Cybercrime Damages $6 Trillion By 2021 - 2017 | Cybersecurity Ventures

[35] Military clearance OPM data breach ‘absolute calamity’ - June 17, 2015 | Navy Times

[36] Cybersecurity Incidents | U.S. Office of Personnel Management

[37] Aura Study Finds Mothers Struggle to Balance Protecting Kids Online and Giving Them Freedom and Privacy - Aura, May 10, 2023

[38] Study identifies basis for sense of trust in older people - December 7, 2012, NIH National Institute on Aging

[39] 2021 IC3 Elder Fraud Report | Federal Bureau of Investigation

[40] 2021 Internet Crime Report | Federal Bureau of Investigation

[41]Project Safe Childhood | U.S. Attorney’s Office, Eastern District of Texas

[42]Deep Dive: FBI estimates 500,000 online predators are a daily threat to kids going online - June 2, 2021 | KOAA News

[43] Child Identity Theft: The Perils of Too Many Screens and Social Media - October 26, 2022 | Javelin Strategy

[44] Preventing Synthetic Identity Theft: A Guide for Parents - February 2023 | Security.org

[45] A Clean Slate for Texas Foster Youth: Policy Recommendations on Preventing and Resolving Identity Theft for Youth in Foster Care, 2018 | Texas A&M School of Law

[46]51 Useful Aging Out of Foster Care Statistics - 2017 National Foster Youth Institute

[47] Colorado looking at more help for former foster care people now among homeless, December 2022, CBS News

[48] Preying on the Vulnerable: Foster Youth Face High Risk of Identity Theft - July 21, 2014 | NBC News

[49] Maryland man loses $38K to “grandparent scam” using replicated voice - CBS Baltimore, April 2023 | CBS News

[50] Florida woman accused of swindling $2.8M from Holocaust survivor in romance scam, January 2023 | NBC News

[51]When Loved Ones Die, Their Identity Is There for the Taking, May 2012 | ABC News

[52] 2022 Annual Data Breach Report - January 25, 2023 | Identity Theft Research Center

[53]Just Why Are So Many Cyber Breaches Due to Human Error? - July 30, 2022 | Security Today

[54] Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations - April 15, 2021 | Cybersecurity & Infrastructure Security Agency

[55]ITRC H1 Data Breach Analysis - https://www.idtheftcenter.org/publication/h1-2023-data-breach-analysis/

[56]https://techcrunch.com/2023/08/04/oregon-health-data-accessed-moveit-ma

[57] The New York Times: A Feature on Zoom Secretly Displayed Data From People’s LinkedIn Profiles (April 2020)

[58] Tech Crunch: Facebook admits it stored ‘hundreds of millions’ of account passwords in plaintext (March 2019)

[59] Federal Trade Commission: Unrollme Inc., In the Matter of (December 2019)

[60] Ars Technica: My browser, the spy: How extensions slurped up browsing histories from 4M users (July 2019)

[61] https://gs.statcounter.com/search-engine-market-share

[62] Vox | Why the new iOS update is such a big deal (April 2021)

[63] Microsoft | Encrypted Hard Drive (June 2023)

[64] Apple | Encrypt Mac data with FileVault

[65] Aura | These 10 WhatsApp Scams Are as Unnerving as They Look (June 2023)

[66] https://privacyrights.org/data-brokers

ĀURA