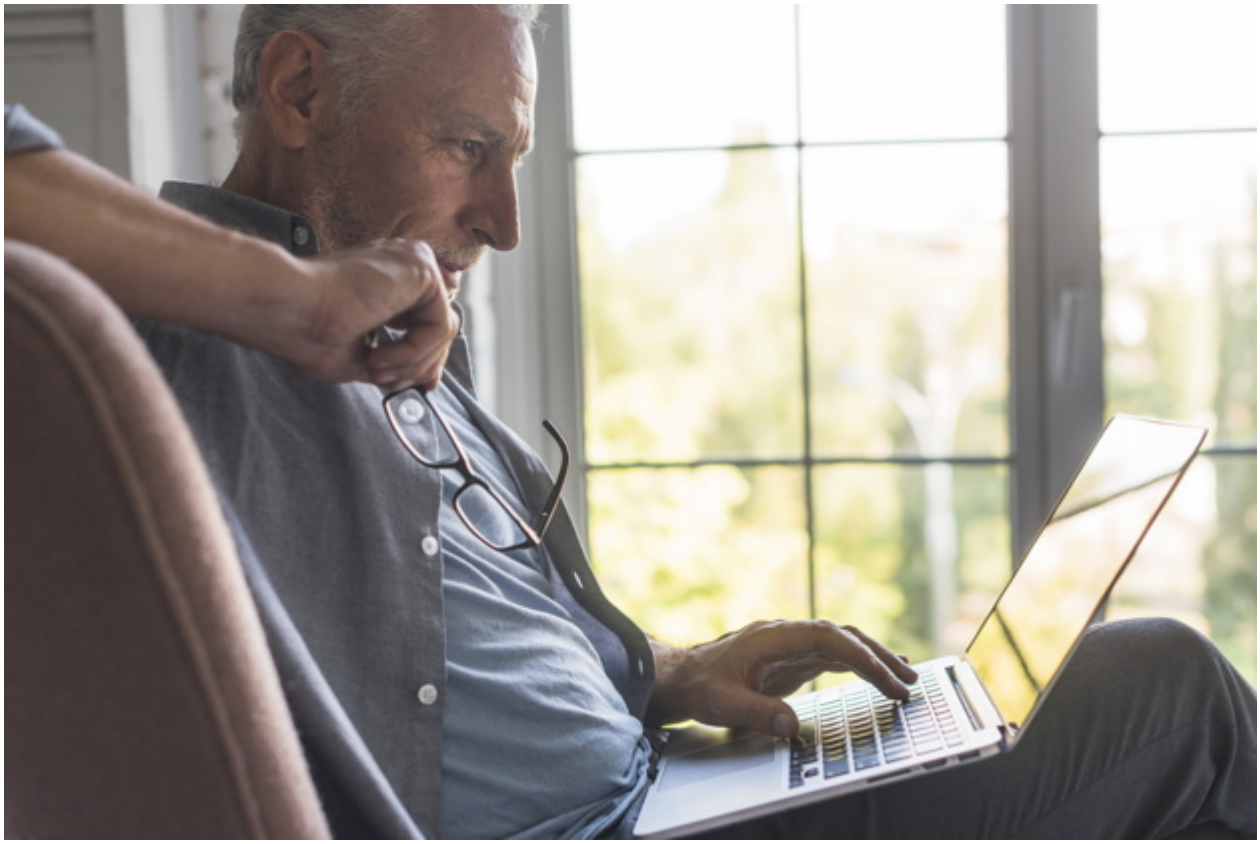


COVID-19: Working From Home And Cybersecurity

According to the FTC's "Consumer Sentinel Network Data Book," the most common categories for fraud complaints last year were imposter scams, debt collection and identity theft. Credit card fraud was most prevalent in identity theft cases — more than 167,000 people reported a fraudulent credit card account was opened with their information.However, as the threat of COVID-19 increases, cybercriminals are targeting Americans who are working from home. The Federal Trade Commission advises consumers to be wary of cybercriminals exploiting coronavirus fears to steal personally identifiable information (PII). Financial information and medical information is especially sensitive right now.

Cybersecurity and COVID-19

Fraudsters are creating scam posts and emails with fake information about COVID-19, according to identity theft protection provider IdentityForce. There is also an increased number of hackers creating malicious websites that spoof legitimate public health resources.

For example, a link can seem like it should lead you to a map of "COVID-19 cases near me" might actually infect your phone or computer with spyware or ransomware. Remember to visit the Center for Disease Control (www.cdc.gov) or World Health Organization (www.who.int) for accurate, safe information about coronavirus trends and statistics.

According to IdentityForce, increasingly common COVID-19 scams so far in 2020 include:

- Fraudulent e-commerce vendors for masks, sanitizers and test kits
- Fraudulent investment sites
- Phishing and vishing through update emails, texts and voicemails
- Spoofed government and health organization communications
- Fake vaccines or “miracle cures”
- Scam employment posts
- Phony charity donation offers

5 cybersecurity tips for working from home

Since so many Americans are settling into their work-from-home routines, we asked ConsumerAffairs’ Information Security team for some tips to stay safe online.

For more on how to keep your devices safe while social distancing or sheltering in place, ConsumerAffairs’ Information Security team recommends visiting sans.org and staysafeonline.org.

Secure your home network: Strong passwords and encryption are the best ways to secure your home network. Change your default administrator password before a hacker discovers the manufacturer’s default. Use WPA2 or WPA3 encryption so hackers can’t read information you send. For more guidance, read about securing your wireless network.

Limit access to your work device: Avoid giving anyone an opportunity to view confidential material without your authorization. Be sure to shut down or lock your work computer when you aren’t around. It’s too easy for friends and family to erase, modify or infect information on your device accidentally.

Careful where you click: Always hover over links before you click to make sure the hyperlink is the same as the link-to address. Be extra cautious about emails from unknown people — especially if they seem random, illogical or threatening.

Be skeptical of job offers: Cybercriminals use bogus employment posts to trick people into money laundering schemes (“money mules”) and collect their PII or financial information. Remote freelancers could be especially vulnerable.

Protect your devices: If you haven’t already, make sure that your anti-virus and anti-malware software is up to date.

Identity theft trends in 2019

In the next year, the Identity Theft Resource Center (ITRC) predicts identity theft protection services will primarily focus on data breaches, data abuse and data privacy. ITRC also predicts that consumers will become more knowledgeable about how data breaches work and expect companies to provide more information about the specific types of data breached and demand more transparency in general in data breach reports.

Cyber attacks are more ambitious

According to a 2019 Internet Security Threat Report by Symantec, cybercriminals are diversifying their

targets and using stealthier methods to commit identity theft and fraud. Cybercrime groups like Mealybug, Gallmaker and Necurs are opting for off-the-shelf tools and operating system features such as PowerShell to attack targets.

- Supply chain attacks are up 78%
- Malicious PowerShell scripts have increased by 1,000%
- Microsoft Office files make up 48% of malicious email attachments

Internet of Things threats on the rise

Cybercriminals attack IoT devices an average of 5,233 times per month. Routers and connected cameras were the main targets of IoT attacks in 2018, accounting for about 90% of activity. IoT attacks involving connected cameras increased by about 12% in the last year as well.

- According to Symantec, cybercriminals most often access IoT devices by using the passwords: 123456, [BLANK], system, sh, shell, admin, 1234, password, enable and 12345.

Formjacking is up 117%

More than 57,600 unique websites were compromised by formjacking in 2018, and cybercriminals continue to take in millions each month by hijacking credit card data from online payment forms.

Ransomware activity is down 20%

Ransomware attacks decreased last year for the first time since 2013 — identity theft experts suspect this is because ransomware attacks target Windows-based applications and more people are storing and sharing data using the cloud. Ransomware threats remain a risk for businesses, as enterprise ransomware has increased by 12%.

New account fraud is up 13%

In 2018, new account fraud accounted for $3.4 billion in losses, up from $3 billion in 2017, according to Javelin Strategy. The most common targets for new account fraud are mortgages, student loans, car loans and credit cards.

Account takeovers are up 79%

The number of account takeovers also increased, rising from 380,000 in 2017 to 679,000 in 2018. Both individuals and enterprises are at risk for account takeovers.

Increased effort to solve the year 2038 problem

Similar to the Y2K problem, the 2038 problem is a bug that will affect the way computers store time-stamps. Computer logic defines time-stamps with the current date and time, minus the number of seconds that have passed since January 1, 1970, when computers originated. In 2038, the number of elapsed seconds will exceed the information that can be stored in a four-byte data type, meaning most computers will need an extra byte to preserve their timing systems.

- The 2038 problem will be a logistical nightmare to solve and could affect databases and make private information public. Without a resolution, hackers will likely search for ways to exploit this bug.

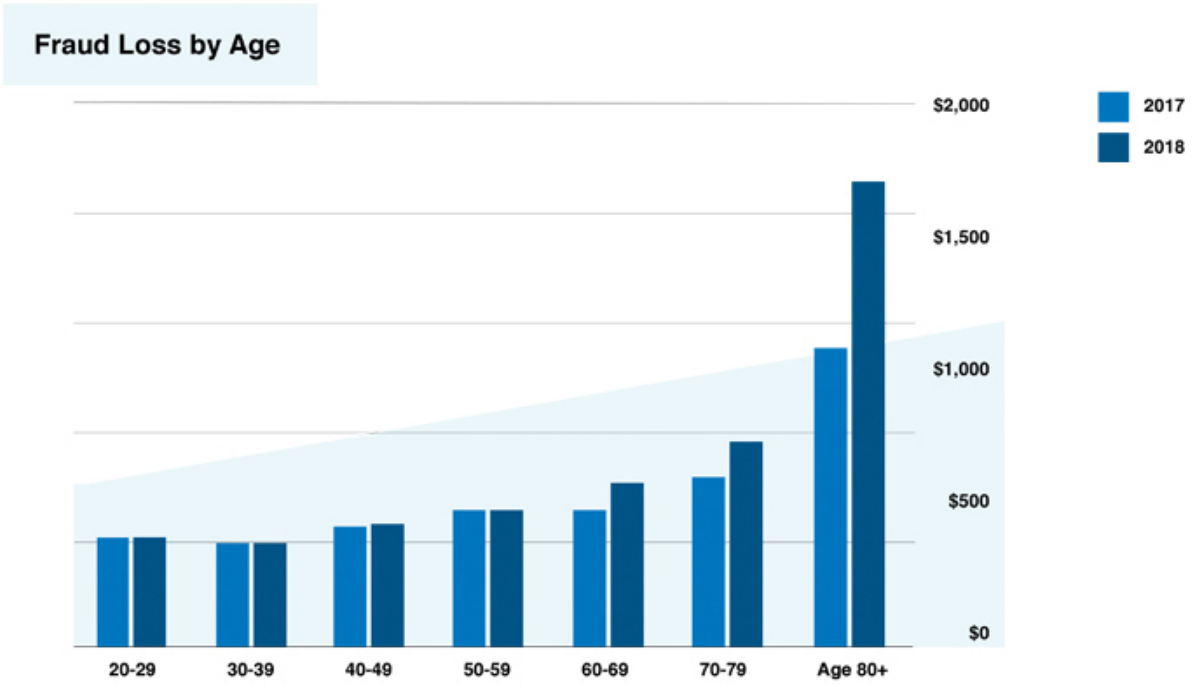
Who is most at risk for identity theft?

Most identity thefts are crimes of opportunity. Identity thieves often target those who don't regularly check for identity theft warning signs and are unlikely to report irregular activity on their credit reports.

Children and seniors

Everyone with a Social Security number is at risk for identity theft, but two demographics are targeted aggressively and often: the very young and the very old.

- Children are targeted because identity thieves can use a child's Social Security numbers to establish a fraudulent "clean slate." Identity theft experts recommend parents monitor their children's credit reports to check for identity theft as often as their own.
- Seniors are targeted most often over the telephone and through internet phishing scams. Some studies suggest that people become more trusting as they age, which explains why it's more difficult for older adults to detect fraudsters.



Younger adults lose money to fraud more often, but when older people experience a fraud-related financial loss, the median amount is much higher, according to the Federal Trade Commission.

Members of the military

While deployed, active duty members of the armed services are particularly vulnerable to identity theft because they may not notice mistakes on their credit reports or receive calls from debt collectors regarding a fraudulent charge. According to FTC reports, military consumers are most affected by credit card and bank fraud.

- 2018 total military consumer credit card fraud reports: **10,590**
- 2018 total military consumer bank fraud reports: **5,723**
- Military consumers' reports of employment or tax-related fraud increased by 85% between 2017 and 2018.
- Military members are also increasingly affected by loan or lease fraud.

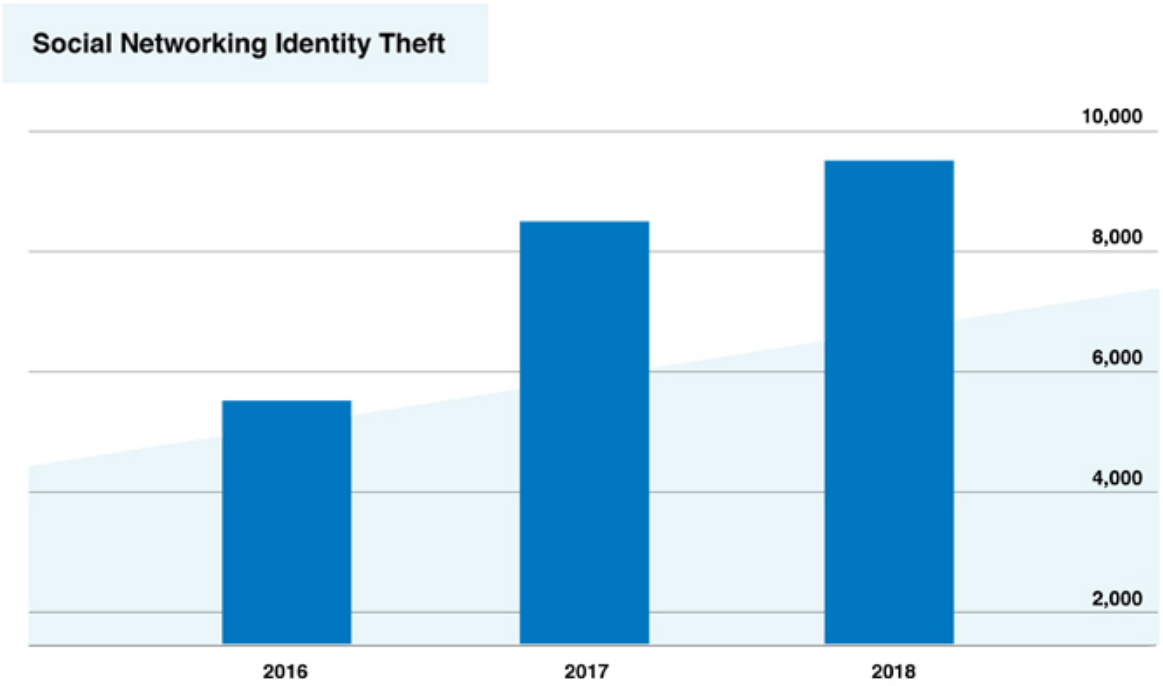
2018 Military consumer loan or lease fraud reports

Fraud type	Total reports	% Difference from previous year
Business/personal loan	1,168	+19%
Auto loan/lease	832	+40%
Real estate loan	385	+36%
Apartment or house rented	380	+79%
Non-federal student loan	257	+18%
Federal student loan	192	+22%

Social media users

It's relatively easy for cybercriminals to discover a person's name, date of birth, phone number, hometown and other sensitive information through social media and networking sites. With this information, an identity thief can target victims for phishing and imposter scams.

- Last year, the FTC processed 9,439 email or social media identity theft reports, a 23% increase from 2017.



According to the FTC, identity theft reports involving social networking are increasing.

Repeat victims

People who have previously been affected by identity theft are at a greater risk for future identity theft and fraud. According to the Center for Victim Research, 7-10% of the U.S. population are victims of identity fraud each year, and 21% of those experience multiple incidents of identity fraud.

For more information about how victims of identity theft can protect themselves from future fraud, read about the identity theft recovery process.

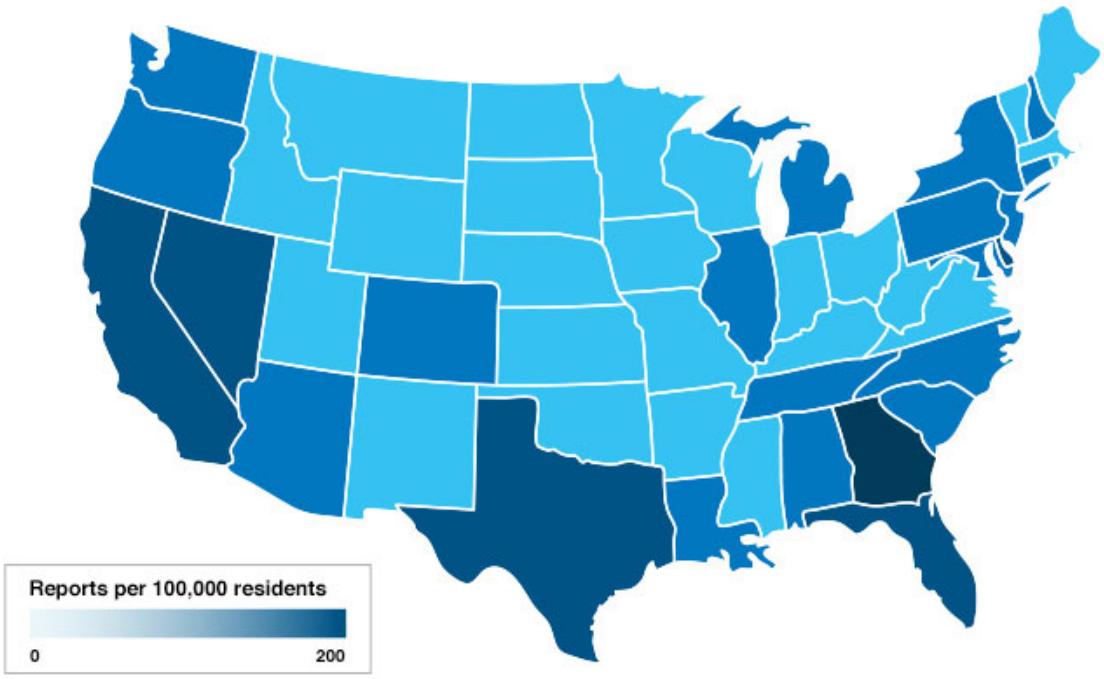
The deceased

Identity thieves can target the recently departed with information gleaned from public obituaries and access the deceased Social Security number through the Social Security Administration's Master Death File. Stealing a dead person's identity is commonly referred to as "ghosting." Ghosting often goes unnoticed by surviving family for months or years.

- Deceased identities stolen per year: **2.5 million**

Where is identity theft most common?

The Federal Trade Commission collects reports from consumers on a range of marketplace experiences and stores them in a secure online database. FTC Data Book statistics also include reports from other organizations, including federal, state, local and international law enforcement agencies. Out of 3 million reports last year, 15% are related to identity theft.



According to the Federal Trade Commission in 2019, Georgia has the highest percentage of identity theft reports per capita, and California has the highest total number of reports.

Identity theft statistics by state

Rank & State	Reports per 100,000	Total reports
1. Georgia	229	23,871

2. Nevada	194	5,816
3. California	186	73,668
4. Florida	180	37,797
5. Texas	159	45,030
6. Delaware	158	1,517
7. Maryland	145	8,747
8. Michigan	140	13,952
9. Illinois	127	16,296
10. Arizona	126	8,853
11. South Carolina	126	6,339
12. New Jersey	125	11,273
13. New York	122	24,248
14. New Hampshire	117	1,565
15. North Carolina	112	11,481
16. Louisiana	111	5,202
17. Colorado	110	6,151
18. Connecticut	108	3,864
19. Alabama	108	5,241
20. Pennsylvania	107	13,725
21. Tennessee	101	6,808
22. Oregon	101	4,179
23. Washington	100	7,380
24. Mississippi	97	2,894
25. Virginia	97	8,196
26. New Mexico	96	2,000
27. Utah	94	2,915
28. Rhode Island	93	990
29. Massachusetts	93	6,387
30. Ohio	88	10,268
31. Missouri	85	5,222
32. Idaho	80	1,368
33. Oklahoma	79	3,109
34. Montana	76	799
35. Indiana	74	4,918
36. Kansas	74	2,142
37. Arkansas	73	2,197
38. Minnesota	73	4,070
39. Hawaii	73	1,021
40. Alaska	69	507
41. Nebraska	67	1,281
42. Wisconsin	64	3,731
43. North Dakota	63	474
44. Wyoming	58	338
45. West Virginia	58	1,051
46. Kentucky	57	2,522
47. South Dakota	56	744
48. Maine	56	744
49. Iowa	53	1,654

50. Vermont	51	316
Washington, D.C.	167	1,156
Puerto Rico	51	1,710

Top 10 metropolitan statistical areas for identity theft reports

Rank & MSA	Reports per 100,000	Total reports
1. Macon-Bibb County, GA	321	738
2. Columbus, GA-AL	308	950
3. Atlanta-Sandy Springs-Roswell, GA	292	16,902
4. Warner Robins, GA	280	532
5. Miami-Fort Lauderdale-West Palm Beach, FL	274	16,617
6. Los Angeles-Long Beach-Anaheim, CA	258	34,334
7. Las Vegas-Henderson-Paradise, NV	232	5,005
8. Dallas-Fort Worth-Arlington, TX	226	16,334
9. Memphis, TN-MS-AR	218	2,929
10. Bakersfield, CA	208	1,841

Identity theft terms

The better consumers understand identity theft, the more equipped they are to protect themselves. Our identity theft glossary below is regularly updated to include the most recent identity theft terms that are in the news.

- **Account takeover:** An account takeover is when a fraudster uses personal information to obtain products and services. Credit card fraud is the most rampant, but skimming and phishing are also common types of account takeovers.
- **Anti-virus:** Anti-virus software runs continuously in the background of a computer and scans for viruses, worms and malware every time the user accesses a website or downloads anything.
- **Bait and switch:** A bait and switch attack is when a hacker buys advertising space on a webpage and then links the advertisement to a page infected with malware.
- **Black hat hacker:** All hackers are capable of compromising computer systems and creating malware, but black hat hackers use these skills to commit cybercrimes.
- **Blockchain:** A blockchain is of a string of time-stamped digital records shared between multiple computers. If the data in one block changes, all subsequent blocks in the blockchain reflect the alteration and become invalid. Blockchains help prevent identity theft and fraud by making it difficult to tamper with the data in a block.
- **Bot:** Short for “robot,” a bot is an autonomous program that interacts with computer systems in a way that appears or attempts to appear human. Hackers can use bots to mine for usernames and passwords used to commit identity fraud.
- **Cookie theft:** Cookie theft is when a cybercriminal makes copies of unencrypted session data and then uses that data to impersonate someone else.
- **Credential cracking:** Credential cracking describes the various methods — word lists, guessing and brute-force — cybercriminals use to obtain passwords. Credential cracking threats are why it’s important to create varied and complicated passwords for all accounts.

- **Criminal impersonation:** Someone commits criminal impersonation when they assume a fake or false identity, usually for political or financial gain.
- **Cybersquatting:** Also sometimes called domain squatting, cybersquatting is when a domain name is stolen or misspelled to attract users for exploitation or profit.
- **Cryptovirology:** Cryptovirology is the study of how cryptology is used to create dangerous malware.
- **Data breach:** A data breach is when private or confidential information is released to an untrusted environment. Cybercriminals can infiltrate a data source physically or remotely bypass network security to expose passwords, banking and credit data, passport and Social Security numbers, medical records and more.
- **Dark web:** The dark web is the part of the internet that can only be accessed through Tor browser software, which keeps visitors anonymous and untraceable. It's not illegal to be on the dark web, but many illegal transactions occur on the dark web (such as buying credit card or Social Security numbers).
- **Deep web:** The deep web is the part of the internet that's not accessible through standard search engines such as Google or Bing. Password-protected and dynamic pages, encrypted networks and the dark web are all part of the deep web.
- **Encryption:** Encryption is a way to scrambled data using computer algorithms to prevent unauthorized access to data or sensitive information.
- **Firewall:** In computing, a firewall is a software program that blocks unauthorized users from getting in without restricting outward communication.
- **Formjacking:** Formjacking is when a hacker infiltrates an e-commerce checkout page to steal credit card information. Similar to an ATM skimmer for the internet age.
- **Ghosting:** In the context of identity theft, ghosting refers to when someone steals the identity of a dead person.
- **Grey hat hacker:** Grey hat hackers' ethics are somewhere between black and white hat hackers. Grey hat hacking involves illegal cyberactivity, but the hacker often reports vulnerabilities to the system's owner and requests a fee in exchange for the information — if a system's owner does not comply with their request, the grey hat hacker usually exploits the newly discovered cybersecurity vulnerability.
- **Honeypot:** A honeypot is a decoy target used to mitigate cybersecurity risks or get more information about how cybercriminals work.
- **Identity cloning:** Identity cloning is a type of identity theft in which a fraudster assumes someone else's identity and attempts to live under that assumed identity.
- **Identity score:** Similar to a credit score, an identity score is a system that gauges an individual's data for legitimacy.
- **Imposter scam:** Imposter scams involve a fraudster posing as a different person for financial or political gain. Usually, the imposter tricks others into giving them money through email, over the phone or via online dating services.
- **Internet of Things:** The Internet of Things, or IoT, describes the interconnectedness of all devices that access WiFi, including cell phones, cameras, headphones and an increasing number of other objects, including washing machines and thermostats.
- **Keylogger:** A keylogger is a computer program that records a person's keystrokes to obtain confidential data.
- **Malware:** A portmanteau of "malicious" and "software," malware describes any software created with the specific intent to cause disruption or damage. Trojans, bots, spyware, worms and viruses are all types of malware.

- **Passive attacks:** Any network attack where the system is monitored or scanned for vulnerabilities is considered "passive attack" because the targeted data isn't modified or damaged.
- **Pharming:** Sometimes called "phishing without a lure," pharming is a type of scam where malicious code is installed onto a device or server to misdirect users onto illegitimate websites.
- **Phishing:** Phishing is a popular type of internet scam in which fraudsters send emails claiming to be from a reputable company to trick individuals into revealing personal information. Phishing attacks decreased from 1 in 2,995 emails in 2017 to 1 in 3,207 emails in 2018.
- **Physical identity theft:** Unlike wireless identity theft, physical identity theft requires an identity thief to be in close proximity to their target. Examples of physical identity theft include stealing a wallet or computer, dumpster diving and postal mail theft.
- **Proxy server:** A proxy server establishes a substitute IP (Internet Protocol) address identity. When you connect online, your computer's IP address is transmitted to websites and establishes your location and may give other identifying details. Proxy servers allow users to connect to the internet anonymously and bypass blocked or restricted websites.
- **PowerShell:** An automated task framework by Microsoft, PowerShell can be embedded in applications to automate batch processing and systems management tools.
- **Ransomware:** Ransomware is a type of malware that threatens to expose or block an individual's or business' data unless a ransom is paid.
- **SIM swap scam:** Sometimes called a port-out scam or SIM splitting, a SIM swap scam is a complex type cell phone fraud that exploits two-factor authentication to access data stored on someone's cell phone. Put simply, if a fraudster has your phone number, they can call your phone company and ask to have the number transferred to "your" new phone. The fraudster then has access to all of your accounts that use two-factor authentication.
- **Skimming:** Skimming is a type of credit card fraud in which the victim's account numbers are copied and transferred to a counterfeit card.
- **Smishing:** Similar to phishing, smishing (or SMS phishing) is when someone attempts to mine sensitive information under a fake identity through text messages.
- **Sockpuppet:** Sockpuppetting is when a person assumes a false identity on the internet for the purpose of deception.
- **Spoofing:** A spoofing attack is when an illegitimate website falsifies data to appear as a trustworthy website to visitors.
- **Spyware:** Spyware is any software designed to gather data from an individual or enterprise. The four primary types of spyware are adware, Trojan horses, tracking cookies and system monitors.
- **Synthetic identity theft:** Synthetic identity theft is when a criminal combines stolen and fake information to create a new, fraudulent identity.
- **System monitor:** Much like it sounds, a system monitor is an application that surveils computer activity. System monitors usually run unnoticed and can record passwords, chats and emails, websites visited and other sensitive or identifying data.
- **Tracking cookie:** Websites use tracking cookies to gather and share data from their visitors. Unlike malware, tracking cookies won't damage computer systems, but they can create privacy concerns.
- **Trojan horse:** Like its classical namesake, a Trojan horse is a type of malware disguised to appear like safe software. Cybercriminals use Trojans to access sensitive data and gain access to private systems.

- **Waterhole attack:** A waterhole attack occurs when a hacker targets a specific group or community. The hacker infects an individual within the targeted group with malware in an attempt to infect the entire group.
- **Wireless identity theft:** Also sometimes called contactless identity theft or RFID identity theft, wireless identity theft is committed by wireless mechanics. Examples of wireless identity theft include phishing and spoofing.
- **Whaling:** Whaling is a phishing attack that targets high-level employees within a company to steal confidential information or sensitive data.
- **White hat hacker:** Unlike a black hat hacker, a white hat hacker uses their ability to break computer networks or bypass security protocols for good rather than evil. White hat hackers are often employed by governments or companies to perform vulnerability assessments.
- **Worm:** A worm is a type of malware that self-replicates and spreads from computer to computer.
- **Virus:** Similar to worms, viruses make copies of themselves. The main difference between viruses and worms is that viruses require a host program to spread.
- **Vishing:** Like phishing or smishing, vishing is when an identity thief attempts to gain sensitive information over the phone.
- **Zero-day exploit:** A zero-day exploit is when cybercriminals target a software the same day weakness in that software is discovered and before a patch can be released to fix the vulnerability.

Bottom line

Anyone with a Social Security number can be the subject of identity theft, but the most common victims are children, seniors, members of the military and social media users. People who regularly check for identity theft warning signs, such as strange credit card charges or new accounts opened in their name without their consent, are less likely to have their information compromised. If you think you're a victim of identity fraud, work with the Federal Trade Commission to restore your accounts and get on the road to recovery.