101 Ways Your Identity Can Be Stolen and Exploited

4-25-2017

Source: https://www.acuantcorp.com/101-ways-your-identity-can-be-stolen-and-exploited/

1. Using your social security number to get insurance
Some crooks obtain your social security number or other private information over the phone posing as someone from your insurance company, and then they use it for themselves.

2. Stealing identifying information from your license
If someone has your driver's license information, they don't even need your physical license to cause all kinds of trouble.

3. Identity fraud for property purchase
A theft could use your identity and social security number to apply for a rental property or to purchase a house.

4. Creating a new identity
Some criminals use others' identities to stay off the grid or because they need a new identity.

5. Using a child's identity
Thefts target children's identities because it often takes a lot of time until the crime is discovered, giving the theft plenty of time to use the child's identity for opening up lines of credit as issuers do not authenticate the age of every applicant being processed.

6. Stealing from your mailbox
Often people get credit card and loan offers in the mail. A criminal could steal these, fill them out using your private information, and use a different address then your own so they don't get any notices.

7. Phishing emails
Phishers target the elderly especially with this technique, as they tend to respond with their information.

8. Nigerian letter scheme, or 419 fraud
This common scam combines an advance fee scheme, where thieves get people to send money and checks, and try to gain access to your bank account.

9. Telemarketing calls
Sometimes you may get a call from some organization or department that seem legitimate and for a good cause. If you feel the need to donate, find the organization's number online and call that directly to assure yourself you are dealing with the organization itself, not a scammer that is pretending to work for them.

10. Sharing your vacation pictures while you're away
Everyone loves to show off their vacation pictures on social networks these days. What you may not think of is that criminals can lurk online seeing that you are away and that your house could be left unattended.

11. Sharing sensitive information on social media
As you update your family and friends with your daily whereabouts, criminals could also see this to learn your schedule. They can figure out when you tend to be away from your home to stage a break-in.

12. Stolen cellular phones
If you have private information like online passwords and any financial information on your phone and it gets stolen, the theft could use this to access your accounts and go on a spending spree. Call your phone company right away to see if they can locate it or to wipe the phone's data remotely.

13. Using your debit card for online shopping
Don't ever use your debit card to shop online because, unlike credit cards, you are not backed by a credit card company for any fraudulent charges.

14. Going through your trash
Whenever you throw out personal information, you should always use a shredder.

15. Changing your mailing address
Changing your mail to another address is easy if you have enough of the suspect's information to do so. You can do it pretty simply online, and mail is sent to the current address to verify the change that a thief can easily intercept – so you are unaware of the change for at least a few days.

16. Illegally tapping into your computer
Any expert hacker can easily hack into your computer, especially if they have your IP address. Doing so will get them access to all of your personal documents, and if you use a password manager, they could find out all of your account login information as well.

17. Having weak wireless security
If you use Wi-Fi at home, which about 58% of American households use according to Strategy Analytics, you should use some form of security and password to keep others out.

18. Using public Wi-Fi
Never do any online shopping or anything personal when you are connected to a public Wi-Fi.

19. Weak passwords
Using weak passwords online and on your computers that are short and don't include numbers or special characters can be easily hacked.

20. Keeping your social security card in your wallet
If your wallet is lost or stolen, you don't want just anyone to have access to this. Always keep your social security card stored in a safe place.

21. Credit card skimming
Thieves can use credit card skimming devices at gas stations, ATMs, and restaurants to make a copy of your credit card, so be sure you know how to spot a skimmer device.

22. Responding to or downloading attachments from spam
Spam e-mails are getting better at reaching your inbox and looking legitimate, but if there is anything that seems fishy from an e-mail, then don't open or respond to it. If you don't know the sender then never open the attachment. Spammers can send from any e-mail address, so don't think an email is safe even if it looks like it is from a reputable source.

23. Never checking your credit
You should have alerts set up with a financial institution in case your credit scores changes due to someone else using your identity and financial accounts to make purchases or open new credit cards.

24. Accessing fake credit card sites
It isn't hard these days to create a legitimate-looking credit card website to fool others into filling out their personal information to apply for a credit card.

25. Going on fake financial or utility websites
A lot of phishing emails look like they are coming from your bank or from PayPal, when really they are just a scam to "update your account information" on a site that is cloned just like the real site.

26. ATM watchers
Thieves set up cameras at ATM machines to watch you enter your PIN number and gather any other identifying information.

27. ATM overlays
Overlays are devices placed over the keypad of an ATM, typically designed to look just like the original keypad. These capture your PIN number, and work with other technology such as skimmers and cameras, to catch your data.

28. Grocery store PIN thieves
Just like with ATM machines, people could overlook you entering your PIN number when you use your debit card at checkout lines.

29. Downloading torrents
Torrent files can be full of malware and viruses that can be used to access your computer and files to be used to steal your identity.

30. Falling for "free" offers, like vacations, gifts, and prizes
Anytime you're offered a luxury item or trip for free, but you're being pressured to sign up now because the contest is almost over, be wary. Identity thieves use urgency to get people to make decisions they wouldn't normally make.

31. Soliciting credit card information by phone
Giving your credit card over the phone from a number you did not yourself call, even if it sounds like a legitimate company, is an easy way for it to end up in the wrong hands.

32. Overusing your SSN for medical identification
When you overuse your social security number for medical identification, your Medicare card becomes vulnerable.

33. Sharing of private data on hacker networks
Hacker networks gather password and authentication information, and often share that information with other hackers or sell it.

34. Bulk gathering of IDs via black market
Major data breaches often collect large numbers of IDs. When this happens, the identification information is often traded and sold on the black market.

35. Failing to destroy old hard drives and computers
Don't just throw them out or sell them on Craigslist. If you sell your computer, also take out the hard drive and replace it with a new one.

36. Stealing your electricity
This is also known as electricity theft or energy theft. Utility theft occurs when individuals bypass energy meters, tapping power lines, and more in order to steal electricity.

37. Job thieving
Undocumented workers or individuals with a criminal history will often use another individual's identification information to obtain employment.

38. Social engineering
Typically, when a swindler knows enough legitimate information about an individual to make themselves seem trustworthy and deceive the victim into divulging sensitive information.

39. Vishing, or "voice fishing"
Voice fishing is a type of scam that involves a phone call or robo-call to get you to call back a legitimate organization, like a government agency. They fake an emergency, or claim that you've won a prize, in order to get that coveted SSN or credit card number.

40. Baiting by pretexting
Often, criminals will do an extensive amount of research on an individual beforehand to scam them into believing they are a legitimate business. They call on the phone collecting your name, address, and phone number, and use this to seek even more information.

41. Man-in-the-middle attack
Criminals intercept information between two individuals, record it, and use the information to steal an individual's identity.

42. Pharming
Pharming occurs when hackers reroute individuals from the desired URL to an impostor website, and get them to reveal credit card and other identity information.

43. Malware-based phishing
This uses harmful computer programs that look like helpful ones, such as anti-virus, and use screen loggers to capture sensitive data.

44. Corporate data breaches
When hackers breach bank or shopping data from a large company, thousands of people can be put at risk for identity theft.

45. Keystroke logging
Keystroke loggers capture every key that you type into a computer, allowing data thieves to retrieve your passwords and even sensitive messages.

46. Rootkits
Rootkits are a class of malicious software that allows programs to run in stealth, without the detection on a computer, in order to have privileged access to the information the computer stores.

47. Scam texting—SMiShing
Thieves send extremely urgent-sounding text messages posing as a trusted organization, and get your information when you click on a link in the message.

48. Viruses and worms
The installation of a virus on your computer can allow hackers to gather your information such as names, dates of birth, and of course, social security, and bank account numbers.

49. False claims for refunds from the IRS
Thieves often steal identity information in order to file multiple claims with the IRS.

50. Passport thieves
Take care of your passport when you're on vacation. This important means of identification in America is often stolen and used as a form of identification by thieves.

51. Publicly listing your hobbies, memberships, and employer
The beginning of an identity thief's search usually involves personal information. Why? People are more likely to respond to requests for information from affiliations and groups they might be a part of. Not being aware of how this information can be manipulated is dangerous.

52. Driver's license theft
Your driver's license is unique to you. Using it, an individual can pretend they're you at traffic stops and more. Even just your driver's license number can be leverage enough.

53. Using your mother's maiden name
This question is often asked as verification when, for instance, your password is forgotten. Simply by learning your mother's maiden name, an identity thief now has a key detail about you that can be used to pretend they're you to get into your bank account.

54. Defrauding banks
Identity theft and bank fraud go hand in hand for obvious reasons. Thieves use personal information and even create fake checks and IDs in order to steal millions of dollars from individuals' accounts at financial institutions. These instances are unfortunately on the rise.

55. Impersonating missing children
This frightening scenario has happened more than once. Individuals can use information about missing children in order to con friends and even family members to believe they've returned after years.

56. Fake being a financial adviser for the famous
An identity thief was able to get enough information on famous people like Stephen Spielberg to successfully pose as their financial adviser—and then stole from their bank accounts.

57. Stealing the identity of a missing person
As strange as it sounds, this has happened, as recently as 2008. A high school dropout used the identity of a woman who had disappeared eight years prior to gain admission to two Ivy League schools. In a related turn, many college students who apply for credit cards and loans for the first time find that their identities had been stolen years prior.

58. Faking one's own death
Identity thieves have been known to fake their own death in order to assume the identity of another individual with a clean record.

59. Synthetic identity theft
This form of identity theft is particularly malicious and complicated. Thieves combine stolen information (for instance, a social security number) and combine it with other real and fake information to create a "new," synthetic identity which can be used to obtain new credit cards and take out loans. These crimes can go on undetected for years.

60. Having a publicly listed number
Pay a little extra to get your number privately listed so that telemarketers can't call you, which lowers your chances of getting into a scam.

61. Keeping credit cards, checks, and bank statements in your car

If your car were to get broken into, all of your private financial information would be at thieves' fingertips.

62. Not using a safe at home
Play it safe in case your home is ever broken into by keeping anything confidential in a safe.

63. Not using a security service
Services like Life Lock have a $1 million guarantee to protect your identity.

64. Not freezing your credit card accounts
Credit report agencies can freeze your accounts so that no one else can open up an account or take out a loan in your name until you unfreeze it. If you don't freeze your account after a suspected breach, more of your data is susceptible to theft.

65. Leaving receipts behind
Always take your receipts with you, even if they only display the last few digits of your card.

66. Not writing "check ID or license" on the back of your cards
Do this instead of signing your signature so cashiers always check your photo ID to verify it is you using your card.

67. Failing to consider one-off credit cards
If you aren't a frequent online shopper or you really want to be safe, you can get one-time use credit cards for online shopping.

68. Shopping on un-trusted websites
Look for https in the URL to be sure the site is secure. Also, look for the Trust e-symbol, or PayPal or Better Business Bureau stamps.

69. Not having anti-virus software on your PC
Install anti-virus software as well as anti-spyware to monitor your system for viruses and hacking attempts.

70. Using the same passwords online
Sure, it's easier to remember them, but then it's easier for a hacker to access all of your accounts.

71. Never changing your passwords
You should change all of your passwords every few months or at least once a year.

72. Logging into accounts on public computers
While they are easier for hackers to access public networks, you may also forget to log out.

73. Putting checks in the mail
Put your checks in a piece of paper inside an envelope or a non-see through envelope so they can't be seen through lights.

74. Leaving bills at your mailbox for pick-up
Always deliver your bills personally to the post office.

75. Moving out
Make sure to call all of your credit card companies, utilities, creditors, your bank, the IRS and any other financial institution when you change your address.

76. Not opting out of credit card offers

Go to optoutprescreen.com to opt-out of pre-approved credit card offers and other junk mail.

77. Not using online billing options
If there is an option for online billing, sign up for it. No more chances for lost mail.

78. Using unsafe mailboxes
If you live in an apartment complex where others can possibly access your mail, open up a P.O. box.

79. Forgetting to check links online
Hover over a link before clicking on it. Doing so shows a preview in the lower left corner of your browser so you know the site you will be visiting. Look out for pages that redirect to others.

80. Accepting strange friend requests
It's just not worth getting your Facebook friends up to 1000 if you have some people who you really aren't sure who they are… even if you have mutual friends.

81. Not wiping your phone
Have an app in case your phone gets stolen that you can remotely clean all of your data. Also do this before selling a phone.

82. Using one email account for everything
Use a different email account for your bank, financial accounts, and social networks. If one is hacked then they don't have access to all of your other accounts.

83. Thinking Macs are impenetrable
While it is more difficult for malware, viruses, and hacks on Macs, it is not impossible.

84. Storing credit card information for later use
Even if it is a store you recognize or shop at a lot, take the time to type credit card information in every time instead of storing it. We've seen that even the biggest stores online can have their data breached.

85. Not using two-step verification if available
For sites like Gmail that offer a second step to verify your account, which is a code that is sent to your phone by text message. If a hacker figures out your password, they will be stuck in the second step of verification.

86. Not changing your home locks and using a "do not duplicate" label on your keys
If someone "borrows" your keys they can very easily go make copies if those keys are without a "do not duplicate" label.

87. Not using a lock on your phone or tablet
Always lock your devices with a code, password, or swipe sequence.

88. Using camera phones
When you're in a situation that requires identifying information to be displayed, whether at the bank, the store, or the gas station; be wary of your surroundings. The ubiquity of camera phones means, even if you're quick, vital information about you can be stolen and stored.

89. Pickpocketing
The old school way of stealing your identity by taking your wallet or phone to get your information is alive and well.

90. Ordering unauthorized credit reports by posing as a landlord
Someone could pretend to be a landlord to run your credit report.

91. RFID scanners
Wireless technology used in some credit and debit cards to allow contactless payments, but thieves can use a RFID scanner if they get close enough to you.

92. Using your place of birth as a security question
Thieves can easily find out the hospital or town you were born in to answer your security questions to gain access to your accounts.

93. Obtaining information for use as revenge or blackmail
Some scoundrels collect information gleaned from susceptible computers and other sources to simply blackmail an individual or business by threatening to go public with sensitive information.

94. Stealing information from doctor's office
Health records from a doctor's office contain vital information about your identity. Many identity thieves try to hack a medical facility's EHR (electronic health records) to steal sensitive, identifying information.

95. Filling out car loan applications
Identity thieves can buy cars by taking a loan application out in the name of another person.

96. Clicking on pop-ups
Always avoid pop-ups. When you click them, they could start a download in the background, which possibly contains a virus or malware.

97. Thieves going through pharmacy waste baskets
Unfortunate as it is, pharmacies don't always shred sensitive information about prescription holders. Waste paper baskets are often full if information thieves can use.

98. Mortgage ID theft
In most cases of mortgage fraud identity theft, victims have no clue that criminals obtained financing in their name and ran with the money until they're faced with an eviction notice.

99. Opening cyber greeting cards
A cyber greeting card sent from a "friend" could contain malware that invades your computer undetected and steals your passwords, bank numbers, and credit card information.

100. Installing electronic surveillance
In a day and age of heavy surveillance, installing cameras to steal credit card numbers, debit card PIN numbers, bank statements, and more is a growing threat.

101. Payroll data breach
Your company's payroll system or an outsourced payroll system can be hacked, which can put customers' corporate bank accounts and employees' personal information in the hands of hackers. This is why it's so important for every business to have identity solutions in place to protect themselves and their customers.