

5 Mindsets to Revolutionize Your Privacy

A mindset is a way of thinking about something, not just a one-time action item that goes away once it is completed. For the best results, incorporate the suggestions below into your everyday thinking. Make the items in bold your habits of privacy, not a “to-do” that you perform and promptly forget. Corresponding *Identity Theft Jujitsu* moves are in all caps.

1. **Stop.** STOP giving away pieces of your identity until you understand where the information is going, what it will be used for and how it will be protected. Don't give it away – to random people asking for your wallet during a speech, over the phone, in response to an email (even from your bank), in exchange for a 10% discount at a retailer, for a chance to win a contest or even to people you trust - until you verify its use and safety. Your default answer should be “NO!” until you understand the risk.
2. **Monitor.** By monitoring the different pieces of your identity, you will catch identity theft before it turns into a nightmare. By BLOCKING small cases of theft from becoming full-blown fraud (like my two cases), you will save yourself a great deal of time and money.

❑ **Action 1: Monitor Your Credit.** You are entitled to 3 free copies of your credit report every year (one from each Credit Bureau) when you visit www.AnnualCreditReport.com. Consult Appendix B in [Stolen Lives](#) to learn how to read your credit report and use it to BLOCK the worst forms of theft.

❑ **Action 2: Monitor Your Identity.** Monitoring your credit only covers about 25% of identity theft. Your identity can also be used to commit crimes (Character Theft), avoid immigration laws, take out “pay-day” loans and drain health and retirement benefits (Benefit Theft). In addition, your identity can be bought and sold over the internet at identity clearinghouses. I strongly recommend that you monitor all of these possibilities with a product like [CSIdentity](#). I use CSIdentity because it monitors much more than most services, costs very little, is used by banks, credit unions and the U.S. Government and includes \$25,000 worth of recovery insurance if your identity is ever stolen. The last time I checked, they had a special promotion code that gives you a 20% discount on the service (about \$10 per month after the promotion). The promotion code was **CSIDfriend** (case sensitive). In the interest of disclosure, I do not receive any money if you sign up for this service. Learn more at www.CSIdentity.com.

3. **Go Paperless.** Paper documents (mail, bank statements, checks, trash, etc.) account for over 90% of stolen identity documents (the rest is digital information). When you remove (STOP) these documents from circulation, you significantly lower your risk of identity theft. Going Paperless is a 3 step process:

❑ **Action 1: Bank Online.** Move your banking and brokerage account access online. As long as your computer is protected (Chapter 7 of [Stolen Lives](#)), banking online, paying bills online, reading statements online and storing sensitive documents on your computer is an excellent way to lower your risk of identity theft. It STOPS sensitive documents from being stolen out of the mail, off of your desk and out of your filing cabinet and LOCKS them behind a password-protected computer. Online account access has also been proven to speed up detection of fraud and drastically lower your out-of-pocket costs.

❑ **Action 2: Shred Everything.** STOP throwing sensitive documents in the trash without CHOPPING them. To learn about types of shredders and for examples of what documents to shred and what to keep, please refer to Chapter 7 of [Stolen Lives](#).

❑ **Action 3: LOCK it up in a SentrySafe.** Every physical identity document you decide to keep (i.e., those that you neither Stop nor Chop) should be LOCKED up in a locking filing cabinet or fire safe. Better yet, buy a SentrySafe Stackable Filing Cabinet and protect your files from thieves and fire all at once. They cost about \$150 and can be purchased online (generally with Free delivery) at [OfficeMax](#).

4. **Opt-out.** When you opt-out, you notify corporations and organizations to STOP sharing your personal identifying information (Name, SSN, Driver's License #, Account #s, etc.) with other companies, organizations or individuals. The less your information is shared, the less it exists in databases that can be breached. From today forward, every time you speak with someone who handles your identity, think "Opt-out!!" and ask them to remove you from all information sharing.

Example: Do you receive financial junk mail like pre-approved credit card offers? They are a significant source of identity theft because they allow thieves to set up credit cards (and other forms of credit) in your name without your knowledge. You can STOP this type of junk mail.

❑ **Action: Opt-out** of receiving pre-approved credit offers by visiting www.OptOutPreScreen.com or by calling 888-5-OPTOUT. Once you've completed this step, begin opting out of ALL information sharing on every account you have (bank, brokerage, mortgage, utilities, phone, etc.) For details, please refer to Chapter 5 of [Stolen Lives](#).

5. **Freeze Access.** There are many ways to freeze access to your identity. When you freeze access, no one is allowed into your accounts (credit file, credit cards, banking, brokerage) without a password. The most powerful example of freezing access is to lock or freeze your credit file.

❑ **Action: Freeze Your Credit.** When you freeze your credit file, no one is able to set up a new account using your credit profile unless they have your personal password. This makes it very hard for a thief to set up a credit card in your name (like my business partner did), to buy a house or car in your name (like my first thief did) or to abuse your credit in other ways. This is a very strong method of BLOCKING major forms of credit theft. To see if your state has a Credit Freeze Law, please visit www.ThinkLikeASpy.com and click on the link that refers to credit freezes.

3 Business Mindsets

1. **Laptop Jujitsu.** Stolen laptops account for a major source of corporate data theft. Apply Jujitsu to your laptop just like you did to your wallet. STOP carrying data that you don't need on your computer at that time. CHOP or destroy hard drives (digital shredding) before donating or disposing of a computer. LOCK your laptop up physically (carry it with you when travelling, lock it in a safe in hotel rooms) and LOCK it up digitally (passwords and encryption software like PGP).
2. **Office Privacy Audits.** Check to see what customer data, employee records and intellectual capital is flowing out through the trash, dishonest employees or vendors, unprotected wireless network connections and unprotected internet access (i.e., those that lack a firewall).
3. **Hiring Policies and Practices.** The number one threat to your business in terms of serious data theft comes from the people you hire and give access to your sensitive business information. Background checks, proactive privacy implementation and suggestive compliance monitoring are a good start.

For help training your team on any of these Mindsets, please contact me directly at 800.258.8076.

