7 Free Survival Strategies To Protect Yourself From Identity Theft

Author: Anthony R Howard
http://www.anthonyRhoward.com

Identity thieves are bolder now than ever. Why? Two reasons. One: there is a vast universe of demand for validated stolen identities. Outsiders call it the Dark Web. For beginners, this is Web you can't get to with a regular internet browser or search engine. Two: Thieves have figured out that because identity theft happens so often, most don't bother to fill out a police report, which means rarely if ever do law authorities actually take action (or even look for the perpetrators) on a scam unless it's of some magnitude. Hackers, competitors, and cyber criminals not only want access to your identity, but just as bad – they want access to your data as well. They want the data that is the lifeblood to your livelihood and your future. A validated identity with data has a higher market value. To hackers and identity thieves, you are in perfect formation to unknowingly share your identity and data that can be analyzed, collected, sold, or even used against you. And to the unscrupulous cyber criminals sitting at the table next to you in the coffee shop or the airport, you are one unencrypted wireless connection away from wishing you had paid better attention to this article. Research and statistics will shock you. Identity theft prevention is like data disaster recovery: no one pays attention to it until it's too late. It's not important….until your data is gone, your system is swiped, or your identity has been stolen. The vast majority of people have already experienced at least one breach and have no idea of how to stop another occurrence besides backing their stuff up to a USB drive or looking for the lock icon on their browser. Combine this with the average cost to buy a new laptop, or repair identity loss, which is at times priceless when factoring in lost productivity, and sleepless nights. You have a serious reason to change the way you protect information. Here are some powerful but yet inexpensive ways to avoid the most common ways of identity and data theft. *Protect Yourself with these 7 Survival Strategies to Inexpensively Decrease Your Exposure to Costly Identity and Data Theft:*

Embrace the human element. I'm not going to tell you to hang around good people who won't steal data because if you're smart enough to be reading this article then you already know that. I will tell you one of the most tragic mistakes people make regarding identity security is to only approach data privacy from the perspective of your laptop or online shopping, which is a very general perspective (your smart phone is also key, see strategy #3). Most don't understand how data theft and data privacy is relevant to them. Good people can easily leak data by simply being careless or leaving it unprotected. Simply put, I could get to your data in less than 15 minutes without trying that hard. This is not because I'm a skilled technology specialist. In many cases, I wouldn't have to use technology. I'd use the human element, simply meaning that laptops are left on desks in libraries and starbucks with data that could compromise them. Passwords are kept under keyboards. Home routers are kept at the default IP address with the default username and password. Bottom line: it doesn't matter what firewall or prevention method you use if don't understand the significance of data privacy and protection, or why it's important. And FYI – don't click on that link. You did not win the American Monetary Fund billion dollar sweepstakes (it doesn't exist), a Nigerian prince you never met did not leave his inheritance to you through western union, and a Ukrainian queen likely does not want to marry you via email.

Strong passwords (free) – No. 'Password' or a derivative of your name, birth date, or address simply will just not do. Any password that is in the dictionary I can get past in less than 5 minutes. I really don't like changing my password every 30 days. It's *really* annoying. Like a toothache. But I do it.

Setting your screen saver for less than five minutes while traveling (free) - Yes, it will get annoying sometimes. No more blankly staring at the screen, or drifting off into an erotic daydream during company time or suffer the screen saver.

Setting an automatic data wipe on your mobile device (smartphone) after 5 unsuccessful logins (free) - make sure the data is backed up though. We want to erase the data not the productivity. I'm a bestselling author with manuscripts I certainly don't want to lose. The phone may be worth $1000. The data and access to your banking passwords and identity, sold to the highest bidder, could be worth a million. Since most mobile devices are synced to laptops, and email accounts, plus have banking apps and passwords, it becomes more critical to protect mobile devices as well.

Encrypted hard drives (Inexpensive) – I could go deep here. To keep it short, go with whole disk encryption. This means that everything on a disk is encrypted, including the programs that can encrypt bootable operating systems partitions. This is a fancy way of saying, good protection for a regular end-user, even before you log on to windows.

Computrace (Inexpensive) – It's Lo-Jack for laptops, I kid you not. If your laptop is stolen, the software inside the computer can locate it for you, freeze the device, delete the data, and even investigate suspicious activity.

Physical Security (free) – You work hard start, run, or mange your business and identity. Work just as hard to protect it. Put your laptop sensitive data in your backpack, or carry it on your person, or perhaps even a trusted hotel safe when you are not using it. If you leave it unintended, it's an open invite to identity and data theft. Do not let anyone you don't know at the airport or coffee shop hit you with the "Hey can I check my email on your computer please?" You might not want to let them into your identity. With the right knowledge, in seconds, they could have your banking passwords.

When you are in an airport, hotel, or café, please remember that is an unsecured environment and I could get to your data in less then 15 minutes while having a cappuccino next to you….if the right precautions (listed above) are not in place. I personally employ these data protection policies.

Authors Bio:

Bestselling author Anthony R. Howard has been an industry recognized consultant and technology expert for the premier global technology firms for over 12 years. Presently he is a leading Technology Specialist for one of the world's largest Information Technology firms where he was named *#1 IT Super Hero by InfoWorld* and *ComputerWorld*, was the winner of the *National Federal Office Systems Award* (FOSE - Nation's Largest Information Technology Exposition Serving the Government Marketplace), and the 2004 winner of Government Computer News *Best New Technology Award*. Several case studies have been published on Howard's solutions across the Information Technology industry. Currently he provides enterprise technology solutions and advisement for America's most distinguished clients including a sizeable amount of work for the U.S. Defense Sector, Department of Justice, and the Department of Homeland Security, and the Georgia Institute of Technology. His projects have been featured in national media outlets including Fox News. He's also the bestselling author of The Invisible Enemy: Black Fox and The Invisible Enemy II: Vendetta. His long awaited novel Devil's Diary: The Coming is launching soon!