02/04/2013

By Adam Levin, Chairman and Co-Founder, Credit.com and Identity Theft 911

A funny thing happened on my way from Los Angeles to Washington, D.C. – I found myself on a flight without Wi-Fi. The prospect of being unplugged for more than four hours on a flying machine without the ability to communicate with (or distract) colleagues, with zero information from the outside world – let's just say I almost lost it.

I had two newspapers and a book by my favorite fiction writer, Vince Flynn, but I was not connected. And somehow, the thought of being alone (even though I was on a full flight) for a large chunk of time was daunting. And, let's face it, the fact that we've all become so co-dependent – with MACHINES – is kind of pathetic. But here we are.

The irony is that it's only when you are suddenly disconnected that you realize how pervasive digital connectivity really is. So I tried to think of the true impact. There were so many implications to being offline and relatively isolated at an altitude of 37,000 feet, and they all centered around the security of the no-tech environment.

1. No shopping. It's never a great idea when flying because some clever soul sitting a few seats away could be soaking up your information or even setting up your computer to be his or her own personal information transmitter.
2. No online banking (again, not a smart idea at 37,000 feet -- see above). No logging into my accounts, no chance of them getting hacked by lack of security on my end.
3. No email greatly reduces the risk of being phished or spear-phished – exposing my contact list to hijacking or subjecting my computer to compromise and turning me into yet another component of a botnet or a spaminator
4. Keeping my cellphone turned off -- and in my pocket -- meant I wasn't leaving my smartphone in the back of a taxi, on the top of a toilet-paper dispenser in a bathroom stall or anywhere else someone might grab it and crack my (very crackable) code – gaining access to my most meaningful contacts or garnering some tasty tidbit of my Personal Identifying Information (PII), possibly the missing link in my life puzzle needed to convince someone at a bank or car dealership that an identity imposter was me.

5. Since I am using my laptop as I write this, an identity thief's field of dreams turns less cheery, because it is (a) in my possession and thus (b) not laying about tantalizingly unattended in the back of my car or on an airport terminal lounge seat screaming (did I mention the wailing toddler in the seat just in front of me?), "Please steal me!" Obviously, and most importantly, my Wi-Fi receiver is turned off.

6. I've got my wallet. I can take it out to check that the limited number of credit and debit cards I carry with me are all there. Incidentally, there is no Social Security card in there. I know my number, and no one else should have such an easy way to get that vital piece of information.

7. I don't need a document shredder. All my personal documents that contain sensitive information are either at my office or at home under strict security protocols. Yes, I am – as the chairman of a company in the privacy business – completely paranoid.

8. The lively 12-month-old sitting next to me (a fellow conspirator of the child in front of me) is probably not a state-sponsored hacking drone, so I think my electronic devices and the sanctity of my writing is fairly secure. (See above, re: paranoia.)

9. No Facebook. I'm not a fanatic (sorry, Zuck), but if I were, it would be impossible to alert any lurking "frenemies" to the fact that I am away from home.

That said, before I declare victory regarding the fortress-like nature of my identity management skills, I must take a moment to reflect upon my various exposures.

Despite my best efforts to stay under the personal data radar, sites like Spokeo possess information about me that they have gleaned and scraped from various public sites and/or filings that haven't been properly redacted by government authorities who have a long and sullied history of defending consumer privacy. (Let's not forget South Carolina's Department of Revenue .) I can monitor it, but it's beyond my control to some extent.

My personal identifying information almost certainly can be found in hundreds of databases, and I have no way of knowing about it. One of them may have already been compromised – it could be as simple as someone selling a list to a third party. Enterprising individuals and syndicates are undoubtedly hoarding facts and probabilities about me that will determine whether or not I become the victim of a crime despite my best efforts to protect myself.

When and where this disaster will strike is a mystery, but it's only a matter of time. In the past year, I have had several credit cards compromised and replaced by credit card companies. In one case, the 16 digits from my card were illegally recorded, either by a data processing device or a website I visited. According to Privacy Rights Clearinghouse , hundreds of databases

containing millions of records were compromised in 2012 alone.

There is nothing I can do while unplugged on a plane about third-party vendors contracted by one of my institutional relationships being breached. My information is out there along with that of millions of other consumers. I can't be sure my doctor's office or the billing department at my favorite store is totally secure. I can't vet every waiter, greeter or owner I trust with my credit card information. I trust my cleaning lady and florist implicitly, but can I be sure that if she needs a substitute for a day or an unfamiliar employee shows up on a service call that they all have my best interests at heart? When I take my car in for service, but forget to remove the registration from the glove box, or drive to a meeting and leave the car with a parking attendant, can I be sure they have no interest in learning more about me than is appropriate? How do I really know the customer service representative at my financial institution or the admin at my insurance agent's office isn't doing a side job for folks who make money by using my personal information in creative and totally unauthorized ways?

As we begin 2013, it's worth remembering how much is beyond our control. The most fastidious, organized and self-protective among us are vulnerable every minute of every day. Too much personal information is out there to protect you from the spillover effects of a totally interconnected global economy, especially if a criminal element is thrown into the mix. No stone-age airplane with no Wi-Fi can save us. We can (and should) be covetous to the point of paranoia.

In my case that means logging on when I get off the plane to make sure I haven't been robbed or unwittingly purchased property in Nigeria. There is nothing crazy about monitoring everything we do, especially our credit, and having a damage control program in place just in case we suffer an identity emergency. If you don't have a plan, make one in 2013.