How to Protect Your Identity and Privacy
Hi. My name is Jason Hanson.

I’m a former CIA Officer and the New York Times bestselling author of Spy Secrets That Can Save Your Life.

As a security specialist, I teach anti-kidnapping, escape & evasion, evasive driving, and much more. One of the topics my clients ask me about most these days is protecting their privacy and identity.

The fact is, identity theft is the #1 complaint received by the Federal Trade Commission (FTC) with over 15 million victims each year and this number continues to grow rapidly. Get this: Estimates of the cost of identity theft to consumers is over $50 billion a year in damages.

Unfortunately, with technology and the hackers who abuse it increasing each year, things will only get worse so you must know how to protect yourself.

The good news is, it’s much easier than most people think and I’m going to show you exactly what you need to do in this special report.

Let’s get started...

“Can you help me? My identity has been stolen.” That was the beginning of an email I received from a producer of a TV show where I’ve made several guest appearances.
After talking with this gentleman, it was clear he had been hacked and I shared with him the measures he needed to take to ensure it never happens again.

I told him that once someone has experienced identity theft, they have to clear up the current mess. This means spending hours or even days on the phone closing credit card and bank accounts and opening brand new accounts.

But, before I tell you what I told this fellow let me share with you how I believe his identity was stolen. In short, it most likely happened because he was surfing the Internet using public Wi-Fi, which is a terrible idea.

In fact, not too long ago I read an article in USA Today that made a great point: “Public Wi-Fi systems such as those found on airplanes, in cafes, or at malls are completely insecure, and anyone using them should think of everything they type as being broadcast to a billboard in Times Square…”

The reason public Wi-Fi is so dangerous is because anyone can “spoof” a Wi-Fi spot and then using easily obtained software they can access all of your data.

Here’s an example: When my wife and I moved to Utah a few years ago we lived in a townhouse community.
When I would log onto the Internet there were almost a dozen different Wi-Fi spots that popped up and I’m sure you’ve seen people name their Wi-Fi all sorts of funny names including FBI or Police. Well, a criminal can do the same thing and create a Wi-Fi spot and name it whatever he wants. For instance, he can go into Starbucks and create a spot called Starbucks1 or he can go to a Holiday Inn and create a spot called HolidayInnWiFi.

The fact is, people will click on these spots and they have no idea they’re not on the real Wi-Fi spot created by Starbucks or Holiday Inn but instead are on a network created by a criminal. As they login and use their passcodes to various websites the criminal is downloading all of their information.

In the article I mentioned above from USA Today, one of the writers for the newspaper had his identity hacked and they were able to trace it back to the GoGo Inflight Internet he used while on a plane. (Someone spoofed the GoGo Wi-Fi and the writer used the fake spot instead of the real one.)
Luckily, it’s very easy to protect yourself when using public Wi-Fi even though the majority of people still don’t do it. This is especially scary since free Wi-Fi is everywhere these days from McDonald’s to the mall.

All you need to do to protect yourself is use a Virtual Private Network (VPN.) The following is the definition of a VPN according to good ol’ Wikipedia...

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network, and thus benefit from the functionality, security and management policies of the private network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunnelling protocols, or traffic encryption.

To put this in layman’s terms, a VPN is a program that encrypts your data over the Internet so that hackers can’t access your data making it safe to surf the Internet when logged onto public Wi-Fi.

These days, VPNs are easy to obtain (I’ll tell you how in a moment) but, as I mentioned, almost nobody uses them. When I hold my Spy course (www.SpySafety.com) and ask people how many of them use a VPN I’m lucky if 10 hands out of 100 go up.

So, even though people may know what a VPN is they still don’t use it and I hope that changes soon.
The VPN that I personally use is called TunnelBear and it costs about $50 a year, which is dirt-cheap. There are also several other VPNs you can use. Do your research if you want and find the one you like best.

Once you’ve chosen a VPN, download it onto your computer and smart phone, and in a matter of seconds you’re up and running.

So, if you don’t have a VPN yet, please change that now. Before you do anything else go to TunnelBear or whatever VPN you want to use and download it so you don’t become an easy victim the next time you’re surfing the Internet at a hotel, airport, or anywhere else.

Also, before I forget, there were two actions I told the TV producer he needed to do immediately so he didn’t have to worry about his identity getting stolen in the future.

The first was to get a VPN and the second was to put a freeze on his credit. If you don't have a credit freeze yet (I’ve had mine for about 15 years) this is something I highly recommend you do and is one of the smartest moves you can take to protect your identity and privacy.

Here’s exactly how to put a freeze on your credit report:
First, a credit freeze blocks companies from running your credit without you first notifying the credit reporting agencies and allowing them access.

In other words, unless you give a company permission, nobody can access your credit so you don’t have to worry about someone buying a car or taking out a mortgage with your credit.

For instance, I was fortunate enough to appear on the ABC television show Shark Tank. The producers on the show called me before my appearance and said, “Jason, we’re trying to run your credit but it won’t allow us to.”

I had forgotten to lift my credit freeze and this was a great reminder of how nobody can access my credit, which is exactly the way I want it. (I did lift the freeze so they could check it.)

After you request a credit freeze, the credit reporting agencies will provide you with a personal identification number (PIN) and you will use this PIN when you need to give someone access to your credit, which is what I did with the producers of Shark Tank, as I mentioned above. (You can lift the freeze by calling the following numbers and using your PIN.)

888-909-8872 for Transunion
888-397-3742 for Experian
800-685-1111 for Equifax
Every state charges different fees for placing a freeze on your credit. It can range from being free to $10.

Here are the links to each credit agency that shows how much it will cost in your state for a credit freeze:

- Equifax: https://help.equifax.com/app/answers/detail/a_id/75/search/1
- Transunion: https://www.transunion.com/credit-freeze/place-credit-freeze

To place a freeze on your credit you must contact all three major credit-reporting agencies separately, which, as noted above, are Equifax, Experian, and Transunion.

You will send a letter by certified mail requesting to have a freeze placed on your credit. It is a very simple and short letter. Here is what I would send to all three agencies:
Dear AGENCY NAME,

I would like to place a freeze on my credit file. My name is:  
My former name was (if applicable):  
My current address is:  
My former address was:  
My social security number is:  
My date of birth is:  
I have enclosed photocopies of a government issued ID and proof of residence. (Utility bill, etc.)  
I have included a police report verifying my identity has been stolen (if applicable).  
I have included a check for the fee of $X.XX.

Sincerely,
YOUR NAME

You will need to send this letter, documents, and check to all three of the credit reporting agencies at the addresses below:

Equifax Security Freeze  
P.O. Box 105788  
Atlanta, Georgia 30348

TransUnion LLC  
P.O. Box 2000  
Chester, PA 19016

Experian Security Freeze  
P.O. Box 9554  
Allen, TX 75013

After you’ve sent all three agencies a certified letter they will respond to your request, usually within 10 business days, with a confirmation
letter of your freeze. Each credit agency will also provide you with the PIN number that you use in the future when you need to access your credit history.

I realize some people may think this sounds like a lot of work. But, just imagine how many hours you could spend on the phone undoing the damage of someone who has hacked your credit and purchased a boat or house or worse.

In other words, a little bit of work now will be much better than a huge headache later if someone hacks your credit and this is exactly why I’ve personally had a credit freeze for about 15 years now.

The truth is, I’ve personally been a victim of identity theft – by the Chinese Government – and as strange as it sounds, I wasn’t worried about it at all because I had taken the steps outlined above to protect myself.

Here’s how the Chinese stole my personal information...

Awhile back, I received a call from a friend who also happens to be ex-CIA. When I answered the phone he said, “Did you get the letter from OPM?”
Not knowing what he was talking about I told him no. He reminded me of the huge data breach that occurred when the Chinese stole background information of U.S. government workers with security clearances.

I remembered this incident but never received a letter in the mail so I forgot about it since I believed I was safe. I told my friend I didn't receive the letter and that it stinks to be him and he better put measures in place to protect himself.

Of course, I spoke too soon and a few days later I received a letter from the Office of Personnel Management (OPM.) A snippet of the letter is below. (Double-click on the letter to see a larger version.)
I called my friend back to let him know that I too had received the letter and he had these encouraging words…

“If you traveled to any foreign countries in true name or in alias while you were an officer then that Country – if you went back – could pick you up while you’re overseas and hold you for espionage based on previous travels and activities that they suspect you committed. We already know that the Chinese have sold those lists of information to several other countries such as North Korea, Iran, Afghanistan, Syria etc. etc.”

Although my personal information is now in the hands of lots of “bad guys” I’m really not that concerned about it, as I mentioned above, because of the following reasons...

1. I don’t plan to travel to places with unfriendly governments where I could get myself in trouble… no Christmas vacation in North Korea this year.

2. I have a credit freeze on my credit report. This means nobody can access my credit to take out a car loan or mortgage or anything like that.

3. I carry an Identity Protection card in my wallet. This protects people from hacking my credit cards. For full details on why these cards are so important and to get one for free, click here.

4. Even though the Chinese have a lot of my information I make sure people
can’t get anymore by shredding everything. I only use a crosscut shredder. (Do not use a shredder that cuts the paper into strips as these can be put back together.)

5. I spend 10 minutes at the end of each month reviewing my bank statements and credit card statements. It’s not exactly the most enjoyable thing in the world, but it allows me to see if there are any fraudulent charges.

Hopefully, your personal information isn’t being sold around the world by the Chinese like mine is, but you should still take the steps above to better protect your identity.

By the way, if you’re still not convinced about the importance of protecting your identity and privacy, here’s one final story about a former Miss Teen USA.

A young woman from California named Cassidy Wolf was on her computer one day when she received an anonymous and threatening email. The man who sent the email said he had thousands of pictures of her, including many of her nude, and that he’d been watching her for over a year.
He was planning to put the pictures all over social media unless she got on Skype with him and agreed to do a series of inappropriate things.

Smartly, Cassidy and her parents got the FBI involved and they eventually caught the dirt bag that was watching her. The dirt bag’s name is Jared Abrahams and he was a computer science student in college at the time.

He’d not only hacked the webcam of Cassidy Wolf but as many as 40 other women, some of whom gave in to his sick blackmail demands instead of calling the police.

In an interview with Business Insider Cassidy said about the whole ordeal, “Your bedroom is your most private and intimate space. To think that someone was watching me in my bedroom for a year and had all my most
intimate moments, heard conversations I had with my mom and my brother, and knew everything about my life — someone can have access to all of that by your computer.”

As a father of two daughters, I get filled with anger just thinking about people doing this to young women. If it happened to one of my daughters I’d sure like to do things to the perpetrator that our legal system frowns upon.

Unfortunately, in the future, there will be even more programs and more ways for criminals to hack people’s webcams and other computer devices.

This is why my computer has a piece of paper taped over the camera. This is such a simple thing to do and only takes five seconds and it ensures that nobody can watch you.

What’s more, I don’t bring my computer into my bedroom. As Cassidy mentioned, the bedroom is an incredibly private space where you likely have conversations with your spouse that you don’t want others to hear. My computer stays in my laptop bag when I get home from work and when it does come out, I’m usually sitting in the living room checking email for just a few minutes.
Also, don’t forget about all those other devices that have cameras too, like your phone and your iPad.

The fact is, it’s sad that we have to do these things, but it’s the price we pay for living in these times. So if you’re reading this special report and your computer doesn’t have a piece of paper taped over the camera, please go do it before you forget.

What it all boils down to is this:

In this special report I’ve given you several ways to better protect yourself. Please start implementing them today so you don’t become one of the millions of victims of identity theft this year.

Also, don’t forget to claim your free Identity Protection Card right here.

Stay safe,

Jason Hanson
www.SpyEscape.com

P.S. For more tools and items to keep you safe, please check out our Spy Store at www.SafeHomeGear.com.