SPY + SURVIVAL BRIEFING

SECRETS, TIPS & LIFESAVING STRATEGIES FROM A FORMER CIA OFFICER

HOW TO PROTECT YOUR IDENTITY AND PRIVACY ONLINE

Dear Friend,

Hi. My name is Jason Hanson.

I'm a former CIA officer and the *New York Times* best-selling author of *Spy Secrets That Can Save Your Life.*

As a security specialist, I teach anti-kidnapping, escape and evasion, evasive driving, and much more. These days, one of the topics my clients ask me about most often is how to protect their privacy and safeguard their identity online.

Identity theft is the No. 1 complaint received by the Federal Trade Commission (FTC), with over 15 million victims each year. The estimated cost of identity theft to all consumers? Over $50 billion a year in damages.

And with the number of hackers increasing each year along with the evolving technologies they use, this problem is only going to get worse. In this day and age, it's vital to know how to protect yourself.

The good news is it's much easier to preserve your identity and privacy than most people think. And I'm going to show you exactly what steps you can take 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 the producer of a TV show on which I've made several guest appearances.

After talking with this gentleman, it became clear he had been hacked. As I explained to him, once someone has experienced identity theft, first they have to clean up the current mess. This means spending hours — sometimes days — on the phone canceling credit cards and closing bank accounts and opening brand-new accounts. Then I shared several steps he needed to take to ensure he would never be hacked again.

Before I tell you what I told this fellow, let me explain how his identity was stolen. Very simply, it probably happened because he was surfing the internet using public Wi-Fi, which is a terrible idea.

Why?

A recent article in *USA Today* put it best: *"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…"*

Public Wi-Fi is so dangerous because literally anyone can "spoof" a Wi-Fi spot. And while you're surfing on the phony network, the network's creator can access all of your data using easily obtained software.

I'm sure you've seen how people name their Wi-Fi all sorts of inventive names, including FBI or Police. A criminal can do the exact same thing: create a Wi-Fi spot and name it whatever he wants. For example, a hacker can waltz into Starbucks and create a spot called Starbucks1. Or he can pop into a Holiday Inn and create a spot called HolidayInnWiFi.

And unfortunately, most people will click on these spots and have no idea they're not on the real Wi-Fi spot created by Starbucks or Holiday Inn. As they navigate the internet using their passcodes to various websites, the criminal is rapidly downloading all of their sensitive information.

Here's a perfect example: One of the writers for the *USA Today* article I mentioned above had his identity hacked, and authorities were able to trace the breach back to the Gogo in-flight internet he used while on a plane. Someone spoofed the Gogo Wi-Fi, and the writer unknowingly used the fake spot instead of the real one.

This idea is especially scary since free Wi-Fi is available practically everywhere these days, from McDonald's to the mall. And the majority of people don't take the steps to safeguard themselves, because they don't realize how easy it is.

THE ONE NETWORK YOU CAN TRUST

All you need to do to protect your information is use a **virtual private network (VPN)**. According to good ol' Wikipedia, a 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 gain the benefits of the private network.

In layman's terms, a VPN is a program that encrypts your data over the internet so that hackers can't access it, making it safe to surf the internet when using public Wi-Fi.

These days, VPNs are easy to obtain (I'll tell you how in a moment). But as I mentioned before, almost nobody uses them. When I hold my spy course and ask how many people use a VPN, I'm lucky if 10 out of 100 raise their hands.

The VPN that I personally use is called **TunnelBear**. It costs about $50 a year, which is dirt-cheap. But there are several other VPNs you can use. So do some research and find the one you like best.

Once you've chosen a VPN, download it on to your computer — and your smartphone — and in a matter of seconds, you'll be up and running.

So if you don't have a VPN yet, please change that now. Go and download whatever VPN you want to use, so you don't become an easy victim the next time you're surfing the internet at a hotel, airport, or anywhere else.

SAFEGUARDING YOUR CREDIT SCORE

Acquiring a VPN was the first step I told the TV producer he needed to take immediately to protect his identity from getting stolen in the future.

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. It's one of the smartest moves you can make to protect your identity and privacy.

A credit freeze blocks companies from running your credit without you first notifying the credit reporting agencies and giving them the green light.

In other words, unless you give a company explicit permission, nobody can access your credit. So you won't have to worry about someone buying a car or taking out a mortgage in your name.

For example, when I appeared on the ABC television show *Shark Tank,* the producers called me and said, "Jason, we're trying to run your credit, but the credit reporting agency won't allow us to."

Clearly, I had forgotten to lift my credit freeze. This was a great reminder that nobody can access my credit without permission, which is exactly the way I want it. (I did lift the freeze so they could check it.)

To place a freeze on your credit, you must contact each of the three major credit-reporting agencies: Equifax, Experian and TransUnion.

Send each agency a letter by certified mail requesting to have a freeze placed on your credit. It can be a very simple, 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

Send this letter, the necessary documents, and checks to the following addresses:

Equifax Security Freeze

PO Box 105788
Atlanta, GA 30348

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013

TransUnion LLC

PO Box 2000
Chester, PA 19016

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

When someone legitimately needs to check your credit, you can release the freeze temporarily by calling the credit agencies and using your PIN. This is what I did for the producers of *Shark Tank.*

Here are the numbers you'll need:

Equifax: 800-685-1111
Experian: 888-397-3742
TransUnion: 888-909-8872

Every state charges different fees for placing a freeze on your credit. The cost usually range from free to $10.

Check the links below to find out how much it will cost in your state for a credit freeze:

Equifax

Experian

TransUnion

I realize some people think this sounds like a lot of work. But just imagine how many hours you might spend on the phone undoing the damage of someone who's hacked your credit and purchased a boat or a house — or worse. A little bit of work now is much better than a huge headache later if someone hacks your credit. This is why I've personally had a credit freeze for about 15 years now.

WHY I'M SUCH A STICKLER FOR CYBERSECURITY

I don't admit this to too many people, but I personally have been a victim of identity theft — by the Chinese government. But as strange as it sounds, I wasn't worried, because I had taken the steps outlined above to protect myself.

Here's the story:

A while 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 the incident. But since I never received a letter in the mail, I assumed I was safe and forgot about it. I told my friend that it stinks to be him and he had 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.)

I called my friend back and told him that I had gotten a 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 the authorities in 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 not that concerned about it, for 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. Again, this means nobody can access to my credit without my knowledge and 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 yourself, **click here**.

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

5. I spend 10 minutes at the end of each month reviewing my bank and credit card statements. It's not exactly the most fun thing to do, but it helps me identify 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 two simple steps outlined above to better protect yourself.

And if you're still not convinced about the importance of safeguarding 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 threatening email. The man who sent it 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 said he planned to put the pictures all over social media unless she got on Skype with him and agreed to do a series of inappropriate things.

Cassidy refused, and she and her parents wisely got the FBI involved. They eventually caught the dirtbag that was watching her. His name is Jared Abrahams, and he was a computer science student in college at the time.

Not only had Jared hacked the webcam of Cassidy Wolf but the webcams of 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 reflected on 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 am 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, criminals keep coming up with more ways to hack people's webcams. And don't forget about all the other gadgets that have cameras too, like your cellphone and your iPad.

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

What's more, I don't bring my computer into my bedroom. As Cassidy mentioned, your bedroom is an incredibly private space where you don't want to be watched. My computer stays in my laptop bag when I get home from work. When it does come out, I'm usually sitting in the living room checking email for just a few minutes.

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 do that now before you forget.

To recap: I've given you several ways in this special report to better protect your identity and your privacy. I hope you start implementing them today so you don't become one of the millions of victims of identity theft this year.

Stay safe,

Jason Hanson