Video: The Expert's Opinion on Your Identity and Cybersecurity

The Expert’s Opinion on Your Identity and Cybersecurity

Paige Hanson

When it comes to cybersecurity, being online, and going digital it’s very important to make sure you first connect securely. By that, we mean connecting with a VPN. It's a virtual private network.

It’s an extra step to log in but what that means it’s encrypting all your internet traffic from your tablet, your device, up into the internet, all of that is encrypted, because when you're on public WiFi or when you're on your home internet, most of the time, that is unencrypted traffic. The internet service provider can actually sell that internet history your website traffic to third parties. And so if all of that sounds scary to you, a VPN will help you.

The first step when you're connecting is to connect to the internet. Then you would fire up your VPN. It requires a few security credentials. Then you are encrypted.

Next, you want to make sure you're on secure websites. You want to look at the website address. It usually says “https.” There's also sometimes a lock symbol, and what that means is that the provider on the other side has that information encrypted.

So now you've done two steps. One, your internet connection is encrypted and two, you're visiting websites that require a user name and password. Those too are encrypted. That, together, makes you less vulnerable on the internet.

There's a million passwords out there and using a password manager helps you with those. A password manager is an app you can download onto your phone, and you only have to remember one password to get into that password manager. The password manager can either create complex passwords on your behalf or store your existing passwords. It alleviates the need to always know every single password or to reuse the same user names and password on different websites.

When you're looking at a password manager you want to use an encrypted solution. How encryption works is, it’s like you’re scrambling the information, the passwords, or whatever data you might have. It only can be read by the intended party. In this case, only your password manager can read it.

If there's some sort of breach the offending party cannot read it because it's not your password manager. The password manager generates other passwords for all of your online accounts so they can be as complex as you want and you're really only having to remember one password.

One of the free things that you can do on most online accounts is to enable two-factor authentication. Sometimes it's called multifactor authentication. It’s like an extra set of credentials in order to access your online accounts. Important accounts like your email, your bank accounts, healthcare accounts, social media accounts… those are things that, if a fraudster were to get into those accounts, can really wreak havoc on your life.

In order to enable two-factor authentication, you need to go into each of your individual accounts and set it up. How it'd work is, let's say you go onto a friend's computer and you want to access your email. Well, all you need to do is type in your user name and password. Then you're going to get a text message on your cell phone because the way you set up two-factor authentication is to send you an alert. Usually it's on your mobile device. As long as I have that series of codes I'm able to then put that into the website, click OK, and now I have access on my friend's computer.

Same goes for a fraudster.

Let's say there was a data breach and user names and passwords were unencrypted and now the fraudster has your user name and password. They are going to try to access your online accounts. They're not going to be able to get in because they do not have that six digit code saying "okay, this allows me access to this online account."

Because we are living our lives so digitally and everything is on our phones if we are using mobile payment all of our apps and things like that are important to us are on our phone, it's very important to keep our devices up to date. Doing regular updates will help you be more secure.

We also want to make sure your phone is password protected. Your thumbprint is just fine, but make sure that your password is always on there just because there's so much personal information on your phone.