jeff@jeffbohr.com 239.595.0482

10 Ways to Protect Your Online Identity

1 Passwords

The most common way to protect your online identity is to focus on creating stronger passwords. When creating a password, choose something that will not be easily cracked or decoded. Never use a word or number that someone can associate with you such as a first, middle or last name, a spouse, child's or pets name, address, phone numbers, employers, or other identifying letters or numbers. Try a passphrase rather than a password. A passphrase can be a favorite song lyric, quote from a book, magazine, or movie, or something your grandkids said last week. Think of a saying or series of words that is easy for you to remember and use the first letter of each word in the phrase, along with a combination of numbers and special characters, as your passphrase. Obviously, your password should be a combination of letters and numbers, and adding a single symbol makes it 100 times harder to hack! Don't stop at the bare minimum, use 12 or more characters as a norm, this will soon be the new minimum! Don't use the same password for everything, use multiple passwords!

2 Look for Encryption

Before making any sort of financial transaction or entering personal data online, look for signs that show whether the website is encrypted or not. To do this, look for two things: the trusted security lock symbol and the extra "s" at the end of http in the URL or web address bar. When you are on the page that's asking for credit card information or personal information, the "http" changes to "https" when it is a secure site. At the same time, a lock symbol will also appear on the right side of the address bar or at the bottom left of your browser window. These two signs show that the site is encrypted, which means nobody will be able to see information as it's sent to the website owner. This keeps your name, phone number, address, credit card number and other sensitive information from being seen by anyone else. Many of the vital online services (Google, Facebook, Twitter, etc.), allow you to only connect to their servers via an HTTPS connection. This will encrypt any stream of data between you and the service, ensuring that anyone using a packet sniffer on a (usually public) Wi-Fi network can't obtain your login data. Never do work at a coffee shop or airport without checking it!

3 Beware the Phishing Scam

To avoid being the victim of a phishing scam, never open emails or attachments from unknown senders, or anything unusual from known senders. Spam email is getting more and more sophisticated. Never respond to any emails requesting account info or passwords. Banks will never ever ask for your information in this way. If in doubt, call the bank directly to check or, better still, delete the email. Additionally, avoid anyone offering money, unfamiliar job opportunities or requests for donations to charities as this might be a plot to obtain your personal information and online identity. Any website pop up that tells you that you have a virus or wants you to call a phone number is a scam. Remember, unless someone is sitting next to you at your keyboard, they have no idea what is going on with your computer, but they are pretty good at convincing you that they do. They prey on fear and have fooled a lot of people who are otherwise computer savvy.

4 Password-Protect Your Wireless Router

The wireless router that accesses the Internet at your home or business should always be password protected. When you do not have a password on your wireless network, anyone in your range can use and access your Internet, even a hacker. Not having a network password allows unauthorized individuals within proximity to hijack your wireless network. Even if they're merely attempting to get free Wi-Fi access, you don't want to inadvertently share private information with other people who are using your network without permission. For extra security, hide your Wi-Fi network: set up your wireless access point or router so it does not broadcast the network name, also known as the Service Set Identifier (SSID).

5 Enable Cookies on Your Web Browser When Required

Another option for setting up your browser to protect your online data is by enabling cookies only when required by a

website. These cookies are details websites store on your computer, including information about what sites you visit and what you do there. Most of them keep the details to themselves, but this is also a way dishonest people get your information. You may need cookies to be enabled to see or interact with some sites, but limit these only to websites that require it.

6 Secure Your Security Questions

Just because security questions are a safety feature doesn't mean you shouldn't put the same thought into them as your password. Use numbers instead of letters. Deliberately misspell things. It's important to provide a secret question with answers absolutely not related to it. For example, for the question "What is the name of your first pet?" register an answer like 'Us6KjTG.' Instead of providing real answers, provide passwords like that one. So, basically the rule is never provide real answers for the secret questions, but make sure to record the answers you do use in a safe place!

7 Enable 2-Step Authentication

Apple, Facebook, Yahoo and Google and many other sites now offer the option of 2-Step, or two-factor, authentication when you login, meaning you will need to enter a secondary pin number which is generated and texted to your phone or tablet. It's an extra step whenever you're logged out, but it's also a safe guarantee that no one will be trying to get into your account without you knowing it.

8 Check your phone's privacy settings

Turning your GPS location settings to "off" can keep you and your family's whereabouts more private. Turn on for only services needed, like maps and weather.

9 Keep a close eye on your bank statements

Really savvy people cross check their receipts with the payment history on their statements, but this isn't absolutely necessary - just keep an eagle eye out for any unfamiliar transactions with vendors you've never heard of.

10 Install and automate operating system updates.

These updates contain critical security patches that will protect your computer or device from recently discovered threats. Failing to install these updates means your computer or device is at risk. It's best to set your operating system to update automatically, so turn on automatic updates if that's an available option.