BeTECHSavvy
Securing Your Digital World

NATIONAL TRADING STANDARDS
Scams Team

How to keep your digital identity

secure & private in a connected world

12 steps to take NOW

Incorporating
Umbrella Consulting

Introduction

This checklist highlights 12 steps you can take now to keep your digital-self secure; your digital identity & privacy is more at risk every day. Do not just give your privacy away!

Learn to take control of your digital self, in the same way that you would take control over your personal health, or your savings, or your right to vote.

Hi... My name is Ben Hill and I am the founder of BeTechSavvy. I have always had a keen interest in computers and have over 20 years of experience in IT security & privacy, on numerous different Operating Systems, operating in various environments.

Having a productive but private online digital life is important for you and your family to get the most from online experiences. With the amount of information that we share online, it is important that we retain the ability to define the boundaries of our digital lives. While many people already have their own go-to tips and tricks, for others, identifying a pragmatic approach to digital privacy and security might seem overwhelming.

I will give honest free advice on any concern or issue of identity and data privacy you may ave.

I am also able to provide practical support and training to customers... so feel free to speak to me!

Benjamin Hill

CEO & Founder

A smart way to help protect your privacy online?

Do not overshare on social media. Providing too much information on Facebook, Twitter, and Instagram could make it easier for cybercriminals to obtain identifying information, which could allow them to steal your identity or to access your financial information.

Unfortunately, many people do not take this advice. In a 2018 US study, the Identity Theft Resource Center found that approximately 52 percent of respondents shared personally identifying information through social media sites.

And that is just the start of the oversharing. The same study found that about 48 percent of respondents shared information about their children, while nearly 33 percent shared information about their location. A total of 42 percent of respondents shared information about their travel plans through social media.

To protect your privacy online, think twice. Does everyone in your social media profiles, need to know everything about you; which could make you an easier target for identity theft. Explore different privacy settings, too. You might want to limit the people who can view your posts to those you have personally invited.

Once online, always online: With anything you post online, it's out there for everyone to see, so be careful with the identifiable information you use in your social media profile and which sites you sign up to.

1. Check social privacy settings

If you have social accounts, those networks have a lot of information about you, and you might be surprised how much of it is visible to anybody on the Internet by default. That is why we strongly recommend you check your privacy settings: It's up to you to decide what info you want to share with complete strangers versus your friends, or even nobody but you.

It is possible to view and adjust certain privacy settings in most Operating Systems including Windows, Mac OS, iOS and Android. It is also possible to install various applications on mobile devices to see even further, what information is being gathered and/or transmitted to the application Developers. As a result, for example, if there is a need to install the Facebook and Facebook Messaging apps, then install the "Lite" versions (see below for the reason why). There are also applications for other operating systems, that allow the Privacy settings to be hardened and telemetry sent to the manufacturers, to be lessened or removed.

Why you may ask; these were designed to be used in countries where the cosy of data is more to use and as such, targeted advertising is not done to the same degree as the revenue is not generated there (Facebook Lite collects data against 23 activities and has no inbuilt trackers. Facebook, on the other hand, collects data against 750 activities and has 8 inbuilt trackers).

Check other applications, to see if they "Lite" versions to install and use these instead! I can provide privacy information on most applications used in mobiles. You may be amazed at how much data is being collected!

2. Don’t use public storages for private information

Oversharing is not limited to social networks. Do not use online services that are meant for sharing information to store your private data. For example, Google Docs isn’t an ideal place to store a list of passwords, and Dropbox is not the best venue for your passport scans unless they are kept in an encrypted archive.

3. Evade tracking

When you visit a website, your browser discloses a bunch of stuff about you and your surfing history. Marketers use that information to profile you and target you with ads. Incognito mode cannot really prevent such tracking; you need to use special tools. Many browsers can block trackers or add extensions to do so. Use these facilities!

4. Keep your main e-mail address and phone number private

Your reward for sharing your e-mail address and phone number? Tons of spam in your e-mail inbox and hundreds of robocalls on your phone. Even if you cannot avoid sharing this info with Internet services and online stores, don’t share it with random people on social networks. And consider creating a separate, disposable e-mail address and, if possible, a separate phone number for these cases.

Create an additional e-mail account and purchase an additional SIM card to use for online shopping and other situations that require sharing your data with strangers.

5. Use messaging apps with end-to-end encryption

Most modern messaging apps use encryption, but in many cases it’s what they call encryption in transit. i.e. messages are decrypted on the provider’s side and stored on its servers. What if someone hacks those servers? Do not take that risk and chose end-to-end encryption. That way, even the messaging service provider can’t see your conversations.

Use a messaging app with end-to-end encryption, e.g. Signal. Note that by default, Facebook Messenger, Telegram etc, do not use end-to-end encryption. To enable it, manually start a secret chat.

6. Use secure passwords

Using weak passwords to protect your private information is as good as shouting that information to passers-by. It’s nearly impossible to memorise long and unique passwords for all the services you use, but with a password manager you can memorise just one master password.

7. Review permissions for mobile apps and browser extensions

Mobile apps prompt you to give them permissions to access contacts or files in device storage, and to use the camera, microphone, geolocation, and so on. Some really cannot work without these permissions, but some use this information to profile you for marketing (and worse).
Fortunately, it’s relatively easy to control which apps are given which permissions. The same stands for browser extensions, which also have unfortunate spying tendencies. Do not install browser extensions unless you really need them. Carefully check the permissions you give them.

8. Secure your phone and computer with passwords or passcodes

Our computers and phones store a lot of data we would rather keep private, so protect them with passwords or biometric authentication. These passwords do not have to be complicated and unique, but they should keep random people out.

On mobile devices, do a bit better: six-digit PINs or actual passwords rather than four digits and screen-lock patterns. For devices that support biometric authentication (whether fingerprint reading or face unlock) that's generally OK, but remember that these technologies have limitations.

9. Disable lock screen notifications

Why protect your phone with a long, secure password, but leave notifications on the lock screen? Now any passer-by can see your business. To keep that information from appearing on the locked screen, set up notifications correctly. Disable lock-screen notifications or hide sensitive information from the lock screen.

10. Stay private on Wi-Fi networks

Public Wi-Fi networks usually do not encrypt traffic, and that means anyone on the same network can try to snoop on your traffic. Avoid transmitting any sensitive data (logins, passwords, credit card data, and so forth) over public Wi-Fi, and use a VPN to encrypt your data and protect it from prying eyes. If you must connect to a public hotspot, use a secure VPN connection.

11. Browse in incognito or private mode

If you do not want your computer to save your browsing history, temporary internet files, or cookies, do your web surfing in private mode. Remember though, these private modes aren't completely private. When you are searching in incognito or private mode, your Internet Service Provider (ISP) can still see your browsing activity. If you are searching on a company computer, so can your employer. The websites you visit can also track you.

So, yes, incognito browsing does have certain benefits. But it is far from the only tool available to help you maintain your privacy while online. Anonymous search engines and virtual private networks can bolster your online privacy.

12. Use a different search engine

If you are like many web surfers, you rely heavily on Google as your search engine. But you do not have to. Privacy is one reason people prefer to use anonymous search engines. This type of search engine does not collect or share your search history or clicks. Anonymous search engines can also block ad trackers on the websites you visit.

---- Remember ----

"When it comes to privacy and accountability, people always demand the former for themselves and the latter for everyone else."

David Brin