10 Tips to Safeguard Your Online Privacy

Author : Cat

Date : October 2, 2018

When you have something important, you make efforts to keep it safe. You wouldn't leave your credit card out on a bench and walk away, or leave your house keys at the mall with your address attached. Sounds far fetched but it's essentially what we are doing with personal information every day. Your online data, from what you enter to the actions you take, is of great value. This information can be used it to gain access to your home, business, finances, or identity. The crux of the issue is that your privacy is not a priority to the companies collecting this information, which means protecting your privacy is entirely up to you.

Follow these 10 tips to protect yourself, your business, and your family:

List all of the networks on which you have accounts.

If you do this once, thoroughly, hopefully you won't have to do it again. To find the networks and apps you have signed in to, try searching the words 'Welcome' or 'Login' or 'Verify'. Dormant networks continue to collect data on you while you surf the web or via your connections.

Once you have the list:

- Remove yourself from networks you do not use
- Make a note of what is left
- Limit the data you submit to only what is needed

Pick non-language passwords

Hackers use dictionary code breakers to check passwords. Any word in the dictionary can be cracked in less than a second (22 microseconds). Instead of words, combine numbers or acronyms.

Ex. Using the nursery rhyme 'Three blind mice, three blind mice, see how they run"

Poor choice: Three Blind Mice

Good choice: 3BM3BMshtr

To keep your passwords, write them down somewhere safe or better, use clues (like "carving knife" above) which would remind you without giving it away to someone else. There are also software password keepers that enable you to generate very complicated passwords for all accounts.

Set up multifactor authentication

Multi factor authentication is when a system requires you to identify yourself in multiple ways at new logins. For instance, if I wanted to sign in to my bank account on a new computer, they would require my password AND the bank would text me a passcode to my phone. This means a hacker with my password could not gain access with only that information. Learn more about multi factor authentication and then apply it to all of your important accounts.

Manage social sign-on

The average computer user has up to 200 accounts so it's no wonder we want to re-use passwords. Many apps and networks will now let you use Social Sign-on, where you log in via Facebook, Google, etc. This has become the biggest source of data breaches and hacks in the last few years. Check for apps that you have given social sign-in permissions. Remove any you don’t need.

Change default passwords on IoT

Another easy target for hackers are devices on the IoT (Internet of Things) that still have their default passwords. These devices include WiFi connected appliances, toys, and health monitoring systems (ex FitBit). If you don't change the password then it's the same as building a new door on your house and not installing any locks on it.

Verify all of your privacy settings.

This is a big one. Privacy settings are complicated which is why it is so important you understand them. Next time you are waiting (dentist's office, on a plane, etc) take the time to go through all of your settings.

- Review general device settings
- Review social network settings
- Pay special attention to Facebook Settings that are hidden
- Set a reminder to do this annually (because they change)

Turn off unnecessary app access

Access to geotagging (location), camera, contacts, and microphone on your phone all need to be granted by you, the user. If you have allowed access then those app companies have the rights to turn on your microphone, or track you wherever you go. If it's not required, turn off:

- access to your microphone
- access to your camera
- device tracking and geo-tagging

Review your digital photos

All things online should be considered permanent and potentially public. I have numerous examples of how private photos became publicly exposed through software bugs at no fault of the user. Review your digital photos and remove anything on your phone you wouldn't want posted on Instagram or texted to your boss.

Search yourself online

Search yourself online by name and check what you find. Then set a Google alert with your name or anything you care about. Any time a new article is added, Google will send you an email. Or have us do an in-depth search for you.

Familiarize yourself with scams

The best defence is knowing what is coming at you. Learn about the various online scams and be wary! If something seems too good to be true, it probably is.

For more information on protecting your privacy visit our website, or contact us to find out how we can help your company or group. We are all responsible for our own digital data, take back control of yours today.