Protect Your Privacy On Social Media

Let’s be honest, there are many reasons for being on social media: To see what your friends are doing, keeping up with news and sharing our opinions, getting fashion ideas and artistic inspirations or to share your vacation photos with your family.

However, you need to take precautions to protect your privacy online against the risks and dangers that lurk under the surface.

1. Read The Fine Print

Yes, we’re referring to that thing you just clicked “**I Accept**” without reading. Facebook’s fine print has a line that says “We reserve the right to send your private pictures to your mom if it shows illegal activities”. Really??! No. We made that up. But the fact that it could be true should be enough to scare you.

Most of us don’t have the time to read the fine print of every website we register on. Our trick is to pay attention to what the tech media is reporting about and trust them to raise the alarm when companies go over the line such as the media storm when WhatsApp changed their privacy policy to allow your data to be shared with Facebook or the Snapchat saga about whether they own the rights to your photos.

2. Default Settings

‘Recommended’ or ‘default’ settings doesn’t mean it’s the safest. Remember that social media websites want to get as many people seeing, liking and sharing your content as possible. Facebook gives you 3 levels of visibility: public, friends and only you, as does Linkedin and other sites.

3. Location

Missed the last train to get back to your hotel at 2am on your solo trip around Europe? Thanks to your public post on Facebook, your family, friends, and even that kidnapper from “**Taken**” knows exactly where you are, and what has happened. Still sounds like a great idea?

4. Personal Information

“Husband just bought us a cruise package! We’ll be away the whole of next week!”

That’ll probably get you a few likes (and plenty of envious hate) from your colleagues and friends, and it’ll also tell the guy in the neighborhood, who’s been eyeing your expensive watch collection, that it’s time to strike.

Keep your personal information, schedules, and travel plans to yourself, or among a trusted group of people. You never know who is watching.

5. Contests

Free iPhone if you share this post, fill out a form and receive a new Playstation, win a trip to Las Vegas if you visit this site…. We could go on and on. Are you really buying this?

Granted, some contests could be legitimate marketing but that doesn’t mean you should let your guard down. While most companies respect and protect the private information you give, criminals won’t and you could quickly find yourself on the receiving end of spam, hacks and other harmful intrusions.

Thus, make sure that the contest actually exists (a quick Google search), and make sure that the post is actually coming from the official account of a reputable company and not from **Show-Me-Your-Money Inc.** or **Everybodywins LLC**.

6. Romance Scams

Extremely dashing guy from South Africa randomly messages you and introduces himself? Or a very friendly girl from Paris sends you a picture and says hi? Time to wake up. Life isn’t a Hollywood film.

And don’t try to convince yourself that this is different, scammers sometimes build their relationship and trust with their victims over many years, patiently waiting for that big payday when their “grandfather contracts a fatal disease and needs a $500,000 cure that has to be flown in from Argentina”.

7. Ads Tracking

Not technically an invasion of your privacy… well, not a malicious one anyway. Although it can be unsettling, and bad for your wallet, to have ads pop up all over the place, reminding you about that brand new smartphone you were looking at on Amazon. On Facebook, go to the Ads section under Privacy settings to disable “**Ads based on my use of websites and apps**”.