Are You and Online Oversharer?

By Christina Edwards on February 21, 2020

We can all get a little over-excited when sharing things online these days. Check-in to your favorite restaurant on Facebook, hashtag the best beers in town on Instagram, or tweet your anger as you board yet another delayed train into work — and that's just the basics. While sharing *is* caring (everyone loves a picture of Sunday morning pancakes) it's possible you're sharing a little too much about yourself.

Giving away your security question answers?

Security questions these days can be pretty generic. What was your first school, name of your first pet, your favorite teacher, etc. They're usually used when you've forgotten your username or password and want to get back into an online account. Pretty useful if you have the memory of a sieve (a common problem), but also pretty handy for hackers too. Cybercriminals are getting smarter by the second. They take their time to study individuals online for opportunities and weaknesses, especially when it means they could get away with a good chunk of cash at the end of it.

Obviously, you're not shouting out the answers to your security questions (if you are, please, please stop) but there are plenty of ways hackers could get hold of them. Imagine your security questions for Paypal are the ones we mentioned above. Favorite pet, first school, best teacher. Now think about what you share across your social media.

1. #Throwback photo on Instagram to your family dog Steve's first night at home? N'aww look how cute he is, those little paws, that face sosmushylookathim. So now we know your favorite pet's name.
2. School reunion on Facebook, big, open list? Marked yourself as attending?Now we know your first school.
3. Pretty lax on the old Facebook profile security? A quick trawl through your open friends list to find anyone listed as a teacher, narrow them down, and job done.
4. Boom, we've got all the answers to your security questions. Into Paypal we go to drain your linked bank account, see ya later and thanks for the cash.

Again, it sounds dramatic, but this is exactly how criminals commit identity fraud. For a more dramatic version, check this out from the movie "Now You See Me".

What about those fun quizzes?

Finding out what type of take-out you are, which career you're most suited to, or simply commenting on a friendly community post about your favorite cat pics all seem innocent and, yes, they can be. But when you're giving away any information about yourself online, you need to think carefully about *exactly* what it is you're sharing. Your personal data is worth more than you could ever know to hackers. So, when you fill out a fun quiz asking your favorite foods and city, think twice about whether or not it's worth giving away such key information about yourself. Because in the wrong hands, this info can be used in exactly the same way as we discussed above.

Why location sharing is risky

Sharing and talking about your location online is one of the easiest things to do. Check-in to that fancy bar, update your status on what movie you're watching, or show off that leg room from your window seat as you embark on a trip — but posting about these everyday actions could actually be putting your safety at risk. Because by doing these things, sure, everyone can comment and share in your joy, but you're also letting a whole load of people know that you are not home.

It really is as simple as it sounds. For example, complaining about that delayed train? Well, a burglar could now figure out what station you commute from, where your house is, oh, and what time that big ol' house is empty. Sounds far-fetched? Sadly it's not.

What can you do?

Well, the first thing you can do is **stop sharing personal info about yourself online**. Remind yourself to think twice each time you post something. Do you really need to share your location? Think about who can see it and if there's any personal info included. Your personal data on social media is worth protecting.

6 handy tips on how to stop oversharing:

1. Know your Facebook privacy settings and check them regularly to make sure that what you're posting is for your friends' eyes only.
2. Don't openly share anything that can locate you, like your hometown, date of birth, or cell number.
3. Be picky about your friends. Don't accept just anyone, even if you think you know them, always check first.
4. Excited about your upcoming holiday? Great. Tell your friends in person, don't share it online.
5. Avoid posting anything about your routine. Go to the same gym class every Monday eve with your partner? Good for you. Keep it offline.
6. Location, location, location. Turn it off. Always!

These basic steps can really push you in the right, and safer, direction when it comes to sharing online.

It doesn’t have to end there. Even if you’re an online lockbox, it’s still possible for your security answers to be guessed using the most basic info about you. It’s simply the nature of the world we live in today.

How to keep your security questions secure

- Lie about your security answers. As long as you can remember them that’s all that matters. They don’t have to be factually correct.
- Spell your answers differently. For example, instead of “Money”, why not use M0n$y or M0nnEE.
- Use a password manager so you have different and random passwords for every account, and can save your security answers in one place.

So there you have it, your quick guide to oversharing online. Hopefully, if you have been oversharing, this points you in the right direction. And if you haven’t, then well done! Happy browsing.