Almost everyone has a presence online which requires them to create multiple accounts that have personal information. And although this is often avoidable, there are many ways in which you can protect your identity to make your online experience less risky. Three online identity experts share their insight into how to do this in easy, actionable ways.

1. Avoid saving credit card information and passwords online

The convenience of being able to save your credit card information for certain sites and passwords, is great. But it doesnâ□□t help when it comes to trying to protect your identity and private information, online.
When you save your credit card information and your passwords and someone snags your phone or laptop, they will be able to easily access your financial information and other personal details. Itâ□□s risky to have your information easily accessible, so itâ□□s best to not rely on the convenience of saved information. It really only takes a couple extra seconds to retype passwords and credit card details, and will keep your identity better secured on the internet.

2. Update passwords regularly

Isabela Calil, a higher education consultant for TEG London knows all too well what happens when people (particularly college students) donâ□□t update their passwords. Updating your passwords regularly helps to keep hackers at bay from all your personal details online. When you do so, your passwords become less likely to be vulnerable to things like data leaks, which can really put your identity at risk. When we have the same password for every online account, it really increases the chances that it will be discovered, and then all your accounts are vulnerable to hackers.
Try to create different passwords for your online accounts, and to change them every four to six months. It helps to have them written down in a secure place, and to not rely on your laptop or phone to remember them.

3. Use a secure network

Cyber attacks increase when you use an unsecure network. This is because you are using an untrusted network that other people are using as well. Most commonly these are places with free wifi like coffee shops, malls or other retailers that offer this perk. Hackers often look around for these unsecured networks in order to access other peopleâ□□s private information.
Glenn Sands, the managing director of Pixa Prints goes on to say, if you need to use one of these networks, avoid accessing really private information like your banking details, and instead wait to do so on your own secured network.

4. Reduce your online shopping & only use sites you trust

Even though many online retailers have secured checkout systems, there are always issues that can occur when it comes to a hacker getting access to your information. This is why itâ□□s important to try and lessen the amount of online stores that you shop at. The less places that have your credit card information, the better. Itâ□□s also ideal to only shop at eCommerce stores that you trust, and to be cautious of where the items you are buying are coming from. Always check the online reviews to ensure the store is legitimate, and check for the secure checkout symbol when making any purchases.

5. Always password protect your computer and phone

The founder of Green in Black and White, Oliver Green says, you never know when you could become a victim of theft when it comes to your phone or computer. This is why you should always password protect these devices, to make it tougher for people to be able to access your information. Always avoid simple passwords like your year of birth, and instead choose something more obscure that would be tough for someone to guess.
You should also never leave your phone or laptop unattended when in a public place, and to invest in screen

protectors that make it difficult for people to see what you are looking at on your devices.