

## Is your information safe?

We live in the digital age. We live in an age where everything we do is online. We bank online, we communicate online, we send pictures online, and we even pay our mortgage or our bills online. With everything we do done over the internet, how safe is our information? Many experts have suggested that “safe” is a word that does not even belong in the same sentence as “information” when regarding internet safety. There are billions of people who use the internet. Not every one of them is the same. It is the same with online vendors and people running their businesses online. Not every one of them has good intentions. It can be very difficult to decipher who is good and bad online; that is now something we can easily depict for ourselves by learning basic internet security.

Although the internet is an excellent utility to guide us through our daily life, it also has a darker side. Many people use the internet to capitalize in the expense of others. The most common type of internet safety violation is the selling of your personal information to marketing companies. This information includes your name, phone number, email, and address. Marketing companies are always looking for people to sell to. That could sadly be you. If a marketing company gets their hands on your information, you will get non-stop phone calls and emails from these people claiming your information “landed on their desk from a friend.” This is not the worst thing that can happen to your information, but it can be very annoying. These nonstop calls and emails can wreck havoc on your daily life because you have to sort through them to find calls and emails from people you actually care about.

The second most common abuse of your information on the internet is the selling of some of your more personal information to hackers. This information can include your credit card number, bank account info, and social networking passwords. Hackers frequently trade this information back and forth throughout the black market looking for larger ways to capitalize on your info. These methods can include bank account withdraws, small, untraceable credit card purchases, and posting affiliate links/spam links over your social media account to get your friends information. Due to several updates, the last one is now more uncommon, which is good news, but it still happens. It is important to never log into a website you do not trust using Facebook, because this is how they get your info.

So how do you stay safe on the internet? There is a lot of bad things going on out there, and you need to make sure your information stays secure. The first thing you can do is be careful where you put your information. Hackers get your info by you placing your info where it should not be. Do not create accounts on websites you do not trust. Never buy anything online unless you do so through a safe payment gateway such as paypal. Also, never directly give your credit card information to a website that does not have an SSL certificate. One of the best ways to stay safe is to get a [Reputation Company to completely remove search results](#). If your information appears on the web, a good reputation company can remove it for you without it getting in to the hands of other people looking for immoral gains. It is also important to teach your family members about internet safety, because they might be asked to give out information about you. Just follow simple internet safety rules and you will stay safe.