



## **Fake ID Usage on the Internet**

The internet is also what is known as a cyber zone. In this cyber zone, people can be at several places at the same time via the internet. Usually, the jurisdiction of an individual using the internet is defined by the laws of the country where the individual is, where the server he is using is located and where the other party he is doing business with is. This three way jurisdiction of the law can cause a conflict which is confusing at times.

There have been many arguments regarding the laws of the internet. Many have said that since it is in another plane entirely, then another set of laws must be made for it. Other also says that it is best to leave internet users alone and not to connect the two planes, reality and virtual worlds together. In spite of so many opinions, the (1) [laws for the internet have still remained under the jurisdiction](#) of the country where the user is physically.

Identity theft in the internet is so easy to do if you do not learn to protect yourself. The main goal of the thieves is to get as much personal information from you as possible. This is so that they use this information for them to assume your identity and use this to their advantage. They will use your credit cards to make purchases; they will use your other personal information to make loans for themselves and they will leave you to pay for all of these when the billing comes. Virtual thieves can get these kinds information from your very own personal computer. Individuals store personal information in their personal computers, information like your tax information, bank accounts, financial documents and other personal documents which may reflect you family or your background. Even data like pictures and videos are not safe from virtual thieves.

One way you can keep yourself and your data safe is by using passwords to keep your computer and any other electronic device you have harder to crack open. It will usually deter most criminal minds especially if your password is pretty difficult to decipher. Not all thieves are that knowledgeable in the technology field. It is also a good idea to change passwords regularly. This may be more difficult than it sounds because it is difficult to keep on remembering passwords let alone those of several electronic devices which you may have. You may try to rotate several passwords among your devices but this is not advisable because virtual thieves might figure this out sooner or later. One more way of deterring thieves from getting your personal information is not to use the "remember your password" feature in your computer. This may be a very convenient tool for you but it is also a convenient tool for the thieves.

Using anti-virus software and regularly updating it is also a good way of stopping thieves from hacking into your computer. Anti-virus software not only stops viruses, Trojans and worms from destroying your computer it also keeps them out. Some worms which can be undetected by (2) [unprotected computers leave a portal](#) or doorway open which can be used by hackers to get into your system. It is also advisable to keep your operating system up to date by using automatic updates features of most operating systems. Manufacturers of the operating systems regularly send updates of their software that may have anomalies to help and prevent degradation of your operating systems. Installing a firewall will also help your computer survive in this very brutal cyber world full of viruses and hackers who mean to do you harm.

Any form of connection to and from your computer is a candidate for hackers and thieves to enter and use your personal information. File sharing is a potentially dangerous thing to do since you may not have any control over what files they can get from you especially if the people you are sharing with are more experienced in hacking than you. File sharing leaves you and your computer open and vulnerable to attacks from the outside.

Now, despite these precautions outline above, you are one of the factors which can lead hackers straight to you and your personal information. Please refrain from replying to dubious or suspicious emails that require your personal information. Some of the emails may be notifications of you having won in a lottery or having been chosen to receive free gift etc. Be suspicious of these emails, especially if you have not entered any



**Fluxcard.com Fake ID Articles**  
**Original Research Articles © Fluxcard.com 2007**

lottery or contest. Refrain from using public computers and if you must, always log out of websites that are confidential.

- (1) <http://www.bbbonline.org/idtheft/virtual.asp>
- (2) <http://www.staysafeonline.info/>