

Protect Your Identity When You're Online

The Internet's virtual world is an endless source of information, a thriving business area, a very active social scene and, last but not least, a place where evil does flourish. And it's not just about hackers, but also about criminals from real-world who are waiting to find out each of your steps. This information is available because of you, from ignorance or neglect...

"Antisocial" media

In December, the most successful social networking site on the Web, Facebook, decided to make a bold move. The company protected personal information of users until last year, then the security settings became open. In other words, anyone browsing the web can find your pictures, e-mail and so on. Moreover, also the thieves admit that before it was much harder to act. Now on the Internet, they watch and wait to find out when people go on holiday and then they give a hit.

What can you do to protect yourself? First of all, do not add any stranger in your list of friends. However, as for social sites, their role is to make as many friends as possible so this may be a really difficult goal. Specialists' advice is to be more careful about your posts: for example, if you go on vacation, you should speak about it only after you come back. Don't publish personal information such as your home address. You shouldn't upload intimate photos. It would miss only to say that you hide the key of the house under the carpet and the flatware would be complete.

Install the updates and don't forget about your antivirus program.

In recent times, hackers target ordinary Internet users. They infect various sites with malware which is then infiltrated into your computer enabling them to steal personal information; they almost change you into a "zombie" who spreads spam and online viruses. What's worse is that the attacks are now almost imperceptible, coming from trusted sites. A research of Google says that no less than 300,000 sites are infected; this is twice that of two years ago. Internet Explorer and Firefox are favorite browsers for the attacks. If you constantly update them, then you can be sure that you can surf safely through the Internet. Nevertheless, vulnerabilities can be covered only with security software. Or you can opt for Google Chrome, which is newer, less known and updated, so the attacks are rarer and more difficult to organize.

Be careful where you put your credit card number!

Do not believe in any advert! Many of them are malware. The most popular attack of this kind is the alert that your computer has viruses so that you should buy software to help you get rid of them. The problem is that you have to pay by entering your card number in a program and a lot of people are deceived by this. Basically, if you close that window, you should get rid of the problem, but to be sure, scan your computer!

Gathering useful information from the Internet may not be very simple or it may be deceiving sometimes, but if you are just a bit attentive to your security while you're online, many doors will be opened for you.