Youth Panel

cyber safety

καλύτερο διαδίκτυο για τα παιδιά

Tips to protect your privacy on Social Networks

By Christakis Nonis, student and member of Cypriot CYberSafety Youth Panel

Nowadays technology has penetrated almost every domain of our everyday life. Therefore, social networking preoccupies a significant position in our routine. According to the measurements for 2017, the number of social media users amounts to 2.46 billion, a huge number considering that this is approximately one third of earth's total population.

The fact that these media have such popularity has triggered the interest of perpetrators, who are constantly inventing ways to deceive the user and / or intercept her personal data. In this article we will investigate some ways by which we can make the use of these services safer.

Be informed about privacy settings

The first step you should take (which many of us ignore), before opening such an account, is to be informed about their privacy policies. We know and we agree that reading the long text on terms of use is boring, but is as necessary and should be done. This text includes important information about potential risks and how the user will benefit the most from the privacy settings of the respective medium.

Make sure your password is strong

Although a simple password is relatively easy to be memorized (for example our phone number), it is just as easy for someone to "guess" it. When creating the password for your account you should avoid simple words or a series of numbers, since in such a case one would be able to decipher it in a very limited time. A powerful password consists of a mixture of characters (both capitals and small ones), numbers and symbols.

Revise your password - Avoid using a single password for all of your accounts

The importance of setting up a strong password is the same as its revision. Ideally, you should change your password every month. You should also avoid reusing codes you have already used in the past. Under no circumstances should you use the same code in all your accounts. This would affect most probably all of them, if you become the victim of an attack on just one.

Use all identifying features

Certain social media tools include more than one verifying stage for their users. This usually involves entering a code that the user receives by SMS. This step does not only constitute an additional security measure, but it also warns in many cases the user when someone tries to access her account.

Take special care when publishing content

Great attention should also be paid to the process of content sharing. Certain websites encourage users to make their posts visible to everyone else. So, before you start sharing your photos or your location, choose the type of users who will be able to see your post (only your friends, only you, etc.).

Do not answer questions regarding yourself or familiar persons

Almost all of us have received messages in our inbox with questions such as: "Are you in this video?", along with a link. Be aware that this is a spam or a virus and you should not click the link. If for some reason you clicked on such a link, make sure you change your password, alert your friends that it is a form of a fraud so that they can avoid it and contact the service of the site to get the necessary guidance and report the event.

Avoid links with misleading titles

Many times you may have seen posts titled "See what happens in the next episode of the X series". Although most of the times it's just clickbaiting, there are cases that they lead to other pages which contain malware. So think twice before you click the link.

Avoid links with misleading titles

A highly widespread method for stealing your codes is phishing. Through this process, the crooks will "convince" you to fill in your information on a page that is similar to the one you use. In order not to be found in a difficult situation, before proceeding with the entry of your information, check that this site is secure and that the URL is consisted only of the name of the social network page.