Тютюнник Р. С. - курсант навчально-наукового інституту № 2 Національної академії внутрішніх справ

ACTUAL ISSUES OF PERSONAL DATA PROTECTION IN THE SOCIAL NETWORKS

In recent years social networking sites are widely used not only for personal communication but also for solving business problems. For example, recruiters often use these resources to find candidates for the respective positions. The user must specify your personal data. How to protect yourself from fraudsters and other criminals in social networks?

Any social network involves some information about the registered user. The list of the data can be quite wide - from the name, age, place of residence to favorite actor, colors, etc.

Management of social networks together with users have a need to protect personal data. One of the most pressing security challenges in this context is to ensure the confidentiality, in other words - the provision of one’s personal data only to a predetermined group of people within a social network (such as friends only). In addition to privacy it is also important to ensure the integrity of personal data as well as mechanisms to ensure the authenticity of the user's page.

Methods of protection. How can we protect one’s personal data? This will require the implementation of the following recommendations:

- Use the security mechanisms provided by the social networks;
- Use common security mechanisms that are not tied to social networks;
- Staying in a social network, perform actions which do not threaten your personal data.

Let's explain what is meant by each of these points.

Almost all social networks have rules of restricting access of different users to the information contained on the user page. For example, you can give access to one of your albums to all users, while to the other - only to friends. Also you can provide the ability to view the posts' comments on your wall only to some of your friends. So, you can attentively configure access to your page in the social networks.

We should also mention the search in the social networks which allows any user to view a specific list of information about a particular profile (even if it is protected from viewing by all other users of the social network). Its essence lies in the search of the (already known) profile using search filters. For example, all information we know about the profile is only the name and the country of residence. Entering this information in the search we get a number of profiles with the same parameters. Then we can add an additional filter such as the age. If the interested profile appears again in the search results, we can continue clarifying other information in a similar way, using other filters. If no, you need to use other filters. Of course the algorithm can be optimized [1].

Common security mechanisms which are not tied to social networks include the use of a secure protocol interaction with Web-servers. In other words, when you enter and stay in the social network, you must use https. This ensures secure transmission of information over the network (but reduces the data transfer rate), including a bunch of login and password. But this protection technology must be supported by an information system (almost all the social networks support it).The data of the user profile which is left by the browser in the form of files or records on the computer should be cleaned regularly. In some cases, such data may be used by malicious software to obtain from it some important information (e.g., the same bunch of login and password). It is also important to install suck pc programmes as antivirus. But do not forget about mobile devices with which recently many people enter the social network. These devices locally store personal data from social networks and also exposed to malware. Thus protect mobile devices too.

Finally, social networks users should be mindful. For example, do not add strangers to friends or join suspicious groups, set incomprehensible applications within social networks. Also do not click on links received from strangers. In general, you need to follow some basic safety rules.

It is important to regard such thing as social engineering which is one of the most effective tools to obtain your personal information. Its essence lies in the creation of certain situations in which people by their own hands give their personal data to malefactor. Typically, these situations involve either introduction of a person in the uncomfortable psychological state in which it is necessary to take quick and usually wrong decision, or, on the contrary, the creation of the atmosphere of trust in which people are ready to talk about their personal information (but it will take much time).

In the context of social networks an example of creating an uncomfortable psychological state can be on the phone call with the following phrase: "Good day! You are called from a social network "network name". My name is Andrey Ivanov, the operator № 4357. The fact is that at the present time somebody is connected to your profile from Canada and Indonesia. Please give me your login and password to protect your account." After such phrase some of the users will certainly give this information [2].

So, here are some tips, how you can protect your account in the social network. I hope, they will be useful enough for you.

Reference list:

1. How to protect yourself and your data when using social networking sites[Електронний ресурс]. - Режим доступу : https ://securityinabox. org/ chapter-9.

2. Усманов Ю. Социальные сети: защита персональных данных или охрана граждан спецслужбами? [Електронний ресурс] / Юрій Усманов. - Режим доступу: http://www.pravoconsult.com.ua/vyzov-sotsialnym-setyam- narushayut-konfidentsialnost-ili-spasayut.