Maria Petukhova
V.I. Mieshkov, research supervisor
I.I. Zuyenok, language adviser
National Mining University, Dnipro, Ukraine

The Tips for Social Networking Safety

The Internet is definitely not secure. Most of us have ever encountered security problems in the social networks. The most common troubles arising in the network are: the issues of confidentiality, hacking and stealing passwords and potential problems in the workplace. Some tips how to deal with these problems are given in this paper. When posting information about yourself in social media, anyone must be prepared that a large number of people all over the world can see it. Thus, your private life becomes public. Even if you take all the measures for your personal information protection from people you don't know, these attempts, may be useless as there are many hacker programs that help to select passwords for popular websites and hack them. Moreover, people face potential problems in the workplace because of social networks use. For example, you can post information about colleagues or your boss that can be interpreted as a disclosure of confidential information, discrediting you in the eyes of the company, that may lead to serious consequences.

Modern HR-recruiters use social media in order to clarify the past of their applicants or search for potential employees. So, they can view your accounts in social media even if you are. not an active job seeker in the labor market. Though your data may be temporary and be deleted at any time, at the same time other people can view your data and copy or even save your photos, videos and posts etc. Moreover, any information that is too frank or discreditable may become known to any interested person. The dangers hidden in social networks are more than real. You can enjoy the use of social networks, but it is worth doing this deliberately and with caution. For this you should follow the next rules. First of all, keep your personal information private. Make sure you make all of your personal information private or visible only to your friends. Tagging or posting your specific location is an exciting feature, but not everyone needs to know where you are at any time as this makes you personally and your home vulnerable, especially if your profile is public.

Always log out of your social media. This is especially true when you're using a public computer at a library or hotel. The reality is that we all have some private information on our social media — even if it's only our name and a photo — and you don't want to give someone easy access to your identity.

Be careful about installing extras on your site. Many social networking sites allow you to download third-party applications that let you do more with your personal page. Criminals sometimes use these applications to steal your personal information. Use strong passwords as they are one of the keys to protecting your identity, so make them effective. Finally, be selective about who you accept as a "Friend" in a social network. Identity thieves might create fake profiles in order to get information from you.