METHODS OF REDUCING THE RISK OF IDENTITY THEFT WHILE USING INTERNET

Chala O.I., Tsymbalist A.V.
Scientific adviser: Ph.D, Assoc. Prof. Kovalenko S.M.
Kharkiv Petro Vasylenko National Technical University of Agriculture
Department of Cybernetics, Alchevskich Str., 44, Kharkov, 61002,
tel. (057) 716-41-70
E-mail: agrocyber@gmail.com

Every year the number of Internet users in Ukraine and in the whole world is increased. According the data, providing by site *internetlivestats.com*, in the summer of 2016 this number in our country was 19 678 089 persons, and about 3 424 971 200 Internet users in the world and this figures are increased every single day.

So, the volume of users' data is increase too. Because today it is common to do a lot of things via Internet from paying utilities to buying flight tickets. Simultaneously with increasing the number of services that Internet sites provide, the number of cyber threat is grows too. For average user the most common ones are activities related to identity theft. Identity theft is term used to refer to all types of crime in which someone illegitimately obtains and uses another person's personal data in some way that involves fraud, deception or utilisation them. Usually (but not always) the goal for this activity is economic gain.

Despite the fact that ways of identity theft evolve rapidly as new medium, e.g. social media, develop quickly (so it is almost impossible to prevent identity theft), it is possible to reduce the probability to become a target via taking particular precautions, such as:

1. Use an encrypted connection by the HTTPS protocol to protect your login and password.
2. Do not log in to social media, e-mail and bank account via public access computer. But if it is necessary, make use of the additional verification processes (such as phone verification, SMS verification), never click on "keep me logged in", always log out, and use the right privacy settings on social media.
3. Use the right passwords: a) use different passwords for different sites; because creation the various password for all accounts is almost impossible, some experts recommend create unique password for most important site (including social media and e-mail) and one password for the rest ones; b) change the passwords every three month; c) the safe password must be made up from at least 8 symbols, and be a combination of letters in the lower and upper cases, numbers and special characters; d) to recover the password, use the binding to mobile phone.
4. Do not clicking on links that come from unfamiliar senders in social media and e-mail. If it is necessary, at least check the URL and do not log in to suspicious sites.
5. Making purchases on online stores, inquire about them, do not trust the free web hosted ones and use virtual keyboard to prevent from keystroke logging. It is better have a special credit card or debit card with daily spending limit
6. Completely destroy all documents that contain sensitive personal data.