Introduction

In order to improve their services, banks included online banking solutions as one of their priorities. As a result, we have a huge expansion of online transactions in the Republic of Serbia in the last several years.

In fact, online banking services leave more time for users to improve their own business or to spend some more quality time with their families, friends or in any other way.

Banks, being service providers, will also have more time for the development of new products, as well as for the availability to the customers.

Taking these benefits into consideration, it is obvious why the number of e-banking users grows daily.

The potential threat during the use of e-banking is the possible abuse of your bank account by an attacker, i.e. hacker. We shall describe some of the most frequent types of misuse related to e-banking.

Phishing attacks

Phishing attacks are the most frequent type of misuse by hackers, whereby the attackers try to obtain your credentials (user name and password) that you use in accessing the e-banking application, or account number, social security number, etc. In the process, they send you an e-mail message presenting themselves as your online bank and asking you to change your credentials, and then send you a link to a fake web page where you are invited to make this change. This way they can steal your credentials, gain access to your accounts and exploit them whenever they please. Additionally, hackers can impersonate any other institution or even present themselves as another individual. Users should know that banks, and all other legitimate institutions, will never ask the user for credentials, so you should pay special attention and ignore messages requiring you to provide or change your credentials during login or use of the e-banking application. Users shouldn't change credentials on demand, but when they find it suitable (the recommendation is to change your password quarterly).

Malware attacks

Malicious code, better known as malware, is one of the frequent types of possible misuse by hackers when it comes to e-banking applications. This software enables the attackers to steal your personal account data, or steal your account, or create a fake Bank web page

presenting it as a legitimate web page for online transactions. Malicious software can collect data you enter on your keyboard during the login process. The data collected this way can be misused by hackers at any time.

During the login process, malicious software can run a hidden window of an additional Internet search engine, which interposes in front of the legitimate bank Internet site you are trying to access, thus transferring the money from your account to another account of hacker's choice.

By using malicious software, hackers can also create a fraudulent Internet site, posing as a legitimate one. Unless users are cautious, possible data leaks can lead to a potential unauthorized access to users' accounts.

This is why it is so important to pay attention to the address line at the top of the Internet search engine page (beginning with HTTP:// or HTTPS://) and check if the Internet address of the bank you are trying to access is correct.

Examples of data tampering include number and letter swaps, such as in the word „Online", where the letter „O" is replaced by the number „0" (zero), or when the Internet TLD extension „.rs" is replaced, for instance, by „.sr", while the rest of the address line remains unchanged. By clicking on such link, one logs in to a fake „e-bank" account, on a fraudulent Internet page.

Recommendations

The described examples are some of the possible misuses, while the hackers daily work is focused on attempts to find new ways of getting your money. In order to prevent possible fraud, it is necessary to pay attention during each login session to your e-banking application. Above all, the following is advisable: creating strong passwords containing at least nine alphanumeric characters (capital and small letters included), keeping passwords safe from third persons, regular password changes (recommendation - quarterly), careful opening of e-mails from unknown senders, avoiding clicking on links that appear suspicious, checking URLs for accessing the Internet e-banking applications etc. It is equally important to install antivirus software and update it on a regular basis.

By applying these recommendations, you will significantly decrease the possibility of any kind of your e-banking accounts abuse. Absolute protection, unfortunately, is not possible. At least not for the moment.