National CERT of the
Republic of Serbia

SRB-CERT

REPUBLIC OF SERBIA
RATEL
REGULATORY AGENCY FOR
ELECTRONIC COMMUNICATIONS
AND POSTAL SERVICES

01 Introduction

Information security is one of the current buzzwords in all society segments, both worldwide and nationally. The Internet stopped being used just for fun and leisure, today it is an integral part of everyday life, both for professional and private purposes. Consequently and unfortunately, the Internet has also been bringing threats and challenges for over twenty years, not only to individual users, but to the complete society: cyber attacks on the information infrastructure of the government bodies, financial institutions, various companies, academic associations and even computers in our homes, have become more and more frequent.

In this document, the National CERT of the Republic of Serbia will share with computer and mobile device users its knowledge and experience in the domain of safe Internet use.

The way we use computers and mobile devices is of utmost importance, since the danger of data loss, identity theft and inability to access data and credentials is more imminent than ever, with the rising rate of computer abuse for accessing other PCs. The end goal of cyber attacks is obtaining illegal financial gain, in most cases. The aim of the National CERT of the Republic of Serbia is to inform the users about the basic principles of safe Internet use, and the benefits it brings.

The aim of the National CERT of the Republic of Serbia is to inform the users about the basic principles of safe Internet use, and the benefits it brings.

It is generally known that millions of people around the world continuously use the Internet. The majority of them are cautious users. However, there are some malicious Internet users who, hidden behind the virtual curtain, try to jeopardize Internet-based activities of other users in various ways.

There are different ways of malicious access to computer systems. They are mostly divided into active and passive ones. The active access includes data changes, which can later be detected by forensic analysis, while the passive access is harder to detect, since it does not involve any change of data within the information system, but rather consists of network „listening to" and/or data interception, and is most commonly used in espionage activities.

Some of the ways the malicious Internet users choose for accessing computers and mobile devices are Phishing, intrusion into inappropriately protected private or public fixed wireless Internet access points (Wi-Fi) or wireless data transfer connections (Bluetooth), or exploitation of vulnerabilities of the installed software solutions.
Simple methods, like Phishing, Spam and similar are used in most cyber attacks.

02 Phishing

Phishing is employed by malicious Internet users to send e-mail messages to as large a number of addresses as possible, in an attempt to make the recipients follow the included instructions. Phishing messages frequently contain a fake link or form, supposedly forwarded to you by your bank or Internet provider, with instructions to fill it in and enter your personal data. In this way, the malicious Internet users try to obtain your personal data, i.e. credentials – user name and password, which they subsequently intend to use to access your accounts, such as Facebook, e-mail and similar.

Consequently, malicious Internet users can change your account content, send messages, photos or video recordings to your friends or other users. This kind of misuse is potentially harmful not only to you, but also to your family members, friends and even to people who receive only one such message and who you actually do not know.

03 Safe Wireless Access

The standard configurations of today's computers and mobile devices are Wi-Fi (fixed wireless access to private or public networks) and Bluetooth (wireless data transfer connection) enabled.

Wi-Fi provides a simple and easy use and access to the desired Internet content, both at home and in public places such as hotels, restaurants, educational or cultural institutions etc. The important thing to remember is that Wi-Fi access is available not only to you, but to all other Internet users in your proximity sharing the same access point. If some of them happen to be malicious users, they shall have the opportunity to take advantage of the vulnerabilities of such data transfer and access your data and accounts. That can include sharing of photos or video recordings from your account, but also sharing photos and videos which do not belong to you, thus causing significant damage. The National CERT of the Republic of Serbia particularly recommends not using public wireless Internet access points while executing financial transactions or checking the account balance, unless the access point is adequately protected. The wireless Internet access points on PCs should be password protected, and passwords should not contain data related to your birthday, pets' names and similar, since these passwords can be cracked easily.

04
Malware

The majority of PC users are already familiar with terms such as Trojan, Worm or Virus. Some of them even suffered from direct consequences caused by such malicious software. Unlike other types of computer misuse, malicious software can cause the biggest damage to end users, as well as to information systems in general.

Special attention should be paid to the malicious software installed into computers exploiting operating system vulnerabilities. Such installation makes it possible for its author to take complete control over the computer, without the owner even being aware of it. In addition to PC operating system (i.e. Microsoft Windows, MAC OS) vulnerabilities, there are also vulnerabilities related to the installed web browsers (i.e. Internet Explorer, Opera, Google Chrome), to the multimedia content reading applications (i.e. Windows Media Player) or documents (i.e. Adobe Acrobat Reader).

The National CERT of the Republic of Serbia would particularly like to warn about one type of malicious software known as „Ransomware“. Malicious Internet users install this type of malicious software into computers, i.e. information systems, in order to encrypt data and disable data access, causing immeasurable damage. Counting on the general users practice not to backup data, the malicious user demands ransom in exchange of encryption keys which will enable the owner to retrieve information and access the infected databases. The main problem with ransomware is there is no guarantee that, after paying ransom, the owner will actually get the encryption keys or, even if he does, be able to access all the data infected by the malicious software. Additionally, if they pay ransom, the victims allow their money to be used for funding criminal organizations. Therefore, the recommendation of the National CERT of the Republic of Serbia, as well as other organizations dealing with information security, is to refuse to pay ransom.

05

Recommendations

There are several recommendations on how to protect your computer from malicious users' attacks, the most important one being the installation of an Antivirus software. This will prevent easy access of malicious users to your PC or mobile device. Additional types of protection are: installation of a Firewall, timely updates of the operating system and computer or mobile device applications, use of automatic updates and creation of strong passwords. A password should contain all types of alphanumeric and special characters, in order to prevent unauthorized access by its complexity. A strong password should not contain personal information, such as the day of birth, names of parents, children or pets, since these are the data malicious users enter first in their attempt to access the computer.

Additional types of PC protection basically include cautious use of computers and numerous benefits of the Internet. Regular backups of all important documents are essential, and so is paying special attention to opening potentially infected attachments received in e-mails. Messages sent by unknown users should not be opened without previous verification. It is recommended to visit only protected Internet web pages, those containing the protocol label http:// or https:// (Hypertext Transfer Protocol Secure) in the address line.

The National CERT of the Republic of Serbia urges parents whose children actively use different kinds of social networks on the Internet to explain to them, in an adequate manner, which data and contents can or should be made public on an Internet account, and which information should remain private. The consequences of inadequately published Internet content may be psychological and can severely affect children, like in the often encountered cases of bullying and online harassment.

06
Conclusion

The Internet is a part of our everyday life and, as such, it is permanently being improved, both qualitatively and quantitatively, with a final goal of making the users' life easier and more interesting. All these benefits also give space to potential misbehaviour, making the users more exposed and vulnerable. Therefore, the National CERT of the Republic of Serbia, in cooperation with other CERT teams, does its best to provide maximum protection to the Internet users.

Be responsible to yourself and to others while using and enjoying the Internet!

REPUBLIC OF SERBIA

RATEL

REGULATORY AGENCY FOR ELECTRONIC COMMUNICATIONS AND POSTAL SERVICES

ADDRESS
Palmotićeva 2
11103 Beograd
Republika Srbija

www.cert.rs