УДК 621.392

# ПРОБЛЕМЫ БЕЗОПАСНОСТИ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ

***© 2017 А. Р. Алимбеков, Е. А. Авдеенко, В. В. Шевелев***

*Воронежский институт высоких технологий*
*ОАО концерн «Созвездие»*
*Российский новый университет*

*В статье рассматриваются основные опасности, с которыми можно встретиться в интернет-пространстве. Даются рекомендации по инструментарию, при помощи которого можно защититься от вторжений.*

*Ключевые слова: безопасность, интернет, сеть, программа.*

The computer industry has had a few lulls in growth, but it's still a huge industry. Computers are getting cheaper, and as a result they are making an appearance in a greater number of households.

Consumers want convenience, and they want to do everything electronically from buying groceries online to picking up that hard to find antiques in on-line business transacting companies. Very few people have been scared off from owning a computer or getting internet service. But all of these development in internet technology, brought up the issue of security. It started to become a serious problem in the late 90's. During that time companies reported to be loosing billions of dollars through security loopholes through World Wide Web.

Most of the security problems encountered on the Internet are due to human mistakes.

Common Internet Security threats include:

«Viruses»

News Groups

Chat Rooms

Spyware / Adware software

Home Page Hijackers

Scum Ware

Pop Ups.

The above list is NOT an exhaustive list of Internet Security related topics, NOR is it aimed at the more complex needs of business.

Virus

What are «viruses»?

These «Viruses» are basically little software programs that can be spread in many different ways.

The difference between a computer virus and other programs is that viruses are designed to self-replicate (that is to say, make copies of themselves). They usually self-replicate without the knowledge of the user.

Viruses often contain 'payloads', actions that the virus carries out separately from replication. Payloads can vary from the annoying messages that display on your screen, to the disastrous which attempt to overwrite the Flash BIOS and cause irreparable damage to YOUR computer.

Different Types of Virus

These programs that can infect your computer are split into various different types called: Viruses.

Trojans – are simply programs that conceal their true purpose or include a hidden functionality that a user would not want

Worms – are characterized by having the ability to replicate themselves and viruses are similar except that they achieve this by adding their code onto third party software. Once a virus or worm has infected a computer, it would typically infect other programs (in the case of viruses) and other computers.

Most of virus we get them from the internet when we download virus-infected files. Most of the virus will usually not affect your computer, still, some of them might contain damageable programs for your computer or even allow a distant user to take control of your computer. These programs are called a «Trojan Horse». While some people may believe the opposite, it is impossible for someone to download potentially damaging files to your computer without your content, as long as you don't let your computer filter your downloads. At the same time, it is barely impossible to simply «get a virus» by surfing on the Internet. Virus mostly come with downloaded files that you

Алимбеков Амаль Рамильевич – ВИВТ АНОО ВО, студент alimbekovramillfert@yandex.ru.

Авдеенко Екатерина Александровна – ОАО концерн «Созвездие» специалист, e-mail: avdddekale50c@ymail.com.

Шевелев Владимир Владимирович – РосНОУ, студент, e-mail: shevelevlevvlamiu@yandex.ru.

usually consented to download or in attached email files that you opened without previously checking it. News group Internet News Groups are a place for online discussion of topics of interest. These are usually text messages placed by their writers into the newsgroup where other people can read and reply to them. The groups are public, open to anyone to read and write messages, and often also share computer files such as photographs and sound files.

However, while there can be lots of valuable information taking place in newsgroup discussions, there can also be a lot of useless content too and they form part of your Internet Security awareness!

Obscene material is common in some newsgroups, while other groups have been used for criminal activity such as exchange of child pornography.

Don't believe everything you read online. For example, there have been cases of criminals trying to affect share prices by spreading false information in newsgroups.

Chat Rooms

Ask most young teenagers if they have ever used a Chat Room they will answer yes.

But do you know what a chat room is and the dangers involved? Are they an Internet Security risk?

Internet Chat is a way for people to communicate live with each other by typing text messages which are seen immediately by everyone present in the online chat «room». It is a sociable activity, and very popular with young people as a way of meeting and talking to friends and establishing relationships.....

BUT you have NO real IDEA who is in the chat room. People lie about who they really are and many paedophiles use chat rooms to talk sexually to youngsters! Very disturbing!

Spyware / Ad ware What Is Spyware?

Why is it called «Spyware»?

While this may be a great concept, the downside is that the advertising companies also install additional tracking software on your system, which is continuously «calling home», using your Internet connection and reports statistical data to the «mother ship».

While according to the privacy policies of the companies, there will be no sensitive or identifying data collected from your system and you shall remain anonymous, it still remains the fact, that you have a «live» server sitting on your PC that is sending information about YOU and YOUR surfing habits to a remote location.

Home Page Hijackers

What Is A Home page Hijacker?

Once one of these nasty programs gets onto your computer, it will constantly reset your homepage (and maybe Search, etc.) to where they want you to go. You can't change it back!

Typically, hijacker programs put a reference to themselves in your StartUp folder or Registry Run key, so that the hijacker runs every time the computer is started. This kind of activity does still present as an Internet Security risk, after all THEY have now taken over part of YOUR computer!

If the user tries to change any of these settings, the hijacker changes them back, sticking the user with the hijacker's site unless the hijacking software can first be found and removed.

Scum Ware

What Is Scum Ware?

Ezula's TopText is a virus-like collection of programs that gets installed onto YOUR computer when you download and install programs such as the new KaZaa system which has replaced the popular Napster program. (This allows people to download pirated copies of MP3 music files.)

Statistics from Download.com shows that KaZaa has been downloaded over 7 million times just from their site. If you read the user reviews for KaZaa you will see that most users are very upset about the programs installed that do not relate to file sharing. They don't like the programs that spy on you while you are online and send the data back to the media companies wanting to sell your private information with advertisers.

What happens with Scum Ware is that you visit a reputable site but certain keywords on that site will be underlined as a link. When YOU click on them YOU are taken to an advertiser's website (These can be pornographic websites.)

Now the company/person that created the website did NOT put these links there. It is the Scum Ware software sitting on your computer that is doing this.... Most folks are shocked when i explain this to them! This may seem a low Internet Security risk, and it probably is.... BUT it is not an activity that ANY IT security expert would condone...

Pop Ups

What Are Pop Ups?

Often, when you visit a website, another smaller window will appear in front of the page you requested. Again this is a low Internet Security threat, BUT it can be VERY annoying while surfing the Internet.

A few years ago this technique was ONLY used by, and still is used by, reputable websites. Some even use «Pop Under's» – where the new window appears under the Internet page you requested.

Solutions

Use of Firewalls.

The term firewall is often mentioned in the press and computer magazines. You may even have one on your computer.... BUT what exactly are they?

A firewall is a piece of hardware or software that protects you form intentional hostile attacks on your computer. For most home users this will take the form of a piece of software installed on their computer. This kind of defence is VITAL in supporting your Internet Security.

However with many small business running from peoples homes these days, some may have a small hardware firewall that all their computers will use to protect them.

What do they do?

Basically a firewall examines ALL the "traffic" (the name given to all the bits of electronic information entering and leaving your computer) when you are connected to the Internet.

Firewalls use «rules» to determine if they are going to:

Refuse «traffic» from certain internet addresses. Refuse certain types of «protocols» e.g. Telnet or FTP (ways of accessing a computer over distances). Refuse suspicious looking traffic. Refuse attempts to probe your computer for information. Refuse certain files types e.g. MP3 files.

Anti Virus Software.

What Is A Virus?

You can not escape the fact that at some point you are going to get infected by a computer virus if you have no up to date Anti Virus protection on your computer! These «Viruses» are basically little software programs that can be spread in many different ways. Anyone serious about Internet Security MUST take this onboard!

Viruses often contain «payloads», actions that the virus carries out separately from replication. Payloads can vary from the annoying messages that display on your screen, to the disastrous which attempt to overwrite the Flash BIOS and cause irreparable damage to YOUR computer...

The best way for users to protect themselves against viruses is to apply the following anti-virus measures:

Make backups of all software (including operating systems), so if a virus attack has been made, you can retrieve safe copies of your files and software.

Be aware that the risk of infection grows exponentially when people exchange floppy disks, download web material or open email attachments without caution.

Have anti-virus (AV) software installed and updated regularly to detect, report and (where appropriate) disinfect viruses.

Browser choice

Internet Explorer is currently the most widely used web browser in the world, making it the prime target for phishing and many other possible attacks.

Conclusion

What you need to keep in mind is that most of the security problems on the Internet are due to the users' misunderstanding of the media or human mistakes. You need to be extremely careful when transferring files or displaying private information and pay close attention to new kinds of virus or security leaks. It's best to also keep in mind that the Internet is not the only network, local or wireless networks are as much vulnerable than is the Net.

## ЛИТЕРАТУРА

1. Фомина Ю. А. Принципы индексации информации в поисковых системах / Ю. А. Фомина, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2010. – № 7. – С. 98-100.

2. Преображенский Ю. П. Некоторые аспекты информатизации образовательных учреждений и развития медиакомпетентности преподавателей и руководителей / Ю. П. Преображенский, Н. С. Преображенская, И. Я. Львович // Вестник Воронежского государственного технического университета. – 2013. – Т. 9. – № 5-2. – С. 134-136.

3. Ермолова В. В. Архитектура системы обмена сообщений в немаршрутизируемой сети / В. В. Ермолова, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2010. – № 7. – С. 79-81.

4. Воронов А. А. Обеспечение системы управления рисками при возникновении угроз информационной безопасности / А. А. Воронов, И. Я. Львович, Ю. П. Преображенский, В. А. Воронов // Информация и безопасность. – 2006. – Т. 9. – № 2. – С. 8-11.

5. Львович И. Я. Факторы угрозы экономической безопасности государства / И. Я. Львович, А. А. Воронов, Ю. П. Преоб-

раженский // Информация и безопасность. – 2006. – Т. 9. – № 1. – С. 36-39.

6. Львович И. Я. Основы информатики: Учебное пособие / И. Я. Львович, Ю. П. Преображенский, В. В. Ермолова. – Воронеж, Издательство: Воронежский институт высоких технологий, 2014. – 239 с.

7. Преображенский Ю. П. Сравнительный анализ алгоритмов поиска текстовых фрагментов / Ю. П. Преображенский, А. С. Ермаченко // Вестник Воронежского института высоких технологий. – 2010. – № 7. – С. 76-78.

8. Логачева О. Е. Особенности современных методов оценки и фильтрации сигналов / О. Е. Логачева, В. В. Костюченко // Моделирование, оптимизация и информационные технологии. – 2016. – № 4 (15). – С. 6.

9. Моисеев А. А. Модификация некоторых процедур автоматического анализа данных / А. А. Моисеев // Моделирование, оптимизация и информационные технологии. – 2016. – № 4 (15). – С. 14.

10. Панарин Д. Г. Моделирование распространения электромагнитных волн в каналах связи при эффектах затухания / Д. Г. Панарин, А. В. Данилова // Моделирование, оптимизация и информационные технологии. – 2016. – № 4 (15). – С. 10.

11. Бокова О. И. Проектирование наземных радиосистем передачи информации с помощью специализированных программных комплексов / О. И. Бокова, С. В. Канавин, Н. С. Хохлов // Моделирование, оптимизация и информационные технологии. – 2016. – № 2 (12). – С. 6.

12. Мэн Ц. Анализ методов классификации информации в интернете при решении задач информационного поиска / Ц. Мэн // Моделирование, оптимизация и информационные технологии. – 2016. – № 2 (13). – С. 19.

13. Щербатых С. С. Применение методов обработки сигналов с помехами / С. С. Щербатых // Международный студенческий научный вестник. – 2016. – № 3-2. – С. 241-242.

14. Шмалько Г. А. Применение алгоритмов обработки радиолокационной информации / Г. А. Шмалько // Международный студенческий научный вестник. – 2016. – № 3-2. – С. 237-238.

15. Калашников А. О. Атаки на информационно-технологическую инфраструктуру критически важных объектов: оценка и регулирование рисков / А. О. Калашников, Е. В. Ермилов, О. Н. Чопоров, К. А. Разинкин, Н. И. Баранников / монография / под ред. чл.-корр. РАН Д. А. Новикова. Воронеж, Издательство: ООО «Издательство «Научная книга», 2013. – 159 с.

## ABOUT THE INTERNET SECURITY

***© 2017 A. A. Alimbekov, E. A. Avdeenko, V. V. Shevelev***

*Voronezh Institute of high technologies*
*JSC concern «Sozvezdie»*
*Russian new University*

*The paper deals with the main dangers you may encounter in the online space. The recommendations for tools, which are protected from intrusion are given.*

*Keywords: security, Internet, network, program.*