Ways to protect against computer viruses

Maxmudov Ulug‘bek Ravshanbekovich

Fergana branch of the Tashkent University of Information Technologies, student

Abduraximov Ozodbek Azimjon o'g'li

Fergana branch of the Tashkent University of Information Technologies, student

Ismoilov Sirojiddin Rasuljon o'g'li

Fergana branch of the Tashkent University of Information Technologies, student

Shamamatova Sayyora Jo'raboy qizi

Fergana branch of the Tashkent University of Information Technologies, student

Annotation: This article lists computer viruses, the damage they can cause to users and computers, and how to protect against viruses like this.

Keywords: alphanumeric character, anti-spyware, anti-malware, firewall, heuristic detection, cross-platform application.

A computer virus is a program code capable of self-copying, and typically contains negative effects such as system hacking and data damage. Viruses are created with the goal of copying from a programmer to many computers and even distributing program code to unsuspecting users. Copying itself is one of the first signs of being a virus, and viruses, the function of which is only reproduction, are also trapped. Many of them also have other effects, releasing music, displaying notifications, and in the worst case, destroying valuable user data. They have the ability to perform all the actions that the creator programmer envisions. Some virus creators are not as skilled as they expect, and as a result, while unplanned, unexpected results such as program collisions are visible.

Why are computer viruses written?

There are many possible reasons behind this, whether in order to increase the personal status of the creator of the virus, or in order to take revenge on the fired Company, the information that is being destroyed can be created in cases where it can significantly affect his lifestyle. Virus programmers like to boast of the scale of the codes they create, calling themselves by code names. Controlling network corruption, for example, gives the creator of malicious code a sense of power.

Where are viruses encountered?

Viruses will be hidden in the bootable code. This means that any downloaded program, a soft disk program left on the machine, creates the risk of copying. Most people believe that viruses can only be present in program copies and in programs where the virus is irritating, but, in fact, this is not the case. In 1992, Borland released a virus with its C++ programming language software (a silver CD surrounded by the original cut), and thousands of copies were shipped worldwide. This may be due to virus testing or a lack of anti-virus software obsolescence updates. At some point, defects were prominent on many personal computer CDs, making it difficult to rely on even reputable source software. In addition, it is not necessary to rely on software that can be downloaded from the internet, but there is a need for frequent use. Here, a problem-averting solution is software and strategy. Despite the fact that there are many ways to attack and install virus programs, there are several ways that can help protect the computer and network from cyber threats.

1. Asking employees to use strong passwords and change them periodically is the easiest way to create strong computer passwords or expressions, but also to expand system security. From 8 to 64 alphanumeric characters and characters like @, #, * and & should be used to create complex passwords or expressions. It is necessary to activate two-step confirmation when possible. Periodic upgrades can help prevent evil forces from breaking through passwords. Pest program attack test-and-error method, in which the program tries to decode the password and gains access to the target computer. The stronger the password, the more difficult it will be for haker to crack and access it.

2. Installing Antivirus software Antivirus software actively checks for viruses, system files or operating system that try to invade email. Choosing a quality software package, it should be borne in mind the prestige and product of the company, the features of the program (m-n, daily update) and compatibility with the computer.
3. Carrying out a full-fledged system check on a daily basis, viruses, spyware and malware are constantly developing. As a result, sometimes they break through system protection methods and infect the computer system. Daily checks must be performed through antivirus, anti-spyware, and anti malware programs to identify, quarantine, and remove evil agents on the network before any or additional damage occurs.
4. Introducing periodic system backup routines many types of evil agents can damage content within the computer. It is necessary to organize a periodic backup procedure to make sure that the computer can recover data in the event of a malicious event. Backup choices such as cloud service or personal external hard drive can be used. The cloud service allows you to save data on the network. An individual external hard drive can be connected to a computer, so there is an opportunity to copy the updated files as needed.
5. Regular updates to the computer system to fix any viruses, abnormalities, it is important to run regular computer system updates. If updates are not allowed, viruses that remain in the system can be used by hackers. With the announcement of the new system version, the user must be aware of this.
6. The use of a firewall firewall is the most important aspect that wraps the computer and it blocks unauthorized access. When starting or configuring the computer now, it is necessary to use the firewall capabilities of the operating system. Firewall settings can be updated according to computer preferences.
7. Careful use of Email can lead hackers to gain an advantage on most roads in email, such as in computer files attached to emails. It is not recommended to open and read addresses that you do not recognize. They need to be deleted immediately. 8. Careful use of the Internet includes spyware and malware, even the safest websites. To infect the virus, it is enough for the mouse to click once. Many fake websites are masked to mimic real websites. When entering URLs, it is necessary to verify that the name of the site, correctly written. It is necessary to get those that suddenly appear, before clicking on ads, graphs and links to other sites.

Antivirus software computer protection software

Antivirus software and computer protection software are focused on evaluating web pages, files, software, and referrals that focus on finding and rooting malwares at the greatest possible speed. Most provide protection against unwanted threats in the process of activity. Because now many processes are organized on the network, and new threats appear regularly, the installation of a protected antivirus program is gaining more relevance. The joy is that nowadays there are a number of excellent products for selective use. These software products must be tested professionally to determine their safety level. Each company has its own list of features, since some aspects of any software are considered more important than the rest. Some of them are:

• User interface (applications that do not have a comfortable appearance are often not well received by buyers)
• Speed of inspection and troubleshooting
* Flexibility including password protection
* Ease of documentation of features and understanding of the manual
* Technical qualification level for configuration and use
• Technical support quality and speed
• Speed of dealing with new viruses and being able to solve the problem
* Network update capability

How do Antivirus programs work?

Antivirus software starts to run by checking computer programs and files against malware's known database. Since there are contributions from hackers and new viruses are constantly created, antiviruses also check for non-existent and possible threats. In general, many applications employ three different types of detection: specific detection, which investigates previously generated threats; general detection, which searches for characters or existing parts or types that depend on a common codebase; and detection in the experimental process(heuristic), verification of unknown viruses by detection through suspicious file structures. When a program finds a viral file, it usually places it in quarantine and gives a deletion mark, making it inaccessible and removing the risk. With devices connected to the internet in a daily way of life and at the same time even more dangerous.

Virus protection options of common antivirus programs

1. **ESET NOD32**, often referred to as NOD32. Released in two different editions, Home Edition and Business Edition. It has the following properties:
• Anti-phishing
* Device control
* Bank business and payment protection developed
• Parental control
* Web camera control
• Protective wall
* Network controller developed
• Network Attack Protection

2. **Kaspersky** . Kaspersky provides protection against internet security malware, email spam, phishing, hacking beats, and theft of tokens. Services offered:

• Data protection
• Data backup
* Web policies-restrictions and record user activity • password manager
• Data encryption
* Network control
* Query activity

3. Avast **Antivirus** is a family of cross-platform (that is, those that can work with different computers or with different software packages) internet security applications developed by Avast for Microsoft Windows, macOS, Android and iOS. Avast antivirus includes the following features:
• Anti-spam
• Data decomposer
* Smart antivirus
• Home network security
* Intelligent inspection
* Secure domain name system

REFERENCES:

1. Umaraliyev, J., Abdurakhimov, O., & Isokjonova, S. (2023, June). USE AND EFFECTIVENESS OF INFORMATION TECHNOLOGIES IN

MEDICINE. In Academic International Conference on Multi-Disciplinary Studies and Education (Vol. 1, No. 11, pp. 148-151).

2. Umaraliyev, J., Turdaliyev, K., Isoqjonova, S., & Abdurakhimov, O. (2023). ITS APPLICATIONS AND PROSPECTS IN EDUCATION. Interpretation and Researches, 1(11). search the horse
3. O Abduraximov, A Tojidinov, U Nazirjonov. IDENTIFICATION AND AUTHENTICATION IN INFORMATION SECURITY. NETWORK DISPLAY TECHNOLOGY. Академические исследования в современной науке, 2023. (Vol. 2, No. 21, pp. 26-32).
4. AO Azimjon o'g'li, TA Ilhomjon o'g'li . NETWORK OPERATING SYSTEMS. XALQARO ANIQ FANLAR TAHLILI, 2023. (Vol. 1, No. 2, pp. 51-54).
5. AO Azimjon o'g'li, TA Ilhomjon o'g'li, NU Nozimjon o'g'li. AVTOTRANSPORT VOSITALARINI KIBERHUJUMLARDAN HIMOYA QILISH BO 'YICHA YO 'L XARITASI . Новости образования: исследование в XXI веке, 2023. (Vol. 2, No. 13, pp. 70-74).
6. Ilhomjon, T. K., Azimjon, A. O., & Nazimjon, N. U. (2023). CLOUD TECHNOLOGIES AND CLOUD COMPUTING. JOURNAL OF SCIENCE, RESEARCH AND TEACHING, 2(8), 79-81.
7. Ilhomjon o'g'li, T. A., & Azimjon o'g'li, A. O. (2023). ANDROID XAVFSIZLIGI, XAVSLIK TIZIMLARINI YAXSHILASH. PEDAGOG, 6(6), 753-757.
8. NU Nozimjon o'g'li, AO Azimjon o'g'li, TA Ilhomjon o'g'li. Information and Communication Technologies in Education LMS Systems. American Journal of Public Diplomacy and International Studies (2993-2157). (Vol. 1, No. 6, pp. 28-31).
9. AO Azimjon o'g'li, TA Ilhomjon o'g'li, NU Nozimjon o'g'li . Lms Systems and Their Description. American Journal of Public Diplomacy and International Studies (2993-2157). (Vol. 1, No. 6, pp. 22-24).
10. NU Nozimjon o'g'li, AO Azimjon o'g'li, TA Ilhomjon o'g'li. Education to Give in Processes Information and Communication Technologies. American Journal of Public Diplomacy and International Studies (2993-2157). (Vol. 1, No. 6, pp. 18-21).
11. TA Ilhomjon o'g'li, NU Nozimjon o'g'li, AO Azimjon o'g'li. Grid Analysis and Design. American Journal of Public Diplomacy and International Studies (2993-2157). (Vol. 1, No. 6, pp. 25-27).

12. NU Nozimjon o'g'li, AO Azimjon o'g'li, TA Ilhomjon o'g'li . Информационные И Коммуникационные Технологии В Образовании LMS Системы. American Journal of Science on Integration and Human Development (2993-2750). (Vol. 1, No. 6, pp. 17-20).
13. AO Azimjon o'g'li, TA Ilhomjon o'g'li, NU Nozimjon o'g'li. The Evolution of Graphical Interfaces for Programming TRACE MODE 6 Algorithms. American Journal of Pediatric Medicine and Health Sciences (2993-2149). (Vol. 1, No. 6, pp. 72-74).
14. TA Ilhomjon o'g'li, NU Nozimjon o'g'li, AO Azimjon o'g'li. Grid Tahlil Va Loyihalash. American Journal of Public Diplomacy and International Studies (2993-2157. (Vol. 1, No. 5, pp. 132-134).
15. NU Nozimjon o'g'li, AO Azimjon o'g'li, TA Ilhomjon o'g'li. Ta'lim Berish Jarayonlarida Axborot-Kommunikatsiya Texnologiyalari. American Journal of Language, Literacy and Learning in STEM Education (2993-2769). (Vol. 1, No. 6, pp. 26-29).
16. AO Azimjon o'g'li, TA Ilhomjon o'g'li, NU Nozimjon o'g'li. Lms Tizimlari Va Ularning Tavsifi. American Journal of Engineering, Mechanics and Architecture (2993-2637). (Vol. 1, No. 6, pp. 36-38).
17. 17.Jamshidbek To‘xtasin o‘g, U., & Azimjon o‘g‘li, A. O. (2023, June). THE TRANSFORMATIVE ROLE AND IMPORTANCE OF TELECOMMUNICATION TECHNOLOGIES IN OUR DAILY LIVES. In " ONLINE-CONFERENCES" PLATFORM (pp. 138-139).
18. Turdaliyev, K., Abduraximov, O., & Isoqjonova, S. (2023). OPPORTUNITIES OF DIGITAL TECHNOLOGIES. Наука и инновация, 1(15), 8-11.
19. Isoqjonova, S., Abduraximov, O., & Turdaliyev, K. (2023). ZAMONAVIY DUNYODA ROBOTLARNING O'RNI HAMDA AHAMIYATI. Talqin Va Tadqiqotlar, 1(10).
20. Nafisaxon, T. U., Jamshidbek To'xtasin o'g, U., Arsenevna, D. E., & Azimjon o'g'li, A. O. (2022). AVTOMATLASHTIRILGAN AVTOTURARGOH IMKONIYATLARI VA QULAYLIKLARI. INNOVATION IN THE MODERN EDUCATION SYSTEM, 3(25), 45-48.
21. K Turdaliyev, O Abduraximov, J Umaraliyev. (2023). FOCL AFZALLIKLARI HAMDA KAMCHILIKLARI. MOBIL SU'NIY YO'LDOSH

VA OPTIK TOLALI TARMOQLAR. Development of pedagogical technologies in modern sciences. 2(4), 123-128.

22. TK Ilhomjon o'g'li, AO Azimjon o'g'li, NH Maxmudjon o‘g‘li, (2022). MASOFAVIY TA'LIM MODELLARI VA MASOFADAN OQITISH TIZIMLARI. SUSTAINABILITY OF EDUCATION, SOCIO-ECONOMIC SCIENCE THEORY, 1(4), 113-116.

23. U Jamshidbek To'xtasin o'g, TA Ilhomjon o'g'li, AO Azimjon o'g'li, (2022). AXBOROTLARNI AVTOMATLASHTIRILGAN BOSHQARUV TIZIMI. PEDAGOGICAL SCIENCES AND TEACHING METHODS, 2(17), 22-25

24. Абдурахимов , О. А., & Махмудов , У. Р. (2023). ПРЕИМУЩЕСТВА И НЕДОСТАТКИ ВОЛОС, МОБИЛЬНЫХ СПУТНИКОВЫХ И ОПТИЧЕС-КИХ СЕТЕЙ. *Educational Research in Universal Sciences*, *2*(6), 147–150. Retrieved from http://erus.uz/index.php/er/article/

25. Jamshidbek To‘xtasin o‘g, U., Elyorbek o‘g‘li, I. A., & Azimjon o‘g‘li, A. O. (2022). IIS VOSITALARI YORDAMIDA VEB-SAYT BOSHQARUVI. Journal of new century innovations, 18(1), 64-69.

26. Ilhomjon o‘g‘li, T. K., Jamshidbek To‘xtasin o‘g, U., & Azimjon o‘g‘li, A. O. (2023, July). ZAMONAVIY TEXNOLOGIYALAR JAMIYATDAGI TARAQQIYOTIDAGI O ‘RNI VA AHAMIYATI. In International Conference on Architecture and Civil Engineering (pp. 1-3).