

## INFORMATION ABOUT RISKS ON THE WEB

We would like to draw your attention to the need to follow security rules when using the Internet, including keeping your antivirus software up to date.

Irresponsible use of the Internet and electronic services may expose the user to various types of threats, such as:

### **Viruses**

Programs that compromise (damage) other programs by adding their code to them to access the computer's contents when the infected file is executed.

### **Worms**

Malware that spreads by exploiting network resources. This class is called worms because of the specific behaviour, which resembles "crawling" from one computer to another by using networks, email, and other communication channels. As a result, worms spread very quickly.

### **Kruegerware or Kruegerapps**

The name of malware that is difficult to fix. The name is derived from Freddy Krueger, a character from the film "A Nightmare on Elm Street", and refers to the software's ability to return to existence. Such viruses regenerate even after being removed from the computer, for example, after using the Windows system recovery mechanism. This term is most commonly used to refer to computer viruses, malware, and spyware.

### **Spyware**

Software that collects data about a specific user or organisation without their knowledge. The victim is completely unaware of the presence of spyware on their computer.

### **Browser hijacker**

Malware that secretly changes the settings of a user's web browser. This can result in changes to the default homepage, redirections to unwanted websites, the addition of unsolicited (sometimes pornographic) bookmarks, or the generation of unwanted pop-ups. Antivirus programs can be used to remove hijackers, and specialised programs have also been developed specifically for this purpose.

### **Jokes**

Software that causes no harm but displays messages suggesting that malware has caused or will cause damage. It often warns the user about an existing danger, for example, displaying messages about hard drive formatting (though no formatting actually occurs), detecting viruses in uninfected files, etc.

### **Riskware**

Software that is not a virus but contains potential threats. Under certain conditions, the presence of riskware on a computer poses a threat to stored data.

### **Poachware**

The name comes from the English word “poach,” meaning to hunt illegally. It is a type of spyware primarily aimed at stealing sensitive data, such as usernames and passwords.

### **Malware**

An abbreviation for “malicious software”, referring to software designed to destroy or damage a computer or the data stored on it. Malware includes viruses, worms, Trojans, spyware, adware, and other harmful software.

### **Trojan horses (trojans)**

Programs that perform unauthorised actions on infected computers, not controlled by the user, such as deleting files, causing system inactivity, stealing private data, etc., depending on the circumstances.

### **Trojan dropper**

A type of Trojan virus aimed at installing malicious code on the victim’s computer. These viruses install other malicious programs on the computer or a new version of a previously installed virus.

### **Trojan clicker**

A type of Trojan whose purpose is to inform the author or the “person controlling it” that the malicious code has been installed on the victim’s computer and to provide information about the IP address, open ports, email addresses, etc. It is typically part of a “package” containing other malicious programs.

### **Trojan downloader**

A type of Trojan used to install malicious code on the victim’s computer. Similar to a Trojan dropper, it is, however, more useful to malware creators. It is much smaller than a Trojan dropper and can be used to download an unlimited number of new versions of malicious code.

### **Trojan proxy**

A type of Trojan that tracks the user’s activity, saves the collected information on the user’s hard drive, and then sends it to the author of the malware or the “person controlling it”. The recorded information includes keystrokes and screenshots, which are used to steal banking data or assist in online fraud.

### **Trojan backdoor**

A type of Trojan that allows its author or the person controlling it to manage the victim’s computer remotely. Unlike legitimate remote administration tools, these Trojans install, run automatically, and operate in secret, without the user’s knowledge or consent.

### **Crimeware**

A spyware program that collects sensitive data from a computer user to gain access to bank accounts or financial services.

### **Bundleware**

A method of distributing software by bundling it with another popular program. This way, spyware programs are also distributed, and unaware users install them themselves.

### **DoS (Denial of Service)**

A type of network attack that causes the targeted system to stop functioning properly. It can affect just one service (e.g., email) or an entire server. DoS attacks exploit existing bugs and vulnerabilities in the system. While this attack does not involve data theft or loss, it causes significant financial damage to companies by blocking their services.

### **Rootkit**

These are tools used to hide malicious activity. They are hidden by malware to evade detection by antivirus software.

### **Spam**

Anonymous, unwanted bulk mail. Spam refers to messages, often political or propaganda-based, that contain requests for help. Another spam category includes messages promising large sums of money, while emails are also used for stealing passwords and credit card numbers.

### **Phishing**

A type of computer fraud where an attacker impersonates another person or institution to steal data or gain benefits (e.g., login credentials, credit card details, etc.). It is an attack based on social engineering.

### **Likejacking**

A form of phishing that involves collecting fans by automatically “liking” a given profile or page on Facebook. The user is lured by attractive content posted on a friend’s wall (often of an erotic nature), but the link does not lead to the promised content. Clicking the post redirects the user to a page that causes them to automatically ‘like’ it without their knowledge, and the information is then posted to their profile. This type of spam spreads quickly among others, and the target page often contains malicious software (such as Trojans, viruses, etc.), further exposing users to risk.

### **Tabnapping**

From English “tab kidnapping” – hijacking tabs. A type of phishing attack that takes advantage of multiple websites being opened in different browser tabs. The attacking site changes the content of another website open in a different tab. If the page swapped in the background is, for example, a bank’s website, the user may unknowingly attempt to log in to a fake page impersonating the actual bank, which will then capture their login credentials.

### **Vishing**

A new form of fraud based on phishing, where scammers use VoIP (Internet telephony) to impersonate primarily financial institutions. One of their common methods is to send spam emails with a toll-free 0-800 number, asking the recipient to update their bank account details. When the number is dialled, an automated system prompts the victim to provide specific account access information.

### **IP Spoofing**

A term referring to falsifying the source IP address in a network packet sent by a computer. This action can be used to conceal the attacker's identity (e.g., in DoS attacks), impersonate another network user, interfere with their online activity, or exploit the privileges associated with another address.

### **Hacking**

Gaining unauthorised access to a computer, computer system, or data/information stored in computer systems. Hacking is often a necessary component in committing a cybercrime.

### **BotNet**

A colloquial term for a network of zombie computers, i.e., computers under the control of hackers using viruses, Trojans, etc. According to statistics, about one-third of all computers on the Internet are compromised by hackers. The user of the compromised computer is usually unaware of this. Computers in a BotNet are most commonly used for DoS attacks or sending spam. To protect against a computer being taken over by a hacker and joining a BotNet, it is essential to use up-to-date antivirus software and a firewall.