

DON'T OPEN ANY OF THE MESSAGES FROM UNKNOWN SENDERS!



**These messages may contain
viruses or someone is trying to
take over your personal data!**

Use the INTERNET safely!

KEEP YOUR PERSONAL INFORMATION IN A SECURE LOCATION!



On line do not share the following information:

- Your name and surname
- Your photographs
- Your phone number
- Your address
- Your ID number
- Your account
- Your passwords

Why???

Because cyber-attackers can misuse all information!

The best protection against cyber-attacks !



Automated backup saves time and guarantees that you will always have the latest versions of your documents.

Such storage is easy to install and it is affordable in terms of the important data protection it offers.

Use this information as an additional criterion for selecting how to back up your data.



Although your copy is written to another external drive, separate computer or USB device, restrict access to them so that other people do not have access to those backups; the devices on which they are written (physical or over a local computer network) on the device on which the original data is stored are not interconnected.


If these backup devices are permanently connected to the local computer network, in case of infection it can be automatically transferred to the storage device. This means that any such backup can be infected, leaving you with no backup from which to restore the original data.

For greater security it is necessary to store the backups in another location, so that in case of natural disaster or theft you will not lose the backup. That is why cloud storage is the most economical and efficient way to achieve this goal.

Cloud storage means that the service provider keeps your data on its infrastructure accessible over the Internet. Your data is thus physically separated from your location and storage is provided, as well as web services without investing in expensive hardware.

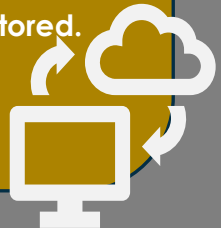
If you do not use your own email server, your emails are already cloud storage. Most of the time, the contacts that are written on your mobile phone are automatically saved in the cloud, as well as a copy of the communication through applications such as Viber, Messenger and WhatsApp.

The benefit of this storage service is the high level of availability that cloud data storage service providers offer for free but limited storage space, which can be increased for an additional fee.



Identify data that is important to your business and without which you cannot function (invoices, delivery notes and other documents with financial, personal and sensitive data).

Always make a copy of this data on an external device and keep it in a safe place away from the devices on which the original data and documents are stored.



Protection from malicious software or "malware"!

The antivirus is included for free in popular operating devices and is used on all computers, laptops, tablets and smartphones. So, your computer or mobile device already has antivirus software protection, but it is usually free and offers minimal protection.

Therefore, carefully consider purchasing a licensed commercial antivirus protection that will improve the security of the devices you use.



A suspicious application is a form of identity fraud that involves a fraudster applying for a new account for services or products while using a false identity. Only applications from e-shops approved by the manufacturer of the operating device (for mobile phones and tablets are the Google Play Store or Apple App Store) should be used to install applications from the Internet on the devices. These applications are tested by the manufacturer in order to provide a certain level of protection. Therefore, you should refrain from installing third-party applications from unknown sources or pirated software, as they are unverified and often contain viruses.



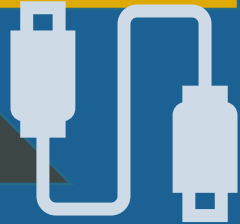
The software of all computers, laptops, mobile phones and tablets should always be updated with the latest versions from software and hardware manufacturers and suppliers. Applying an IT update is one of the most important things you can do to improve your security.



A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security procedures. A firewall is the first line of defense in network security and creates a secure zone between your computer network and external networks such as the Internet. All operating devices include a free firewall, which is easy to activate and it is recommended that it be switched on at all times.



Such storage devices are commonly used to transfer data between organizations and people. If only one careless user inadvertently plugs in an infected memory device it can do great damage.



ATTENTION!!!

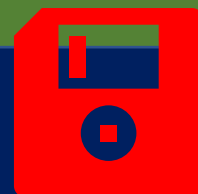


RECOGNIZE THEM AND PROTECT YOURSELF FROM PHISHING ATTACKS!!!

Steps to deal with cyber incidents!



Back up your data regularly and keep it in a safe place. You can find more information about risk assessment by searching the Internet. It is advisable to have your own Procedure for managing the IT systems that you need most when working. Examples are email systems and your website, accounting and archiving. Plan an incident plan, that is, think about what would happen if you suddenly did not have access to these systems or data. Make a list of priority-based systems, based on an understanding of what is important so that there is no downtime in order to take appropriate care.

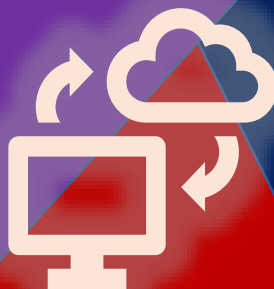


Cyber incidents such as unauthorized access to IT systems and theft or destruction of data and assets are considered criminal offenses. Always keep all information about the incident that occurred, such as access logs and modified files.

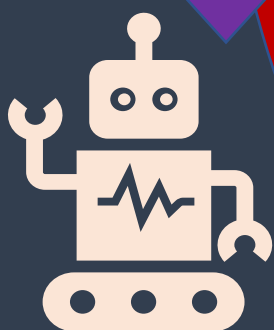
Do not hesitate to report the incident that happened to you. Be aware that reporting and sharing information with other stakeholders will prevent a recurrence of the same incident. You can report an incident to MKD-CIRT at the following internet address:

<https://mkd-cirt.mk/prijava-na-incident/>

Once a cyber incident has occurred, it is important to review what happened and learn from the errors found. Take action to overcome the identified deficiencies, thereby reducing the likelihood of a similar incident occurring again and increasing your safety.



It is mandatory to check the activity of antivirus protection, and if you cannot do this yourself, consult a professional who will review what happened. To overcome certain problems, you can find instructions for them by searching the Internet. Resolving an incident means re-accessing services, systems and data that were unavailable. Depending on the type of incident, you can respond by cleaning infected devices, changing passwords, recovering backup data, installing updates, and updating operating systems and applications.



Signs of cyber incidents



If computers are slow, if you receive emails with blackmail, when you cannot access your accounts and data or if other people inform you that they receive strange emails sent from your addresses.



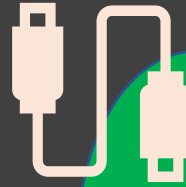
If you suspect a cyber incident, the next step is to find out exactly what happened. The answers to the questions who and when reported a problem, which services and systems are covered by the problem, which data are deleted or inaccessible (if any), when you first found out about the problem and which parts of the work are covered.



BEWARE OF SIGNS!!!

SAFE USE

Your devices (tablets, PCs, or phones) are more likely to be stolen or lost. Most devices include free web-based tools that you can use in case of loss to track their location, remotely lock and delete data. You can use these tools for your personal and business devices.



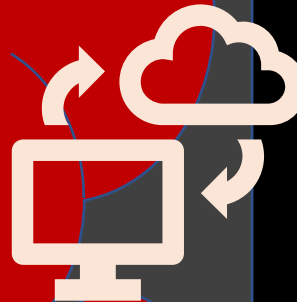
Using a more complex password as opposed to a simple one that can be easily guessed or extracted from your social media profile can prevent hackers from accessing your device and data.



Update your devices regularly and keep them updated automatically. Manufacturers of operating systems such as Android or iOS regularly release security updates. When the device manufacturer stops supporting and releasing new security updates for a particular type of device, then consider replacing them with new ones.



Applications that you have installed on your devices need to be regularly updated with patches from software vendors. This procedure allows new features to be added and all security vulnerabilities previously detected to be repaired.



Using public or open Wi-Fi locations such as hotels and restaurants is not recommended because you do not know who controls the hotspot. If you connect to such locations, you run the risk of giving your data access to an unwanted external entity. Therefore, use your 3G or 4G mobile network, which already has built-in security measures, as a precaution. Always use the tethering option (for your other devices, such as laptops, to share your 3G / 4G connection from your mobile phone), or the USB dongle wireless device from your mobile network.



BE SAFE !!!

STEPS FOR CORRECT USE OF PASSWORDS

2FA requires two different methods to "prove" your identity before you can use a particular service, usually a password plus another method. This may be code sent to your smartphone (or code generated by a banking token) that you must enter next to your password to further enhance security.



It is common practice to change passwords if you suspect that login details are compromised when using a particular service. Write down the passwords for important accounts (such as email and banking) and keep them safe (but not on the devices themselves). They should be complex enough, for example using a phrase of three random words and a total length of at least 8 characters, as well as contain characters from the following groups: uppercase, lowercase, numbers and special characters.



"PASSWORD MANAGER" is a computer program that allows users to store, generate and manage their passwords for local applications or network services. PASSWORD MANAGER helps generate and recover complex passwords, store such passwords in an encrypted database, or calculate them on a previous request.



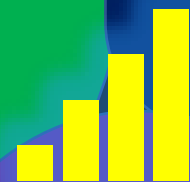
In addition to passwords, additional protection can be provided by using a Personal Identification Number (PIN), fingerprint or face scan, and encrypting or encrypting data as ways to authenticate.



For each device (PC, phone, tablet, or online service), use a password to restrict access to these devices and services if they contain sensitive data. In addition to passwords, additional protection can be provided by using a Personal Identification Number (PIN), fingerprint or face scan, and encrypting or encrypting data as ways to authenticate.



The established practice when creating a password is that its length should consist of at least 8 characters, to contain three of the four groups of characters (lowercase letters, uppercase letters, numbers and special characters).



Always change the default passwords set by the manufacturers that come with all devices (smartphones, laptops, network routers and other types of active computer and network equipment). Check devices and applications regularly to see if default passwords have been changed.



"PASSWORD MANAGER" means locally installed software applications, access to network services through web portals and hardware devices on local access, which serve as keys.