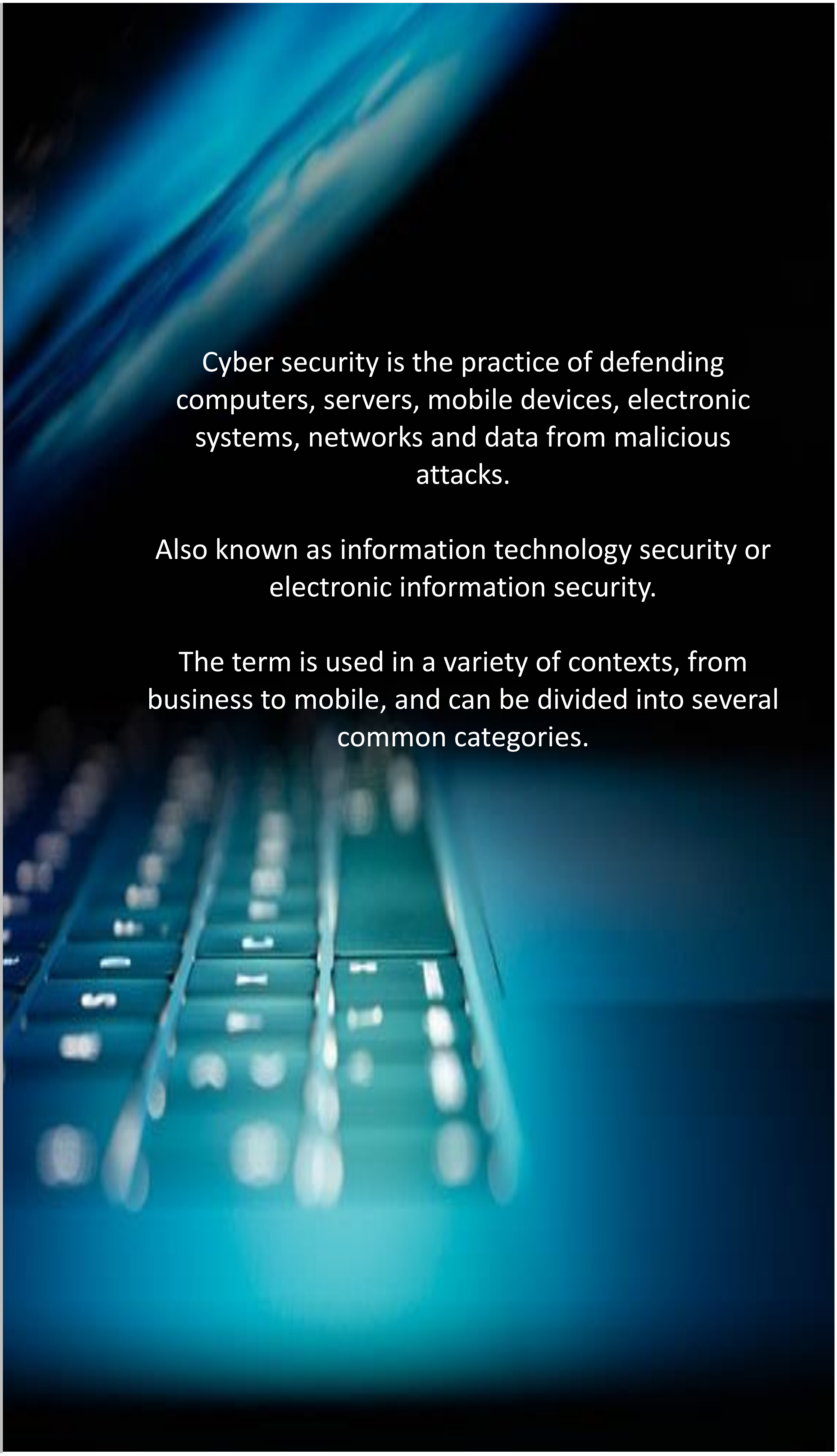
EDUCATE YOURSELF ABOUT CYBER SECURITY

Protect your online accounts

Securities and Exchange Commission of the
Republic of North Macedonia

October 2021

WHAT'S CYBER SECURITY



Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks and data from malicious attacks.

Also known as information technology security or electronic information security.

The term is used in a variety of contexts, from business to mobile, and can be divided into several common categories.

CATEGORY OF CYBER SECURITY

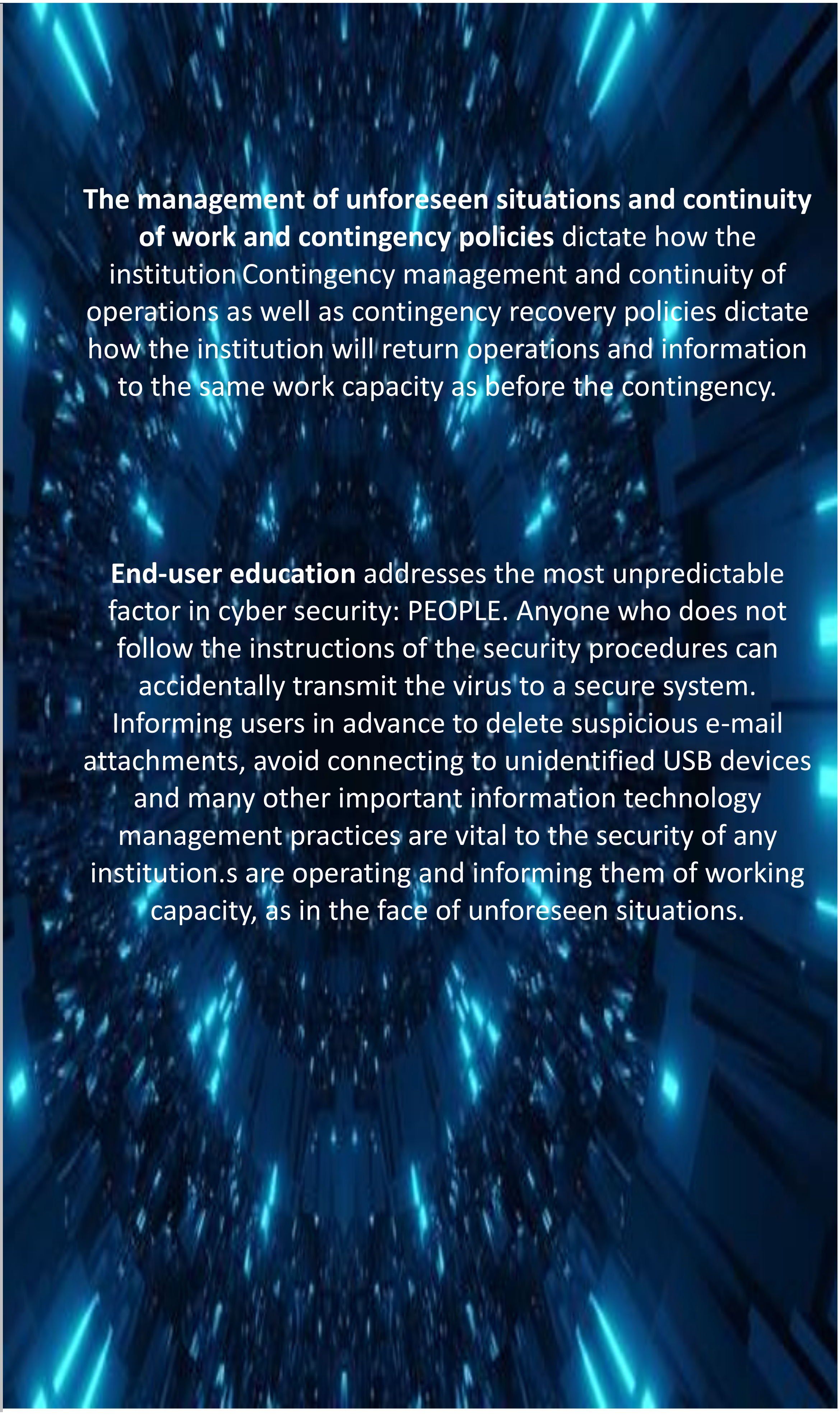
Network security is the practice of securing a computer network from intruders, whether it is targeted attackers or opportunistic malware.

Application security focuses on storing software and devices without threats. A compromised application may provide access to data that is designed to protect it.

Information security protects the integrity and privacy of data in both storage and transit.

Operational security includes processes and decisions for managing and protecting data access. This includes the permissions that users have when accessing a network and the procedures that determine how and where data can be stored or shared.

CATEGORY OF CYBER SECURITY



The management of unforeseen situations and continuity of work and contingency policies dictate how the institution Contingency management and continuity of operations as well as contingency recovery policies dictate how the institution will return operations and information to the same work capacity as before the contingency.

End-user education addresses the most unpredictable factor in cyber security: PEOPLE. Anyone who does not follow the instructions of the security procedures can accidentally transmit the virus to a secure system. Informing users in advance to delete suspicious e-mail attachments, avoid connecting to unidentified USB devices and many other important information technology management practices are vital to the security of any institution.s are operating and informing them of working capacity, as in the face of unforeseen situations.

TYPES OF CYBER ATTACKS

Cyber crime "cybercrime" involves individuals or groups targeting financial gain systems or systems that may cause disruption.

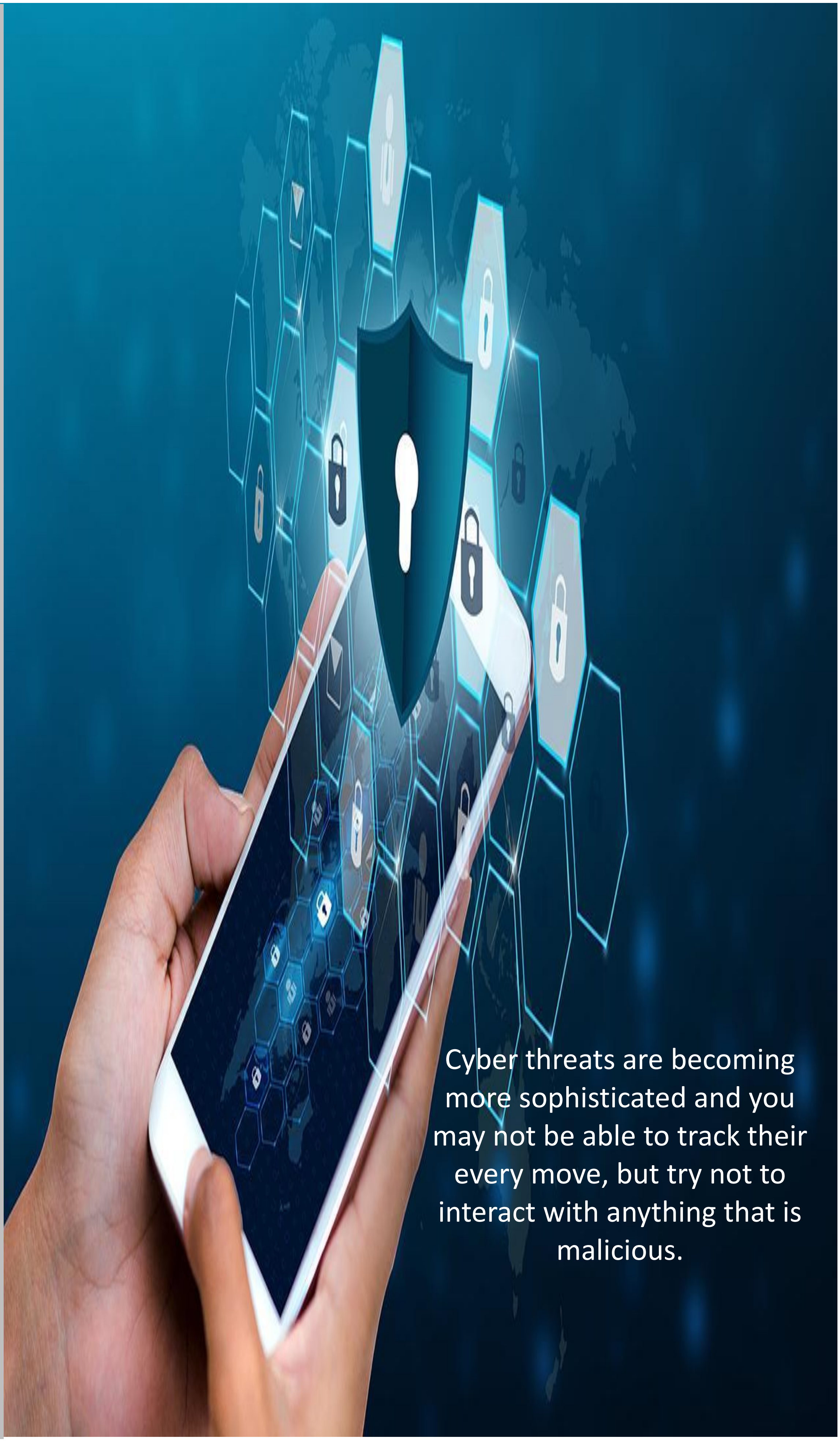
A "cyber-attack" often involves politically motivated gathering of information.

CYBER PROTECTION WARNINGS

Security and Exchange Commission of the
Republic of North Macedonia

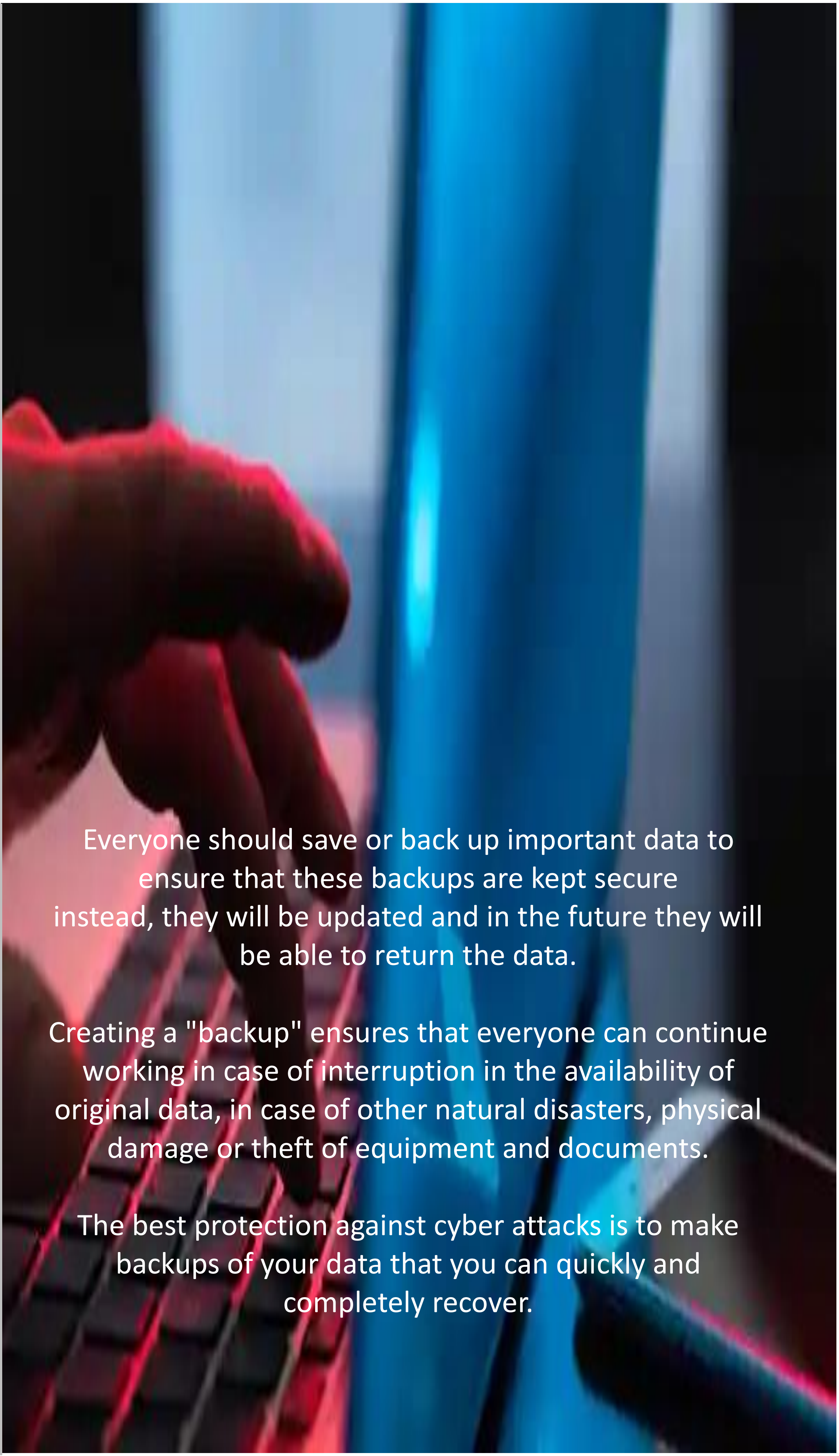
October 2021

CYBER THREATS



Cyber threats are becoming more sophisticated and you may not be able to track their every move, but try not to interact with anything that is malicious.

ALWAYS MAKE A COPY OR "BACKUP" ON YOUR DATA

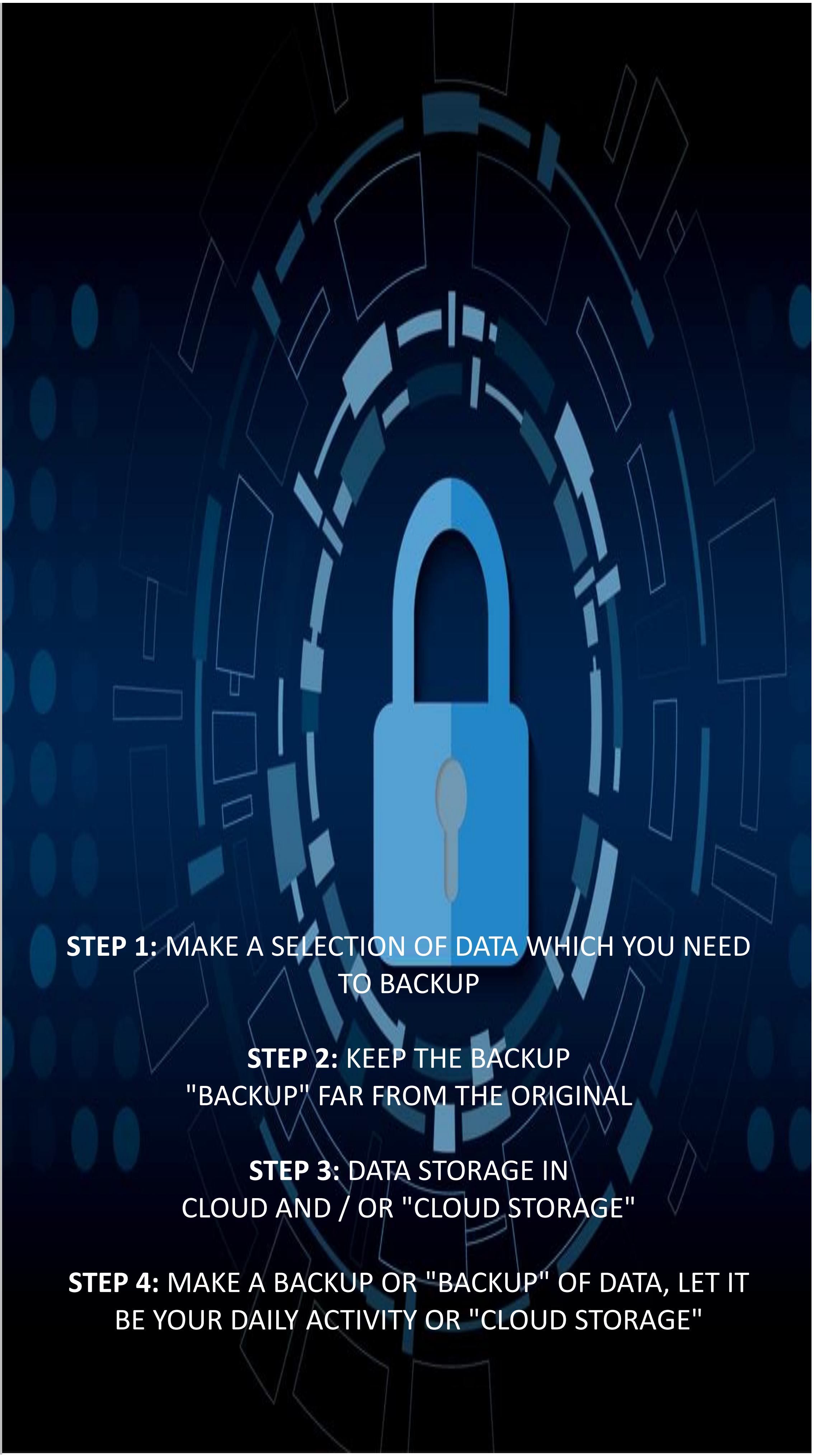


Everyone should save or back up important data to ensure that these backups are kept secure instead, they will be updated and in the future they will be able to return the data.

Creating a "backup" ensures that everyone can continue working in case of interruption in the availability of original data, in case of other natural disasters, physical damage or theft of equipment and documents.

The best protection against cyber attacks is to make backups of your data that you can quickly and completely recover.

ALWAYS MAKE A COPY OR "BACKUP"
ON YOUR DATA



STEP 1: MAKE A SELECTION OF DATA WHICH YOU NEED TO BACKUP

STEP 2: KEEP THE BACKUP "BACKUP" FAR FROM THE ORIGINAL

STEP 3: DATA STORAGE IN CLOUD AND / OR "CLOUD STORAGE"

STEP 4: MAKE A BACKUP OR "BACKUP" OF DATA, LET IT BE YOUR DAILY ACTIVITY OR "CLOUD STORAGE"

PROTECT YOURSELF FROM MALICIOUS SOFTWARE OR "MALWARE"

Malware is software created by a cyber hacker to corrupt or damage a computer by deleting important data, misusing your devices, and blackmailing or encrypting documents, viruses, and programs that self-replicate and infect the legitimate software.

STEP 1: USE ANTIVIRUS SOFTWARE FOR DEVICE PROTECTION

STEP 2: ACTIVATE A PROTECTION WALL OR "FIREWALL"

STEP 3: BEWARE OF SUSPICIOUS APPLICATIONS

STEP 4: MAINTAIN THE INFORMATION EQUIPMENT

STEP 5: CHECK THE DISCS, USB DEVICES AND MEMORY CARD

PHYSING ATTACK

Security and Exchange Commission of the
Republic of North Macedonia

October 2021

BEWARE OF PHYSING ATTACK

A phishing attack is a social engineering attack that is often used to steal user data, including login credentials and credit card numbers or text message. The recipient is then tricked into clicking on the malicious link, which could lead to the installation of malware, freezing the system as part of an attack, or detecting sensitive information.

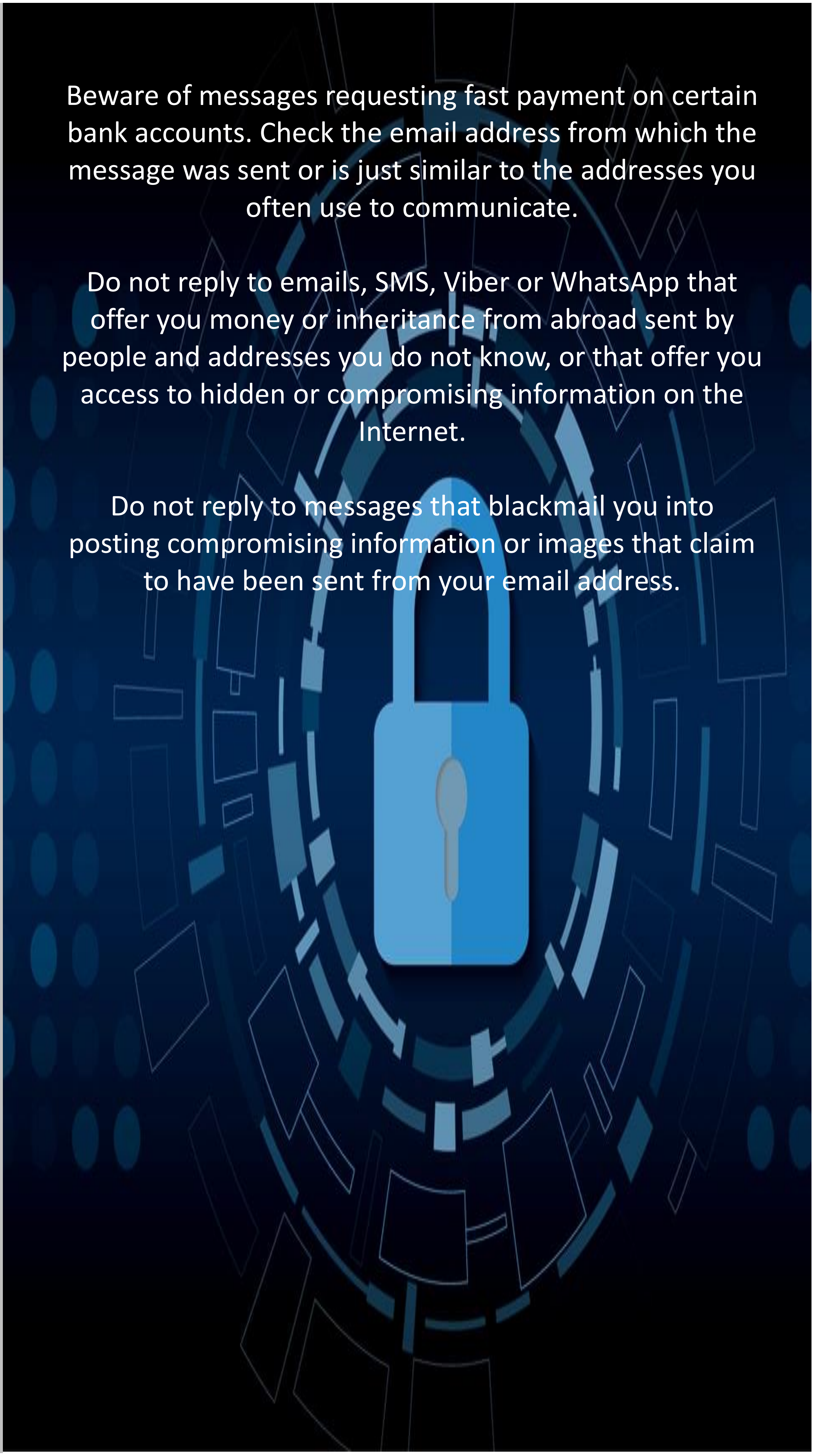
SIGNS FOR RECOGNIZING PHISHING ATTACKS

Some attackers will try to create messages that at first glance look very much like official messages by including logos and graphics similar to yours or the institutions you work with, so look carefully at the message to see if there are any signs of counterfeiting.

If the subject of the message addresses you with your e-mail address or says "respected", "colleague" or uses a similar generic term, it may be a sign that the sender does not know you and the message may have been sent as phishing scam.

Be suspicious of messages in which you are asked to act quickly or details such as "send a message within 24 hours" or "Winners of ..., click here immediately".

SIGNS FOR RECOGNIZING PHISHING ATTACKS



Beware of messages requesting fast payment on certain bank accounts. Check the email address from which the message was sent or is just similar to the addresses you often use to communicate.

Do not reply to emails, SMS, Viber or WhatsApp that offer you money or inheritance from abroad sent by people and addresses you do not know, or that offer you access to hidden or compromising information on the Internet.

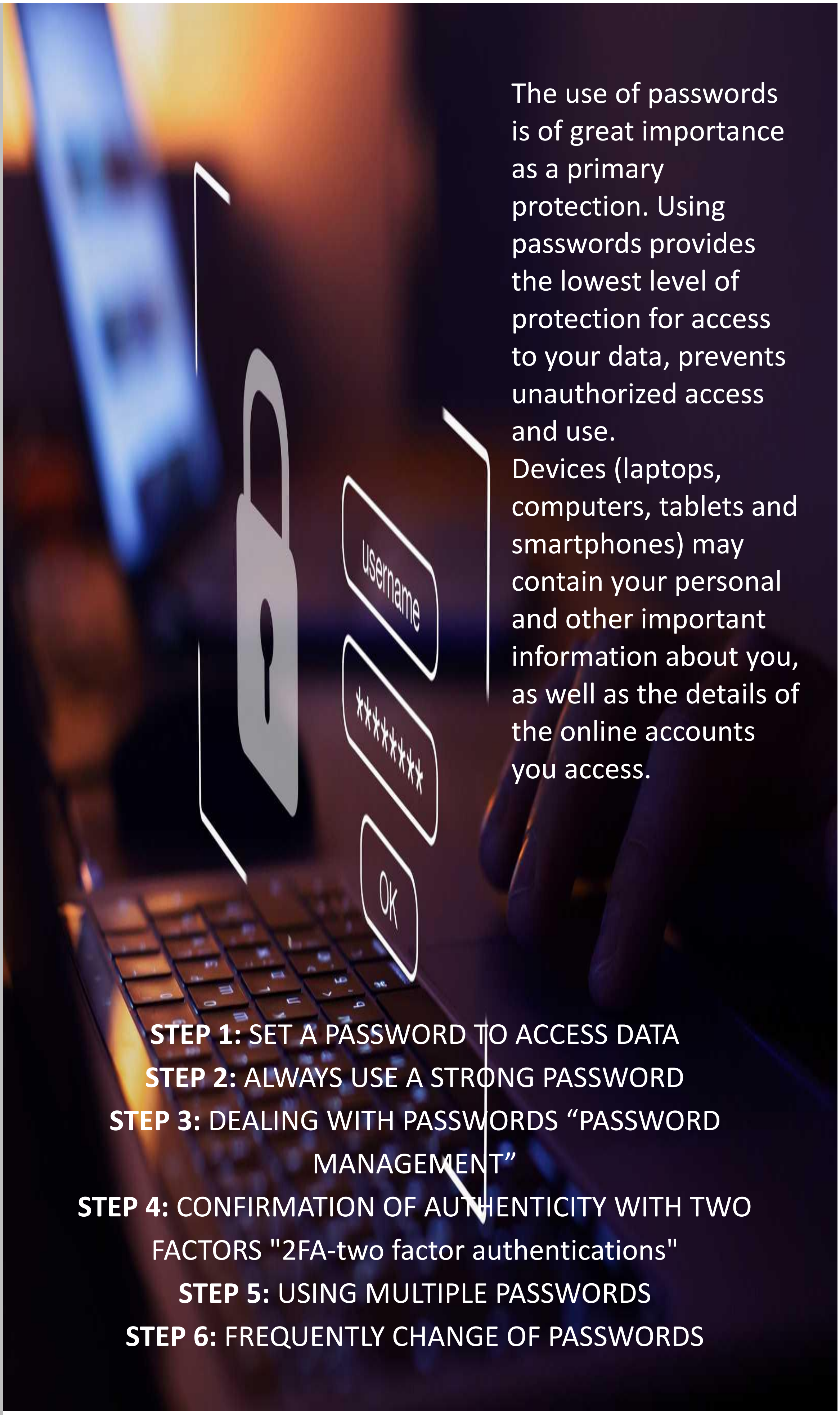
Do not reply to messages that blackmail you into posting compromising information or images that claim to have been sent from your email address.

CREATING AND MANAGING THE PASSWORD FOR ACCESS AND CORRECT USE OF DEVICES

Security and Exchange Commission of the
Republic of North Macedonia

Octomber 2021

STEPS FOR CORRECT USE OF PASSWORDS



The use of passwords is of great importance as a primary protection. Using passwords provides the lowest level of protection for access to your data, prevents unauthorized access and use.

Devices (laptops, computers, tablets and smartphones) may contain your personal and other important information about you, as well as the details of the online accounts you access.

STEP 1: SET A PASSWORD TO ACCESS DATA

STEP 2: ALWAYS USE A STRONG PASSWORD

STEP 3: DEALING WITH PASSWORDS “PASSWORD MANAGEMENT”

STEP 4: CONFIRMATION OF AUTHENTICITY WITH TWO FACTORS "2FA-two factor authentications"

STEP 5: USING MULTIPLE PASSWORDS

STEP 6: FREQUENTLY CHANGE OF PASSWORDS

RECOMMENDATIONS FOR SAFE USE OF SMART DEVICES

Mobile phones and tablets are often used for a variety of needs and operations, so here are the steps and recommendations for their safe use:

STEP 1: SAFE ACCESS TO DEVICES
STEP 2: LOST OR STOLEN DEVICES CAN BE TRACKED, LOCKED OR DELETED
STEP 3: REGULAR AND OFTEN UPGRADE OF DEVICES
STEP 4: REGULAR AND OFTEN UPDATE OF APPLICATIONS
STEP 5: DO NOT CONNECT TO UNKNOWN WI-FI LOCATIONS

VARIOUS CYBER INCIDENTS

A cyber incident is an unauthorized access or attempt to access an institution's IT systems. These include malicious attacks that aim to steal data, blackmail or misuse your data and IT systems, or cause harm. Examples of cyber incidents are denial of service, an attack that disables the availability of your services and interrupts your current normal operation. Accidents can also be caused by physical damage, natural disasters or theft.

STEP 1: ALWAYS BE PREPARED FOR CYBER INCIDENTS
STEP 2: IDENTIFICATION OF A CYBER INCIDENT
STEP 3: TERMINATION AND RESOLUTION OF THE CYBER INCIDENT
STEP 4: CYBER INCIDENT NOTIFICATION AND SHARING THE INFORMATION
STEP 5: LEARN FROM THE CYBER INCIDENT