Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan

Information Security Committee

CYBERSECURITY ISSUES

Recommendations

PROTECTION OF THE INFORMATION SPACE

Information security is becoming one of the most important issues of global digitalization.

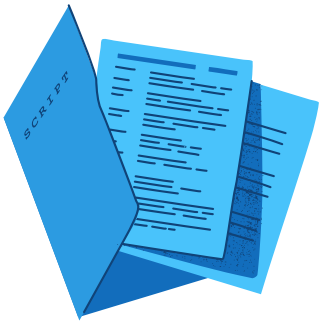
In the Global Cybersecurity Index (GCI) of the United Nations International Telecommunication Union (ITU), Kazakhstan has rapidly improved its position. The increase in the level of achievement of indicators in the GCI allowed Kazakhstan to achieve certain results according to the analysis carried out by experts of the UN ITU, where the Republic of Kazakhstan has risen by 9 positions and currently occupies 31st place (previously 40th) in the GCI.

On behalf of the Head of State, the Concept of digital Transformation, development of the ICT industry and cybersecurity for 2023-2029 was adopted, approved by Decree of the Government of the Republic of Kazakhstan dated March 28, 2023 No. 269 with separate goals and objectives, as well as a separate direction for the development of cybersecurity.

This Concept regulates additional measures aimed at strengthening the country's cybersecurity, in particular, measures are provided for technical protection, improving radio monitoring, protecting personal data and raising public awareness.

On December 11, 2023, the Head of State signed the Law of the Republic of Kazakhstan «On Amendments and Additions to some Legislative Acts of the Republic of Kazakhstan on information security, informatization and digital assets».

This Law is aimed at strengthening the protection of personal data and defining new mechanisms of interaction in ensuring the information security of informatization facilities, including government agencies.



CYBERSECURITY ISSUES (RECOMMENDATIONS)

THE CYBERSECURITY ECOSYSTEM

The main elements of the cybersecurity ecosystem are: human capital, cybersecurity market development, and technical protection.

In order to develop human capital in the country, there are

There are 8 higher educational institutions and 25 secondary specialized educational institutions that produce information security specialists.

For the 2022-2023 academic years, up to 3009 educational grants in the field of information security were increased (compared to 2021-2022, up to 2,600 were allocated).

In 2023-2024, 3,723 educational grants were allocated in the field of information security.

85 specialists were educated in the specialties «Information (cyber) security and cryptography», «Information Security» in leading foreign higher educational institutions under the «Bolashak» program.

THE CYBERSECURITY ECOSYSTEM

In order to develop the market of high-quality professional services in the field of information security, there are 3 specialized public organizations, 50 companies in the field of information security are involved. 514 strategic facilities with critical infrastructure have been identified. 41 private operational information security centers have been established, there are 3 computer Incident Response Services (FIRST) and 9 private testing laboratories.

In order to provide technical protection, the National Information Security Coordination Center was established and began its work in 2018. Additionally, in the future, the issue of protected backup infrastructure will be worked out for cases of disorganization of its work during peacetime emergencies, during martial law and wartime.

In 2022, the State Operational Information Security Center (GSOC) was established, and the industry Operational Information Security Center (SOC) was also established.

In 2022, the Personal Data Access Control Service (PDC service) was launched. This service is designed to obtain the revocation of a citizen's consent to access his personal data. The service also protects personal data from unauthorized access or distribution.

In 2023, 113 information systems have already been connected to the PDC service.

The level of public awareness

Thus, in order to determine the level of public awareness of threats to information security (cybersecurity) and personal data protection, a sociological study on public awareness of threats to information security (cybersecurity) and personal data protection was conducted by order of the Information Security Committee of the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan in September-November 2023.

In the process of sociological research, it was covered:

3 cities of national importance (Astana, Almaty, Shymkent)

17 districts and villages of regions in the Republic

11371 participating respondents

Participants: citizens of the Republic of Kazakhstan aged 18 and over;

Number of questions in the questionnaire blocks:

- **socio - demographic block - 10;**
- **the main block - 30;**
- **additional block - 20;**

The level of public awareness

A total of 11,371 respondents took part in the survey of sociological research conducted in the Republic over 3 months. Analyzing the results of the survey, it can be noted that today there is an increase in the level of awareness of the population of Kazakhstan on information security.

Indicators of public awareness of threats to information security (cybersecurity) and personal data protection:

- 62,9% — in 2018
- 73,5% — in 2019
- 78% — in 2020
- 75% — in 2021
- 77,4% — in 2022
- 80,4% — in 2023

The results of a sociological study conducted in 2023 show that the majority of respondents:

- **gain knowledge about the protection of personal information when using social networks – 90.52 %;**

- **are aware when using their "electronic digital signature" – 85.06 %;**

- **they know about the potential risks of children using the Internet – 76.65 %;**

Data security threats

Information security in the field of informatization (Cybersecurity) is the state of protection of electronic information resources, information systems and information and communication infrastructure from external and internal threats.

IT IS IMPORTANT TO KNOW:

Information security is an inseparable part of our lives. As a rule, information security means three important principles:

- **Confidentiality** — only those who have the right to access information should have access to it.
- **Availability** — information should be available at any time when it is needed.
- **Integrity** — the information must be reliable.

Violation of one of the principles may lead to violation of others.

How does malware get into a user's computer?

Types of cybersecurity threats:

- **Phishing** is a common form of online fraud based on the inattention of online users.
- **Hacking** a website is gaining access to internal data or to the admin panel of a web resource illegally.
- **Social engineering** is the psychological manipulation of people in order to commit certain actions or disclose confidential information.
- **A DDoS attack** is an overload of an information system with an excessive number of requests that block the processing of requests.
- **Trojan horse** is malicious software that masks its true purpose. At the same time, unlike a virus, a Trojan is not able to duplicate or infect files on its own.
- **The ransomware program** locks the computer and then demands a ransom in order to unlock it.

Distribution methods:

links to malicious websites in email

social media posts

they convince you to download the infected file

visiting an infected site

using an infected USB drive on a computer

collect passwords from websites and other computers they hacked

CYBERSECURITY ISSUES (RECOMMENDATIONS)

RECOMMENDATIONS:

Take a close look at the sites and resources you visit, check the domain names and carefully read what you agree to before clicking «yes, I agree».

Before opening the letter you received, write a few words in response on it, because if the sender is correct, the party who sent the letter will definitely respond.

Set up complex passwords and/or two-factor authentication to access your personal data.

Open a separate virtual card for online purchases and insert only the amount calculated for the purchase inside.

Have you been subjected to cyber attacks in the last year?

According to the survey, over the last year, the population of Kazakhstan has been subjected to the following types of cyber attacks:

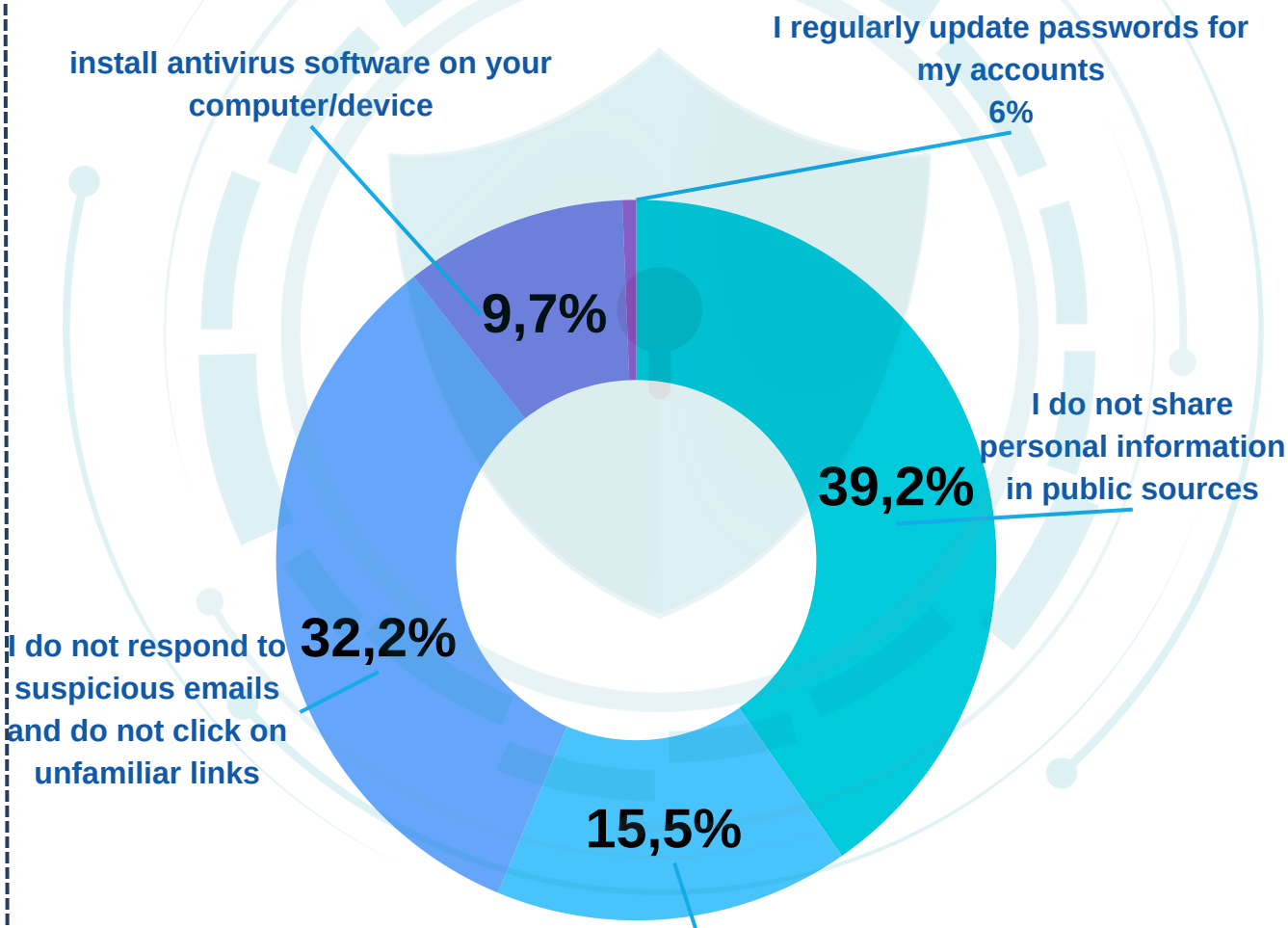
- **computer viruses – 22.8%;**
- **malicious spam – 16.9%;**
- **account hacking – 8.1%;**
- **hacker attack – 3.6%;**
- **cyber fraud – 6.9%;**

	2023	2022	2021	2020
Computer virus attack	22,8%	51,7%	16,5%	32,1%
Malicious spam	16,9%	34,5%	23,0%	13,4%
Hacking social media accounts	8,1%	28,4%	14,5%	3,9%

CYBERSECURITY RECOMMENDATIONS:

- **Update passwords regularly.**
- **Use two-factor authentication.**
- **Issue separate bank cards for children.**
- **Restrict access to applications and remove geolocation.**
- **Set up privacy in social networks.**
- **Use email to forward documents.**
- **Download the software only from official websites.**
- **Give preference to the mobile version of the resource, rather than the site.**

WHAT SECURITY MEASURES DO YOU USE WHEN WORKING ON THE INTERNET?



CYBERSECURITY ISSUES (RECOMMENDATIONS)

INFORMATION SECURITY PREVENTION

DO RESPONDENTS CHECK INFORMATION ABOUT THE SITES THEY REGISTER ON?

The results of the social survey show:

40,4% percent of respondents check information about websites regularly;

42,5% percent of respondents check information about websites sometimes when the resource raises any doubts;

16,9% percent of respondents never check information about websites;

What should you do if you notice suspicious activity on your bank account in online banking, online store, etc.?

5,96% respondents will share information about suspicious activity on social networks;

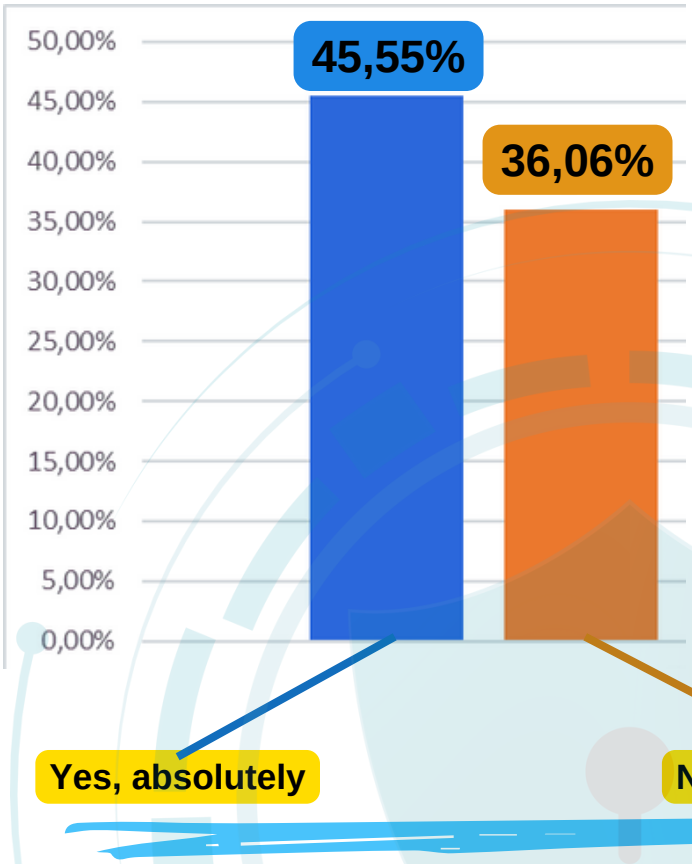
68,91% respondents will be immediately notified to the bank about suspicious activity;

12,35% respondents will leave everything as it is, perhaps this is a system error;

RECOMMENDATIONS
(information security prevention)

- **Regularly install updates for your software – operating systems, application programs, antivirus and other programs.**
- **Enable the automatic software update feature when it is available.**
- **Uninstall software that you don't use or when you don't receive developer updates.**
- **Avoid installing unlicensed software or software from unverified sources.**
- **Regularly create a copy of the data that is important to you on other devices.**

INFORMATION SECURITY PREVENTION



The respondents' response to the survey:

«Do you know about the activities of the authorized body for information security and how to contact it?»

According to respondents, the main measure for suspected cybersecurity violations is?

Contacting law enforcement agencies	10,79%
Contacting an IT-specialist	55,36%
Contacting the authorized body in the field of information security	15,37%
They do not consider it necessary to do anything	3,70%

In case of any non-standard suspicions of an information security violation:
-contact the responsible specialists immediately;
-you can also contact the computer response service/ phone:
1400 or +7 (7172) 55-99-97,
e-mail:
info@ kz-cert.kz

RECOMMENDATIONS ON INFORMATION SECURITY

CYBERSECURITY ISSUES (RECOMMENDATIONS)

PASSWORD POLICY

It is forbidden to store passwords electronically on the desktop.

It is allowed to disclose the password values in case of production necessity.

Passwords must be at least 8 characters long and must be updated quarterly.

MAIL

It is forbidden to open emails and suspicious attachments from strangers.

For any suspicious e-mail request, an alternative communication channel (for example, a telephone) must be used to confirm the request from the recipient.

It is always necessary to check the spelling of the sender's and recipient's addresses.

ANTIVIRUS SOFTWARE

You must use licensed antivirus software.

Be sure to check any media for viruses when connected to your computer.

Scan all files from incoming email for viruses by setting up automatic scanning.

SOCIAL ENGINEERING

It is forbidden to disclose IP addresses and a combination of login and password to third parties.

It is forbidden to install the software yourself.

INTERNET AND SOCIAL NETWORKS

It is not allowed to follow links from an unknown sender.

It is prohibited to visit websites containing materials of a terrorist, extremist, unconstitutional or other destructive nature.

It is forbidden to accept agreements when visiting sites whose meaning you do not understand.

It is forbidden to use passwords for accessing the local network in other programs and on websites.

In order to avoid threats related to the use of cookies (small files), it is recommended to periodically analyze stored cookies.

ADDITIONAL CYBERSECURITY RECOMMENDATIONS FOR GOVERNMENT EMPLOYEES

- It is prohibited to connect the internal networks of a government agency (GA) to the Internet.
- The Internet connection must be carried out only through a Single Internet Access Gateway.
- When working with Internet resources and e-mail, it is prohibited to disclose government, official and commercial information that has become known to an employee out of official necessity or otherwise.
- Employees of civil defense and local executive bodies (LEB), when carrying out official correspondence in electronic form, use only departmental e-mail in the performance of their official duties.
- It is forbidden to leave computers and Internet networks in the open without supervision. In case of leaving the workplace, it is mandatory to lock the computer (– Windows key combination +L).
- It is prohibited to connect to the Unified Transport Environment (ETS) of GO, the local GA network through wireless networks, wireless access, modems, radio modems, modems of networks of cellular operators and other wireless network devices.

RECOMMENDATIONS FOR THE PROTECTION OF PERSONAL DATA:

WHEN SIGNING THE CONSENT, PAY ATTENTION TO:

- purposes of personal data collection and processing;
- the period or period during which the consent is valid;
- the possibility of transfer to third parties;
- the possibility of cross-border data transfer;
- the possibility of distributing personal data in public sources.
- a list of personal data collected by the operator;

When providing personal data anywhere, the mandatory requirement is the consent of an individual or the basis provided by Law.

Without your consent, personal data cannot be transferred by the operator to other persons and organizations.

Also, in order to protect personal data from illegal dissemination, it is strongly recommended to familiarize yourself with the privacy policy of the organization's personal data, as well as pay close attention to the conditions of their processing.

YOUR RIGHTS ARE PROTECTED BY LAW:

According to paragraph 2 of Article 20 of the Law of the Republic of Kazakhstan «On Personal Data and their protection»:

Of the Republic of Kazakhstan on personal data and their protection and the standards in force in the territory of the Republic of Kazakhstan. This obligation arises from the moment of receipt of electronic information resources containing personal data and before their destruction or depersonalization.

The collection and processing of personal data is carried out only in cases of ensuring their protection.

In addition, in accordance with Article 56 of the Law of the Republic of Kazakhstan «On Informatization», owners and owners of information systems who have received electronic information resources containing personal data, the owner and (or) operator of a database containing personal data, as well as third parties, are required to take measures to protect them in accordance with this Law,

On December 11, 2023, a new protection system was introduced under the law «On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan on information security, Informatization and digital assets":

The law provides for the following innovations in terms of:

endowing the authorized body in the field of personal data protection (Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan) with the function of state control over compliance with the legislation of the Republic of Kazakhstan on personal data and their protection;

the establishment of a ban on the collection and processing of copies of identity documents containing personal data;

informing citizens about the facts of personal data leakage;

the formation of a voluntary refusal to receive bank loans;

WHAT TO DO?

Upon detection of illegal collection and leakage of personal data

citizens can contact the Information Security Committee of the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan to take measures to curb violations.

This can be done by writing through the e-Government portal (section «Electronic appeals"), you can also write to the chairman's personal blog (*https://dialog.egov.kz/blogs/3932160/welcome*)

egov

THE REQUESTS MUST CONTAIN:

1. Full name, contacts of the applicant;
2. Description of the situation in which the violation was committed;
3. The period and timing of the violation;
4. Reliable materials confirming the violation;
5. The name of the organization that committed the offense.

If you find that someone collects and processes your personal data without your consent, you have the right to contact this person of the organization with a request to destroy illegally collected data. In addition, you also have the right to revoke your previously given consent to the collection and processing of your personal data. In case of inaction or refusal of the operator to destroy the data, you can complain to the authorized body in the field of personal data protection – THE INFORMATION SECURITY COMMITTEE OF THE MINISTRY OF DIGITAL DEVELOPMENT, INNOVATION AND AEROSPACE INDUSTRY OF THE REPUBLIC OF KAZAKHSTAN.

Appeals can be submitted in any convenient and accessible way.

USING AN ELECTRONIC DIGITAL SIGNATURE

What is an electronic digital signature (EDS)?

Simply put, an electronic digital signature (EDS) is a citizen's own signature in electronic form, on which documents can be signed.

What can happen if an EDS falls into the hands of scammers or someone else:

If the EDS is not password protected, documents or financial transactions can be signed through it.

For business entities, obtaining an EDS can lead to the employment of "fictitious workers".

Registration of several persons without notification in the apartment by the name of the owner of the digital signature.

The following measures should be taken to protect your own digital signature:

When you first receive an EDS from a PSC, there may be a simple password, so it should be replaced with a complex password.

Do not transfer the EDS to unauthorized persons. They can sign documents on your behalf when the responsibility lies with you.

Do not send EDS in special chats or messengers.

Provide the computer or laptop on which the EDS is stored with virus protection programs.

When saving the EDS in files, do not save its password with the file name.

Don't take the EDS on someone else. There are several ways to get an EDS: through Public Service Centers (PSC) or through eGov.

Avoid installing unverified or unreliable programs on smartphone gadgets with your computer.

Update your key immediately if you have lost your EDS or if it has fallen into the hands of others.

Protecting the safety of children on the Internet

To date, there are more and more sources on the Internet resource that pose a danger to children. If we mention some of them: prohibited conspiracies, resources and groups that encourage children to commit suicide or to negative bullying actions that harm children.

Cyberbullying is a very urgent problem for the safety of children today. In such situations, parents should pay attention:

- A bad mood after spending time on the Internet.
- He becomes extremely secretive, especially when it comes to using unwanted information on the Internet.

- Aggression or an outburst of anger.
- Anxiety and/or agitation in the child.

- They often ask for money.

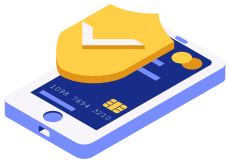
What measures should parents take to protect children from cyber threats:

* Limit the time you use the Internet.

* Take control of the content viewed by children on the Internet and various networks.

* Discuss potential threats on the Internet with your children.

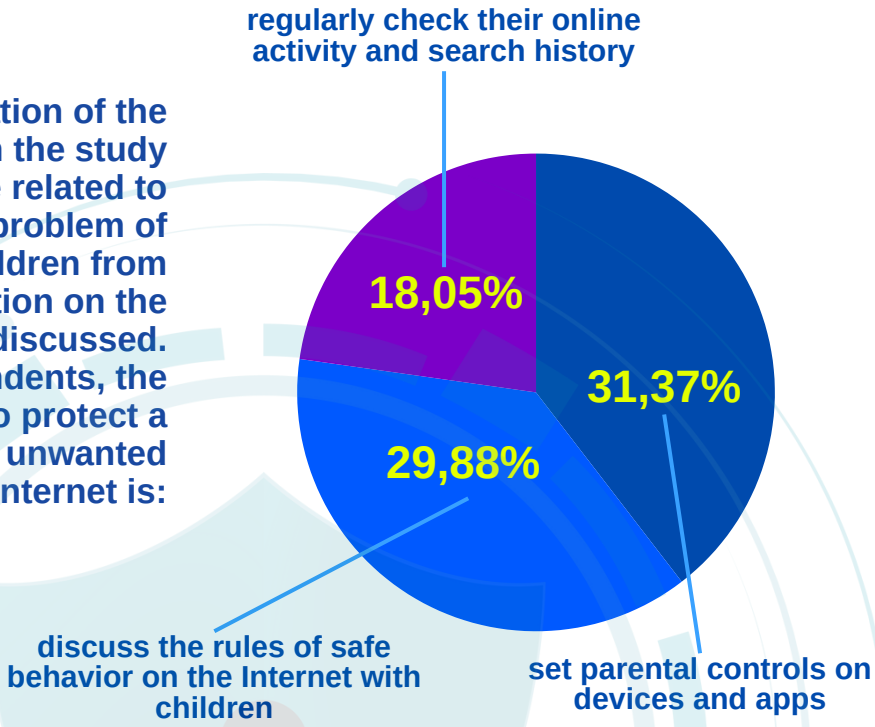
* Explain to the children that you can complain about negative content to the moderator of the resource.



* If children encounter an unpleasant situation on the Internet, help them overcome this situation without raising their voices.

Rules of information security of CHILDREN AND ADOLESCENTS ON THE INTERNET

In the continuation of the dialogue with the study participants, an issue related to the current problem of protecting children from unwanted information on the Internet was also discussed. According to respondents, the main measure to protect a child from unwanted information on the Internet is:



Recommendations for parents:

- Create a list of house rules for visiting the Internet with the participation of teenagers and demand its unconditional fulfillment. Discuss with your child the list of prohibited sites (the «blacklist»), opening hours on the Internet, and a guide to communicating on the Internet (including in chat rooms).
- A computer with an Internet connection should be located in the common room.
- Do not forget to talk to children about their friends on the Internet, about what they are doing in such a way as if we are talking about friends in real life. Ask about the people that children communicate with through instant messaging services to make sure that these people are familiar to them.
- Use tools to block unwanted content as an addition to standard Parental controls.
- It is necessary to know which chats your children use. Encourage the use of moderated chats and insist that children do not communicate privately.

Constantly monitor your child's Internet usage! This is not a violation of his personal space, but a precautionary measure and a manifestation of your parental responsibility and care.

HOW CAN I RESTRICT CHILDREN AND TEENAGERS' ACCESS TO THE INTERNET?

CYBERSECURITY ISSUES (RECOMMENDATIONS)

1. Teach children not to give out their personal information by means of e-mail, chats, instant messaging systems, registration forms, personal profiles, and when registering for contests on the Internet.

2. Teach children not to download programs without your permission. Explain to them that they may accidentally download viruses or other unwanted software.

3. Teach your child to inform you about any threats or worries related to the Internet. Remind the children that they are safe if they have told you about their threats or worries.

4. Help them protect themselves from spam. Teach teenagers not to give out their real email address on the Internet, not to respond to unwanted emails and use special mail filters.

5. Explain to the children that in no case should you use the Network for bullying, spreading gossip or threatening other people.

6. Discuss the problems of online gambling and their possible risks with teenagers. Please remind that children cannot play these games according to the law.

SECTION FOR PROFESSIONALS

Recommendations that should be remembered by business owners, employees of the relevant industry, IT-specialist, information security officer:

1 INFORMATION SECURITY POLICY DEVELOPMENT

The management of an enterprise or organization should develop and implement an information security concept. This document is fundamental for the development of internal regulations and a system of protective measures.

2 CREATING PROTECTION ON SEVERAL LEVELS.

A multi-layered approach to cybersecurity will reduce the risk of an attack by cryptographers. It involves combining several protective tools. If a threat bypasses one level of protection, then at the next level it will face a new obstacle.

3 REVIEW OF THE POLICY ON THE USE OF PERSONAL DEVICES FOR WORK PURPOSES.

Remote employees sometimes use their own laptops or mobile devices to work and connect to the corporate network. However, a reliable antivirus or other security tool is not always installed on personal devices.

4 USING EMAIL FILTERS.

Of course, mail filters cannot guarantee that an organization will not receive a phishing email, but they increase the level of security. 46.1% of respondents indicated that they open only well-known and reliable emails.

5 USING A PASSWORD MANAGER.

Organizing the use of a password manager by employees-it creates and stores long and complex passwords and transfers them to the input fields in applications.

SECTION FOR PROFESSIONALS

6 DATA BACKUP.

Regularly back up not only the data that is stored on your computer, but also those that you store on mobile devices. This way you can quickly recover the necessary information if the device is lost or stolen.

7 EMPLOYEE TRAINING.

In most cases, employees do not know that their actions can be dangerous. You can reduce the risk of human error by increasing the awareness of your organization's employees about cyber threats, including threats related to social engineering.

In case of a threat to information security, the study showed that 55.4% of respondents turn to IT-specialists.

8 DRAWING UP AN ACTION PLAN IN CASE OF A CYBER ATTACK.

You need to be prepared for an emergency. To reliably protect businesses, employees and customers, it is important to have a detailed plan of action in case of an attack.

9 ENABLE PASSWORD PROTECTION.

To protect the average attacker from a mobile device, it is necessary to use a complex password or PIN code. 33.6% of respondents indicated that they use an individual complex password for each account.

POWERS OF THE INFORMATION SECURITY COMMITTEE

Within the framework of the Decree of the President of the Republic of Kazakhstan dated October 6, 2016 No. 350, the Information Security Committee was established.

1. **DEVELOPMENT**
   Development of measures in the field of information security (with the exception of state secrets).

2. **CONTROL**
   State control in the field of information security in the field of informatization, protection of personal data, electronic document and electronic digital signature and secured digital assets.

3. **PREVENTION**
   Prevention of compliance with Uniform requirements in the field of information and communication technologies and information security.

4. **FORMING**
   Creation of a list and monitoring of critical information and communication infrastructure.

5. **MANAGEMENT**
   Management and distribution of domain names in the space of the Kazakhstan segment of the Internet.

6. **EXTRADITION**
   Issuance of an act based on the results of tests for compliance with information security requirements.

7. **ORGANIZATION**
   Organization of the implementation of the National Information Security Incident Response Plan.

8. **CONSIDERATION**
   Consideration and prosecution for violations in the field of personal data.

9. **IMPLEMENTATION**
   The implementation of accreditation of certification centers.

10. **AWARENESS**
    Raising public awareness of threats to information security (cybersecurity)

11. **PARTICIPATION**
    Participation in the implementation of educational programs.

12. **ASSISTANCE**
    Assistance in the formation of professional standards.

13. **INTERACTION**
    Interaction with international organizations, national regulators and cybersecurity centers.

14. **PERMISSION**
    Issuance of a permit for the issuance and circulation of secured digital assets.

15. **SUPPORT**
    Support of scientific research in the field of information security.

WHERE SHOULD I CONTACT IN CASE OF COMPUTER INCIDENTS?

During a computer incident, it is necessary to contact!

Response service

1400

(8 (7172) 55-99-97

info@kz-cert.kz

The National Computer Incident Response Service is a single center for users of national information systems and the Internet segment, providing collection and analysis of information on computer incidents, advisory and technical support to users in preventing computer security threats.

THE COMPETENCE OF THE SERVICE INCLUDES THE PROCESSING OF THE FOLLOWING COMPUTER INCIDENTS IN ORDER TO IDENTIFY AND NEUTRALIZE THEM:

- attacks on network infrastructure nodes and server resources;
- unauthorized access to information resources;

- scanning of national information networks and hosts;
- selection and capture of passwords and other authentication information;

- distribution of malicious software, unsolicited correspondence (spam);
- hacking of information network security systems;

A brief analysis

of the results of a sociological study on information security (cybersecurity) and personal data protection

By order of the Republican State Institution «Information Security Committee of the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan», a sociological study on information security (cybersecurity) and personal data protection was conducted.

The result of the survey determined the general indicator of public awareness of the existing threats to information security (cybersecurity) and personal data protection at the level of 80.4%.

In general, the results of a sociological study on information security (cybersecurity) and personal data protection indicate the growing importance of information security issues in the daily lives of citizens:

- the level of ability to recognize phishing attempts was 74.64%;
- 90.52% of the population knows about the protection of personal information when using social networks.

The results of the study show a positive dynamism in the formation of public awareness in the field of information security (cybersecurity) and personal data protection. However, the challenges of this area require constant improvement of measures and mechanisms to ensure the stable protection of citizens' interests in the digital age.

In this regard, taking into account the conducted sociological survey, the research group has developed appropriate recommendations and proposals for further ensuring the information security of citizens and the protection of their personal data in the digital space.

RECOMMENDATIONS

By order of RSU «Information Security Committee of the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan»

Republic of Kazakhstan 010000, Astana, PR. Mangilik El 55/14, Block C 2.4

telephone: +7 (7172) 64-93-96, +7 (7172) 64-93-99

e-mail: **moap@mdai.gov.kz**
https://www.gov.kz/memleket/entities/infsecurity?lang=ru

Astana, 2023.