powered by

MSSP GLOBAL

AI & DIGITAL MINISTRY

citizensec

citi zen sec

Cybersecurity Magazine

Knowledge is protection.
We will help you understand the risks and learn how to protect yourself
and your loved ones together.

2025

MSSP

;)

Attention! CitizenSec Cybersecurity Magazine with practical tips to prevent blue screens and protect you from glitches, viruses, and other cyber threats.

Clear guidance from experts with 10 years of experience.

Learn once, save and protect yourself always!

Citizensec - Cyber Hygiene and Methodology
powered by mssp.global

citizensec

"CitizenSec" is a project developed by mssp.global experts in cooperation with specialists of the Information Security Committee of the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan. The material is based on more than 10 years of experience in the field of cybersecurity.

Our mission

Our mission is to increase cyber culture by teaching the necessary knowledge and skills for the digital world.

Contents

Social engineering. How do scammers operate? 06

What methods and psychological techniques they use to mislead people, and learn to recognize them.

Phishing and spam 09

The main methods of phishing scams and how to protect yourself with practical tips

A strong password, what is it? 15

How to create strong passwords, as well as which passwords are most vulnerable to hacking.

Don't touch my phone! 18

Your phone stores everything from personal data to finances. Learn how to protect it from threats.

Is it true? Is there Wi-Fi here? 21/23

Fact-checking and misinformation: how to protect yourself, as well as all the ways to use Wi-Fi safely.

You've made your bed, now lie in it 25

Learn how to keep your personal data and your assets safe with our tips.

Show me the money! 30

Financial Security: how to protect your money from fraudsters.

Sweet Kids, Safe Clicks 32

Simple ways to protect your children from cyber threats and scammers on the Internet.

02

Social engineering. How do scammers operate?

What methods and psychological techniques they use to mislead people, and learn to recognize them.

Your account will be blocked if you do not meet the requirements. I'm calling from your bank, we need to confirm your information. Congratulations! You've won the lottery. To claim your prize, fill out the form with your details and pay a small delivery fee.

Your account will be suspended after 24 hours. We've detected suspicious activity on your account. To verify your identity, follow the link and confirm the data. If you do not do this, your account will be disabled. You've won a gift!

Social engineering

Social engineering is the act of manipulating people into revealing confidential information, triggering malware, or performing actions that benefit the attacker.

> ! Scammers play on your emotions using fear, urgency, and trust to trick you.

tactics used by scammers

They use fear and urgency.

MAIL 1h ago

"Your account will be blocked unless you follow the instructions."

"I'm calling from your bank. We need to verify your information."

They pose as representatives of trusted organizations.

They create a false sense of emergency

A suspicious transaction was detected on your account. To cancel it, confirm your card details within 10 minutes.

You're one of our top clients, and we'd like to offer you something special.

They gain your trust with flattery

They pressure you with social proof.

Thousands of people have already taken advantage of this offer.

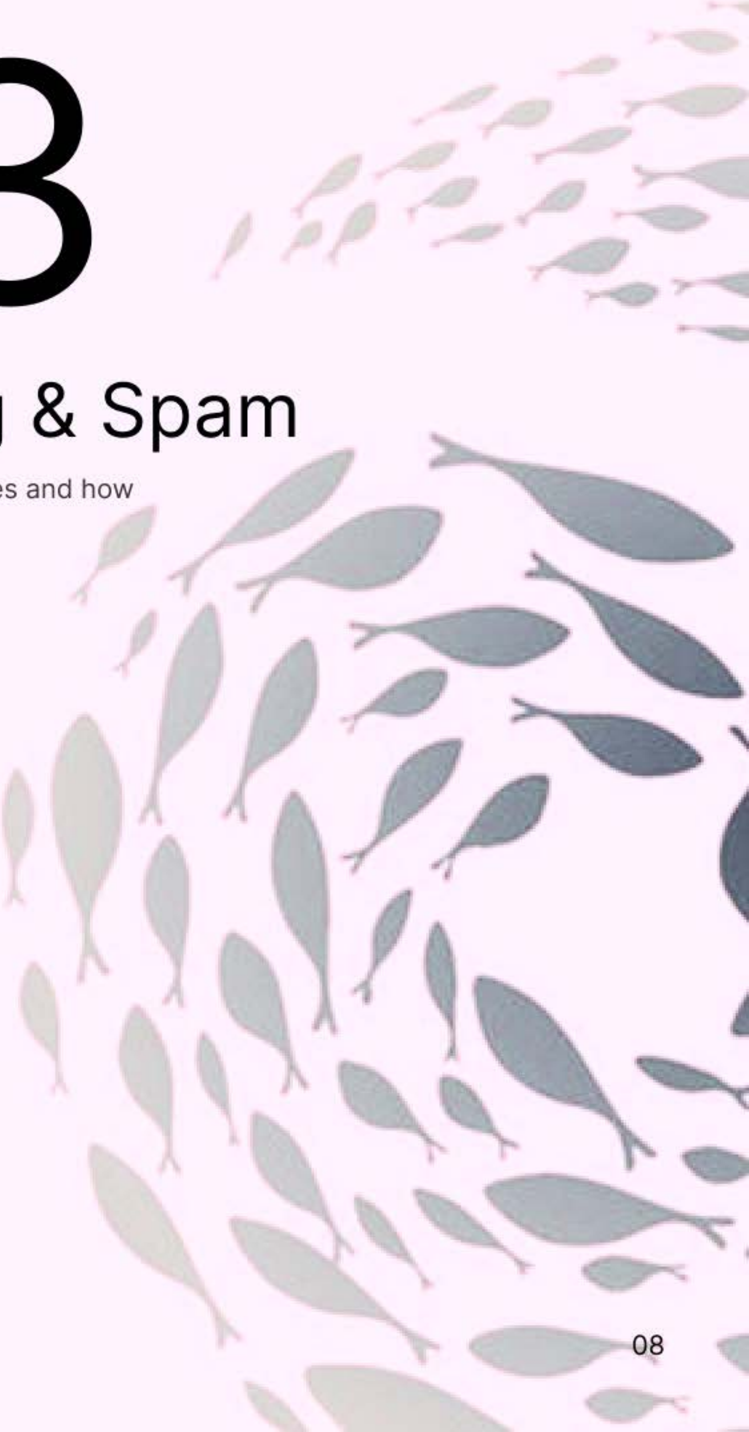
If a message triggers ***strong emotions*** — pause. Don't share personal information or send money in a rush.

Always verify the information through official channels or contact the organization directly.

03

Phishing & Spam

Key phishing techniques and how to protect yourself.



Phishing

It's like fishing — but instead of catching fish, scammers are after your personal data. Phishing attacks come in the form of fake emails, text messages, or instant messages designed to trick you into giving away sensitive information.

Phishing

The traditional method with fake emails with malicious links or attachments aimed at stealing confidential information.

SEO Phishing

Fake websites that look real and appear at the top of search engine results.

Vishing

Scammers call you pretending to be from a trusted organization, using various scenarios to extract information.

Smishing

Fraud via text messages that often contain malicious links or urgent requests.

Malvertising

Malware hidden in online ads — clicking them can infect your device.

Spear Phishing

Targeted phishing attacks using personal information about you to appear more convincing. About a specific person

Spam Phishing

Mass phishing campaigns sent to thousands of users at once.

How do I know if it's phishing?

1 Stop, look, think.

2 Warning signs:

- Errors in the letter or address.
- Check the sender's address and links.
- Be careful with letters that evoke strong emotions.
- Check the address bar of the site.

3 Do not open suspicious attachments.

4 Don’t make assumptions, always check.

5 Do not be fooled by tricks and lucrative offers, keep a cool head.

Anatomy of a phishing scam

001

Creating compelling content for a phishing attack.

1. Relevant topics are often used.
2. Creating fake emails with links to phishing sites or infected attachments.

002

Mass sending of phishing emails.

Attackers use bulk mailing servers or compromised accounts to send phishing emails so they appear legitimate.

003

Catching attention and deceiving the victim.

Messages are emotionally charged or urgent (e.g., “This offer expires in a few hours”) to provoke quick reactions.

004

Capturing data and obtaining confidential information.

The link leads to a fake website that closely resembles a legitimate one, where users unknowingly enter sensitive data.

005

Using stolen information.

Credentials and other stolen data are used to access the victim’s real accounts.

006

Covering their tracks.

Attackers erase evidence to avoid detection and prosecution.

007

And this is already an agent...

And what about password cracking — how do they succeed so often?

04

A strong password, what is it?

How to create strong passwords, as well as which passwords are most vulnerable to hacking.

PASSWORD

The stats say it all

80% of hacked accounts used common or easily guessable passwords.

Even Mark Zuckerberg got hacked — he used the same password across multiple accounts.

Sound familiar?

We know... you've probably done it too. And yeah, remembering dozens of passwords is hard.

Brute-force attacks — that's when hackers try every possible combination to guess your password. Weak passwords can be cracked in just seconds.
The fix is simple: Use strong, unique passwords for every account.

THE WEAKEST LINK

Decision: Use a password manager.

Password types by importance:

Regular Importance
These passwords are used for everyday tasks and less critical services. Examples:

- Social media.
- Email services.
- Messengers.
- Various websites and online stores

High Importance
These passwords protect access to the most important and sensitive data. Examples:

- Bank accounts and financial apps.
- Hard drive encryption.
- Password manager access.
- Accounts with administrative access.

Tip:

A password manager will help you securely store all your passwords and use unique, complex combinations for each account. This will reduce the risk of hacking and protect your data.

Don't store all your passwords in one place.

Organize them by importance.

Use **password managers**. They provide secure storage and management of passwords.

Create **complex and unique passwords.** Use built-in password generators in password managers for this.

Never share passwords **in full**. If you need to share a password, split it into parts and send them via different communication channels.

Recommended Password Managers: Dashlane, 1Password, KeyPassXC, Bitwarden, Enpass.

05

Do not touch my phone!

Your phone stores everything from personal data to finances.
Learn how to protect it from threats.

Device Protection

Gadgets are always with us – they are pocket computers where our entire life is stored: from watches and photos to work and finances.

Problem:

Malicious apps threaten your personal and financial security by stealing banking data and passwords.

Modern scammer schemes include video calls to collect biometrics, which allows you to apply for loans and conduct transactions on your behalf.

Decision:

Key security measures for our devices:

1 Set a complex password, PIN code, and use biometrics to protect your device.

2 Download apps only from official sources: Apps from Google Play or the App Store are safer.

3 A reliable antivirus helps detect and block malware.

4 Restrict app access to your data to protect your information.

5 Set up features that allow you to track your device's location and remotely wipe data in case of theft.

6 Save important data regularly so you don't lose it if your device is stolen or broken.

06

Is the cover true?

Fact-checking and disinformation:
how to protect yourself?

Fact-checking and disinformation: how to protect yourself?

Disinformation is intentional misrepresentation, while misinformation is the dissemination of incorrect information by mistake. Both lead to distrust, polarization, and harm to society.

To avoid spreading fakes:

- **Check the news on official sources and fact-checking platforms such as Factcheck.kz and StopFake.kz.**
- **Develop critical thinking and media literacy.**
- **Be attentive to the protection of personal data.**

07

Is there Wi-Fi here?

All ways to use Wi-Fi are safe.

Public Wi-Fi hotspots are convenient, especially on vacation or on trips, but they can be insecure. Let's take a look at the problems, risks, and how to protect yourself.

Problems and risks of public access points:

No Encryption:
Many public networks do not encrypt data, making them vulnerable to eavesdropping. As a result, your personal information, including passwords and financial data, can be stolen.

Fake Access Points:
Scammers can create fake networks that look legitimate. By connecting to such a network, you unwittingly give them access to your data.

Man-in-the-Middle Attacks:
Scammers can intercept data transmitted between you and the network, allowing them to modify or steal your information.

Решения

1. **Use a VPN:** A secure VPN channel hides your activity and prevents data interception.

2. **Turn off auto-connect:** Do not automatically connect devices to open networks to avoid accidentally connecting to fake hotspots.

3. **Check the network:** Before connecting, make sure that the network really belongs to a public institution and not to an attacker.

4. **Use mobile internet:** Temporarily switch to mobile data if the Wi-Fi network is not secure.

5. **Avoid confidential transactions:** Do not make banking transactions or purchases through public networks.

6. **Use Two-Factor Authentication:**
Enable two-factor authentication for all important accounts.

@cmfplc

08

You’ve made your bed, now lie in it!

Learn how to protect your personal data and assets with our tips.

item count:
total:

card: ****5677987
auth: 586843379
cardholder:

What is Personal Data?

Personal data is any information that identifies you as an individual. It is divided into two types:

1. **Public Data:** Information that can be accessed by others with your consent (e.g., full name, ID number, address).

2. **Restricted Access Data:** Information that is protected by law (e.g., medical, financial, or commercial information).

Identification Data: ID number, full name, date of birth, passport details.

Contact Data: Address, phone number, email address.

Financial Data: Bank accounts, income and expenditure information.

Medical Data: Medical history, test results.

Educational Data: Diplomas, certificates, education level.

Professional Data: Workplace, position, professional skills.

Family Status Data: Information about marriage, children, relatives.

Movement Data: Visit history, geolocation.

What to Consider When Sharing Data?

Before sharing your data, pay attention to:

- **Purpose of Data Collection and Processing:** Why are they collecting your data?
- **Data Retention Period:** How long will your data be used?
- **Data Transfer to Third Parties:** To whom and for what purpose can your data be transferred?
- **Cross-Border Transfer:** Can your data be transferred abroad?
- **Public Accessibility of Data:** Will your data be published?

Your rights are protected by law!

In Kazakhstan, the protection of personal data is regulated by several laws:

- Law of the Republic of Kazakhstan “On Personal Data and Their Protection” — regulates the collection and processing of data, as well as citizens’ rights.
- Law of the Republic of Kazakhstan “On Informatization” — protects data in information systems.
- Civil Code — guarantees the right to protect personal and family secrets.
- Criminal Code and the Code of Administrative Offenses — establishes liability for violations of personal data protection laws.

Your Rights:

To receive information about who processes your data and how it is handled.

To modify or delete your data.

To withdraw your consent for data processing.

What to Do in Case of a Violation of Your Rights?

If your data has been illegally collected or used:

1 Contact the organization that violated your rights and demand that the data be deleted.

2 Submit a complaint to the Committee on Information Security of the Ministry of Digital Development, Innovation, and Aerospace Industry of the Republic of Kazakhstan via the e-otinish portal.

In your complaint, include:

- Full name and contact details.
- Detailed description of the violation.
- Evidence (screenshots, emails, organization names, etc.).

How to Protect Your Data?

- Read the privacy policy before agreeing to data processing.
- Do not post sensitive information on social media.
- Use strong passwords and never share them with third parties.
- Regularly check who has access to your data.

EDS: Security Secrets

An electronic digital signature (EDS) is the digital equivalent of a handwritten signature, ensuring the authenticity, integrity of the data, and the identity of the signer.

Risks:

If cybercriminals gain access to your EDS private key, they could sign documents on your behalf.

Protection Measures:

- Store keys in a secure location (smart cards, USB tokens).
- Regularly update the software used for EDS.
- Use strong passwords and change them frequently.
- **Revoke unused or lost EDS keys!**
  - This is crucial, as these keys are often the primary target for cybercriminals.

Liability:

Administrative: For failing to implement protection measures and transferring the EDS (Article 640 of the Code of Administrative Offenses of the Republic of Kazakhstan).

Criminal: For unauthorized access to the system (Article 205 of the Criminal Code of the Republic of Kazakhstan).

In case of violations, contact the Committee for Information Security of the Ministry of Digital Development, Innovation, and Aerospace Industry of the Republic of Kazakhstan.

09

Show me the money!

Financial Security: how to protect your money from fraudsters.

Financial security issues:

- Phishing – fake websites/emails to steal data.
- Skimming is the installation of devices on ATMs to copy data from bank cards.
- Loan fraud is the illegal registration of loans in your name.

Solutions to protect finances:

+ **Caution with ATMs**
  Check ATMs for skimmers (suspicious elements on the keyboard or card insertion point).

+ **"Stop Credit" through eGov**
  Enable the feature to prevent loans from being issued without your consent (via eGov or mobile app).

+ **Secure online payments**
  Shop on trusted sites.
  Use a separate card for online payments with a limited amount.

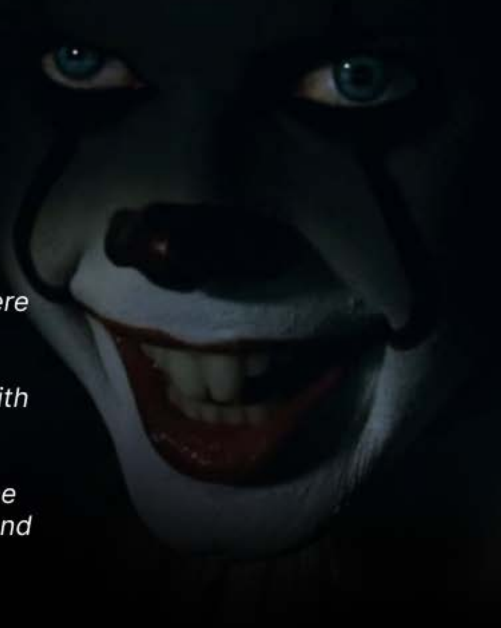
+ **Card Usage Rules**
  3D Secure: Activate protection through the bank to receive SMS codes to confirm transactions.

+ **Two-factor authentication (2FA):**
  Set up additional protection in banking apps and websites.

10

Sweet Kids, Safe Clicks

Simple ways to protect your children from cyber threats and scammers on the Internet.



Cybersecurity for Kids

The story of AI technologies: Recently, there was a case where scammers used AI to create a fake voicemail on behalf of the child's parents. The child received a call with a request to leave school and go with a stranger. Allegedly, his mother sent him. Thanks to vigilance and proper training, the child realized that something was wrong and informed the adults about it, avoiding serious consequences.

Content Restriction:

Tip: Use DNS and router settings to restrict access to unwanted sites.

Example: Install DNS services such as OpenDNS, Yandex DNS server, or Google SafeSearch to filter content.

Parental controls:

Tip: Install parental control apps like Google Family Link to keep an eye on your child's online activity.

Use of AI technologies:

Tip: Stay up to date with modern technologies such as voice or face spoofing with AI. Explain to your children that not everything on the Internet is true.

History: Tell a story about how scammers can use AI to create fake videos or voicemails to trick them.

Code word with a child:

code **Tip:** Create a special code word that your child can use in emergency situations to let you know about the problem safely and discreetly.

1 **Constant Dialogue:**
Tip: Regularly discuss online activities with children and explain possible threats.

2 **Safety Training:**
Tip: Teach children to recognize dangerous situations, such as suspicious messages or offers.

3 **Contact Verification:**
Tip: Carefully check who your children communicate with on the Internet. Explain to them that not all people online are who they say they are.

4 **Creating a Safe Environment:**
Tip: Create a safe space in your home to discuss any questions or problems related to the Internet. Let the children know that they can ask you for help in any situation.

MSSP

citizensec - Cyber Hygiene and Methodology

powered by

MSSP GLOBAL

AI & DIGITAL MINISTRY

citizensec