Data Protection

КРИСТИНА

1.

- What are considered personal data?

Personal data is any information that allows the identification of a specific person. This can include name, address, phone number, email, photograph, date of birth, social status, medical records, financial data and others.

ЖЕНЯ

- Why is data protection important?

Confidentiality: Personal data can contain confidential information such as social status, financial data, medical records, etc. If this data falls into the wrong hands, it can lead to identity theft, fraud or other problems.

Personal safety: Some personal data, such as addresses and phone numbers, can be used to track or stalk people. If this data is available to unauthorized persons, it can pose a threat to personal safety.

Legislation: There is legislation that requires the protection of personal data. Violation of this legislation can result in fines or other legal consequences.

КРИСТИНА

2.

Risks of Personal Data Breaches:

- What can be the consequences of personal data breaches?

1. Identity theft risk: criminals can use stolen personal data to access financial accounts, credit cards and other valuables.

2. Reputation loss risk: personal data breaches can have a negative impact on the reputation of a company, especially if it fails to protect its customers' data.

3. Violation of legislation: companies that do not protect their customers' personal data may be subject to fines and other legal consequences.

ЖЕНЯ

- What methods do criminals use to access personal data?

1. Phishing: criminals send emails or messages that look like official requests from banks, companies or other organizations and ask users to provide their logins and passwords.

2. Malware: criminals can use malware, such as viruses, Trojans and spyware, to gain access to computers and steal personal data.

3. Social engineering: criminals can deceive users and gain access to their personal data, such as asking them to provide their logins and passwords.

4. Data security breaches: criminals can exploit vulnerabilities in data security systems to gain access to personal data.

ЖЕНЯ

3.

Measures to Protect Personal Data:

1. Do not respond to emails or messages that request your logins and passwords. Instead, contact the organization directly to ensure that the request is official.

2. Install antivirus software and update it regularly.

3. Use complex passwords and do not use the same password for different accounts.

КРИСТИНА

4. Use two-factor authentication where possible.

5. Update software and operating systems on your computer and mobile device.

6. Use a VPN when working with public Wi-Fi networks.

КРИСТИНА

- What technologies are used to protect personal data?

1. Data encryption: a technology that converts data into an unreadable format to prevent unauthorized access to it.

2. Firewalls: software that controls access to the network and blocks unwanted traffic.

3. Antivirus software: a program that detects and removes malware that can threaten the security of personal data.

ЖЕНЯ

4. VPN is a technology that creates an encrypted tunnel between the user's device and a server to protect data from unauthorized access.

5. Biometric authentication is a technology that uses unique physical characteristics of the user, such as fingerprints or facial recognition, to verify authenticity.

6. Multifactor authentication is a technology that requires the user to provide two or more forms of identity confirmation, such as a password and a verification code.

7. Blockchain is a technology that uses a decentralized data storage system to provide security and transparency in information exchange.

КРИСТИНА

4.

Data Protection Legislation:

Key provisions of data protection legislation include:

1. Consent to the processing of personal data.

2. Purpose of collecting and processing personal data.

3. Ensuring the security of personal data.

4. Data subject rights.

5. Responsibility for violating data protection legislation.

ЖЕНЯ

5.

Finally, I would like to say that, protecting personal data is an extremely important task in the modern world, where more and more information about us is stored digitally. Unauthorized access to this information can lead to serious consequences such as theft of personal funds, fraud, identity theft, etc. Additionally, compromising personal data can damage the reputation and trust in companies and organizations that store this data. Therefore, protecting personal data should be a top priority for anyone who works with digital information.