D. Bozhok, Student
N. Shkoliar, PhD in Ped., As. Prof., language advisor
Khmelnytsky National University

PROTECTION OF PERSONAL DATA ON THE INTERNET

The purpose of this study is to investigate the issue of personal data protection on the Internet. The Internet has changed our lives in many ways, and every day more and more people are becoming victims of cybercriminals who use the information they collect for their own benefit. In this regard, the protection of personal data is becoming an increasingly important topic that requires detailed study.

In today's digital world, protecting personal data is a very important issue for individuals, organizations, and governments. The Internet provides many services, but it can also be a possible place for identity theft. In this research, we will look at how you can protect your personal data online.

First of all, you need to understand what personal data is. This is any information that can be linked to an identified person. This can be a first name, last name, address, phone number, email, banking information, place of work, as well as any other information that can be associated with your identity.

Personal data need to be protected for many reasons among which there are the following:

1. Confidentiality: personal data may contain sensitive information about a person, such as name, address, phone number, email, financial data, medical information, etc. This data can be used by criminals for identity theft, fraud, or other crimes.
2. Financial security: attackers can use personal data to hack into bank accounts, credit cards, and to open new loans or obtain other financial services.
3. Medical security: personal medical data can be used to commit medical fraud, hack into medical record storage systems, or open additional medical records.
4. Business security: personal data of customers can be used by malicious actors to carry out cyber attacks on businesses, steal competitive information or other types of fraud.
5. Legal requirements: many countries have laws governing the collection, storage and use of personal data. These laws ensure that individuals have the right to protect their privacy and control the use of their personal data. Therefore, organizations must comply with these requirements to avoid fines or other legal consequences [1].

The right to privacy and protection of personal data is one of the fundamental rights under the United Nations Convention on the Rights of the Child (Article 16). This right applies equally to the digital environment.

According to Helen Nissenbaum, a professor of information technology at Cornell University, privacy is not a right to secrecy or control, but a right to the proper flow of personal information. It means that depending on the situation and context, a person can evaluate and decide what to share with others in the digital environment. In other words, a person has the right to know how and for what purposes their data is used, who stores it and for how long, and who has access to it. A person can also request the deletion of personal data or the correction of incorrect data [2].

When it comes to children, the question arises whether they are able to understand what personal information should not be shared with others, in what situations, and why. Although they are very concerned about what personal information will fall into the hands of their parents or friends, children do not understand why large corporations (such as Facebook, Instagram or Snapchat) are interested in such information. According to some studies, children take care of their privacy in their relationships with others, nevertheless, they share it publicly; that is, they are not aware of the misuse of personal data for commercial purposes and in an institutional context (e.g., at school, in a medical institution).

Due to the fact that they are not sufficiently aware of the risks, consequences, protections and rights related to the processing of personal data, children deserve special protection of privacy on the Internet (GDPR) [3].

Personal data on the Internet can be divided into three categories:

1. Active digital footprints – information (about themselves or others) that users leave when using the Internet, usually consciously, although not necessarily intentionally (for example, when buying certain goods, downloading content from the Internet, uploading photos, creating profiles on social networks).

2. Passive digital footprints – information that users leave on the Internet while using it, mostly unknowingly (e.g., through cookies, fingerprints, location data, use of smart things and smart toys).

3. Information obtained by analyzing the first two categories of data using algorithms (through the profiling process), possibly in combination with other data sources.

Among the most common types of threats to personal data on the Internet are the following:

1. Trolling is a type of interaction in online discussions when the interaction is aimed at provoking an emotional response, emotional reaction, emotional arguments, insults and long useless discussions, flaming, and escalating conflicts in readers to achieve the goals of the Internet troll.

2. Cyberbullying (online harassment) – most often involves repeated offensive messages directed at the victim (for example, hundreds of SMS messages to a mobile phone, constant calls) with an overload of personal communication channels. Unlike an altercation, attacks are longer and more one-sided. Attacks also occur in chats or forums (places of conversation on the Internet), and in online games, attacks are most often used by griefers – a group of players who aim not to win a particular game but to destroy the gaming experience of other participants.

3. Phishing – is an attempt to obtain confidential information, such as passwords or credit card numbers, by spoofing websites or emails. This can lead to the loss of financial assets or identification data. More than 90% of hacker attacks start with so-called "email phishing". This is a type of fraud that relies on the gullibility of Internet users who simply open infected emails and their attachments, often triggering the creation of malicious and dangerous programs on their computers.

4. Identity theft is the process of obtaining personal information for the purpose of using it for criminal purposes, such as opening new credit accounts or using other financial services.

5. Viruses and malware are programs that can use a user's personal information without their knowledge or consent, such as keyloggers and spyware.

6. Data breaches are cases where personal information falls into the hands of the wrong people due to data leakage from websites or services.

7. Social engineering is the process of manipulating users to obtain their personal information, for example, by collecting data through social networks or faking trusted contacts.

8. Spam is the excessive sending of unsolicited email that may contain malware or phishing attempts.

9. Unauthorized access is the process of illegally gaining access to personal information, for example, through hacked accounts.

10. Dissing is the transmission or publication of compromising information about a victim online. This is done with the intention of ruining the victim's reputation or damaging their relationships with other people.

11. Happy Slapping is filming videos in which aggressors beat or abuse the victim in order to post the video on the Internet. This type of violence has recently become widespread in Ukraine.

12. Frapping – gaining access to a person's account (hacking) on social media to post questionable content on their behalf, engage in dialogues or insult other users.

13. Catfishing – creating a copy of the victim's profile on social networks based on stolen photos and other personal data.

14. Cyberstalking is the act of covertly tracking the persecuted and those who move around idly, usually done quietly, anonymously, with the aim of organizing criminal acts such as attempted rape, physical violence, and beatings. By tracking unwary users on the Internet, the criminal receives information about the time, place and all the necessary conditions for a future attack.

One of the most important things a user can do to protect their personal data is to use a strong password and update it regularly. Passwords should be long, contain a variety of characters and numbers, and be unique for each website or service. Two-factor authentication to further protect an account can also be used.

However, in addition to using strong passwords and two-factor authentication, a user can also find many programs and browser extensions that can help keep their data safe. For example, a tracking blocker program preventing websites from tracking online activities can be installed. A browser extension that checks for unsafe sites when the Internet is browsed can also be useful. If there is a suspicion that the data have been compromised, the passwords should immediately be changed and the appropriate authorities should be notified of compromising the data.

For security reasons, software should be installed to protect a computer and mobile devices. Antivirus software and firewalls can help protect a device from malware and keep data safe.

Using open Wi-Fi networks, such as the ones in cafes or public places also calls for discretion. A good idea is to use your own secure Internet access or use a virtual private network (VPN) that encrypts your traffic and provides an extra layer of protection. Be careful when using social media and apps. Many of them collect a lot of information about you and your friends that can be used for advertising or even criminal purposes. Before allowing access to your information, you should read the Privacy Policy carefully and only share the information you need.

In addition, it is important to know what rights you have regarding the protection of personal data, especially under the General Data Protection Regulation (GDPR) and other laws. These rights include the right to access your data, the right to rectification, erasure, and portability, as well as the right to restrict processing and to complain. All of these measures help protect personal data online, but the most important thing is to be careful online. Confidential information should never be shared with strangers or questionable websites that may put your data at risk should never be visited.

It is also recommended that software and antiviruses should periodically be updated on a computer and mobile devices, which will help prevent attacks by intruders and keep data safe.

In general, the protection of personal data on the Internet is an extremely important topic in the modern world, as the growing number of digital devices and services we use increases the risks of losing and misusing our information. Therefore, it is necessary to comply with personal data protection measures and pay attention to them in order to maintain their confidentiality. Be careful and use data protection guidelines to maintain your privacy and security online.

REFERENCES

1.Techtarget-Resource access mode: https://www.techtarget.com/searchdatabackup/definition/data-protection.

2. U. Ustimovich. Large-scale data leak: hackers "leaked" almost 53 million records with personal information of Ukrainians. URL: https://thepage.ua/news/masshtabnaya-utechka-dannyh-hakery-slili-dannye-ukraincev.

3.digitalni - Mode of access to the resource: https://digitalni-vodic.ucpd.rs/en/personal-data-protection-and-privacy-on-the-internet/.