

DIGITAL FOOTPRINT: PRESENT AND FUTURE

Valevaty D.N., student

Ilyankou V.D., student

Scientific supervisor – Matusevich O.A., senior lecturer

English language department №1

Belarusian National University of Technology

Minsk, Republic of Belarus

Nowadays, a modern user leaves a digital footprint every day. Sometimes a modern person does not even know about its existence, and if people guess, they do not notice how they easily leave it on the global Internet. Currently with the development of modern information technologies, the digital footprint is becoming an increasingly important aspect of our lives. The first reputation about a person appears on the trail: according to their statements on the Internet, their photos, and so on.

In order to make it easier to understand what a “digital footprint” is, we will simply designate it. It is the data that the user leaves while applying the Internet. All this information is now collected and processed by Artificial Intelligence (AI).

Every time you use the device, do not forget about the digital footprint. Often, the person who left it may want to delete it- but this, unfortunately, will not work.

The digital footprint can be active and passive. The passive digital footprint includes your Internet Protocol (IP) address, cookies, and data from mobile apps. With this type of tracking, information is saved and enters the network without the user's knowledge.

An example of this is the location, the time when the users visited the site, what they were looking for on the Internet. The users themselves leave an active digital footprint on the global Internet by uploading videos to video services and social networks such as YouTube, VKontakte, Telegram and the like. Every day, the active digital footprint grows due to the transfer of videos, photos and other files that you can leave on the global Internet.

A fingerprint (Browser Fingerprint) is a unique identifier for the configurations of a web browser and an operating system, which is formed based on the collected data by various tracking technologies. You can

avoid data fingerprints thanks to Virtual Private Network (VPN) and proxy servers. There is an option to manually change the time on your device, the language of the search engine and many other options to avoid or reduce the number of browser fingerprints [1].

Where does it come from? Data is collected through clicks on links, likes, online purchases, banking applications, and browsing resources on the Internet. A person who uses the app to track their health (often in conjunction with special bracelets or watches) further expands their digital footprint. A special place should be given to cookies and data that the users themselves publish and leave on the Internet. Cookies are a tool that helps resources track user activity on websites. Moreover, you need to pay attention to trackers – this is a special program that collects data about the sites that you visit and then it helps the system to show the user personal ads.

The digital footprint has both positive and negative aspects. It should be noted that usually users leave information about themselves on social networks and other sites: surname name, father's name, date of birth, city, hobby, bank card number and so on. These data are actively exploited by scammers who use a variety of schemes to deceive, and subsequently use a person for their own purposes (money transfer, transmission of any data, and the like. Unfortunately, despite the fact that information work is actively carried out with the population, allegations of fraud by telephone or Internet scammers are regularly received.

The active consumers of this resource are, of course, advertising agencies and other representatives of the advertisement industry. Every click on the link, every like, every view is read and the advertiser shows exactly the advertisement that users will be interested in and with some probability will attract and force them to click on it. This opportunity provides more and more ways for “total surveillance”.

As Maxim Emm, an expert in the field of information security and technology, stated: “These technologies, if we talk about Facebook, will primarily be used to more accurately sell their ads” [2].

The protection of personal data is becoming an increasingly important task in the world of digital footprint.

As users, we must actively monitor our data and use privacy settings on various platforms to restrict access to our information. In addition, companies and organizations must strictly comply with the rules for maintaining the security and confidentiality of user data. Modern securi-

ty systems can only help us, but the last word remains with the human user. There are several methods to protect your digital footprints. The main thing in the security system is you should not leave any unnecessary information about yourselves on the global Internet [1].

It is worth taking a careful approach to choose a browser that you will later use for your tasks. It is not recommended to apply public Wi-Fi networks, even ordinary users can look at devices connected to a given point, and scammers can find out users' personal data, as well as redirect to fake social networking sites and other popular services or applications. It is worth logging in to the site using a username and password, but not authorization via social networks. You can reduce your digital footprint, but not delete it in any way. You must first delete all cookies that are stored on the device, because they store your passwords, your bank card data. It is also worth deleting the history of your search engine, since it is through it that scammers and other people can learn a lot, if not everything, from your state of health to your hobbies.

One rule should be remembered: “The less your data is stored on the Network, the lower the risk of theft”. You should remove inactive accounts from your online applications or services. Moreover, they also contain information about your bank cards, phone number, and some even have your residential address, place of work or study, and numerous other data.

We come to the conclusion: now the digital footprint is all around us and it is difficult, even impossible, to avoid. You should not be afraid to use the modern Internet, although you should be careful when clicking on the link. There are a lot of ways for you to protect yourselves, but the main thing is to remember about digital etiquette, to know and to follow it. If you comply with it, you will significantly reduce your digital footprint, scammers will not be able to apply any data, because you will not even leave them on the global Internet.

References

1. What Is Fingerprinting? [Electronic resource] – Mode of access: <https://ssd.eff.org/ru/module/what-fingerprinting>. – Date of access: 13.03.2024.
2. Future Projects of Artificial Intelligence for Info [Electronic resource] – Mode of access: <https://barokoks.github.io/future-projects-of-artificial-intelligence>. – Date of access: 24.02.2024.