Oksana Drozdova, Lubov Mashei
Science tutor *L. Bedritskaya*
BSEU (Minsk)

PASSWORDLESS AUTHENTICATION: ARE WE READY TO GIVE UP PASSWORDS?

Authentication is the process of verifying who a user claims to be. It goes without saying that password authentication was a great starting point, but now it's just a relic of the past and it's just not enough.

Apple, Google and Microsoft will provide support for a single passwordless authentication standard on their platforms already this year. Android and iOS mobile operating systems, Chrome, Edge and Safari browsers, Windows and mac OS will support the passwordless authorization protocol created by the FIDO Alliance [1].

To improve security, we need a better way to uniquely identify users. This is where biometrics come in. Passwordless authentication is a verification method in which a user gains access to a network, application, or system without a knowledge-based factor (such as a password, security question or PIN).

Below are the most common methods used for verifying:

1. Biometrics: Biometric authentication uses these unique physical traits to verify if a person is who they say they are, without requesting a password.
2. Magic Links: allow users to log into an account by clicking a link that's emailed to them, rather than typing in their username and password.
3. One-Time Passwords/Codes: is an automatically generated code sent to a known device owned by the user after they attempt to log in. They must enter the code, typically sent via text message or email.
4. Push Notifications: Users receive a push notification on their mobile devices through a dedicated authenticator app and open the app through it to verify their identity [2].

The following types of biometrics are known. The first type is behavioral biometrics. They are passive, because they do not require the user to interact with the system in a specific way to authenticate (e.g. click a button or typing). Next, there is physical biometrics, which verifies a user based on physical traits like their face shape, fingerprint, or retina by using technologies like Face ID, Touch ID, Windows Hello and so on. A person's fingerprint does not change over time, due to these reasons, as well as that fingerprint scanning does not cause discomfort in a person, this method has become the most common method of identification. The biometric identification systems are based on the analysis and comparison of the iris. It differs from the first one by its greater complexity in use, higher cost of equipment and strict registration conditions.

Why will passwordless authentication replace passwords? There are some reasons:

1. Users could sign in to applications and services faster.
2. There are no passwords to create, store, or remember.

According to the survey that was conducted among people at the age from 18 to 66, here are some confirming results: 13.5% of the questioned have never forgotten

passwords, 51.9% have changed passwords once or twice, 19.2% – 3-7 times, 15.4% – more than 7. The next question was about the password autosave function, which websites provide. 34.6% of the surveyed always use it, 48.1% answered that it depends on the site, 17.3% – never use it. Moreover, 71.2% of the surveyed use more than 8 symbols for passwords, 28.8% – less. This means that in addition to the daily information necessary for work and life, people need to keep in mind large passwords to various social networks. It leads to the fact that 21.2% of people write down the passwords, 17.3% – do it sometimes.

3. Gain a higher degree of trust and security as the biometric authentication occurs on the device, not the server, so there is no chance of your face or fingerprint data being stolen from a web server.

50% of the surveyed who use passwords have never been hacked, 42.3% – 1-2 times, 7.7% – more than twice. Nevertheless 23.1% of them always use different passwords for different social networks, 9.6% – 'always the same', 67.3% – 'sometimes the same'.

4. All new smartphones and most new laptops come with these new technologies built in, which makes it conducive to simple login flow.

5. A fairly high recognition accuracy.

6. Companies engaged in the development of fingerprint scanning devices are constantly improving their algorithms and have significantly succeeded in this.

7. Biometrics dramatically reduce IT support costs because no password management is required, an organization can save money by not investing in password management software tools or security training on how to best design and store a password. It is estimated that organizations can save roughly $1.9 million by going passwordless [3].

The last question of the survey was about willingness to give up passwords at all. 59.6% of those questioned are ready to try passwordless authentication, 36.5% – are satisfied with passwords, 3.8% – have never heard of it. It means that innovation will not be fully supported by the population of the Republic of Belarus. Moreover, due to political situation information technologies have begun to develop slowly and the passwordless authentication function is unlikely to be available in the coming years.

Passwordless authentication is certainly the future, where you do not need to be afraid of your data, you do not need to remember hundreds of passwords from all sites and applications, and spend time restoring them. It will take several years, but a considerable amount of money will be spent before it becomes a ubiquitous routine.

REFERENCES:

1. The Verge [Electronic resource]: The tech giants want to roll out FIDO passkey technology in the coming year. – Mode of access: https://www.theverge.com/2022/5/5/23057646/apple-google-microsoft-passwordless-sign-in-fido. – Date of access: 13.03.2023.

2. Auth0 [Electronic resource]: What Is Passwordless Authentication? – Mode of access: https://auth0.com/blog/what-is-passwordless-authentication/. – Date of access: 13.03.2023.

3. Strongdm [Electronic resource]: What Is Passwordless Authentication? (How It Works and More). – Mode of access: https://www.strongdm.com/blog/passwordless-authentication. – Date of access: 13.03.2023.

Julia Elsukova
Science tutor *L. Vasilevskaya*
BSEU (Minsk)

THE DIGITAL DIVIDE: CAUSES AND WAYS OUT

The use of the Internet has a high degree of analysis of the life of society in the XXI century. However, there is a problem of citizens' access to state information and communication technologies. The purpose of this paper is to analyze causes and consequences of the digital divide and suggest ways to overcome it.

An international report [1] presents the results of measuring digital development in the world. The analysis of the report data [1; 2] shows that each region, each country has different levels of digital inequality in the use of digital infrastructures, Internet services. The problem of digital inequality is more typical of countries with transitional economies and, in particular, of certain segments of the population: the poor, rural residents, the elderly and people with disabilities. For example, in Scandinavian countries more than 90% of the population has access to the Internet, while in African countries this figure fluctuates around 30%. The digital divide at the national level is determined by the number of Internet users in urban and rural areas. According to the population census in the Republic of Belarus, the difference between the shares of urban Internet users and rural Internet users is 16.3% [3].

The conducted analysis of the relevant literature has revealed the main causes of the digital divide: the lack of motivation to use the Internet, the high cost of computer equipment and connection to the global network, and the lack of ICT skills among the population. Factors of digital inequality can also include the level of education, income, and race.

The causes and factors of the digital divide affect socio-economic development and have the following *consequences*:

1. Households with high levels of education are more likely to use computers and the Internet. People with higher education are 10 times more likely to have access to the Internet in the workplace than those with only a high school education [4]. In direct correlation with the level of education is the level of household income, which also plays a significant role in increasing the digital divide.
2. Information and communication technologies are more accessible to highly developed countries, which increases their investment attractiveness. Countries with low levels of economic development become less attractive for outside investment, further exacerbating the digital divide.