Beznosiuk I.V., Ilyenko S.S., Ilyenko A.V.

National Aviation University

MODERN PRINCIPLES AND SOLUTIONS FOR PASSWORD MANAGEMENT IN INFORMATION NETWORKS

INTRODUCTION. It is no secret that the Internet and digital technologies are becoming an integral part of our lives. Today, everything from shopping to training, from prescribing to verifying identity documents, takes place in mobile applications or in a web browser. This has led to an increase in the number of users of electronic resources and, as a result, an increase in the number of logins and passwords required for memorization. Many people use very weak passwords to make them easier to remember and repeat them on different websites. Very often you may encounter a situation where the password contains various associative data: date of birth, personal data, street name, nickname of the pet, and so on. The **purpose** of this paper is to analyze and consider the practical bases, modern principles and solutions for password management in information networks.

Let's take a look at the top 10 password management principles.

1. Create a hard, long passphrase. Strong passwords make it much more difficult for hackers to break into systems. Strong passwords are more than eight characters long and consist of upper- and lower-case letters, numbers, and symbols.

The US National Institute of Standards and Technology (NIST) recommends creating long passwords that are easy to remember and difficult to crack.

2. Apply password encryption. Encryption provides additional protection for passwords, even if they are stolen by cybercriminals. Your best bet is to consider end-to-end encryption, which is irreversible. This way, you can protect passwords as they are transmitted over the network.

3. Implement two-factor authentication. Two-factor authentication has quickly become the standard for managing access to company resources. In addition to traditional credentials such as username and password, users must verify their identity with a one-time code sent to their mobile device or with a personalized USB token. The idea is that

with two-factor (or multi-factor) authentication, simply guessing or cracking the password is not enough for an attacker to gain access to the system.

4. Add additional authentication methods. Use additional methods that are not password-based. For example, as part of multi-factor authentication, users can use biometric verification - for example, sign in to an iPhone with a fingerprint with Touch ID, or authenticate on a Windows 10 PC using Windows Hello facial recognition.

5. Check your password. Make sure your password is strong by testing it with an online testing tool. The Microsoft Security and Protection Center has a password testing tool that can help you create passwords that are less likely to be cracked.

6. Use different passwords for each account. Otherwise, if one account is hacked, other accounts with the same credentials can be easily compromised

7. Protect your cell phone. Mobile phones are now commonly used for doing business, in-store payment and more, but this causes many security concerns. Protect your phone and other mobile devices from hackers by providing your device with a strong password, using fingerprint or face recognition.

8. Avoid writing passwords. Avoid storing passwords in digital form or on paper, as this information can be stolen by attackers.

9. Be vigilant. No matter how complex your passwords are and how careful you are about security, passwords are not safe if spyware tracks what you type on your keyboard. Make it harder for cybercriminals as soon as possible with modern anti-malware and vulnerability management solutions to harden your systems to prevent and mitigate weaknesses that could allow attackers to enter and / or roam your environment.

10. Use password managers. When using a password manager, you only need to remember one password, as the password manager stores and even generates passwords for different accounts, automatically logging in if necessary.

There are a lot of standard software products for organizing safe password recovery. Dashlane, Onesafe, LastPass and other password managers, which may provide a handy functionality for saving money. True, they often do not care about the rules of safety of special tributes. Anyone who finds themselves near a monitor with an open program will be able to see the user's passwords.

The main prompts of the most popular password managers are now visible.

• **LastPass** allows you to synchronize passwords between different attachments;

• **1Password** can integrate with the popular Pwned Passwords service. The Danish password manager can notify the function of those who have entered the password before being hacked by hackers;

• **Dashlane** is a rich platform password manager, and you can restore access to your saved passwords on any mobile attachment at any hour;

• **KeePass** can be viewed from one of their password managers, but they have not stored their confidential data in a dark store, and can display a response code.

• **RoboForm** can not only take all passwords in good hands, but also steal your passwords from phishing attacks;

• **Sticky Password** allows you to copy data from old forms and provide the ability to manage additional passwords.

CONCLUSION. Password managers not only store your passwords, they help you generate and store strong and unique passwords when you sign up for new websites. This means that when accessing a website or application, you can open your password manager, copy the password, paste it into the authorization field, and gain access. Password managers often contain browser extensions that automatically substitute passwords for you.

References:

1. Andrew C. C. Why You Need a Password Manager. Yes, You. [Electronic source] / Cunningham Clifton Andrew // Wirecutter. – 2019. – Resource access mode: https://www.nytimes.com/wirecutter/blog/why-you-need-a-password-manager-yes-you/.

2. Derek A. S. Top 15 Password Management Best Practices. [Electronic source] / Derek A. Smith // Virginia – 2019. – Resource access mode: http://web-control.ru/novosti/news_post/top-15-printsipov-upravleniya-parolyami.

3. D. Akhawe, A. Barth, P. E. Lam, J. Mitchell, and D. Song. Towards a formal foundation of web security. In Proceedings of the 23rd IEEE Computer Security Foundations Symposium, 2010.