GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ)
ISSN (E): 2347-6915
Vol. 12, Issue 5 May (2024)

PASSWORD SECURITY IN INFORMATION TECHNOLOGY

Mullajonov Baxodirjon Arabboyevich
Researcher Journalism and Mass Communication University of Uzbekistan

ABSTRACT

This scientific article analyzes the importance, risks, and effective methods of protecting passwords in information technology. Passwords are a crucial part of information security, used by users to protect their accounts. The article discusses methods to enhance password security and ways to improve password systems in the future. As computer technologies rapidly evolve, the need for security is becoming increasingly important. As computer networks grow, so do the number of threats from these networks. Therefore, we must protect ourselves from the threats that come with technology.

Keywords: Password security, information technology, cybersecurity, authentication, password manager, two-factor authentication, information security, password, computer viruses.

INTRODUCTION

As information technology permeates all areas of our lives, protecting personal and corporate data has become a pressing issue. Passwords are a fundamental element of information security. They are used to authenticate users and protect their information from unauthorized access. Despite this, there are risks such as password theft, cracking, or guessing. This article examines important aspects of password security and methods to enhance it.

The internet has enabled attackers to operate from anywhere on the planet. Risks arising from poor security practices and knowledge include:

- Identity theft;
- Money theft;
- Unauthorized access to legal privileges;
- Sanctions and criminal liability if rules are not followed.[8,376]

One of the most important areas of information security is password security and reliability. According to researchers at Boston University, it is possible to choose passwords that are both difficult to crack and easy to remember. To ensure your password is strong and not easily cracked by malware, pay attention to the following when creating passwords:

- Include both alphabetic characters and numbers;
- Use special characters such as @ # $ % ^ & *, but avoid spaces as some systems do not recognize them;
- Try creating words from letters, symbols, and numbers. For example, the word “445zamat” can be written as a3@//\at;
- Intentionally misspell words or write them phonetically. For example, “falokat” can be written as “palakat”;
- Use words that do not make sense together, such as “coldpen”;
- Replace letters or numbers with symbols, and vice versa. For example, b@)(0№a (which represents “baxona”).

Choosing a password can be challenging for many people. It should be difficult for others yet easy for the user to remember.[7,275]

One of the key principles in password security is not using the same password across multiple systems. Many people make this mistake, which means if your password is cracked on one network, your security on other systems is also compromised.[6,57]

There are many malicious programs designed to crack passwords, and they are widely available. Any developer can create such programs, which attempt to guess your password by repeatedly trying different combinations. These programs can crack passwords in the following number of attempts:

- If the password consists of an English word from the Latin alphabet – approximately 600,000 attempts;
- If the password consists only of numbers – 100,000,000 attempts;
- If the password consists only of lowercase letters – 208,827,064,576 attempts;
- If the password consists of both uppercase and lowercase letters – 53,459,728,531,456 attempts;[1,123]
- If the password consists of numbers, letters, and symbols – 1,853,020,188,851,840 attempts.[2,76]

The length of the password also matters in establishing good security. For example:

- An 8-character password with letters, numbers, and symbols can be cracked in 645 trillion combinations;
- A 9-character password with letters, numbers, and symbols can be cracked in 45 quadrillion combinations;
- A 10-character password with letters, numbers, and symbols can be cracked in 3 quintillion combinations.[5,124]

When using passwords, it is important to choose them as securely as possible. One should take data security seriously and avoid using simple passwords.

Globally, it is believed that the more complex the password, the higher its security. However, people often use simple passwords for ease of memory. Using numbers and punctuation marks in passwords increases their security. Some password-cracking programs use dictionary words, so it is recommended that passwords consist of 12 or more characters including numbers and symbols.

To make passwords even more reliable, they should be changed every two to three months. At the very least, passwords for three main accounts – bank, email, and social networks – should be changed regularly, especially if they are used for authorization on other systems.[4,90]

Key Aspects of Password Security:

1. **Creating and Storing Passwords:**

- Passwords should be at least 12 characters long and include letters, numbers, and special characters.
- Users are advised to change their passwords regularly.
- Passwords should never be disclosed to others or stored in plain text.

2. **Password Managers:**
   - Password managers help users create and securely store strong and unique passwords.
   - These applications store passwords in an encrypted form and reduce the number of passwords that users need to remember.
3. **Two-Factor Authentication (2FA):**
   - Two-factor authentication systems add an extra layer of security by requiring a second form of verification.
   - 2FA systems use a password along with an additional code or biometric data.[3,17]

Modern Threats to Password Security:

1. **Brute Force Attacks:**
   - This method systematically tries all possible passwords.
   - Strong passwords and 2FA effectively protect against such attacks.
2. **Phishing Attacks:**
   - Phishing attempts to trick users into revealing their passwords.
   - Users should be cautious when entering their information and learn to recognize phishing attempts.
3. **Password Reuse:**
   - Using the same password across multiple accounts is dangerous because one compromised account can jeopardize others.
   - Password managers can help create and manage unique passwords for each account.

Recommendations for Enhancing Password Security:

1. **Creating Strong and Unique Passwords:**
   - It's essential to create unique and strong passwords for each account.
   - Using a password manager can simplify this process.
2. **Enabling Two-Factor Authentication:**
   - Activating 2FA on all critical accounts is recommended.
   - This adds an additional layer of security and protects accounts in case of password compromise.
3. **Regularly Changing Passwords:**
   - Regularly changing passwords helps maintain account security.
   - If an account is suspected to be compromised, the password should be changed immediately.

Password security is of paramount importance in information technology, crucial for protecting users and their data. Using strong passwords and modern authentication methods is essential. In the future, improving password systems and developing new security measures will play a significant role in ensuring information security. Users must be cautious, use strong and unique passwords, and implement two-factor authentication. Additionally, using password managers and regularly changing passwords will further enhance cybersecurity.

REFERENCES

1. Anderson, R. (2020). “Security Engineering: A Guide to Building Dependable Distributed Systems.” Wiley.
2. Bishop, M. (2019). “Introduction to Computer Security.” Addison-Wesley.
3. Blocki, J., Blum, M., & Datta, A. (2014). “Human computable passwords,” CoRR, vol. abs/1404.0024.
4. Garfinkel, S., & Spafford, G. (2019). “Practical Unix and Internet Security.” O'Reilly Media.
5. Goodin, D. (2021). “The Art of Deception: Controlling the Human Element of Security.” Wiley.
6. KeePassXC Password Manager. Retrieved August 2, 2021, from https://keepassxc.org.
7. Kurbanov, Sultanboy. (2022). Methods and models of surface formation in the process of three-dimensional modeling. Asian Journal of Research in Social Sciences and Humanities, 12, 272-280. 10.5958/2249
8. Raximov, Sh. (2023). Teaching the Subject of Computer Graphics and Design Using the SWOT Analysis Method, Education News: Research in the 21st Century, 1(10), 375-377.