5 common password-setting errors should be avoided

Usually, we tend to create simple and memorable passwords for our accounts so that we can quickly log in. But it is the easy-going that causes many accounts to be stolen.

Creating a simple password or writing it down are the most common mistakes users make. Here are the 5 most common mistakes that users make when talking about passwords.

1. Use one password for multiple accounts

Usually, people create passwords that are easy to remember, which means they are short and simple, although most services today have a minimum requirement for the length and types of characters to have.

Once we have an account and password, and then sign up for another service, we often don't want to remember more of the password, so we reuse the remembered password. This is a common mistake for many people.

According to a survey by Google, 52% of respondents use one password for multiple accounts, of which 13% use one password for all accounts.

The most serious problem with password reuse is that it makes you vulnerable to attack with other accounts when one is exposed.

2. Create a simple password

People who like simplicity in password generation lead the group being 'hacked'. Many hackers attempt to 'hack' an account simply by guessing login credentials.

NordPass's annual published list of more than 500 million passwords shows that simple passwords such as 12345, 123456, 12345678 and 123456789 rank among the most popular.

In addition to simple forms, a similar mistake many people make is to include personal information in passwords, such as spouse names, children, pets, date of birth . in passwords.

3. Save text passwords

Another mistake is writing down the password. This happens with forms like writing them down, taking notes, saving them to spreadsheets or document documents .

If you really want to write it down due to fear of forgetting, they should be words to help you remember and should be kept in a safe place. In the case of on-device storage, you may face many risks. If hackers attack your device and rummage it, they'll gain access to the accounts with minimal effort.

4. Share passwords

According to a statistic, 43% of respondents admitted having shared passwords with others. These include passwords for streaming services, email accounts, social media accounts, and even online shopping accounts.

Forms of sharing passwords include entering your password on someone else's computer, sending it to others via email or through a text messaging app .

Although the majority of people who share passwords say they share with those they are close to, it still puts the security of the account dangerously low.

5. Periodically change passwords

Some organizations force users to change their password every 2 or 3 months for security reasons. But changing your password frequently without proof of password breach doesn't make your account any more secure.

Studies show that when people are forced to change their passwords frequently, they don't think much about creating new passwords. This makes the user create a simple predictable password, for example increase / decrease a number, change a letter to a symbol, add or remove a special character, or switch the order of letters. numbers or special characters in passwords… Research has also shown that, once an attacker knows a password, they can guess the next password without much effort.

In short, creating a strong and consistent password may seem like a daunting task for many people, but there are ways to make it easier for you. As mentioned, creating an unpredictable passphrase is always better than a simple one and adding an extra layer of security by enabling 2FA (2-step verification) if available should be essential. If you find it difficult to remember all passwords, then the password manager is the answer, that way you only need to remember one password, but make sure it's one that is compliant. follow good advice.