How to choose a password

Many Internet users are tolerant to choose a password for social networking or e-mail accounts, although this is a gross tolerance that can expose them to the risk of hacking due to the ease of guessing these words and numbers.

It is therefore necessary to make the community aware of the need to choose complicated passwords (or secret numbers) in terms of emphasis on the method used in their composition, unpredictability and guessing through random password creation software.

The following are the most important methods and ideas agreed upon by most information security professionals to create strong and safe passwords.

Method 1:

Create any combination of your choice so that it is easy to remember and choose the first character of each word and try to apply the five steps as in the following example:

YOU HAVE TO BE SMART, THE EASY DAYS ARE OVER

1. First letters of each word: YHTBSTEDRO

2- Replace (TO) with 2: YH2BSTEDRO

Replace letter (O) with zero: YH2BSTEDR0

4. Change letters from being capital letters to small letters: yh2BSTEDr0

5. Add special symbols: & yh2BST_EDr0

If the password is: & yh2BST_EDr0

And it is possible to use it in any account consider using it with an abbreviation of the account name after the mark & as a reminder or any other user-preferred format as per the following example:

  – Use with e-mail e.g. Hotmail: ht&yh2BST_EDr0

- Or use with social networking like Twitter consider a change of position of short form: &yh2BST_TEDr0 &tw

The same steps are applied with the rest of the accounts in the manner that the user considers appropriate to avoid forgetting the password.

Method 2:

Choose any two or more unrelated words and create a password:

1 - Merge the words with one another taking into account the change of some characters.

2 - Add symbols and numbers to the words.

Example:

Book & bike

The password would be like this:

bo@0k+BiKe

Knowing that this method is not as strong as the previous method.

What do you do if your password is stolen?

Be sure to monitor all information you protect with passwords such as monthly financial statements, credit reports, online shopping accounts, and more. Powerful and secure passwords can help protect you from fraud and identity theft however, there are no guarantees. No matter how strong your password is if anyone hacks the system where it is store, they can get the password. If you notice any suspicious activity indicating that someone has accessed your information, notify the responsible authorities as soon as possible. Get more information about what to do if you think your identity has been stolen or involved in fraud in a similar way.

In conclusion, here is a set of tips in the field of information security:

1 - Avoid the choice of words that are easy and frequent even if written in a different language because the hacker can easily penetrate this type of

words and secret numbers using software made specifically to serve this end.

2 - Avoid publishing your personal data such as (date of birth or phone number ...) on social networking sites (Facebook - Twitter ...) and beware of using them to choose your password.

3. Avoid electronic penetration. The password must not be less than ten digits provided that it contains numbers, letters and symbols such as ~' ! $#@%&^-_[+={]}..

4 - Avoid repeating letters, numbers and symbols in the password and avoid keeping them in the computer or mobile phone.

5 - Try as much as possible to change your secret numbers monthly, especially in bank accounts and every five months for other accounts.

6. Treat your passwords and traffic phrases with the same care you give to the information you protect.

7. Do not disclose the password to others.