Creating a Strong Password

What is a password?

- In the simplest terms, a password is a secret word or phrase that is used to gain admission to a place or service.
- A password is information associated with an entity that confirms the entity's identity.
- Although there are several ways of attacking password-protected systems, using a strong password can protect against such attacks.

Why do we need passwords?

–Passwords are used for *authentication*
•Authentication is the act of linking oneself to their electronic identity within the system to which they are connecting.

–The system uses your password to verify that you are the legitimate owner of the user/account identifier
•This is commonly referred to as "login"

Think for a while about your PINs, passwords, and password quotes which you use in your day-to-day life. You use them when using ATMs to withdraw money, to access your computer, to log in to your email, to log in to your social media websites, and many more. You might think it is a hassle to remember all your passwords. You might even care very little about getting attacked? Attackers have the potential not just to get access to your account(s), but to also do irreparable damage by using your personal data. Providing access only to relevant parties will help you to secure your data and information by way of authentication. The best way to do this is to use a strong password.

How do you select a strong password?

Most people are used to creating passwords that are easy for them to remember. This includes words that they are very familiar with, their own birthdays etc. These methods are among the worst when picking a password, as an attacker can easily guess your selected password(s). It is better to avoid using passwords that you (and anyone else) can remember easily.

Ways of attacking passwords

There are different types of password attacks.

Dictionary attacks
• A dictionary attack is defined as "The guessing (often automated) of a password by repeated trial and error." You can avoid such an attack by using passwords with random letters and intentional misspellings.

Social engineering attacks
•A social engineering attack can be defined as "The process of using social skills to convince people to reveal access credentials or other valuable information to the attacker."

While social engineering attacks are more modern and precise than dictionary attacks, they can be avoided by using the Internet in a safe manner. This includes not sharing your sensitive information (Passwords, PINs etc.) over the Internet.

Some tips to create a strong password

- The best way to create a password is to use a word or a word phrase and making a trick or mnemonic device to remember it.
  E.g. [W]adiya [k]adana [n]araka [l]ami [h]ema [n]owe [a]pi can be converted to WkN1hn@
- Mixing uppercase and lowercase (capital and simple) letters
- Use of special characters (,.”?!@$%^&*) to complement alphanumeric characters (a-z, 0-9)
- Use a password with as little real life meaning as possible
- Use a long password (minimum of 8 characters)
- Use different passwords for different accounts
- Use an extra layer security or enable this feature when possible and where available – This is called two factor verification (Sites such as Gmail and Facebook and most secure online banking systems allow or even require this)

How do you protect your password?

It is your duty to choose a strong password and protect it. Do not reveal your password to others, and do not make it easily accessible. This includes writing your passwords in pieces of paper and leaving them near your computer. Such carelessness will make it easy for attackers to gain access to your personal details. Do not tell your passwords to anyone else without good cause and be aware of those trying to get your passwords over the phone and via emails, SMS etc.
Always ask your ISP to give you an advanced authentication method without giving simple access methods. Try to use encryption protocols such as Kerberos or Public key Encryption.

Most computer programs, especially web browsers, facilitate the option of remembering your passwords. This option should be used sparingly and only on computers that are not publicly shared, such as one in a library or an Internet café or your office computer. You also need to make sure that you have logged out of all services (social media, e-banking etc.) properly before you leave the public computer system.

Remember that it is always your duty to protect yourself when using the Internet.

Your password is like your house key… So treat it as such….

If you have any questions, please inform us:

https://techcert.lk/en/report-form
Tel - +94 11 4 462 562
e-mail - help@techcert.lk

This document was prepared by the Training Division of LK Domain Registry in collaboration with the Internet Society Sri Lanka Chapter.
For more details please visit http://nic.lk/index.php/training-materials.