How to Use Facebook in a Secure Way

Facebook is one of the most popular social media websites in the world. Social media is a mechanism of building, creating, and maintaining inter-personal relationships or connections via the Internet.

Users of social media websites typically share photos, videos, and information about their day-to-day activities. According to the latest statistics, Facebook has over 300 million users, which amounts to an aggregate usage of more than 6 billion minutes per day.

Recent research has shown the following reasons for Facebook's popularity in today's cyber-environment.

- Users can potentially upload an unlimited number of photos and videos to their accounts, and can share them with friends
- Users can update themselves about their friends' shared statuses every minute.
- Users can play internet games with their friends
- Users have the ability to send E-gifts to friends

Like every other technology, Facebook has some limitations and issues with personal security and privacy. The main issues concern personal threats/attacks done online owing to a lack of privacy. The numbers of targeted personal attacks on Facebook has been on the incline over the past few years, and is currently considered a significant threat to all Facebook users in their online and personal lives.

Social media effectively makes your information available to everyone with access to the Internet. This will include information about you, your daily activities, your friends, your whereabouts, and where you have visited. This can pose a threat to you and your friends. It may even harm your life.

Listed below are a few ways of using social media websites such as Facebook in a secure manner. It is recommended that you use these methods as a way of circumventing issues of privacy and security.

1. Use https://www.facebook.com to login to your Facebook account. You will be protected from password thieves owing to information being encrypted.
2. Use SMS authentication method (Two factor authentication: you will receive a short code via SMS before login to your account)
3. Do not put highly personal details on public display on Facebook (especially your address, date of birth, contact no, etc.). You can change/edit the "privacy settings" as you wish and limit the availability.
4. Change/edit your privacy settings to send a notification to your email when you log in to your Facebook account.
5. Before you add new friends, ensure that you know them personally, and that they cannot access your data before you add them.
6. Double checks the web address before you enter your details to the website. Many phishing websites may spoof the web address of a social media website to gain user

information. If a user clicks on a phishing email they think was sent by a trusted site, there is a high probability of viruses and other malware being downloaded to the computer automatically, thereby causing damage. Some attackers use phishing techniques to gain personal information from users and try to log in to their accounts using information thus gathered.

You can check the digital certificate of a website to check whether the website is the intended one or another. E.g. – https://www.facebook.com

7. Think twice before you add your friends. It is always better to confirm by phone or email if they have actually sent you a request.
8. Facebook allows you to chat with your friends. Do not chat with people you do not know. Do not share your information via chat with others. If you are suspicious of someone, ensure that you block them as soon as possible.
9. It is a good idea to choose strong passwords for your online accounts, especially in the case of social media websites. Do not use the same password for all accounts. Use different passwords for different accounts. (E.g. Facebook, Yahoo!, Gmail, etc.)
10. Use a trusted device/computer to log in to your account, as public computers or computers belonging to unknown parties may have software such as key loggers that record your data and information without your permission.
11. Do not share your password with others.

Social media websites are a great source of entertainment, and complement relationships with your real life friends. If you are not careful to use it in a secure manner, it has the potential to cause you and your friends a great deal of trouble. It is therefore better to use it wisely as guided by TechCERT in order to minimise your online threats.

If you need any assistance regarding a security incident on Facebook (or social media), please report the said incident in the link below. We will do our level best to support you with this matter.

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.