Hacking of Facebook Accounts - Are you a victim...?

Facebook has become a favourite meeting place for people to keep in touch with friends on-line. As a result, millions of people (both young and old) are on Facebook, so much so that if you are not on Facebook it’s like you don’t belong to the modern tech-savvy society!

In recent times however Facebook has also become a favourite hunting ground for internet hackers resulting in people with malicious intent searching for their victims within the Facebook network.

The net result is that Facebook related crimes are on the increase. Identity theft is the most common crime on Facebook. This is where hackers create a fake profile after stealing your information from the internet and pretend to be you.

Hackers use a number of different techniques to make money out of Facebook using stolen information. The following is an actual scenario that happened recently to an unsuspecting Facebook user;

Sugath is a teenager and an ardent fan of Facebook. One day when he logged in to his Facebook account he noticed that there was a “friend” request from an attractive girl by the name of Kavindra who had a set of nice photos on her profile. Sugath did exactly what any teenager would do and accepted the invitation.

He then got a chat request from Kavindra. Sugath was exited and was blind to the obvious and started chatting. At some point during the chat Kavindra wanted to have a video chat and sent a link (or URL), for Sugath to click and start the video chat. Eager to see the attractive Kavindra ‘live’ on screen, Sugath proceeded to login using the link sent by this unknown female. The link took Sugath to his Gmail account login page. He tried to login to the site with his Gmail username and password and got an error message, asking him to try again. He immediately conveyed this to Kavindra. She said that there seems to be an issue and concluded the chat session promising a video chat at a later date. Sugath was exited and was dreaming of chatting with her again.

But when Sugath woke up the next morning he realized that he was in big trouble, when he could not login to either his Facebook account or his Gmail account. He was horrified when he realized that the last time he used his Gmail credentials on-line was to access the Video Chat URL with Kavindra. It dawned on him very quickly that he had been duped by the attractive Kavindra. He soon received a call from a Facebook friend to say that there was a post saying “if you want your account password contact Naveen via Skype” in his Facebook wall. When Sugath contacted that person over Skype he demanded money in exchange for his password and that the payment should be made on-line …. And it was a substantial amount of money!

Did this all happen due to his negligence or ignorance, or simply because he was naïve?

The fact of the matter is that millions of Facebook users are vulnerable and can be easily duped into disclosing vital information. Hackers who pose as pretty girls or handsome men on Facebook are earning big money by hacking into E-mail accounts and Facebook accounts and holding the owners of these accounts to ransom.

This appears to be an organized group of hackers acting in collusion and willing to carry out criminal activity for financial gain. Indications are that these cyber criminals are on the increase, so beware and be alert. Here are some tips;

How to be secure on Facebook?

- Don't accept a "friend" request unless you are certain of his / her identity.
- Don't get influenced by the attractive photos or messages sent along with the request.
- Don't click on any links provided by unknown people.
- Don't give any of your E-mail or Facebook account credentials ie. User Name, Password to anyone else.
- Stay within your "friend" list and don't make any private information public in Facebook

For more details on how to use E-mail and Facebook securely visit the SLCERT website www.slcert.gov.lk

If your account is compromised…

If your Facebook account is compromised you can seek assistance from SLCERT. We are here to protect the Sri Lankan Cyberspace from Cyber Criminals.

Kanishka Yapa
Information Security Engineer
Sri Lanka Computer Emergency Response Team (SLCERT)

**** All names used in the above example have been altered to protect the identities of the actual parties involved*

About SLCERT

Formed in 2006, the Sri Lanka Computer Emergency Response Team (SLCERT), a fully owned subsidiary of the ICT Agency of Sri Lanka, is a semi-government entity mandated with the protection of Information and Information Systems within the state sector, while extending its services to the private sector and general public. Its services range from responding to and investigating information security breaches, to preventing security breaches by way of awareness creation, security assessments and security capability building. It is a full member and the national point of contact, for both the Asia Pacific Computer Emergency Response Team (APCERT) and the Forum of Incident Response Security Teams (FIRST), which are regional and global associations, respectively, formed to coordinate security efforts between nations. Learn more at www.slcert.gov.lk