Don't be a victim of SMS Phone scam

Today, SMS is an integral part of communication – which includes news alerts, personnel notifications, etc. Recently hackers have added SMS to their growing arsenal. SMS contains a message congratulating you on winning a lottery and provide a call back number and/or a website link.

The following is an actual incident that was reported to SLCERT.

Sugath is a mobile user who mainly communicates through SMS. He has news alert, face functionality enabled on his cell phone. One day he received a SMS with the following message:

"Congratulations!! You just won the US National Lottery worth US $3 Million. Please contact the number provide or visit the web page to collect your winning amount"

In the SMS a contact number and a website URL was included. Sugath decides to call the lottery department and clarify the information using the contact number provided in the SMS. The call is answered by a human voice from the other end. She asked Sugath for the following information:

- *Contact details (Name, Address, Telephone Numbers, etc.)*
- *Bank Details (Which account the money should debited)*
- *Internet Bank ID*
- *Personnel Identification Numbers (PIN)*

Finally Sugath was asked to deposit $200 to an off-shore bank account, for processing and document chargers.

After deciding to deposit the money to the foreign account Sugath realized that he can not reach the contact using the number provided in the SMS.

It is important that users are aware of such text messages. Though the content of the SMS might defer the intent and the procedures are the same by most of the hackers.

Your can avoid from those type of scams by following these instructions:

1. Ignore any notifications of win in a lottery specially if you have not purchased such lottery
2. Do not give your bank account details to anyone
3. Do not take any instructions from strangers regarding bank account matters such as change user ID /PIN
4. Do not make any advanced payments to claim any price money
5. Do not respond to such messages, e-mails or calls
6. Be wary of get-rich-quick offers. They are probably scams.

More information is available on the SL CERT website – www.slcert.gov.lk.

**** 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