SLCERT Lead Info. Security Engineer Charuka Damunupola

'BANKING SECTOR NEEDS MORE ROBUST KYC PROCESS'

● SLCERT Lead Info. Security Engineer Charuka Damunupola emphasises need for banking sector to improve combating financial scams via stringent 'know your customer' processes/procedures/checks to prevent unauthorised account creation

BY BUDDHIKA SAMARAWEERA

Online financial scams have become an ever-present threat in the digital world, with fraudsters using increasingly sophisticated tactics to exploit unsuspecting individuals and businesses. From phishing electronic mails and text messages to fraudulent websites that mimic legitimate platforms including those of government institutions, these scams aim to steal sensitive financial information or money. As technology advances, scammers find new ways to deceive people, making it vital for everyone to be aware of common warning signs and learn how to protect themselves.

Sri Lanka Computer Emergency Readiness Team (SLCERT) Lead Information Security Engineer Charuka Damunupola discussed some important matters pertaining to online financial scams, in an interview with *The Daily Morning*.

Following are excerpts from the interview:

How can online financial fraud be defined?

An online financial scam can be defined as a fraudulent activity conducted through Internet connected devices or digital platforms with the intent to deceive and financially exploit individuals or organisations. It encompasses a range of deceptive practices aimed at gaining unauthorised access to financial information including bank account details, misappropriating funds, or tricking people into transferring money or providing sensitive financial details.

What are the forms of such fraud?

Online financial fraud can take several forms, with phishing being one of the most prevalent. Phishing involves sending deceptive messages, often via email or text, containing links that direct one to a fake website designed to look like a legitimate site. This fraudulent site may ask for sensitive personal information such as their National Identity Card (NIC) number, date of birth, address, phone number, and sometimes even the usernames and passwords of their digital accounts. By collecting this information, fraudsters can gain unauthorised access to their bank accounts and carry out financial crimes. Another common form of online financial fraud involves impersonation, where scammers pretend to be from reputable organisations like banks or telecommunication companies to extract personal information. These scams can occur through phone calls or other digital communications. In some cases, scammers use the gathered information to use bank accounts of other persons online, allowing them to conduct unauthorised transactions or withdrawals.

Have you identified an age group or other specific group of people who regularly fall victim to such scams?

Reports and complaints received by us show that people from various age groups and backgrounds can fall victim to online financial scams. From schoolchildren and university students to professionals like doctors, anyone can be targeted. Scammers often tailor their tactics to specific demographics, such as offering online job opportunities to students or pitching investment schemes to professionals.

Can online financial scams not appear to be scams at first?

Yes, financial scams can involve sophisticated tactics that exploit people's vulnerabilities or create panic to manipulate them. For example, individuals seeking jobs abroad might be targeted by scammers posing as recruiters or job placement agencies, asking for fees or personal information under the pretence of facilitating employment. Similarly, they (scammers) might lure those in financial distress with offers such as quick loans, only to demand upfront payments or personal details. Scammers may also use fear based tactics, such as claiming that nude photos of a person have been leaked online, to convince them to provide them (scammers) with their social media account related details. These approaches are particularly insidious because they prey on a person's emotional state, making it challenging to detect the fraudulent intent initially.

Do scammers usually approach victims with an understanding of them, or randomly approach individuals?

Scammers often use both random and targeted approaches to commit online financial scams. In a common random approach, they send out scam related messages or links to thousands of people, typically through email, text, or social media platforms. The hope is that even a small percentage of recipients will fall victim to the scam, making it profitable for the scammers. On the other hand, targeted scams are more focused and tailored to specific groups or individuals. For example, scammers might target professionals with investment schemes.

> *Currently, fraudsters have been able to open accounts under other persons' names, using such accounts to facilitate financial scams. This makes it difficult to trace the real individuals involved in such scams*

What is the relationship between pyramid schemes and online financial scams?

Pyramid schemes have been around for many years, but, with the rise of digital platforms, they have become more prevalent and easier to execute. Online platforms allow scammers to reach a broader audience and create sophisticated schemes that appear legitimate at first glance. Some pyramid schemes are presented as applications or online services, promising users with quick returns on investment. Pyramid schemes that involve crypto currencies are particularly notable for their online reach and high level of sophistication. These schemes often promise short-term benefits to attract participants and build confidence, but ultimately, they lead to large-scale financial scams when the scheme collapses. The rapid growth and sudden fall of these schemes can result in significant financial losses for those involved.

Are online payment platforms operating in Sri Lanka secure enough?

Currently, legitimate payment platforms are secure. The Central Bank of Sri Lanka (CBSL) has prepared a series of guidelines with regard to platforms such as mobile applications used for financial purposes. Such platforms should be implemented in accordance with those guidelines. A security audit is also done before releasing such an application. Therefore, they have sufficient security in the current situation.

What changes are needed in Sri Lanka's banking sector to prevent online financial scams?

One significant area for improvement in our banking sector to combat financial scams is the 'know your customer (KYC)' process. Currently, fraudsters have been able to open accounts under other persons' names, using such accounts to facilitate financial scams. This makes it difficult to trace the real individuals involved in such scams. To address this issue, banking institutions need to implement a more robust KYC process. This can help ensure that the person opening a bank account is properly identified and verified. Improved KYC procedures would involve stricter checks on personal identification documents, biometric verification, and enhanced due diligence for new customers. By strengthening the system for collecting and verifying personal information during the account opening process, banks can reduce the risk of unauthorised account creation and make it easier to track and investigate financial scams.

What does the SLCERT do, besides informing people, to prevent online financial scams?

In addition to raising public awareness about financial scams, we forward the complaints that we receive to the Computer Crimes Division of the Criminal Investigations Department (CID). We collaborate with the CID to provide them with the necessary evidence and information to aid in their investigations. Furthermore, we work closely with banks and other financial institutions to implement preventive measures and enhance security practices to reduce the occurrence of such scams.

Are the current legal provisions sufficient to combat online financial scams?

While there are quite sufficient legal provisions to address online financial scams, we sometimes encounter technical challenges. Often, financial scams are orchestrated from abroad, requiring cross border cooperation and information sharing with foreign authorities for investigations. In some cases, the existing legal framework might not be enough to tackle these complex internationally occurring scams. As a result, navigating the legal processes to obtain information from other countries can be challenging and time consuming.

How is the SLCERT's relationship with the CBSL and other private and public banks?

We offer technical support to the CBSL to ensure that guidelines pertaining to matters such as the maintenance of applications used for financial transactions are robust. Additionally, we have a dedicated team within our organisation focused on providing technical assistance for financial scam cases. This team interacts with various banks and financial institutions to facilitate investigations and share relevant information. Sometimes, banks and financial institutions are reluctant to disclose details when their customers become victims of financial scams, fearing reputational damage. In these situations, our team works closely with such institutions to ensure that appropriate measures are taken to address the fraud while maintaining confidentiality.

Are financial scams occurring through online marketing and e-commerce platforms?

It is the Consumer Affairs Authority (CAA) that looks into such issues, allowing consumers to file complaints about fraud or other forms of unfair practices on online platforms. This avenue enables customers to report instances where they have been deceived or experienced unethical conduct while shopping online.

> *Improved KYC procedures would involve stricter checks on personal ID documents, biometric verification & enhanced due diligence for new customers*

What evidence is required in online financial scam-related cases?

A variety of evidence can be crucial for investigations. This includes account details where funds, if any, have been transferred, phone call recordings that capture suspicious conversations, links to fraudulent websites, and text or email messages used in the scam. Each of these pieces of evidence would help the authorities trace the origin of the scam and identify those responsible.

Have the security of government agencies' websites been evaluated, and are they secure?

We have developed a set of guidelines to ensure the security of government agency websites, and they have been shared with the relevant institutions. Furthermore, we have provided information security and cyber security policies to these agencies to help safeguard their websites against fraud and cyber attacks. The Government agencies also prepare annual reports detailing the security measures in place for their websites. Our services are not limited to government agencies; private institutions can also reach out to us.