PROTECT YOURSELF FROM FINANCIAL CRIME

Crypto fraud

It is important to be aware that scammers are actively promoting unauthorized cryptocurrency investment schemes through compromised or hacked social media profiles. In some cases, false notifications may appear to be from SDB, referring to crypto investment credit. We want to make it clear that SDB does not support or endorse such transactions, in compliance with the restrictions imposed by the Central Bank of Sri Lanka on crypto investments.

Scams

Scammers might send you SMS messages from unknown phone numbers, often about packages being delivered to your address. Do not share your personal information, account or card details, or one-time passwords (OTP) with someone you don't know. Avoid opening any links sent by SMS, email, or through website pop-ups.

Stay vigilant against malware-related fraud

There is a rise in malware-related payment fraud cases observed internationally. Malware, phishing, and ransomware are becoming increasingly common forms of attacks and can affect individuals. Malware is any software used to gain unauthorized access to mobile devices and computers to steal sensitive data, disrupt system service or manipulate information.

Bank safely

During these challenging times, fraudsters may exploit the situation for personal financial gain. Stay vigilant and avoid falling prey to scams. As the festive season approaches, remember to stay alert when using SDB Debit cards / UPay for online purchases and digital payments. Protect your financial and personal information by enhancing your awareness of fraud.

Tips for transacting safely online:

Are you confident in the safety of your online purchases? While online shopping offers convenience, price comparisons, and savings, its popularity has also increased risks, such as scams and card detail theft. Fortunately, by adhering to a few straightforward rules, you can enjoy a safe and secure online shopping experience.

Keeping you safe from possible Phishing, Vishing and Smishing attacks

A scam

A scam is a fraudulent scheme or deceptive practice aimed at taking money or goods from unsuspecting individuals. Scams exploit trust to steal personal information or money, often using sophisticated tactics and elaborate lies. With the rise of online connectivity, online scams have become more common. It's essential to stay vigilant and cautious when interacting online to protect yourself from falling victim to scams.

Phishing

Phishing is a cybercrime where individuals receive fraudulent communications, such as emails, calls, or texts, from imposters posing as legitimate organizations. The goal is to trick targets into revealing sensitive information like personal details, banking information, card numbers, or passwords. This stolen information is used to gain unauthorized access to accounts, resulting in identity theft and financial harm to the victims. To stay safe from phishing attacks, it's crucial to verify the authenticity of requests for personal information and exercise caution when sharing sensitive details online.

Here are important points to remember to protect yourself from scams:

- Never provide your PIN or password verbally, in writing or through email.
- Do not download any software or allow remote access to your computer unless you initiated the contact and are certain of the legitimacy.
- Be cautious of requests to transfer money into another account, even if claimed to be for safety reasons.
- Avoid withdrawing or depositing money based on unsolicited requests.
- Do not hand over cash, PINs, cards, or cheque books to anyone visiting your home unexpectedly or without proper identification.

If you suspect a scam or fraud:

If you suspect fraud on your account, debit card, or online banking, or if you think your credentials have been compromised, you may be a victim of cybercrime. Please contact us immediately on our 24-hour Customer Service Hotline at **+94 11 5 411 411** or visit the nearest SDB branch for assistance.