ශ්‍රී ලංකා මහ බැංකුව
இலங்கை மத்திய வங்கி
CENTRAL BANK OF SRI LANKA

මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதற் பிரிவு
FINANCIAL INTELLIGENCE UNIT

අංක 30, ජනාධිපති මාවත, කොළඹ 01, ශ්‍රී ලංකාව
இல. 30, சனாதிபதி மாவத்தை, கொழும்பு - 01, இலங்கை
No. 30, Janadhipathi Mawatha, Colombo 01, Sri Lanka

Ref: 37/09/0010/0002/024

October 01, 2024

To: Compliance Officers of Financial Institutions

Dear Compliance Officer,

Red Flag Indicators – No. 04 of 2024
Red Flag Indicators to Combat Website Spoofing Scams

Please find the attached Red Flag Indicators, No. 04 of 2024 relating to the recently reported Website Spoofing Scams.

Yours faithfully,

Director
Financial Intelligence Unit

☎ 011-2477125
011-2477509
011-2477692
011-2477708
flu@cbsl.lk
dflu@cbsl.lk
www.flusrilanka.gov.lk

Red Flag Indicators for Financial Institutions to Combat Website Spoofing Scams

The Financial Intelligence Unit (FIU) has observed an alarming rise in sophisticated website spoofing scams targeting Financial Institutions (FIs), particularly banks, in Sri Lanka.

Modus Operandi of scammers:

Scammers are replicating legitimate banking websites with near-identical URLs, tricking customers into entering sensitive information such as login credentials and OTPs. These fraudulent websites often appear credible, exploiting minor differences in web addresses and convincing phishing tactics. Subsequently, the scammers send out text messages, claiming that an individual won a prize or entered into a draw, or fill up a survey and ask them to log into the financial institutions' online portal. The unsuspecting victim clicks the link, goes to the fake website, and enters their login details. Once the scammers have these credentials, they can access the victim's real bank account. The fake site will also ask for the OTP (one-time password) that the victim receives from the bank, deceiving the victim into handing over full access to his/her account.

Despite ongoing awareness campaigns, many individuals still fall victim to these schemes, resulting in significant financial losses. In response, the following best practices (this list is not exhaustive) are provided for FIs to detect and prevent these scams, to protect both institutions and its customers from fraud.

1. **Monitor and Detect Website Spoofing:**

- Implement systems to regularly scan the web for fake websites mimicking the institution's domain. Immediate action should be taken to report to relevant authorities and shut down fraudulent sites.
- Use domain monitoring tools to alert your cybersecurity team about any newly registered domains similar to your institution's.
- Ensure the official website and online portals are secured with HTTPS and display clear indicators like security certificates and lock icons.

- Conduct frequent audits of institutions' website security to ensure it's resistant to common attacks.
- Proactively monitor web traffic to online banking services, identify anomalies based on access to IP addresses, port numbers, and, where possible, device details and take appropriate measures to scrutinize users connecting from with unusual traffic, VPNs, foreign IPs to local accounts and etc.

2. **Enhance Multi-Factor Authentication:**

- Ensure OTPs or any multi-factor authentication measures are not easily retrievable by unauthorized parties.
- Introduce additional layers of verification, such as biometric authentication, when significant transfers or logins from new devices are detected.

3. **Strengthen Customer Communication:**

- Send periodic reminders to customers to carefully verify the URL of the institution's website before logging in.
- Educate customers that the institution would not request sensitive information, such as passwords or OTPs, via SMS, email, or unsolicited phone calls. Customer should ensure any call received by them for such information is actually from the institution prior to revealing sensitive information.
- Encourage customers to report suspicious messages, emails, or links that they encounter, providing a hotline or email specifically for fraud reporting.

4. **SMS/Email Alert Mechanism:**

- Set up real-time SMS or email alerts for all types of transactions and encourage customers to enable these services to immediately detect unauthorized activity.
- Automatically alert users if there are multiple failed login attempts or attempts from unusual locations.

5. **Raise Awareness and Responses about Phishing Tactics:**

- Regularly conduct phishing simulations and education campaigns for both employees and customers to help them recognize phishing attempts.
- Encourage customers to avoid clicking links in unsolicited SMS or email messages and to manually type the institution's URL into the browser.
- Release public notices and press releases when instances of scams are detected, especially those targeting your institution. Share examples of recent tactics scammers use, emphasizing verification procedures.
- Train customer service teams to quickly escalate cases involving suspected spoofing or scam attempts.
- Build up interactive taskforces among sector institutions to maintain vigilance and interaction and to share relevant information to maintain awareness.