FINANCIAL INTELLIGENCE UNIT OF THE BAHAMAS

PUBLIC ADVISORY

No. 2 of 2025 23 September 2025

PROTECTING YOURSELF FROM SMISHING AND PHISHING SCAMS

The Financial Intelligence Unit (FIU) of The Bahamas is issuing this urgent public advisory to inform you about the increasing prevalence of Smishing and Phishing scams targeting individuals within our community. These deceptive tactics are employed by criminals to steal your sensitive personal and financial information, potentially leading to significant financial loss and identity theft. It is crucial that you understand these threats and take proactive steps to protect yourselves.

Understanding Smishing and Phishing:

- **Phishing** refers to fraudulent attempts to acquire your confidential details (such as usernames, passwords, bank account numbers, credit card information, and national identification numbers) through deceptive electronic communications. These often take the form of emails, fraudulent websites that mimic legitimate ones, or misleading phone calls. Scammers frequently impersonate trusted entities, including financial institutions, government agencies, utility companies, or well-known businesses, to manipulate you into divulging sensitive data.

- **Smishing** is a similar scam that utilizes SMS (Short Message Service) or text messages sent to your mobile phones. These messages often contain alarming or urgent content designed to provoke an immediate response. They may instruct you to click on a malicious link, call a fraudulent phone number, or provide confidential information via text message.

Common Tactics Employed by Scammers:

1. **Impersonating Legitimate Organizations:** They meticulously mimic the branding, logos, and language of trusted entities to appear authentic. Be aware that even official-looking communications can be fraudulent.

2. **Direct Requests for Sensitive Information:** A key red flag is any unsolicited communication asking for your passwords, PINs, full account numbers, or other confidential details. Legitimate organizations will never request this type of information through unsolicited emails, texts, or phone calls.

3. **Use of Malicious Links and Attachments:** Phishing emails and Smishing texts often contain links that redirect you to fake websites designed to steal your login credentials or install malicious software (malware) on your device. Attachments may also contain malware.

4. **Threats and Demands for Payment:** Scammers may threaten you with negative consequences, such as service termination or legal action, if you do not provide information or make immediate payments.

5. **Creating a Sense of Urgency or Fear:** Scammers often fabricate scenarios that suggest an immediate threat to your finances or personal security, such as unauthorized transactions, account lockouts, or legal repercussions if you fail to act swiftly.
6. **Enticing Offers and Regards:** They may lure you with promises of prizes, refunds, or special offers to trick you into revealing your personal or financial details.

Critical Steps to Protect Yourself:

1. **Exercise Extreme Caution with Unsolicited Communications:** Be highly suspicious of any unexpected emails, text messages, or phone calls requesting your personal or financial information, regardless of how legitimate they may appear. The FIU, financial institutions, government agencies, and other reputable organizations will never ask for your sensitive details through unsolicited means.

2. **Independently Verify the Sender's Identity:** If you receive a communication claiming to be from a reputable organization, do not click or respond directly. Instead, independently verify the communication through official channels:

    - **For your bank:** Contact them directly using their official website or phone number that you have independently verified.
    - **For government agencies:** Visit their official website or call their publicly listed contact number.
    - **Do not** use the contact information provided in the suspicious communication!

3. **Never Click on Suspicious Links or Download Attachments:** Avoid clicking on links or opening attachments in emails or text messages from unknown or unverified senders. If you accidentally click a link, do not enter any personal information on the subsequent website.

4. **Be Wary of Urgent or Threatening Language:** Scammers use urgent language to pressure you into acting without thinking. Take your time to assess the situation and never feel compelled to provide information immediately.

5. **Protect Your Personal Information Diligently:** Be extremely cautious about sharing your personal details online and over the phone. Only provide sensitive information through secure methods that you have directly accessed and verified.

6. **Password Protection:** Employ strong, unique passwords for all your online accounts and enable multifactor authentication (MFA) whenever available. MFA adds an extra layer of security by requiring a second verification step beyond your password.

7. **Keep Your Devices and Software Updated:** Ensure your computer, mobile phone, and all software, including antivirus and anti-malware programs, are up to date to protect against known vulnerabilities.

8. **Report Suspicious Activity Immediately:** If you receive a suspicious email, text message, or phone call, or if you believe you may have been a victim of a scam, report it immediately to your financial institution and the Royal Bahamas Police Force, Financial Crimes Investigation Branch at 356-6019, 356-6025, or 502-9991.

The FIU is committed to safeguarding the financial system and protecting the public from financial crime. By remaining vigilant and adhering to these protective measures, you can significantly reduce your vulnerability to Smishing and Phishing scams. Please share this advisory with your family, friends, and colleagues to help raise awareness across The Bahamas.

Stay informed and stay protected.

Mr. Emrick K. Seymour Sr., CM, KPM
Director
Financial Intelligence Unit
Poinciana House, 31B
Annex Building, 2nd Floor
East Bay Street
P.O. Box SB-50086
Nassau, Bahamas
Tele: (242) 397-6300/ (242) 326-3815
Fax: (242) 322-5551
Email: director.fiu@fiubahamas.bs