ROYAL ST. VINCENT AND THE GRENADINES POLICE FORCE
PUBLIC RELATIONS AND COMPLAINTS DEPARTMENT
P.O. Box 835
Kingstown
Tel: (1-784) 485-6891 or (1-784) 485-6697 or (1-784) 457-1211 Fax: (1-784) 456-2816
E-mail:relations.complaints@gmail.com

Your reference **December 02, 2024**

PRESS RELEASE

WhatsApp Phishing Scam Alert

December 02, 2024 - Kingstown: The Royal St. Vincent and the Grenadines Police Force (RSVGPF) wishes to alert the general public of a 'phishing' scam currently ongoing on social media. It has been brought to the attention of law enforcement that the WhatsApp accounts of several persons have been compromised. In some cases, hackers claim victims have won a sum of money and request personal information such as names, addresses, and bank account numbers to facilitate a transfer. In other instances, victims are instructed to send money via "Zelle."

According to Google, "Zelle" is "a fast and easy way to send and receive money with friends, family, and others you trust, even if they bank somewhere different than you. All you need is your recipient's email address or U.S. mobile phone number, and money will be sent directly from your account to theirs in minutes. No account numbers are shared."

This phishing scam is just one of many techniques cybercriminals use to steal personal information and commit fraud. Such malicious tactics, including social engineering, malware, and impersonation, are designed to exploit unsuspecting users. The RSVGPF, therefore, strongly urges the public to remain vigilant and exercise caution when using social media applications.

To reduce the risk of falling victim to these scams, the following measures are advised:

1. Avoid providing personal information such as your name, passwords, or account details to anyone who does not have a legitimate need for it.
2. Use strong, unique passwords to secure your devices, emails, and social media accounts.
3. Report any suspicious activities immediately to law enforcement or your service provider.

4. If you have doubts about the identity of the person you are communicating with, ask them a question that only the two of you would know and assess their response. If their answer raises further suspicion, or you are unsure, stop communicating with the person altogether.

5. Exercise caution when clicking links, even if they are sent by someone you know, as this could compromise your device and allow sensitive information to be stolen through potential exploits. Always verify the source and intent of the link before clicking.

Let us work together to protect ourselves and our loved ones from these malicious activities.

Have a safe and incident-free Yuletide Season.

-END-