**Cyber Security Incident Response Team**
Ministry of ICT,
St. George's
Grenada

**Email**: csirtgnd@gov.gd
**Website:** www.csirt.gov.gd
**Facebook**: facebook.com/csirtgnd
**Twitter & Instagram**: @csirtgnd
**WhatsApp number**: 1(473) **423-2478**

# PRESS RELEASE

## CSIRT Gnd Alert – Increased Phishing Attacks on Social Media Profiles and Pages

**January 16, 2024** – The Grenada National Cyber Security Incident Response Team (CSIRT Gnd) is concerned about the increase in phishing attacks leveled against WhatsApp and Facebook social media accounts and pages belonging to Grenadians. In addition to the old phishing tricks, we are now seeing more malicious sponsored posts and an increase in fake lookalike profiles specifically designed for our people. We are also deeply troubled by the number of reported cases of compromised accounts resulting from users falling victim to these attacks.

CSIRT-Gnd wishes to remind the public of the following:

1. Do not accept friend requests on social media without first verifying the requestor.
2. Do not accept friend requests just because someone you know has done so.
3. Always check and ensure that a message is coming from the entity it purports to be coming from before responding to it or clicking any link(s) therein.
4. You should never share any code you receive with anyone unless you are prepared to give up control of your account or device to whoever is asking you to share it with them.

Grenadians are also called to be on the lookout for deepfake content which seeks to dupe them into either sharing their personal information with bad-actors, visiting malicious websites, or investing in get-rich-schemes that will result in them losing their money.

Admittedly, being safe online requires some effort on the part of Internet users, but this pales in comparison to the amount of effort needed to recover a compromised account or recuperate money sent to scammers. The following are four (4) things one can do to improve their level of security and online safety:

1. Ensure that strong passwords or passphrases are used, and that proper password hygiene is practiced.
2. Enable two-factor authentication once the option is available.
3. Properly assess ALL links and attachments before clicking on them or downloading them.
4. Keep your device and software up to date. Updates should be installed as soon as they are made available.

Anyone needing assistance verifying content or offers found online, or for general online safety information and advice can reach out to the National Cyber Security Incident Response Team on WhatsApp and Telegram on (473) 423-2478; via email at csirtgnd@gov.gd; or on Facebook, Instagram and X at @csirtgnd.