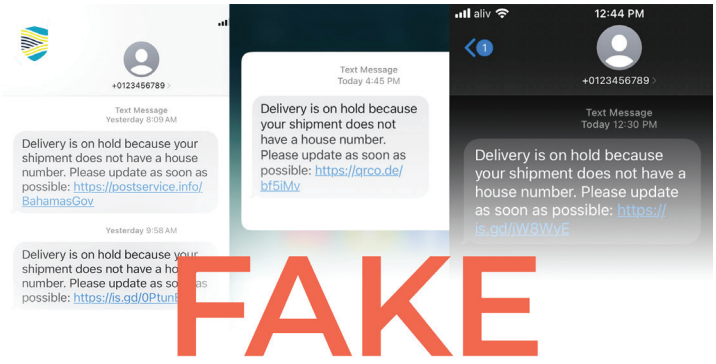
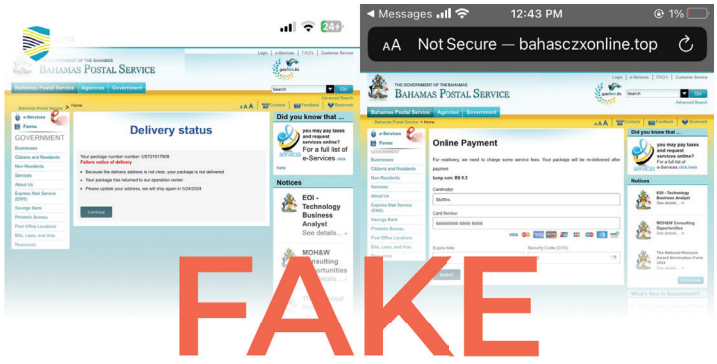
FOR IMMEDIATE RELEASE

CIRT-BS OBSERVES UPTICK IN PARCEL DELIVERY "SMISHING" SCAMS IMPACTING MEMBERS OF THE GENERAL PUBLIC

New Providence, The Bahamas—The National Computer Incident Response Team of The Bahamas (CIRT-BS) is observing an uptick in parcel delivery scams involving threat actors impersonating Bahamas Postal Services' (BPS) website to solicit payment and personal identifiable information from members of the general public.





Reported screenshots of smishing text messages from malicious actors containing spoofed URLs and strange hyperlinks

Spoofed version of Bahamas Postal Services' website soliciting payment information.

In the attacks, actors are sending SMS messages from the telephone number "+0123456789" advising recipients that their "delivery" is on hold and requesting they visit a malicious webpage that spoofs BPS' website. Once on the webpage, the user receives a prompt to enter payment information.

CIRT-BS wishes to advise the public that these attacks are fraudulent and that SMS messages are not a standard means of communication for BPS. In a statement of clarity, Postmaster General Jennifer Johnson advised, "In the event a package or registered item is received by the post, a notice card is placed in the addressee's postal box and/or a phone call is made (if a number is recorded on package), informing the customer to come to the post office, with the proper official ID."

Should you find yourself on the receiving end of a "smishing" attempt, CIRT-BS recommends the following actions:

1. **Verify communication.** If you believe you are receiving an SMS message update about a legitimate delivery, contact your shipping company through its official means of communication.
2. **Do not click on links.** If you receive an SMS message about a delay for an unexpected delivery asking you to click a link, do not click the link (especially if the hyperlink is unclear), and block the number.
3. **Go to the source.** If you ordered an item around the time you received a delivery update SMS message, go to the website where

you placed your order and review the tracking updates there.

4. **Report.** Remain vigilant, especially when making payments, and report "smishing" attempts to **https://www.cirt.bs/report**/. If you have become a victim of a smishing attack, follow the appropriate steps to notify your financial institution, query suspicious transactions, cancel the compromised bank card, and request a new one.

CIRT-BS is a component of the Government of The Bahamas' Digital Transformation to Strengthen Competitiveness project, financed by the Inter-American Development Bank (IDB) in 2019. This project falls under the Ministry of Economic Affairs' Digital Transformation Unit. For additional information on CIRT-BS or to report an incident, please visit **www.cirt.bs**. Connect with CIRT-BS on social media using the handle, **cirt_bs**.

For media inquiries, please contact **press@cirt.gov.bs**.

27 May 2024
National Computer Incident Response Team of The Bahamas (CIRT-BS)
Commonwealth of The Bahamas