2nd November 2022

Dear Client:

RE: FRAUDULENT EMAIL

We are aware of a fraudulent email sent to RF clients. As such, we are providing you with notice concerning the incident and the tools to help you protect your login credentials.

What happened?

An email that appeared to come from Tanya Johnson, RF Associate, was sent on November 2nd, 2022 with the subject, "Incoming Document from RF Bank & Trust (Bahamas) Ltd." The content redirects to https : // rfgroup . rfgroupclient . us /. This URL does not originate from RF.

The purpose of the malicious email is to gain access to recipients Microsoft password by prompting you to enter your Microsoft login credentials.

What we are doing

Our Information Technology team is performing its appropriate system checks and has identified all clients who have received the fraudulent email.

What you can do

To protect yourself from the possibility of malware that may impact your devices, we recommend that you do not open the email, enter your login details or click on any links associated with the email. We encourage you to always practice caution when you receive an email prompting you to provide personal information, including login details.

If you did click the email, we suggest changing your Microsoft password immediately.

For more information

If there is anything else we can do to assist you, please contact David Van Onselen or Cleora Farquharson via 242 603 6000 or david.vanonselen@rfgroup.com/ cleora.farquharson@rfgroup.com