

You may be receiving some emails that appear as though they emanated from Skye Bank.

They may contain the names of some of our management staff or even our Directors. Some of them may require you to send in information on your Bank details, Pin codes and even your personal information as contained in our database of you. They might also claim to have access to large sums of (\$)US dollars for you domiciled with us, these are scam mails and you should be very careful to avoid being a victim to fraudsters.

At Skye Bank, we are concerned about these trends by fraudsters and hackers and their attempt to infiltrate customers' details or accounts with us. As part of our confidentiality and security clause, as well as our commitment to online security, we want to ensure that our customers have the privilege of their financial security while on our website and as such have developed some security tips for all our customers to recognize when they receive emails or letters from potential fraudsters.

Read the tips below to ensure you are receiving a genuine Skye Bank communication.

- 1. Skye Bank would never ask you to disclose your account number or Pin code on the internet**
- 2. Skye Bank would never ask you to disclose personal information on the internet.**
- 3. Skye Bank site would always carry a security certificate which would be visible on access to our site.**

The official Skye Bank web address remains [www.skyebankng.com](http://www.skyebankng.com) . Be sure that the site you are on is a genuine Skye Bank site.

If you are still in doubt, please get in touch with your nearest branch or call us on (000 234 1) 8531655, 8948103, 07028390633-5