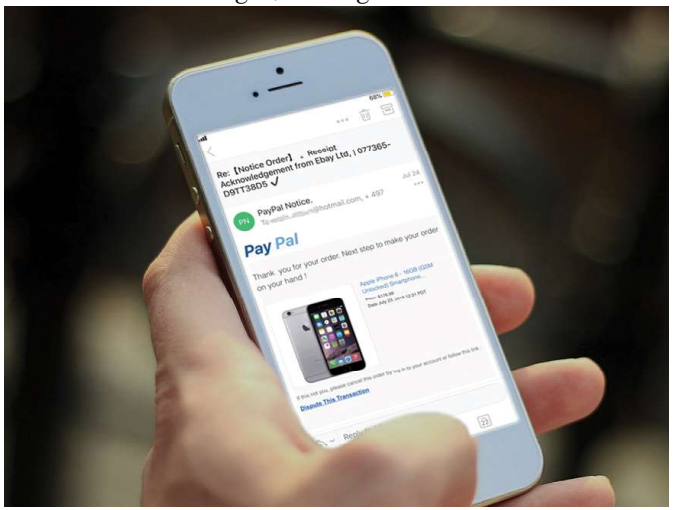
Do not take the bait: Watch out for phishing attacks.

BE SMART - DON'T BE A SCAM VICTIM!

Shopping online, receiving your monthly bank statement, communicating with colleagues or clients at work – email is still one of the most widely used methods. Additionally, people have become dependent on smartphones, and social networking platforms, like Facebook, Twitter, and others, to stay in touch with friends and families

Unfortunately, cyber-criminals are also using the same means of communication to try and defraud people. One of such scams is where fraudsters are fooling people into taking an action, such as clicking on a malicious link, sharing their confidential information, or even to open an infected email attachment - commonly known as phishing.

Criminals usually send out mass messages, hoping that many will take the bait, and be easily tricked into revealing their personal information such as passwords, credit card, social security or bank account details. Aside of emails, such scams are increasingly taking various forms including phone calls, SMS or social media messages, among others.



Very often, fraudsters are coming up with convincing messages that tap the emotional triggers of potential victims. For example, you may receive an email or call from someone pretending to be a representative of your bank, claiming there is a problem with your account, and asking for your details so they can keep your account safe. Such details are used by scammers to steal your hard-earned money.

Phishing is also a means of targeting high-profile individuals or organisation, with the aim of stealing valuable or sensitive information. Criminals may even send what is called 'spoofing emails' or create 'spoofing websites' forging the email, logo and details of a well-known company, so that it appears legitimate. Spoofing emails usually come with malicious attachments, which if clicked on will allow cyber-criminals to gain access to your device and system, and ultimately your valuable information, which they can use to conduct their criminal activities.

Some useful tips to avoid getting hooked by phishing scams:

- Do not respond to calls, text or emails from unknown sources
- Be suspicious of messages with generic salutations like 'Dear Customer'
- Be suspicious of calls, messages or emails with a sense of urgency, prompting you to take an action before something bad happens
- Remember that big companies including your bank, will never ask for your personal details over the phone or email
- If the message claims to originate from a friend or your bank, but it sounds suspicious, call that friend or your bank to verify
- Do not click on link, attachments received from unsolicited emails

If you think you have been targeted by a phishing scam you can also seek advice from:

The Central Bank of Seychelles on:	The Financial Intelligence Unit on:
4282000	4383406/4383407
enquiries@cbs.sc	enquiries@gov.sc

Be on the lookout for more information about how to spot a scam.

Always remember: If it sounds too good to be true, it probably is!