# Protect Yourself from the SmSh

SmShing is a term used to describe phishing SmS/text messages (SmS phishing). Cyber criminals use mobile phone text messages to lure victims into calling back a fraudulent phone number, visiting fraudulent websites or downloading malicious content via mobile phone.

Always critically assess any email or text that seems suspicious. Cyber criminals will try to create a sense of urgency to get you to react in a panicked state. Stop and take the time to think the message through, then decide what response is appropriate.
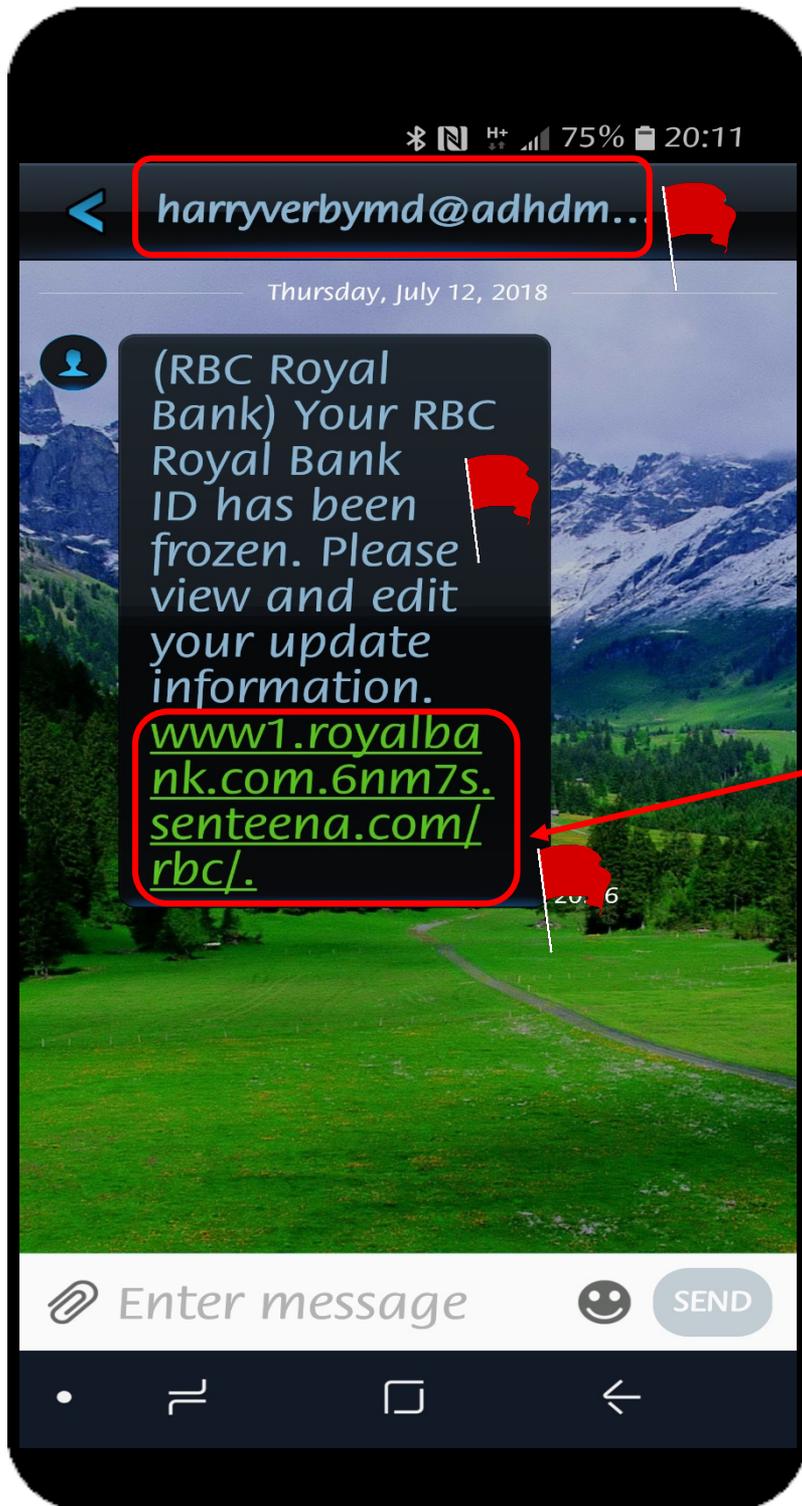
Ask yourself, do I recognize the sender? Does the message appear to be from a company I do business with?

Do not reply to SMS/text messages from numbers that you don't recognize.

Is this the way the company would normally contact me?

Don't share your login, personal or financial details over SmS. Legitimate companies will never ask for sensitive information via text message.

Is the link a valid url? Does the url seem authentic?

www1.royalbank.com.**6nm7s.senteena.com/rbc**

Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain.

Be cautious where you input two-factor authentication codes.

Legitimate companies may **send** you an authentication code via SmS when you're signing in to a secured website. Cyber criminals could send you fake SMS messages **asking** for this code.

Do not call any phone number attached to the SmS/text message.

If in doubt, validate the sender using verifiable, alternate means.

Do not click on links in suspicious SmS/text messages.

If necessary, open the link in your mobile browser and navigate directly to the website in question – without clicking on the link. But even if you do not complete the phish, cyber criminals can still gain incremental bits of useful information.

If you inadvertently click on a link in a SmSh or if you suspect a text message is a SmShing attempt, contact the OPP Service Desk at 1-888-677-4873 option 9.