BIZCOMMUNITY

Be wary of 'Coronamania' cybercrimes

By Mark Rose

17 Jul 2020

During the Covid-19 pandemic, which has turned the world upside down, banking clients should exercise extreme caution when dealing with financial transactions online. Recent statistics estimate cybercrime to cost South Africa more than R2,2bn per annum.

Clients must be cautious about falling prey to spammers ready to prey on unsuspecting people as the search for speedy updates on Covid-19 is being used surreptitiously to lure one onto websites that could trap one into sharing one's personal details.

Cybercrimes include phishing attacks, spreading malicious software (malware), and stealing login credentials and credit card details. Warnings, in particular about opening documents purporting to be from the World Health Organisation (WHO) or a similar supposedly trusted source, have been doing the rounds.

Key industry player, the South African Banking Risk Information Centre (SABRIC), has already issued a warning to bank clients that cybercriminals are exploiting the spread of coronavirus for their own gain using 'Coronamania' panic to spread coronavirus scams.

According to SABRIC, these new scams include spoofed emails offering products such as masks, or fake offerings of vaccines, leading to phishing websites. These emails come from seemingly realistic and reputable companies, which manipulate people into clicking on links. Some of these websites prompt the user for personal information, which ends up in the hands of cybercriminals.

Cybercriminals are also using SMS phishing, more commonly known as SMishing, to trick victims into clicking on a link disguised as information on a coronavirus breakout in their area to steal their credentials. Some of these texts claim to provide free masks or pretend to be companies that have experienced delays in deliveries due to the coronavirus.

Once criminals have the correct level of confidential information about a victim's bank account, they can impersonate the victim and transact using the correct credentials but without authority.

Here are some safety guidelines:

- Avoid opening emails and text messages from unknown sources or visiting untrusted websites. Do not click on links or icons in unsolicited emails or SMSs, and never reply to these emails or SMSs. Delete them immediately.

- Do not blindly accept the content of unsolicited emails or SMSs as being the truth. If you are concerned about what is being alleged in these messages, please verify the sender's details through their website before contacting them to confirm the legitimacy of a message.

- If you receive a notification from a supplier or customer stating that their bank account details changed, verify the new account details before making payment, by using Nedbank's 'Account Verification' Services. This allows one to verify that the bank account belongs to the correct recipient and is valid, thereby reducing fraudulent redirection of payments and collections.

- Activate 'notification services' on your business bank accounts with Nedbank to receive instant alerts to changes in your bank account balance and status.

- Scrutinise your bank statements regularly for irregular payments and switch to digital statements that can be delivered daily to your email address.

- Use trusted sources, such as government websites for up-to-date, fact-based information about Covid-19.

- Do not reveal personal or financial information in any email or SMS, and do not respond to email requests for this information.

- Regard urgent security alerts, offers or deals as warning signs of a hacking attempt.

- If an email makes you feel anxious, fearful, curious or if it sounds too good to be true, rather follow your gut feel – stop and verify before clicking on anything.

ABOUT THE AUTHOR

Mark Rose, Executive Head of Strategy and New Business Development at Nedbank Business Banking