



Republic of Namibia

Financial Intelligence Centre

P.O.BOX 2882, Windhoek
Tel: + 264 61 2835100, Fax +264 61 2835259

Web address: www.fic.na
E-mail address: helpdesk@fic.na

SMISHING SCAM

ISSUED: MAY 2021

1. Background:

Over the years, the use of mobile telecommunications devices (hereinafter referred to as Cellphones) has grown immensely. Cellphones are quite handy in communications and other functionalities. In recent years, cell phones are increasingly being used to process financial transactions (e.g e-money, mobile wallets etc). Despite such benefits, cellphone services are sadly also exposed to abuse to advance financial crimes. The Financial Intelligence Centre (FIC) has worryingly observed an increasing trend in what is commonly known as “Smishing” scams. The word “Smishing” comes from combining “SMS” which refers to Short Message Service. Generally, smishing refers to a typical ‘phishing cybersecurity attack’ carried out over a cell phone/mobile text message. It is also known as SMS phishing.

Fraudsters use these schemes as a way of illicitly soliciting funds from members of the public through deceptive, dishonest, and fraudulent means. These scams often result in huge financial losses for victims. The losses from such scams prejudice persons and often result in laundering activities. Laundering activities generally have the potential to undermine the integrity of our financial system. The FIC is sharing this publication to help contribute to efforts geared towards combatting Money Laundering activities.

2. How do these fraudulent scams operate?

Scammers are increasingly enhancing the sophistication and complexity of their methods. There has been growth or increased use of the “Smishing” scam.

Most people are familiar with typical phishing scams whereby an unsolicited email may request you to provide sensitive information, usually to those involved in identity theft. However, criminals continue to change their strategies and recent trends suggest that criminals are also sending SMS communications requesting sensitive or other private information. With these schemes, cybercriminals simply send SMSes under the guise of some legitimate business or operation, usually requesting the recipient to click on a malicious link.

There are various ways employed to solicit sensitive and confidential information if one clicks on such links. What has been quite common is cybercriminals tricking recipients to download malicious software (malware) that installs itself on recipient’s cellphones. Such malware often appears as a legitimate application, which further tricks users into presenting their sensitive information as they make use of, or access same. The malware would usually share such sensitive information with the cybercriminals.











Cybercriminals are known to use such confidential or sensitive information to commit fraudulent activities. Depending on the type of information sourced, personal information is often used to impersonate people in the advancement of crimes or to access financial services under the pretext of being the owners (or authorized users) of such privileged information.

Smishing scams might also be designed to infect mobile devices with malware or to encourage users to visit dangerous websites. Below are some common techniques used by cybercriminals¹:

- 1. A cybercriminal may send anyone an SMS text message from a spoofed number with a Uniform Resource Locator (URL) link;
- 2. URL link may trick persons into downloading malicious software that could install itself on user's cellphone. This SMS malware may appear as a legitimate app, tricking the user into typing in confidential information and sending this data to the cybercriminals;
- 3. The content and number that the text originated from may appear to be from the legitimate business/institution. At times, criminals could write their SMS as if they represent an institution the recipient has dealings with;
- 4. Spear smishing is another technique whereby cybercriminals may target a specific individual with personal information. For this purpose scammers may research a user's social media activity in order to entice their target with highly personalized and attractive text message; and
- 5. Spear phishing end goal is the same as any SMS phishing attack, however, it is significant to note that these scammers come armed with your personal information to give their trick a real feel.

¹ <https://www.thebalance.com/smishing-scams-315808>

3. How do one protect him or herself from these Scams?

 <p>Check the SMS for spelling, and grammar errors. Cyber criminals often work internationally and use translation tools;</p>	 <p>Call institutions directly if doubtful to verify information. Legitimate institutions do not request account updates or login information via texts;</p>
 <p>Do not share financial or payment information using a web form received via SMS;</p>	 <p>Avoid saving sensitive information such as credit card numbers on cell phones;</p>
 <p>Do not click on links from unknown senders or those who are not trustworthy;</p>	 <p>Question offers, often financial, which may seem too good to be true;</p>
 <p>Visit the sender's website independently rather than providing information in the message;</p>	 <p>Take time to consider the offers and planned response before responding to text messages;</p>
 <p>Verify the sender's contact details to ensure it matches that of the company it purports to belong to;</p>	 <p>Install anti-virus programs on cell phone and perform regular updates.</p>

REMEMBER

If you become a victim of a smishing scam, or through any other fraudulent activity, immediately file a report with the FIC at the Bank of Namibia or contact the nearest police station to initiate a criminal investigation.