SEXTORTION SCAM

Sextortion is a form of extortion mainly targeting teens and middle-aged to elderly men. To a lesser extent females and other younger members of society are also targeted. It involves the use of compromising photographic or video content of a sexual nature or nudity being sent by the victim to the scammer.

INDICATORS

- Any messages on WhatsApp from unknown individuals of the opposite sex, Facebook, or other social media friendship requests.
- Friendship requests or WhatsApp messages containing images of a sexual nature or nudity.
- Large transactions from mainly middle-aged men from southern Africa to the Ivory Coast, Ghana, Benin, Morocco, and the Philippines.
- Receivers of the funds have family names of west African ethnicity.
- Multiple senders remitting to the same recipient without a clear relationship or purpose.

MODUS OPERANDI

Sextortion syndicates use social media platforms such as WhatsApp, Facebook, Instagram, YouTube, and Twitter to entice individuals. Dating sites are also popular. In general, a person will receive an invitation via Facebook, YouTube, Twitter, or Instagram to connect on WhatsApp.

The victim is sent a greeting from the scammer. Soon into the chat they will receive sexually explicit images with a request for the victim to reciprocate with a naked photo or video of themselves. Once the victim sends the photo or video, the scammer threatens to share the explicit content on the Facebook pages or other social pages of the victim's family, friends, or employers as a form of blackmail in exchange for a large payment. The victim is ordered to make the payment via a money remitter, bank transfer, Bitcoin, cash transfer to an ATM or via cash transmissions at supermarkets.

Amounts demanded always start off high – anything from US$2 000 upwards. However, scammers would often lower the amount to "accommodate" the victim, depending on the profile of the victim.

High profile victims in the past included chief executives of large companies, ambassadors, and cabinet ministers of various countries.

Often the scammer's phone number is located in the same country as the victim or will be manipulated to appear to be from that country. Money transfers in many cases, however, are directed to countries in West Africa.

TAKE ACTION! This is what you can do

- Do you really want to befriend someone you have never met?
- Be sceptical of social media posts by strangers who want to befriend you.
- Do not send compromising pictures of yourself or anyone else to anyone. Ever.
- Conduct fraud awareness campaigns at your place of business.
- File suspicious and unusual transaction reports with the Financial Intelligence Centre.

Case study provided by:

WESTERN UNION WU
moving money for better
www.westernunion.com

FIC
Financial Intelligence Centre
www.fic.gov.za