PUBLIC ALERT

WhatsApp-Based Cybercrime

1.0 Background

The Cyber Security Authority has observed a worrying trend of increased reports of unauthorised access and online scams perpetrated through the takeover of social media accounts particularly, WhatsApp.

The compromised social media accounts are used to commit fraudulent activities such as investment fraud, online shopping scams, job recruitment scams, romance scams, and solicitation of funds, among others.

A second trend has to do with a WhatsApp user being lured to expose his/her nudity over a video call with someone they think they know. The session is recorded by the other party (or an associate) without the knowledge of the victim. The malicious actor then comes back to extort money from the victim in exchange for not releasing the video.

2.0 Modus Operandi

2.1 Account Takeover

A potential victim would either receive a call from an unknown number, or a message from a friend (whose social media account may have been compromised) requesting the victim to share a one-time password (OTP) (usually a 6-digit verification code) sent to the victim's number as a text message.

The scammers apply social engineering, typically creating a sense of emergency and request for the OTP which was sent to the victim. The victim would thereafter lose access to the account after providing the scammers with the verification code.

The scammers, after gaining access to the victim's account then target persons and groups on the victim's contact list as the next potential victims. Through this, the scammers would impersonate the victim's friends and promote other fraudulent activities or solicit funds. The scammers' request would be on the pretext of helping them to join online groups such as work or school groups or sign up and claim prizes for fake lucky draws allegedly conducted or joined.

2.2 Sextortion (Sexual Extortion)

A potential victim would typically make a new friend on a social media platform e.g., Facebook. Eventually the two parties exchange WhatsApp numbers and the chats continue over there, establishing a level of trust and familiarity.

After some time, a video call is initiated over which the victim ends up being persuaded to go nude. Unknown to them, the session is recorded by the other party.

Some days afterwards, the other party (or an associate) will contact the victim indicating that they have these videos and will threaten to release them in public unless they receive a specified payment. In some cases, the criminals will go ahead to share it online, provide a link (URL) to where it is and indicate it would only be taken down when they are paid. The demands typically do not end once the first payment is made.

3.0 Preventive & Mitigation Measures

3.1 Countering Account Takeovers: Enable 'Two-Step Verification'

a. Open WhatsApp **Settings**.
b. Tap **Account** > **Two-step verification** > **Enable**.
c. Enter a six-digit PIN of your choice and confirm it.
d. Provide a valid email address you have access to or tap **Skip**.

Note: Providing the email address is recommended. Otherwise if you forget your PIN, you will have to wait 7 days before you can reset it.

e. Tap **Next**.
f. Confirm the email address and tap **Save** or **Done**.

3.2 Avoiding Sexual Extortion Schemes

a. Avoid initiating and/or participating in video calls of an intimate nature i.e. where nudity is displayed, sexually explicit acts are performed etc.
b. If you receive a ransom demand, do not make payment. Instead, report it immediately to the CSA's Cybersecurity/Cybercrime Incident Reporting Points of Contact for guidance.

4.0 General Recommendations

The following measures are recommended to prevent online scams:

- Never share your social media application account verification codes with anyone.
- Protect all your social media application accounts by enabling the 'Two-Step Verification' or 'Two-Factor authentication (2FA)' feature.

- Be aware of who has physical access to your phone. If someone has physical access to your phone, they can use your account without your permission.
- Do NOT be impulsive - Beware of unusual requests from strangers or even your social media contacts.
- Do NOT believe - Be wary of claims that you have won a prize, especially if you have not participated in any campaign or lucky draw. Check official websites to determine whether the lucky draw offers are legitimate. Always verify the authenticity of the request by contacting your friend, but do not do so through the social media platform as the account might have been taken over by scammers.
- Do NOT give - Do not transfer money or give out your personal information, bank account or credit/debit card details, and One-Time Password (OTP) to anyone, including family and friends.
- If you are contacted by anyone claiming to have images and/or videos of you of an intimate nature requesting a payment in exchange for not releasing them to the public, report it immediately to the CSA's Cybersecurity/Cybercrime Incident Reporting Points of Contact for guidance. Do NOT make any payments.

The CSA has a 24-hour Cybersecurity/Cybercrime Incident Reporting Points of Contact (PoC) for reporting cybercrimes and for seeking guidance and assistance on online activities; Call or Text – 292, WhatsApp – 050 160 3111, Email – report@csa.gov.gh

Issued by Cyber Security Authority
December 5, 2022