13 Dec 19

MINISTRY OF DEFENCE
CYBER CELL

CYBER SECURITY ADVISORY 14/2019
SECURITY AND PRIVACY ISSUES – INSTANT MESSAGING AND SOCIAL MEDIA APPS

1. **Aim**. The aim of this advisory is to sensitize personnel on security and privacy issues related to usage of instant messaging and social media applications.

2. **Background**. Instant Messaging applications such as Whatsapp, Telegram, Signal, Facebook Messenger, Skype etc. and social media apps such as Facebook, Twitter, LinkedIn etc. are being used by all personnel and their family members. However, many a times, advertently or inadvertently, sensitive information gets leaked through these media. Some of the risks associated with these are given in succeeding paragraphs.

3. **Associated Risks**.

(a) **Instant Messaging Applications**. Threat actors have been using various methods to stage all sorts of phishing attacks. Nowadays, an attacker can send custom SMS/ MMS messages to modify the network and internet settings in the device via clever social engineering campaigns. In recent case involving Whatsapp, the attackers, using cleverly crafted custom message or attachments stole sensitive data and monitored camera/ microphone of the individual (CVE -2019-11931) thereby putting the individual under virtual surveillance device.

(b) **Social Media Applications**. Social Media Sites can also pose risks such as exposure to inappropriate or upsetting content like mean, aggressive, violent or sexual comments or images. Moreover, after compromise of an individual's credentials, the malicious actor can upload inappropriate content such as embarrassing or provocative photos or videos of the individual or his close friends/ relatives, share personal information with strangers, cyber bullying etc. thereby causing much inconvenience/ reputation damage. In a recent case after compromising the social media account.

4. **Guidelines**. In order to safeguard personnel from various risks indicated above, following are recommended:-

(a) **Messaging Applications**. Secure your messaging applications using security and privacy settings in the applications as indicated below:-

(i) **Privacy Settings**. Control your Privacy Settings to ensure that your personal data is visible only to you and your selected contacts. Others should not be able to see your information.

(ii) **Identify the Sender**. Always request Account Info of the sender

of the message while you receive any messages or attachments. Open all types of attachments after verifying the sender.

(iii) **Post Messages as Required**. You should have information about all the group members. Only post relevant messages which are applicable to the group members.

(iv) **Clear Chats Periodically**. Clear messages inside a chat so that the information is not stored more than the required duration. Make the habit of cleaning messages in a periodic manner.

(v) **Read Receipts**. Turn off read receipts to avoid somebody from monitoring your active hours.

(vi) **Spams**. Delete and report spam as in general most spammers also send malwares.

(vii) **Join relevant groups only**. Leave the groups if you are added by someone you don't know. Even if you know the person who added you, monitor the group for some time and quit if the same is not relevant to you.

(viii) **Blocking**. Block unwanted/ unknown users and ensure that group members are known persons.

(ix) **Access Restriction**. Enable two factor/ multi factor authentication/ verification like app lock/ OTP etc. to avoid unauthorized access.

(x) **Selection of Application**. Use apps which inherently provide better security/ privacy. Comparison of various apps is placed at Appendix.

(b) **Social Media Applications**. Following is recommended in order to secure your Social Media Account:-

(i) **Use a strong password**. The password must be complex which includes upper case, lower case, symbols and numeric values. The same needs to be sufficiently long. Use different passwords for different applications.

(ii) **Set up Security Answers**. Set up security questions and answers to recover your account in case of an attack. This option is available on most social media sites.

(iii) **Device Security**. If you have a social networking applications installed in your phone, protect your device with a strong password.

(iv) **Be selective with Friend Requests**. You should have a friends list with only the persons who you know personally. If you do not know the person, do not accept their request. It could be a fake account.

(v) **Click Links with caution**. Social Media Accounts are regularly

hacked. Look out for the language or content that does not sound like something your friend would post.

(vi) **Be careful while sharing data**. Do not reveal sensitive personal information i.e. home address, financial information, phone number etc. The more you post, the easier it is to have your identity stolen.

(vii) **Anti-virus Software**. Licensed Anti-Virus Software needs to be used to protect your operating system and applications.

(ix) **Read the site's Privacy Policy**. Read the privacy policy of the site/ application and use its privacy and security settings to control who can see your personal information.

5. These guidelines may be disseminated to all concerned agencies with in MoD.

COMPARSION OF SECURITY / PRIVACY FEATURES OF INSTANT MESSAGING APPS

Comparisons Item	Apple I Message	Facebook Message	Signal	Skype	Telegram	Viber	Whats App	Wire
Company Jurisdiction	USA	USA	USA	USA	UK/Berlin/Germany	Luxembourg/ Japan	USA	Switzerland
Implicated in giving customers' data to intelligence agencies	Yes	Yes	**No**	Yes	**No**	**No**	Yes	**No**
Provides a transparency report	Yes	Yes	Yes	Yes	**No**	**No**	Yes	Yes
General stance on customers' privacy	Poor	Poor	**Good**	Poor	Poor	Poor	Poor	**Good**
App collects customers'' data	Yes	Yes	**Minimal**	Yes	Yes	Yes	Yes	**Minimal**
Encryption turned on by default	Yes	**No**	Yes	Yes	No	Yes(if device supports it)	Yes(if device supports it)	Yes
Cryptographic primitives	RSA-1280(encryption), ECDSA 256(signing)/ AES 128/ SHA-1	Curve 25519/ AES-256/ HMAC-SHA256	Curve 25519/AES-256/HMAC-SHA256	RSA-1536 & 2048/ AES 256/ SHA-1	RSA 2048/ AES 256/SHA-256	Curve 25519 256/ Salsa 20128 HMAC-SHA 256	Curve 25519/ AES-256/HMAC-SHA 256	Curve 25519/Cha Cha20/ HMAC-SHA 256
App and server are completely open source	No	No	**Yes**	No	No(Clients and API only)	No	No	**Yes**
Anonymous sign up to get App possible	No	No	No	No	No	No	No	No
Manual verify contacts' fingerprints for using apps?	No	**Yes**	**Yes**	No	No(session only, does not provide users' fingerprint information)	**Yes**	**Yes**	**Yes**
Do you get notified if a contact's fingerprint changes?	No	No	**Yes**	No	No(session only, does not provide users' fingerprint information)	**Yes**	No(Setting turn off by default)	**If contact was previously verified**

Comparison Item	**Apple i Message**	**Facebook Message**	**Signal**	**Skype**	**Telegram**	**Viber**	**Whats App**	**Wire**
Is personal information (Mobile Number, contact list, etc.) Protected?	No	No	Yes	No	No	No	No	**Yes**
Can messages be read by the company?	**No**	**Yes**	**No**	**Yes**	**Yes**	**No**	**No**	**No**
Does the app enforce perfect forward secrecy?	No	Yes	**Yes**	Could n't find any information	No(session keys do change after being used 100 times)	Yes	Yes	**Yes**
Does the app encrypt metadata?	No	No	**Yes**	Information N/A	No	Information N/A	No	**Yes**
Does the app use TLS/ Noise to encrypt network traffic?	Yes	Yes	**Yes**	Yes	No	Yes	Yes	**Yes**
Does the App allow a Two factor of authentication?	No	No	No	No	**Yes**	No	**Yes**	**Yes**
Are messages encrypted when backed up to the cloud?	No	Information N/A	N/A, Signal is excluded from iCloud/ iTunes &Android backups	Information N/A	Information N/A	Information N/A	iOS: Yes Android: No	Information N/A
Does the app have self-destructing messages?	No	Yes	**Yes**	No	Yes	No	No	**Yes**

(Source:https://www.securemessagingapps.com)