Shoot the messenger

By DIRK AVERESCH

Messenger apps can leak your personal info and those of your contacts.

WHEN getting started on a new messenger app, most of us will just download it, upload our contacts and start chatting.

This is a mistake, say researchers, who have found that this function can be exploited by attackers to access personal information from you and contacts.

Users of messaging apps need to get into the habit of being sceptical of the default privacy settings, especially when syncing contacts to a new chat app.

That's because hackers are able to abuse that handy function that lets you sync and upload contacts from your smartphone to the messaging app, according to a study carried out by the University of Wuerzburg and the Technical University of Darmstadt.

The study showed that hackers can collect sensitive data on a large scale and without any significant restrictions from the messaging apps *Signal* and *WhatsApp*, which access the mobile phone's contacts, regularly uploading them to the service provider's servers for synchronisation.

This works by requesting masses of random phone numbers from the messengers to find contacts (known as crawling).

The information that can be disclosed when contacts are being synced or collected through crawling attacks, depending on the messenger and the privacy settings you choose.

The personal data and metadata that could be accessed in the research included profile pictures, usernames, statuses and the amount of time you spend online.

The researchers had communicated the results of the study to the messaging services before publishing it.

WhatsApp said it then improved security measures to help detect future large-scale attacks. And Signal has reduced the number of possible queries, making crawling more difficult.

For the study, 10% of all mobile phone numbers in the United States were queried for WhatsApp and 100% for Signal.

The analysed data also revealed some interesting statistics about user behaviour: around 50% of all WhatsApp users in the US have a public profile picture, while 90% have a public About Me text.

And 40% of all users registered with Signal also use WhatsApp – although the researchers assumed that more Signal users would be more concerned about their privacy. After all, unlike WhatsApp, Signal does not analyse or evaluate users' metadata.

Bit by bit

If the data obtained via crawling is pursued by attackers over a longer period of time, they can create precise models of users' behaviour, the researchers warn.

And if this data was compared with data from social networks and other public sources, detailed profiles could be created and used, for example, for scams and phishing attacks.

In an investigation of the programming interface (API) of the *Telegram* messaging app, the researchers also found that the contact identification service also reveals sensitive information about people with a telephone number but who are not registered with Telegram.

The contact comparison between the smartphone address book and messengers' servers is routinely criticised by security researchers and data protection experts.

However, the messaging services fear they will lose users without this feature, which adds convenience.

It would be safer and less objectionable in terms of data privacy, but also more tedious and annoying if each contact had to be added individually by the user. – dpa