# FakesApp: Using WhatsApp to spread scams and fake news

In a disturbing revelation, Check Point researchers have discovered a vulnerability in WhatsApp that allows a threat actor to intercept and manipulate messages sent by those in a group or private conversation. By doing so, attackers can put themselves in a position of immense power to not only steer potential evidence in their favour, but also create and spread misinformation.

The vulnerability so far allows for three possible attacks:

- Changing a reply from someone to put words into their mouth that they did not say.
- Quoting a message in a reply to a group conversation to make it appear as if it came from a person who is not even part of the group.
- Sending a message to a member of a group that pretends to be a group message but is in fact only sent to this member. However, the member's response will be sent to the entire group.

The demo video of attack displays how these attacks could play out for real.

- In the first scenario, the words of one party are manipulated by the attacker in order to provide himself with an answer that could greatly benefit him.
- In the second scenario, we see how cyber scammers could spread misinformation about a certain product to cause great damage to a company.
- In the third scenario, we see how people can be manipulated into revealing secrets that they would otherwise withhold.

## Make it go viral

As of early 2018, the Facebook-owned messaging application currently has over 1,5 billion users with over one billion groups and 65 billion messages sent every day. According to a report by global digital agencies, mobile users accounted for 172 million, most of whom used only two Facebook-owned platforms: WhatsApp and Messenger.

In addition, WhatsApp also has plans to roll out additional functionalities for businesses to help them do commerce and manage customer support through the app. Vulnerabilities such as the ones described above make the potential opportunities for scamming rife.

## WhatsApp with the fake news?

Due to its very nature of being an easy and quick way to communicate, WhatsApp has already been at the centre of a variety of scams. From fake supermarket and airline giveaways to election tampering, threat actors never tire of ways to manipulate unsuspecting users.

The ability to social engineer on a mass scale was already seen at a level where even people's lives were at stake. In Brazil, rumours quickly spread on WhatsApp about the dangers of receiving a yellow fever vaccine – the very thing that could have stopped an epidemic of the deadly virus during its 2016 rampage that infected 1500 people and killed almost 500.

More recently, last month vicious rumours, also spread via WhatsApp, led to a spate of lynching and murders of innocent victims in India.

WhatsApp is also taking an increasingly central role in elections, especially in developing countries. Earlier this year, again in India, WhatsApp was used to send messages, some of which were completely false.

Ultimately, social engineering is all about tricking the user and manipulating them to carry out actions they will later regret. With an ability to manipulate replies, invent quotes or send private messages pretending to be group ones, as seen in this research, scammers would have a far greater chance of success and have yet another weapon in their arsenal.

What's more, the larger the WhatsApp group, where a flurry of messages are often sent, the less likely a member would have the time or inclination to double check every message to verify its authenticity, and could easily be taken in by the information they see. As already seen by spam emails that fake the sender's name to appear to be from a source the receiver trusts, this latest vulnerability would allow for similar methods to be used though from a totally different attack vector.

## How to protect yourself from misinformation

While there are no security products that can yet protect users from these types of deceptions, there are several ideas to keep in mind to avoid being a victim of fake news, conspiracy theories and online scams in general.

If something sounds too good to be true, it usually is. And likewise, if something sounds too ridiculous to be true, it probably is.

Misinformation spreads faster than the truth. Although you may be seeing the same news from multiple sources, this does not make it more factual than were it to come from a single source.

Check your 'facts'. It is recommended to cross-check what you see on social media with a quick online search to see what others may be saying about the same story. Or even better, do not get more of your news from social media websites at all.