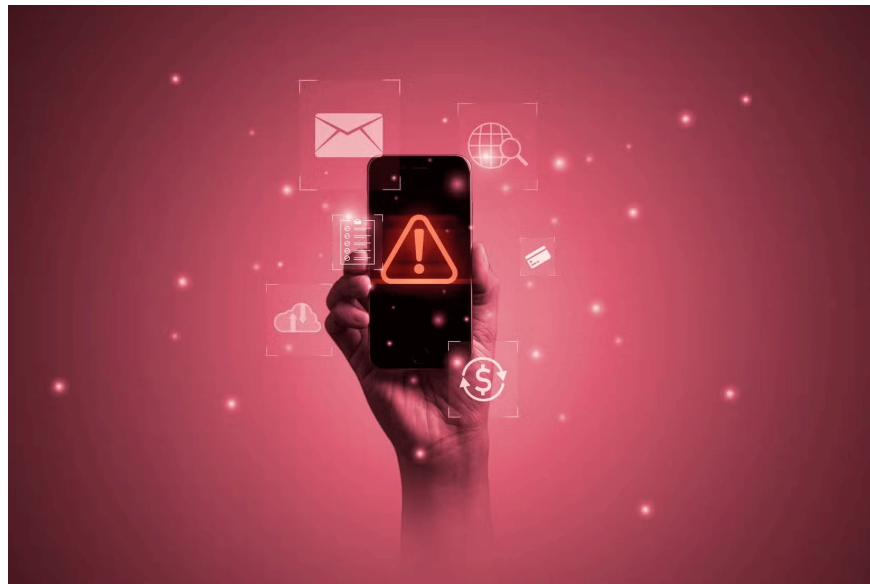


4 Ways WhatsApp Messages Can Be Hacked

Hacks targeting WhatsApp can compromise the privacy of messages and contacts. Here are five ways the WhatsApp app can be hacked.

As one of the world's leading instant messaging platforms, it's no surprise that WhatsApp is a frequent target for hackers. As such, you'll want to understand how your WhatsApp account can be compromised and take serious steps to protect your WhatsApp account, messages, and personal data.

1. Install malware



Sometimes, hackers don't need to hack your WhatsApp account directly. Sometimes, they just need to install a nasty piece of malware on your device and let it do all the heavy lifting.

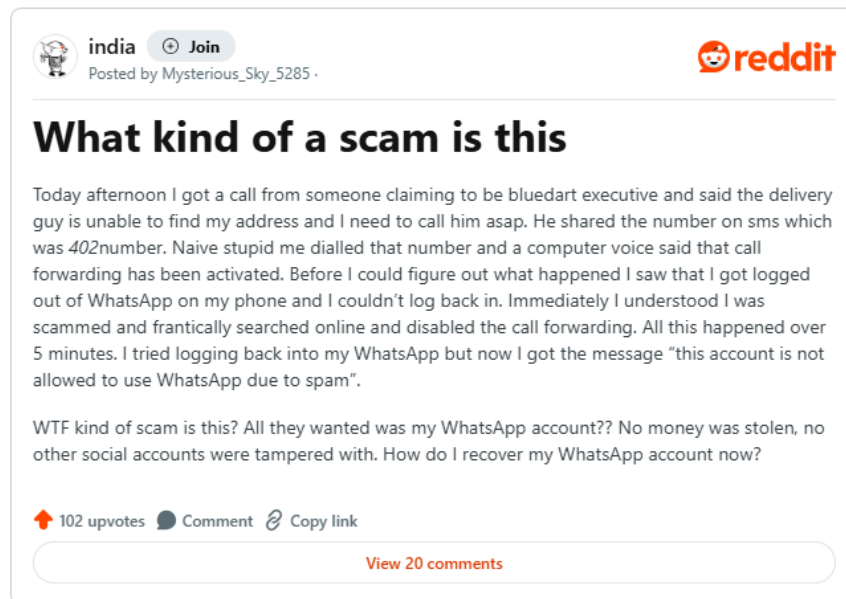
Someone can access your WhatsApp messages using malware in a number of ways. Malware with keyloggers can run silently in the background and record what you type. This includes anything you send to your friends, but can also contain data like usernames and passwords you enter.

Some malware will instead collect your messages directly. This includes malware that goes through your WhatsApp chats and sends them back to the hacker, but it can also include viruses that hijack your phone's screen recording feature and use it to record video of what you're watching. If you happen to be chatting with someone while the malware is recording your phone, the cybercriminal can see what you're talking about.

2. Call Forwarding Scam

While malware will primarily monitor your messages, there are ways hackers can gain direct access to your WhatsApp account. These usually involve tricking you into giving hackers the means to circumvent your account's two-factor authentication (2FA).

By far the easiest way for hackers to break your account's 2FA protection is to have WhatsApp send them login codes instead of you. One of WhatsApp's 2FA methods is to give you login codes over your phone, so hackers can use call forwarding to redirect those calls to themselves.



To achieve this, the scammer will convince you to enter a Man Machine Interface (MMI) code to redirect your calls to them. They can use a variety of tricks, but the most common method is to convince you that you need to call someone and then convert the MMI code to their phone number.

Once you set up call forwarding, a cybercriminal can log into your account and select a voice call to get your 2FA code. WhatsApp tries to call you, but the call is forwarded to the scammer, who then has access to your login code.

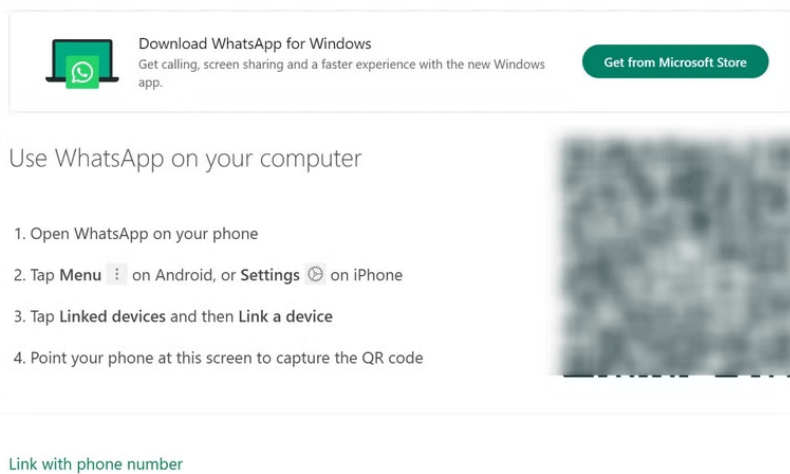
3. Social Engineering to get login code

Cybercriminals can also get your 2FA login code by asking you for it. Of course, they often say it's something else, not the only thing, that's preventing them from accessing your account.

This particular attack targets SMS-based 2FA, where WhatsApp sends you a 6-digit code that you have to enter into the app to log in. In this attack, the scammer will contact you and convince you that the 6 digits are actually something else and ask you to provide it.

A campaign reported by Nottinghamshire Police in the UK saw scammers telling their victims that the six-digit code was actually a passcode for an important video call. People would hand over the code, thinking it would let them into a special group, unaware that the person on the other end of the line was about to steal their account.

4. Fake QR Code on WhatsApp Web



When you want to use WhatsApp web, you have to scan a QR code with your phone. Unfortunately, cybercriminals have figured out how to interfere with this process and create fake WhatsApp web pages that display malicious QR codes. Once scanned, the scammer will have access to your account.

The Straits Times reports that the scam starts with a web search for WhatsApp Web. Usually, the official WhatsApp website is the top result, but scammers are good at getting fake websites to appear at the top of search engine results. And because people tend to trust the first result, they click on it without realizing they've fallen for the scam.

The fake site looks exactly like WhatsApp web, except it has a malicious QR code that can steal people's accounts. Some people don't even realize they've given up personal information after scanning the code, as there's no obvious clue what's happened other than not being able to log into WhatsApp web.

To learn more about whether WhatsApp is safe, check out **TipsMake.com**'s guide to WhatsApp security threats users need to know about.

You finished reading the article "**4 Ways WhatsApp Messages Can Be Hacked**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.