5 WhatsApp user security threats need to know

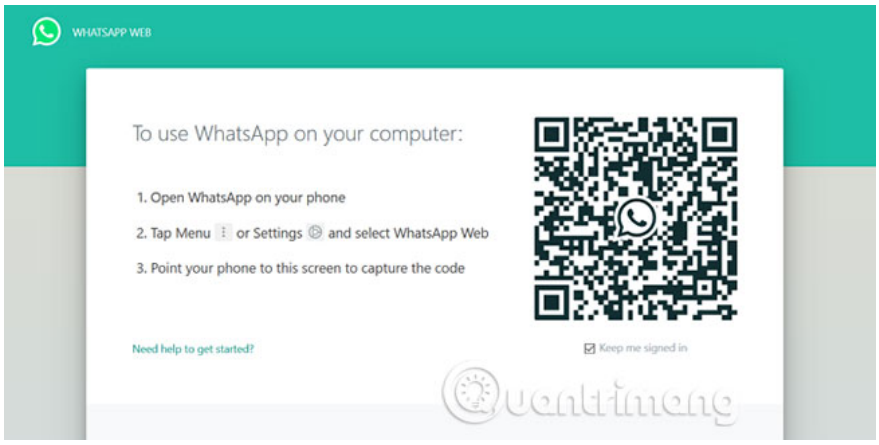
Not surprisingly, security concerns, malware threats and spam for WhatsApp have begun to appear. The following article will summarize everything you need to know about WhatsApp's security issues.

WhatsApp, Facebook-owned platform, is one of the world's most popular messaging apps. It is estimated that more than one billion people use this application, with more than 65 billion messages a day.

Not surprisingly, security concerns, malware threats and spam for WhatsApp have begun to appear. The following article will summarize everything you need to know about WhatsApp's security issues.

The WhatsApp user security threats should be noted

1. WhatsApp Web malware



WhatsApp's huge user base, makes this app a lucrative prey for cyber criminals. Many of these hackers focus on WhatsApp Web. For years, WhatsApp allows you to open a web page or download a desktop application, scan the code with the phone application and use WhatsApp on your computer.

App stores on phones (apps on iOS App and Google Play of Android) are safer than other unknown apps on the Internet. When searching for WhatsApp on this app store, you will know right away which app is the official app. But not all the Internet is the same.

Cybercrime, hackers and scammers all try to take advantage of this. There have been cases where an attacker has spread malware in the form of WhatsApp desktop applications. If unfortunately, you mistakenly download a malicious WhatsApp application, the installation may spread malware or damage your computer system.

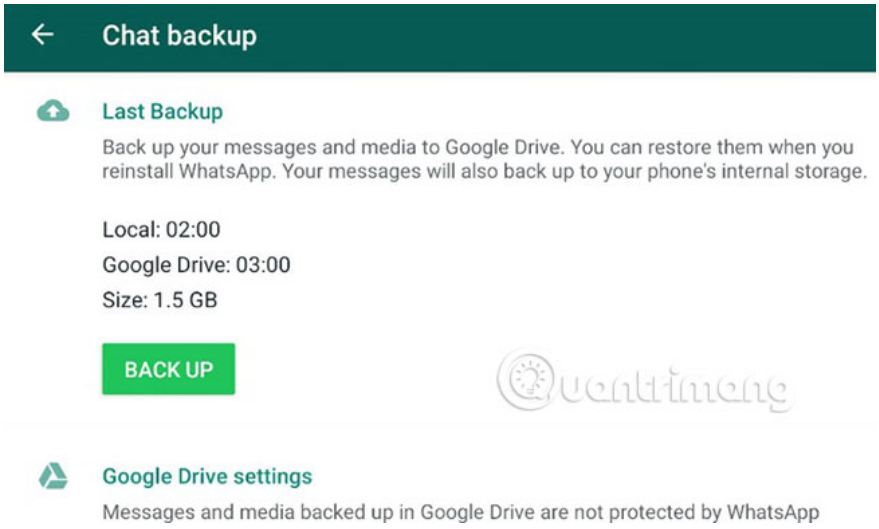
In some cases, hackers can install spyware (spyware) from the WhatsApp vulnerability.

Other bad guys have tried a new approach, creating phishing websites to trick users into providing personal information. Some of these websites pretend to be a Web WhatsApp site, asking you to enter a phone number to connect to the service. However, they actually use that phone number to send spam or contact data that is leaked or hacked on the Internet.

The best way to stay safe is to only use applications and services from official sources. WhatsApp provides a web application for you to use on any computer, called WhatsApp Web. There are also official applications for Android, iPhone, macOS and Windows devices.

Download WhatsApp for Android | iOS | macOS | Windows (Free).

2. Backups are not encrypted



The messages you send on WhatsApp are encrypted at the end. This means that only your device and the recipient can decrypt them. This feature prevents your messages from being blocked while transmitting, even by Facebook itself. However, this feature is not secure for messages, when they are decrypted on your device.

WhatsApp allows you to back up your messages on Android and iOS. This is an essential feature because it allows recovery of WhatsApp messages accidentally deleted. There is a local backup on the device, in addition to a cloud-based backup. On Android, you can backup your WhatsApp data to Google Drive. If you are using iPhone, the destination for the backup is iCloud. These backups contain decrypted messages from your device.

Backup files are stored on iCloud or Google Drive unencrypted. Because this file contains decrypted versions of all your messages, they are theoretically vulnerable to attack and weaken WhatsApp's terminal encryption feature.

Since there is no choice of backup location, you must believe that cloud storage providers will keep your data secure. Although so far, there are no large-scale hacks affecting iCloud or Google Drive, but that doesn't mean that won't happen in the future. There are many different ways an attacker can use to gain access to your cloud storage account.

If you choose to back up your WhatsApp data to the cloud, that will somewhat undermine the end-to-end encryption of this service.

3. Share data with Facebook

February 19, 2014

Facebook to Acquire WhatsApp

- *Acquisition accelerates Facebook's ability to bring connectivity and utility to the world*
- *Leading mobile messaging company will continue to operate independently and retain its brand*
- *WhatsApp co-founder and CEO Jan Koum to join Facebook Board of Directors*

MENLO PARK, CALIF. – February 19, 2014 – Facebook today announced that it has reached a definitive agreement to acquire WhatsApp, a rapidly growing cross-platform mobile messaging company, for a total of approximately $16 billion, including $4 billion in cash and approximately $12 billion worth of Facebook shares. The agreement also provides for an additional $3 billion in restricted stock units to be granted to WhatsApp's founders and employees that will vest over four years subsequent to closing.

Facebook has been the focus of many criticisms in recent years. One of those criticisms is about market monopoly and against Facebook's competition rules. So when Facebook decided that they wanted to add WhatsApp to the 'big Facebook family', the European Union (EU) only approved the deal, after Facebook assured them that both Facebook and WhatsApp companies, together with their data, kept separate.

But soon after, Facebook failed. In 2016, WhatsApp updated security policy and allowed sharing data from WhatsApp to Facebook. Although the entire range of data sharing is not disclosed, but information such as phone numbers and data about your application usage, when and when you last used WhatsApp, is be transferred to Facebook.

WhatsApp also claims that none of your information is publicly displayed on Facebook, but implies that they will instead be hidden in Facebook's inaccessible profile. Because of the overwhelming response to this announcement, WhatsApp allows users to refuse to share data. However, over the years, WhatsApp has quietly removed this option.

This is likely to be prepared for Facebook's future plans. According to a January 2019 report in the New York Times, Facebook is starting to create a unified infrastructure for all of its messaging platforms. Ie Facebook, Instagram and WhatsApp will work together. Therefore, although each service will continue to function as a standalone application, all messages will be sent on the same network.

4. Phishing tricks and fake news

'WhatsApp murders': India struggles to combat crimes linked to messaging service

In the past year the murders of at least 30 people accused of being 'child-lifters' have been linked to platform

Michael Safi *in Delhi*

@safimichael

Tue 3 Jul 2018 07.14 BST

368

In recent years, social network service providers have been criticized for allowing fake news and false information to spread on their platforms. WhatsApp also suffered the same situation.

Two of the most notable cases are in India and Brazil. WhatsApp is related to widespread violence, occurring in India in 2017 and 2018. Messages with details about fake kidnappings have been forwarded and spread on this platform, with domestic Content is customized to match the information in each locality. These messages have been widely shared to many users, but the sanctions for handling those who spread this fake news are still quite lax.

In Brazil, WhatsApp is the main source of fake news during the 2018 election. Because this kind of misleading information is easy to spread, business people in Brazil have established companies, creating information. Wrong against candidates via WhatsApp. Bad guys can do this because the phone number matches your username on WhatsApp, and they bought a list of phone numbers to target.

Both problems took place in 2018, an extremely terrible year for Facebook. Misinformation on the digital platform is a problem, but what annoys many people is WhatsApp's indifferent attitude to this issue.

However, after that, the company made a few changes. WhatsApp sets limits for forwarding, you can only forward up to 5 groups, instead of limiting up to 250 previous groups. WhatsApp also removed the shortcut for forwarding in some areas.

5. WhatsApp Status

For years, WhatsApp's status feature, a short line of text, is the only way for you to let people know what you're doing at the time. This feature has turned into WhatsApp Status, a copy of the famous Instagram Stories feature.

Instagram is a platform designed to be public, although you can make your profile private if you want. On the other hand, WhatsApp is a more intimate service, used to communicate with friends and family. So you can assume that sharing a status on WhatsApp is also private.

However, the truth is not as it appears to be. Anyone in the WhatsApp contacts can view your status. Fortunately, it is quite easy to control who you can share your status with.

Navigate to **Settings> Account> Privacy> Status** and you will be shown three security options for status updates:

1. My contacts
2. My contacts except .
3. Only share with .

However, WhatsApp does not make it clear whether the contacts you have blocked can view your status. Thankfully, the company did a reasonable job of keeping blocked contacts from viewing your status, regardless of your privacy settings. As with Instagram Stories, all videos and photos added to the status will disappear after 24 hours.

WhatsApp safe?

So WhatsApp is safe to use after all? WhatsApp is a confusing platform. On the one hand, the company has implemented end-to-end encryption for one of the most popular applications in the world. But on the other hand, there are still many security concerns for WhatsApp. One of the main issues is that it is owned by Facebook, subject to many privacy-related risks and misinformation campaigns like its parent company.

If these reasons upset your messaging application, there are WhatsApp alternatives that help protect your privacy. However, if you decide to stick with WhatsApp, check out the tips for effective chat on WhatsApp Desktop.

You finished reading the article "**5 WhatsApp user security threats need to know**" 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.