

Click to prove  
you're human



























[illegible]



[26] [27] [28] [29] [30] [31] [32] [33] [34] [35] [36] [37] [38] [39] [40] [41] [42] [43] [44] [45] [46] [47] [48] [49] [50] [51] [52] [53] [54] [55] [56] [57] [58] [59] [60] [61] [62] [63] [64] [65] [66] [67] [68] [69] [70] [71] [72] [73] [74] [75] [76] [77] [78] [79] [80] [81] [82] [83] [84] [85] [86] [87] [88] [89] [90] [91] [92] [93] [94] [95] [96] [97] [98] [99]

[1] WhatsApp Payments (marketed as WhatsApp Pay) is a peer-to-peer money transfer feature. The service became generally available in India and Brazil, and in Singapore. WhatsApp Business transactions include:[239][240][In July 2017], WhatsApp received permission from the National Payments Corporation of India (NPCI) to enter the Indian payments market.[241] WhatsApp announced that it will partner with NPCI to launch its own digital payment system called "WhatsApp Pay".[242] WhatsApp's new payment system was expected to become operational by August 2022.[246]See also: Diem (digital currency)[On February 28, 2019, The New York Times reported that Facebook was "hoping to develop some cryptocurrency that could be incorporated into WhatsApp." The project reportedly involved more than 50 engineers under the direction of former PayPal president David A. Marcus. This "Facebook coin" would reportedly be a stablecoin pegged to the value of a basket of different foreign currencies.[247]In June 2019, Facebook said that the project would be named Libra, and that a digital wallet named "Calibra" was to be integrated into Facebook and WhatsApp.[248] After financial regulators in many regions raised concerns, Facebook stated that the currency, renamed Diem since December 2020, would require a government-issued ID for verification, and the wallet app would have fraud protection. Calibra was rebranded to Novi in May 2020.[249][250][251]Meta (formerly Facebook) ended its Novi project on September 1, 2022.[252][253]WhatsApp has repeatedly imposed limits on message forwarding in response to the spread of misinformation in countries including India and Australia. The measure, first introduced in 2018 to combat spam, was expanded and remained active in 2021. WhatsApp's Meta stated that the forwarding limits had helped to curb the spread of misinformation regarding COVID-19.[254][255][256]**Main article:** Indian WhatsApp lynchings  
Also see: WhatsApp University  
India, WhatsApp encouraged people to report messages that were fraudulent or incited violence after lynch mobs in India murdered innocent people because of malicious WhatsApp messages falsely accusing the victims of involvement in abduct killings.[257] There were several instances between 2017 and 2020, after which WhatsApp announced changes for Indian users of the platform that labels forwarded messages as such.[258]An investigation on the issue of social media in politics, it was found that WhatsApp was being abused for the spread of fake news and hate speech against minorities and political opponents. In January 2020, WhatsApp released guidelines for Indian users to help them identify and avoid spreading false information. It also urged users to report suspicious messages to local law enforcement agencies.**Article:** Reception and criticism of WhatsApp security and privacy features  
WhatsApp was initially criticized for its lack of encryption, sending information via plaintext.[261] Encryption was first added in May 2012,[262][263][264] End-to-end encryption was only fully implemented in April 2016 after a two-year process. As of September 2021[update], it is known that WhatsApp makes extensive use of outside contractors and artificial intelligence systems to examine certain user messages, images and videos (those that have been flagged by users as possibly abusive), and turns over to law enforcement metadata including critical account and location information.[265]In 2016, WhatsApp was widely praised for the addition of end-to-end encryption and earned a 6 out of 7 points on the Electronic Frontier Foundation's "Secure Messaging Scorecard".[266] WhatsApp was criticized by security researchers and the Electronic Frontier Foundation for using backups that are not covered by end-to-end encryption and allow messages to be accessed by third-parties.[267][268]In May 2019, a security vulnerability in WhatsApp was found and fixed that allowed a remote person to install spyware by making a call which did not need to be answered.[269][270]In September 2019, WhatsApp was criticized for its implementation of a "delete for everyone" feature. iOS users can elect to save media to their camera roll automatically. When a user deletes media for everyone, WhatsApp does not delete images saved in the iOS camera roll and so those users are able to keep the images. WhatsApp released a statement saying that "the feature is working properly", and that images stored in the camera roll cannot be deleted due to Apple's security layers.

[271]In November 2019, WhatsApp released a new privacy feature that lets users decide who they want to share photos with.[272]In December 2019, WhatsApp confirmed a security flaw that would allow hackers to use a malicious GIF image file to gain access to the recipient's data. When the recipient opened the gallery within WhatsApp, even if not sending anything back, the hacker could steal all the data on the phone without needing consent. WhatsApp quickly patched the bug, stating that the exploit required the victim to interact with the malicious link. However, the fix was flawed and the exploit could still be used by forcing the device to uninstall and reinstall of the app.[276]The bug was discovered by Check Point in August 2019 and reported to WhatsApp. It was fixed in version 2.19.246 onwards.[277][278]For security purposes, since February 1, 2020, WhatsApp has been made unavailable on smartphones using legacy operating systems like Android 2.3.7 or older and iPhone iOS 8 or older that are no longer updated by their providers.[279]In April 2020, the NSO Group held its governmental clients accountable for the allegation of human rights abuses by WhatsApp. In its revelation via documents received from court, the group claimed that the lawsuit brought against the company by Google App threatened to infringe on its clients' "national security and foreign policy concerns". However, the complaint did not reveal names of the end users, which according to a research by Citizen Lab include, Saudi Arabia, Bahrain, Kazakhstan, Morocco, Mexico and the United Arab Emirates.[280]On December 16, 2020, a claim that WhatsApp gave Google access to private messages was included in the anti-trust case against the latter. As the complaint was heavily redacted due to being an ongoing case, it did not disclose whether this was alleged tampering with the app's end-to-end encryption, or Google accessing user backups.[clarification needed][281]In January 2021, WhatsApp announced an update to their Privacy Policy which stated that WhatsApp would share user data with Facebook and its "family of companies" beginning February 2021. Previously, users could opt-out of such data sharing, but the new policy removed this option. The new Privacy Policy would not apply until October EU, as it is illegal under the GDPR. Facebook and WhatsApp were widely criticized for this move.[118][119][282] The enforcement of the privacy policy was postponed from February 8 to May 15, 2021.[120][283] Users announced they had no plans to limit the functionality of the app for those who did not approve the new terms.[122]On March 15, 2021, WhatsApp announced that it would start rolling out updates to support Windows Phone devices starting in early 2022. WhatsApp CEO Jan Koum revealed that he had personally tested the application on his Lumia 950 XL before announcing the decision to bring the app to Windows phones, which was seen as a positive sign for Microsoft. On January 29, 2021, an FBI document was uncovered by Rolling Stone, revealing that WhatsApp responds to warrants and subpoenas from law enforcement within minutes, providing user metadata to the authorities. The metadata includes the user's contact information and address book.[285]In January 2022, an unsealed surveillance application revealed that WhatsApp started tracking seven users from China and Macau in November 2021, based on a request from US DEA investigators. The app collected data on who the users contacted and how often, and when and how they were using the app. This is reportedly not an isolated occurrence, as federal agencies can use the Electronic Communications Privacy Act to covertly track users without submitting any probable cause or linking a user's number to their identity.[286]At the time of writing of this section of the history of 2022, it was revealed that San Diego-based startup Boldend had developed tools to hack WhatsApp's encryption, gaining access to user data, at some point since the startup's inception in 2017. The vulnerability was reportedly tracked down in January 2021. Boldend is financed, in part, by Peter Thiel, a notable investor in Facebook.[287]In September 2022, a critical security issue in WhatsApp's Android video chat feature was reported. An integer overflow bug allowed a malicious user to take full control of the victim's application once a video call between two WhatsApp users was established. The issue was viewed on the day it was officially reported.[288]In 2025, WhatsApp alerted 90 journalists and other members of civil society that they had been targeted by spyware used by the Israeli technology company Paragon Solutions.[289]As of 2023[update], WhatsApp is widely used by government institutions in the UK, although such use is watched as problematical since it hinders the public, including journalists, from obtaining accurate government records when making freedom of information requests.[290]The Information Commissioner has said that the use of WhatsApp poses risks to transparency since members of Parliament, senior officials and police officers may communicate privately through the app rather than publicly accessible channels. This raises concerns about accountability and oversight, particularly given the app's popularity among politicians and law enforcement agencies, rather than government-issued devices. When the official inquiry into the pandemic began seeking evidence in May 2023, this presented issues for its ability to gather the material it sought. A personal device of the former Prime Minister, Boris Johnson, had been compromised by a security breach, and it was claimed that it could not be switched on to recover messages.[293] Further, the Cabinet Office had claimed that since many messages were not relevant to the inquiry, it only needed to hand over material it had selected as being relevant. The High Court, in a judicial review sought by the Cabinet Office, declared that all documents sought by the inquiry were to be handed over unrestricted. In 2024[unreliable source date=June 2024], it was reported that around 500,000 National Health Service (NHS) staff used WhatsApp and other instant messaging systems at work and around 29,000 had faced disciplinary action for doing so. Higher usage was reported by frontline clinical staff to keep up with care needs, even though NHS trust policies do not permit their use.[295]In March 2019, WhatsApp released a guide for users who had installed unofficial modified versions of WhatsApp and warned that it may ban those using unofficial hacks.[296]**Main article:** WhatsApp snooping scandal  
May 2019, WhatsApp was attacked by hackers who installed spyware on a number of victims' smartphones.[297]The hack allegedly deployed by Israeli surveillance technology firm NSO Group, injected malware onto WhatsApp users' phones via a remote-exploit bug in the app's Voice over IP calling functions. A Wired report noted the attack was aimed to inject malware via calls to the targeted phone, even if the user did not answer the call.[298]In October 2019, WhatsApp filed a lawsuit against NSO Group in a San Francisco court, claiming that the alleged cyberattacks violated U.S laws including the Computer Fraud and Abuse Act (CFAA).[299] According to WhatsApp, the exploit "targeted at least 100 human-rights defenders, journalists and other members of civil society" among a total of 1,400 users in 20 countries across Africa, Asia, Europe, Latin America, Middle East, North America, Oceania, South America and Southeast Asia. WhatsApp accused NSO Group of installing spyware on the phones of individuals close to the Washington Post journalist Jamal Khashoggi.[303]In 2021, an FBI document obtained through a Freedom of Information request by Property of the People, Inc., a 501(c)(3) nonprofit organization, revealed that WhatsApp and iMessage are vulnerable to law-enforcement real-time searches.[304][305][285]In January 2022, an investigation by The Wire claimed that BJP, an Indian political party, allegedly used an app called Tech Fog which was capable of hacking inactive WhatsApp accounts en masse to mass message their contacts with propaganda. According to the report, a whistleblower from app access was able to hack a test WhatsApp account controlled by reporters "within minutes".[306][307]It was later determined that the post-political events investigated there had been kept free by false information; The Wire fired the staff member involved and issued a formal apology to its readers.[308]December 2015, Reuters reported that terrorist organization ISIS had been using WhatsApp to plot attacks during November 2015 Paris attacks.[309]According to The Independent, ISIS asked WhatsApp to provide it with lists of mobile numbers belonging to British citizens living in Iraq, Syria, Libya, Tunisia, Egypt, Jordan, Lebanon and Turkey, so that they could target them. WhatsApp refused the request, citing its commitment to protect user privacy and confidentiality. WhatsApp also informed the British government of the request and provided them with details of the attempt. WhatsApp also took steps to ensure that its services were secure and reliable, and that it was able to respond to emergency situations. WhatsApp also worked closely with law enforcement agencies to investigate the matter and prevent further attacks. WhatsApp also continued to improve its security measures and to provide better protection for its users' data and communications. WhatsApp also worked to build trust with its users and to make it easier for them to manage their privacy settings. WhatsApp also continued to expand its reach and to serve more people around the world. WhatsApp also continued to innovate and to add new features to its app. WhatsApp also continued to work with governments and law enforcement agencies to打击恐怖主义和犯罪活动。WhatsApp also continued to work with industry partners to improve interoperability and to enable seamless communication between different platforms. WhatsApp also continued to invest in research and development to stay ahead of emerging threats and to ensure the long-term success of its business. WhatsApp also continued to focus on improving customer experience and to provide better support to its users. WhatsApp also continued to explore new ways to monetize its services while maintaining its core values of privacy and security. WhatsApp also continued to engage with its community and to listen to feedback from its users. WhatsApp also continued to strive for excellence in everything it did and to set a benchmark for innovation and leadership in the tech industry.

[310]Further, after a six-month probe which involved the infiltration of 79 WhatsApp groups, the National Intelligence Agency reported that out of about 6386 members and admins of these groups, about 1000 were residents of Pakistan and gulf nations. Further, for their help in negating anti-terror operations, the Indian stone pelters were getting funded through barter trade from Pakistan and other indirect means.[314]In May 2022, the FBI stated that an ISIS sympathizer, who was plotting to assassinate George W. Bush, was arrested based on his WhatsApp Data. According to the arrest warrant for the suspect, his WhatsApp account was placed under surveillance.[315]There are numerous ongoing scams on WhatsApp that let hackers send viruses or malware.[316] In May 2016, some WhatsApp users were reported to have been tricked into downloading a third-party application called WhatsApp Gold, which was part of a scam that infected the users' phones with malware.[317]Another application that promises to allow access to their WhatsApp friends' conversations, or their contact lists, has become the most popular hit against anyone who uses the application in Brazil. Clicking on the message actually sends paid text messages. Since December 2016, more than 3 million people have clicked and lost money.[318][319]A message called GB WhatsApp is considered malicious by antivirus vendors. It claims to offer unlimited space for storing photos and videos, but in reality, it steals your data and sells it to advertisers. It also contains ads and pop-ups. It is recommended to avoid using it. WhatsApp has blocked GB WhatsApp completely in China.[322][323]On April 9, 2024, Apple removed WhatsApp from the App Store in China, citing government orders that stemmed from national security concerns.[324][325]This section needs to be updated. The reason given is: Mentioned deadline has long passed. Please help update this article to reflect recent events or newly available information.(February 2023)On May 9, 2014, the government of Iran announced that it had proposed to block the access to WhatsApp service from Iranian residents. "The reason for this is the assumption of WhatsApp by the Facebook founder Mark Zuckerberg, who is an American Zionist," said Abdolsamad Khorrarnabadi, head of the country's Committee on Internet Crimes. Subsequently, Iranian president Hassan Rouhani issued an order to the Ministry of ICT to stop filtering WhatsApp.[326][327]



