www.dka.global

Messaging Apps & Communication Platforms *Comparative Analysis*

February 2021

DEEP KNOWLEDGE ANALYTICS

Table of Contents

User concerns regarding privacy in messaging apps have spiked in recent years. Incidents of data breaches have alarmed many customers and forced them to reconsider their standard attitudes towards messaging apps and the security of their personal information. Some situations and events have steadily deteriorated public trust, resulting in many users wondering whether they have lost control over their own data.

Users of messaging apps and platforms report concerns about businesses, advertisers and governments accessing and using their data. These growing privacy concerns have prompted advocacy for tighter regulations. In addition, they have placed companies responsible for safeguarding personal data under greater scrutiny.

At the same time, developments in Information Technologies are bringing new, more sophisticated solutions for messaging and corporate communication.

Deep Knowledge Analytics conducted its own independent analysis to identify and benchmark the most secure and convenient messaging apps.In this case study we are assessing convenience, security and accessibility of 18 popular messaging apps. The study also features a short analysis of corporate communication platforms.

Introduction

Messaging apps are essential for our daily activities, including business communication, personal communication, and other domains. For some specific spheres, such as journalism and protest activities, secure messaging is a central concern, of the utmost importance.

The development of Information Technologies has brought numerous advancements to messaging apps. Once suitable only for exchanging texts, most of them now allow voice messaging, voice calls, video calls, and numerous other features. At the same time, the cases associated with Edward Snowden, Pavel Durov, and Cambridge Analytica (among others) have eroded public trust in secure and private messaging by revealing that surveillance of private information on social networks and messaging apps by governments and third parties is a very common practice. This has created significant public backlash, fueling the emergence of security-focused apps which offer privacy as their main advantage. Nevertheless, with more attention to privacy, users still care about the convenience and price of the messenger apps.

The present special case study aims to scrutinize the most popular messengers and communication platforms to find out which of them combine the best user experience with the most robust security and privacy. The study separately assesses the most secure and the most convenient messaging apps, as well as the messaging apps harmoniously combining these qualities.

Methodology of the Assessment

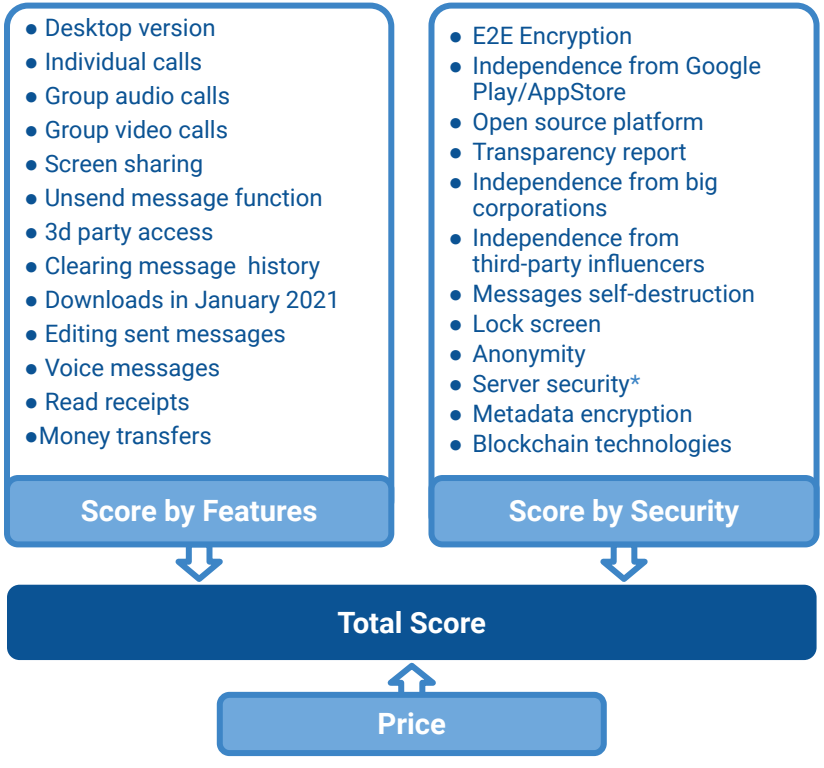
This study by **Deep Knowledge Analytics** compares 18 messaging apps and tools according to 25 variables, to find the most secure, versatile, and accessible apps currently available. The variables were grouped into separate categories: Security, Features, and Price.

The **Security Category** includes such variables as server security*, end-to-end encryption systems, metadata encryption, blockchain technology, anonymity (e.g. does the app require the phone number?), platform type (open source vs. non open source), transparency report, independence from Google Play or App Store, message self-destruction, lock screen, and independence from big corporations and third-party influencers.

The **Features Category** encompasses such variables as desktop version availability, individual calls, group audio calls, group video calls, screen sharing, voice messages, read receipts, editing sent messages, unsend message function, clearing message history, 3rd party access, and number of downloads in January 2021.

The **Price Category** is a separate category specifying whether the app is free, paid, or freemium (free, but with certain features requiring payment or subscription).

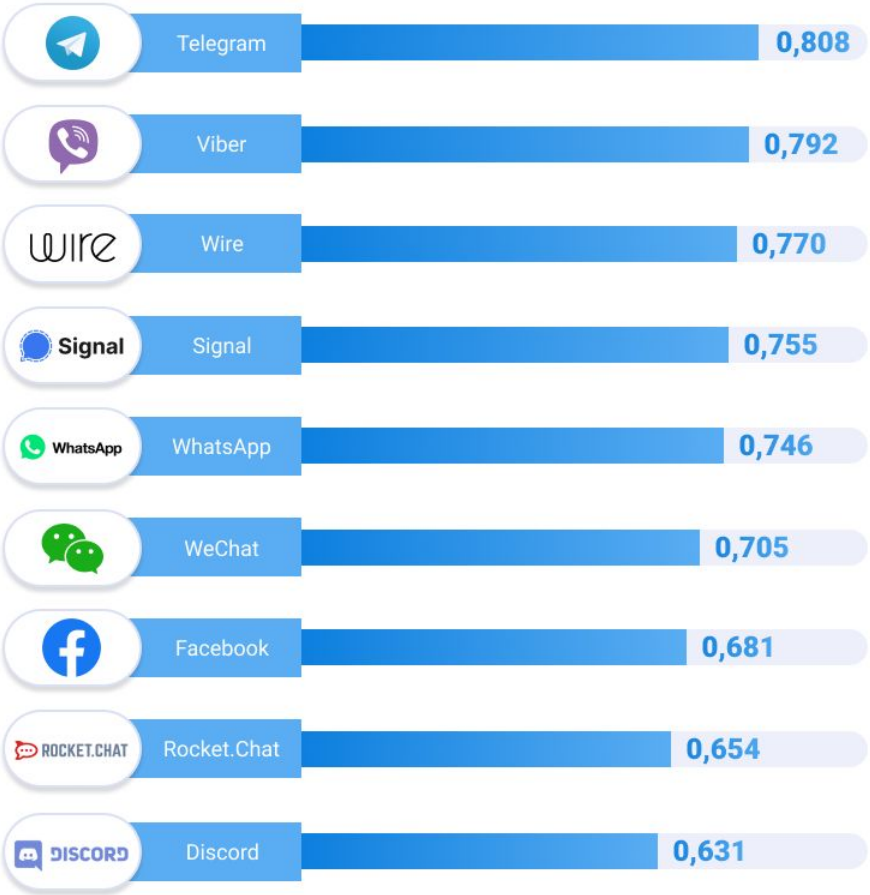
The score for each variable is coded as 1 if the variable condition is present or true for a given app, 0 if the variable condition is absent or false, and 0.5 if some features are accessible only in the paid version or if they have to be activated additionally. The Total Score is an average of Score by Features, Security, and Price. The analysis also provides separate Score by Features and by Security. The assessment is based on analysis of databases compiled for the purpose of this study from a variety of open sources.



*Servers are categorized into centralized, federated (decentralized), and peer-to-peer (P2P). Depending on the task, some messengers can deploy P2P elements into the first two types. In this case, we give 1 point to P2P networks, 0.75 to federated with P2P elements, 0.5 to federated, 0.25 to centralized with P2P elements, and 0 to centralized servers.

Score by Features

DEEP KNOWLEDGE ANALYTICS



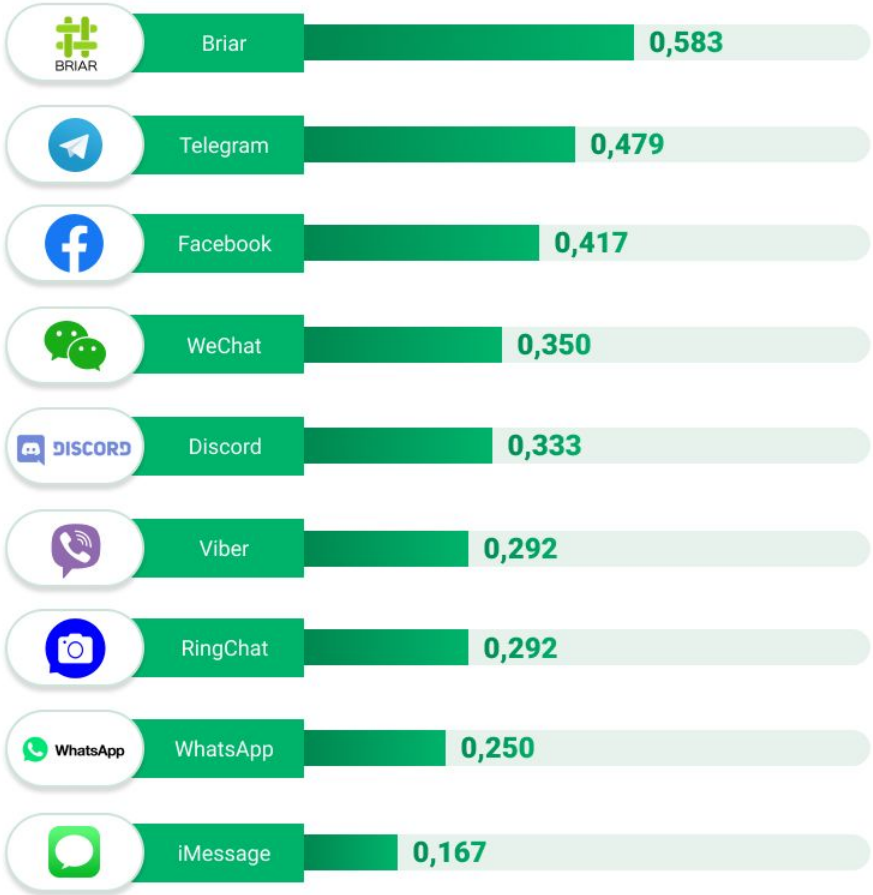
Features Parameters

	Desktop Version	Individual Calls	Group Audio Calls	Group Video Calls	Screen Sharing	Unsend Message Function	3d Party Access	Clearing Message History	Money Transfers	Downloads in January 2021	Editing Sent Messages	Voice Messages	Read Receipts	Features
Telegram	1	1	1	0	0	1	1	1	0.5	1	1	1	1	0.808
Viber	1	1	1	1	1	0.5	0	1	0.5	0	1	1	1	0.792
Wire	1	1	1	0	1	1	1	1	0	0.004	1	1	1	0.77
Signal	1	1	1	1	0	1	1	1	0	0.81	0	1	1	0.755
WhatsApp	1	1	1	1	0	1	0	1	1	0.698	0	1	1	0.746
WeChat	1	1	1	1	0	0.5	0.5	1	1	0.159	1	1	0	0.705
Facebook	1	1	1	1	1	1	0	1	0.5	0.349	0	0	1	0.681
Rocket.Chat	1	1	1	1	1	0	1	0	0	0.001	1	1	0.5	0.654
Discord	1	1	1	1	1	1	1	0	0	0.206	1	0	0	0.631
Wickr	1	1	0.5	0.5	0.5	1	1	1	0	0.006	0	1	0	0.577
Tox	1	1	1	0	1	0	1	1	0	0	0	0	1	0.538
Element	1	1	1	1	0	0	1	0	0	0.001	0.5	0	1	0.5
Threema	0	1	1	0	0	0	1	1	0	0.001	0	1	1	0.462
iMessage	1	0	0	0	0	0	1	1	0.5	N/A	0	1	1	0.458
Pryvate	1	1	1	0	0	1	1	0	0	0.063	0	0	0	0.389
RingChat	1	1	0	0	0	0	1	0	0	0	0	1	1	0.385
Session	1	0	0	0	0	0	1	0	0	0.001	0	1	1	0.308
Briar	0	0	0	0	0	0	1	0	0	0	0	0	1	0.154

0 1

1 - Yes; **0** - No; **0,5** - Partial

Score by Security



Security Parameters

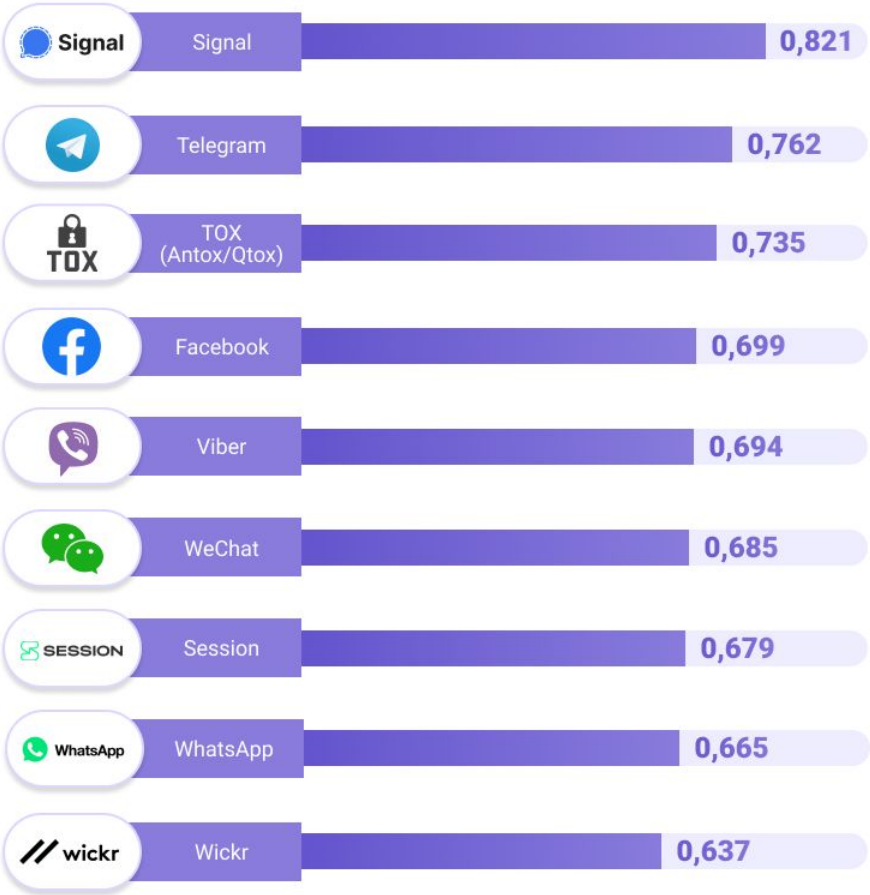
	End to End Encryption (E2EE)	Independency from Google Play/AppStore	Open Source	Does the Company Provide a Transparency Report?	No Big Corp Behind	Zero Influencer Endorsement	Self-destructing Messages	Lock Screen	Does Not Require Phone Number	Server Security*	Metadata Encryption	Blockchain Technology	Security
Wickr	1	1	1	1	1	0	1	1	0.5	1	1	0.5	0.833
Session	1	1	1	0	1	0.5	1	0	1	0.75	1	0.5	0.729
Signal	1	1	1	1	1	0	1	1	0	0.5	1	0	0.708
Threema	1	0	1	1	1	1	0	1	0.5	0.75	1	0	0.688
Tox	1	1	1	0	1	1	0	0	1	1	1	0	0.667
Pryvate	1	0	1	0	1	1	1	0	1	1	0	1	0.667
Element	1	1	1	0	1	1	0	0	1	0.75	N/A	0	0.614
Wire	1	1	1	1	0.5	0	1	0	1	0	0.5	0	0.583
Rocket.Chat	0.5	1	1	1	1	1	0	0	1	0.5	0	0	0.583
Briar	1	0	1	0	1	1	0	0	1	1	1	0	0.583
Telegram	1	1	0.5	0	1	0	1	1	0	0.25	0	0	0.479
Facebook	0.5	1	0	1	0	0	1	1	0.5	0	0	0	0.417
WeChat	0.5	1	0.5	1	0	1	0	0	0	0	0	0.5	0.350
Discord	0	1	1	1	0	1	0	0	0	0	0	0	0.333
Viber	0.5	1	0	0	0	0	1	1	0	0	0	0	0.292
RingChat	0.5	0	1	0	1	1	0	0	0	0	0	0	0.292
WhatsApp	1	1	0	1	0	0	0	0	0	0	0	0	0.250
iMessage	1	0	0	1	0	0	0	0	0	0	0	0	0.167

0 — 1

1 - Yes; **0** - No; **0,5** - Partial

Total Score

DEEP KNOWLEDGE ANALYTICS



Total Score

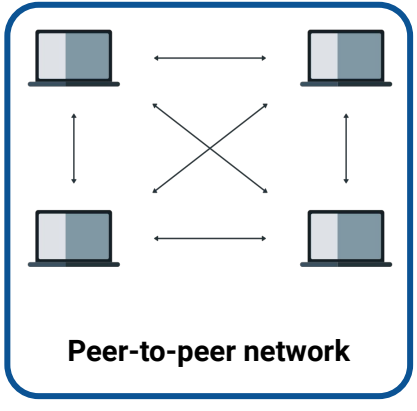
	Features	Security	Price	Total score
Signal	0.755	0.708	1	0.821
Telegram	0.808	0.479	1	0.762
Tox	0.538	0.667	1	0.735
Facebook	0.681	0.417	1	0.699
Viber	0.792	0.292	1	0.694
WeChat	0.705	0.35	1	0.685
Session	0.308	0.729	1	0.679
WhatsApp	0.746	0.25	1	0.665
Wickr	0.577	0.833	0.5	0.637
Rocket.Chat	0.654	0.583	0.5	0.579
Briar	0.154	0.583	1	0.579
RingChat	0.385	0.292	1	0.559
Threema	0.462	0.688	0.5	0.55
iMessage	0.458	0.167	1	0.542
Element	0.5	0.614	0.5	0.538
Pryvate	0.389	0.667	0.5	0.519
Discord	0.631	0.333	0.5	0.488
Wire	0.77	0.583	0	0.451

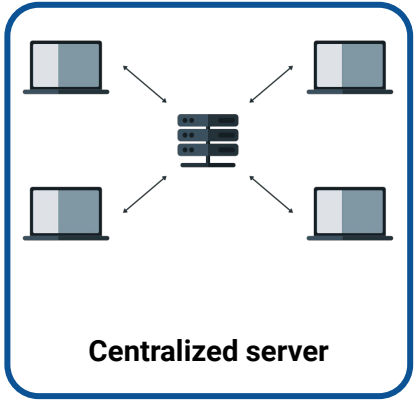
1 - Free; **0** - Not Free

Trade-offs between Features and Security

The analysis demonstrates that the majority of the messengers **cannot provide both convenience and security**. This inability results from the mutually exclusive strategies they use. One of the most important parameters affecting this inability to maximize both security and convenience is file storage. Messengers provide centralised or decentralised (P2P) cloud storage solutions. The second type are considered to be more secure: instead of storing data on centralized servers that can be hacked, they store multiple instances of data on the drives of a decentralized network of other users. Moreover, without a centralized server, there is no single point of failure for P2P systems. There is no one server that can suffer a catastrophic failure, accidentally burn to the ground, or be seized by a third party. Data is stored on the disks of multiple (possibly even hundreds) of people, who may be located all over the world. As demonstrated by the success of the P2P BitTorrent protocol, this makes P2P systems almost impossible to censor, block, or shut down, as there is no central organization which can be pressured or coerced. At the same time, it is the source of the potential disadvantage of exposing IP addresses to remote calling peers. It is worth noting that while P2P networks can offer good performance in terms of throughput, this can come at a cost of latency, due to the fact that file pieces must often be retrieved from the other side of the world — and possibly even over dial-up connections — at substantial performance cost.

A centralized system, on the other hand, allows developers to design systems for maximum performance and provides a level of predictability that is simply not possible with a decentralized system, in which an enormous number of variables (such as the distance between users, each peer's connection speeds, and device capabilities) are outside of anyone's control. Additionally, a centralized system offers many useful features that users of traditional storage platforms take for granted that are very difficult, if not impossible, to implement using a P2P model.

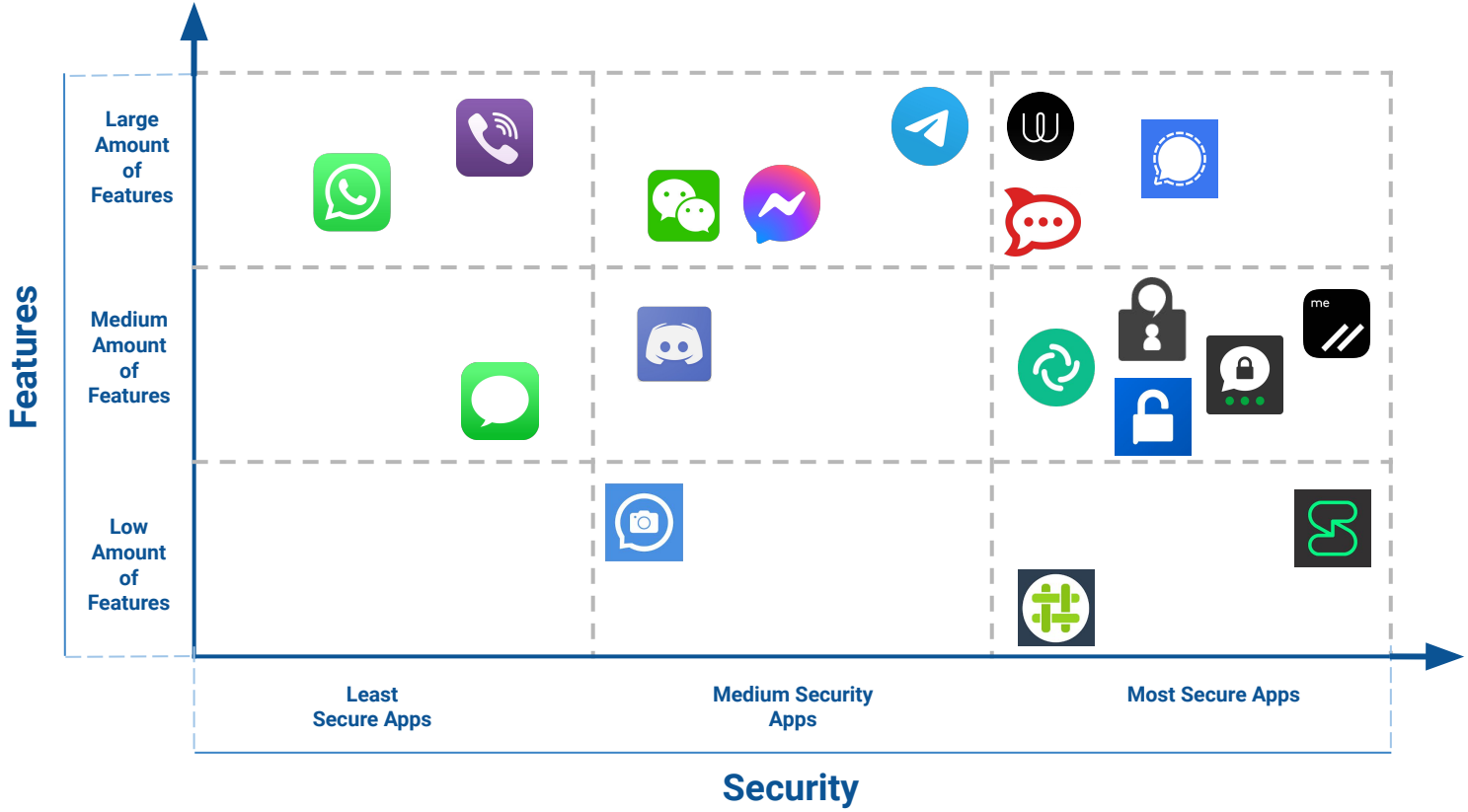




Source: ProtonMail

Trade-offs between Features and Security

- Signal
- Telegram
- Tox
- Viber
- Facebook
- Session
- WhatsApp
- Wickr
- RingChat
- Rocket.Chat
- WeChat
- Briar
- Threema
- Element
- iMessage
- Pryvate
- Discord
- Wire



Operating System, Hardware and Other Issues

While the current analysis focuses on apps themselves, the question of messaging security is also connected with the related but distinct factors of Operating System (OS) and hardware. Without making exhaustive conclusions, it is important to state that using the most secure apps does not guarantee privacy and security as personal data (e.g., Geolocation) may be accessed not only through the apps but through the OS and hardware itself.

Some phone manufacturers offer their own specific messaging services, such as **Apple's iMessage** and **BlackBerry Messenger** (which was later made available for other platforms). Such strategies may be unrewarding in terms of convenience, as they complicate communication between users of different platforms and thus have a significantly lower client base. At the same time, they can benefit from higher security through the integration of hardware, OS, and apps for enhanced security.

One likely trend in terms of future technological developments in secure messaging is an increase in the attention paid towards OS and hardware considerations, to guarantee higher standards of security. This approach was once enhanced by Blackberry (with their phones being used by the highest governmental officials), but did not withstand general market competition with other phone and software manufacturers.

Moreover, sophisticated encryption mechanisms may be useless once the intruder gets physical access to the phone, manages to produce a duplicate of a user's Sim-card by borrowing the phone for some time, or obtains personal information required for verification (such as passwords or personal details).

For example, **Telegram** is a popular messenger used for communication and coordination between protesters, who trust this messengers' privacy policies over others. However, in many cases these policies can be nullified with the ability of security forces to use physical violence, threats, and blackmailing to get access to their phones and Telegram accounts with personal information. As such, the developers of messengers have to consider even such brutal scenarios as those described above, which can be easily overlooked during the initial development process.

The struggle for messaging security may be compared to an evolving race in which both intruders and developers search for increasingly creative solutions for their opposed goals. Even if some messaging tool offers sufficient protection from the majority of privacy threats today, there is a risk that hackers would find new breaches and pose new challenges for developers. And, as mentioned above, those challenges may be both sophisticated and high-tech, or very primitive but still effective.

Source: Norton

Corporate Communication Platforms

	Web Version	Screen Sharing	Screen Recording	Background Blurring	Whiteboard and Drawing Tools	Ease of Use	Max. Conference Participants		Access to Messages After The End of The Conference	Independency From Google Play/AppStore/Microsoft Store	End-to-End Encryption (E2EE)	Open Source	Transparency Report	Free Access to All The Functions	Number of Daily Users (millions)	Total Score
							Total Possible Number	For Free								
Zoom	1	1	1	1	1	1	1000	100	0	1	0.5	1	1	0.5	300	0.857
Microsoft Teams	1	1	1	1	1	0.8	300	100	1	0	1	0	1	0.5	115	0.738
ClickMeeting	1	1	0.5	1	1	0.8	25	25	0	1	0.5	1	N/A	0.5	N/A	0.703
Wickr	1	1	0	0	0	1	50	50	1	1	1	1	1	0.5	N/A	0.675
Skype	1	1	1	1	1	0.9	250	50	1	0	0	0	1	0.5	40	0.636
Rocket.Chat	1	1	0	0	0	0.9	N/A	N/A	1	1	0.5	1	1	0.5	12	0.611
Google Meet	1	1	1	1	0	0.9	250	100	0	0	0	0	1	0.5	100	0.525
Slack	1	1	0	0	0	0.9	15	15	1	1	0	0	1	0.5	12	0.466

0 1

1 - Yes; **0** - No; **0,5** - Partial

Corporate Communication Platforms

Companies in the globalized age look for the best solutions for managing their communication online. The Covid-19 pandemic and lockdowns all over the world has significantly intensified the need for convenient and secure corporate communication platforms.

Zoom, with wide range of features and easy-to-use interface, dominates the sphere of corporate video conferencing, even despite the known presence of several security concerns.

Microsoft Teams and **Google Meet** are the next most popular video conferencing tools. Their main advantage is smooth integration with other services and tools offered by Microsoft and Google.

ClickMeeting is characterized by a wide range of features and high security standards. Nevertheless, except for its free trial, the service requires having a paid subscription. ClickMeeting is mostly used for webinars.

Wickr champions the security scores, but limited usability and paid subscription requirements for teams larger than 10 people make it comparatively unpopular compared to other platforms. At the same time, Wickr serves as a useful illustration of inability to maximize convenience and security simultaneously.

Skype, which once used to dominate the video conferencing sphere, is still one of the most convenient and popular options, despite several security disadvantages.

RocketChat and **Slack** are mostly known as corporate business communication tools. Nevertheless, they also feature built-in video conferencing tools. RocketChat also stands out for its security.

The Case of Clubhouse

Clubhouse is neither a corporate communication platform nor a video conferencing tool. Nevertheless, it became one of the most discussed platforms on social media. Even though the app was only launched in March 2020, it gained significant popularity following Elon Musk's live talk on January 31. The app does not possess any outstanding features (just the opposite, in fact), and all communication within the app happens through voice conferencing.

Nevertheless, the participation of celebrities such as Elon Musk and Mark Zuckerberg, the atmosphere of exclusivity (as participants can join only through invitation by other participants) and the unique voice conference format has made even other platforms (like Facebook and Twitter) consider adopting similar formats.

It is difficult to predict now whether the format of Clubhouse is a short-term fad or a tendency that will have a lasting impact on communication and social media in the future. Nevertheless, this case study demonstrates how rapidly trends may evolve and how social factors still play a crucial role in the popularity of communication platforms and social media.

Source: Vox

Conclusions

The present analysis demonstrated that only a few messengers score high on both features diversity and security. Moreover, the apps that are both secure *and* convenient (such as Wire, Signal, Rocket.Chat, Wickr), rarely become mainstream apps (such as Facebook Messenger, WhatsApp).

Signal has no rival in terms of its Features-Security ratio. Alongside its extra security protocols, it also includes all of the basic messaging tools users are going to need, including read receipts, group chats, and voice and video calls.

Tox is aimed at users with high-security needs, worried about spying and censorship. Everything that passes through Tox is encrypted at both ends with open-source libraries. The program has no central servers that can be raided, shut down or made to hand over data. But it is also an effective instant messaging app in its own right.

Telegram is a cloud solution and cannot be considered "completely secure": Not only are messages not end-to-end encrypted by default, they are permanently stored on a server, where the service provider (or hackers) could read them at any time.

Facebook Messenger enables opt-in end-to-end encryption for secret person-to-person chats, not for groups and not by default. This implies that messages which are not "secret" are at risk of being accessed by more than just users and their chat recipients.

Conversations in **Session** are secured using client-side E2E encryption. Only the sender and the recipient of a message can read it. Once Session is completed and fully developed, it should be extremely secure, very private, anonymous, and generally excellent. However, the product remains at a low developmental stage, and is not yet market ready (i.e., the Onion request system is not yet functional, causing Session to use proxy servers as workarounds).

WhatsApp does apply end-to-end encryption, but user data can still be used for marketing purposes according to their privacy policy, the service is not GDPR-compliant, and it requires both personal data and address-book access, which serve to lower its security.

WeChat is exposed to third-party circumvention due to its known security holes like, for example, a lack of end-to-end encryption. Moreover, all WeChat accounts, no matter how and where they were registered, are subject to constant monitoring by the Chinese government.

Wire received heavy criticism in 2016 for several security issues. While Wire seems to have recovered from most of its security scares, the app still hasn't gained the confidence of users.

Overall, this analysis demonstrates that, despite many advancements in the security of apps, there are not yet any 100% secure messaging apps, although there are many relevant options.

DISCLAIMER

DEEP KNOWLEDGE ANALYTICS

The information and analysis provided in this document were prepared by Deep Knowledge Analytics (DKA). The sources of information contained herein are deemed reliable by DKA, however, DKA makes no representations regarding to the accuracy or completeness of such information. Though the information herein is believed to be reliable and has been obtained from public sources believed to be reliable, we make no representation as to its accuracy or completeness. Hyperlinks to third-party websites in this report are provided for reader convenience only. Opinions, estimates and analyses in this report reflect the opinions of DKA as of the date of this report. DKA has no obligation to update, modify or amend this report or to otherwise notify readers in the event that any topic, opinion, estimate, forecast or analysis set forth herein changes or subsequently becomes inaccurate. This report is provided for informational purposes only.

CONTACT US

www.dka.global
info@dka.global