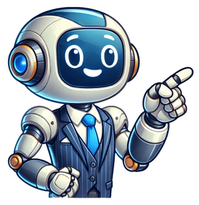
Click to prove you're human



Wire is a well-regarded corporate collaboration suite with secure messaging, group chat capabilities, file-sharing, and the ability to collaborate securely with external clients. In this Wire messenger review, the focus is on the personal secure messaging app. We're going to look at its capabilities, its usability, and its security. We're also going to talk a bit about how the company has shifted its focus from the consumer to the corporate market, and what that might mean for the future of the personal app. Does it still have a future? Is Wire the answer for people who want private and secure communications with other like-minded individuals? I think you'll find this Wire review interesting, so let's get started. End-to-end (E2E) encryption Encryption algorithms: Proteus protocol, WebRTC (DTLS, KASE, SRTP) with PFS Open source Self-destructing messages Published transparency reports GDPR compliant Wire has a free version Registration requires email address or phone number Some logging of personal data Does not support 2FA Small number of Wire users (roughly 500,000) Company focuses on corporate market, not individuals Now we'll briefly examine the features of Wire messenger. Here are some key features to consider when deciding whether Wire is right for you: 100% open source code. The code is available on GitHub. The code was independently audited by X41 D-SEC GmbH. The option to register using a (potentially throw-away) email address offers more privacy than those services that force you to enter a phone number when your create an account. The service is fully GDPR compliant. For personal users this means that your data is protected by strong privacy laws as well as strong encryption. Clients for Android, iOS, macOS, Windows, Linux (experimental), and popular browsers The company behind the Wire app is Wire Swiss GmbH. The company was founded in 2012 by former Skype and Microsoft employees, Jonathan Christensen, Alan Duric and Priidu Zilmer. They launched the Wire app in 2014. One important security milestone came in 2016 when they added end-to-end (E2E) encryption to Wire. Not surprisingly given its name, the company is based in Switzerland, with offices in Berlin and San Francisco. Switzerland is one of the best jurisdictions in the world for any kind of secure online service, so this is a plus. While all user data does flow through the company's network of EU-based servers, the only time messages are stored there is if the recipient is not currently on line. Thanks to the E2E encryption that Wire uses, even messages awaiting transfer to their recipients are encrypted and cannot be read by the company. As soon as a message is delivered to the recipient, it is deleted from company servers. All sent and received messages are stored in encrypted form on your devices. So to answer the original question, all user data is stored locally, in encrypted form, on user devices. Storing all user data encrypted on user devices is a strong security move. Even if someone were to hack the Wire servers, none of your data (except messages waiting to be transferred) would be there to steal. One of the great things about Wire is that they have not only had outside testing done, but that they have published results. In case you are like me and don't have the time/energy/expertise to analyze the open source code that comprises their system, here are some published findings by experts you can review instead. In early 2018, Kudelski Security and X41 D-sec GmbH published the results of security reviews they conducted on Wire the previous year. The reviews identified various problems that the team at Wire resolved according to this Medium post. You can find links to the results of the reviews at the bottom of the Wire Security & Privacy page. While it is great that they did these audits, that was way back in 2017. Hopefully the company will commission another audit soon. In 2016, a researcher in the Cryptography, Security, and Privacy (CrySP) lab at the University of Waterloo analyzed the Wire Security and Privacy white papers in a fairly detailed post that the team at Wire responded to. The post cites several concerns about the implementation of the Wire protocol at the time. It includes responses from Wire, and updates showing that the company had resolved most of the concerns raised in the original post. I like that Wire put the effort into responding to this post and making changes to their system to resolve the issues cited by the researcher. It makes me more confident in the strength of their technology. Note: The original 2016 analysis and the 2018 update were based on the opinions of one of the researchers at the lab. The analysis includes a prominent disclaimer that the opinions expressed in the post do not necessarily reflect the opinions of other CrySP researchers or the university. Apparently the lawyers run amok in Canada too. For purposes of this review, I used the Wire desktop apps for Windows and Linux (an AppImage). I also worked with the browser interface and the Android app. All the versions are very similar, with minor differences depending on the platform. For example, the Android app included phone-specific issues, such as the ability to upload photos from your phone. From the main pricing page, you can see the free version of Wire that is available for download. Click the green Download Now button, and you end up at the Download page where you can download the version that is right for you. From here, installing Wire is just like installing any other app for a particular operating system. You'll need to create a username and password. You'll also need to supply either a phone number or an email address. Using your phone number to create an account is not ideal from a privacy perspective. One way to boost your privacy is to use a throw-away email address, and delete it once you've replied to the Confirmation email Wire sends you. Check out our guide to the best temporary disposable email services or our guide on secure email services that respect your privacy if you decide to register with an email address instead of a phone number. If you are planning to use Wire on a Linux device, you might want to use the AppImage version of the Experimental Binary for Linux. I had trouble getting the Ubuntu binary to run, so switched to the AppImage, which worked perfectly. AppImages install slightly differently than regular Linux apps, but the Wire AppImage installed the same as any other AppImage. Note: If you want instructions on working with AppImages on a Linux system, this It's FOSS guide should get you up and running quickly. As you can see below, the Wire user interface is clean and modern looking. Your contacts appear on the left side of the window, and your current conversation on the right. As part of its security system, Wire clients negotiate new encryption keys for every message. Even if someone somehow figures out the encryption keys used for a single message, those keys will only help decrypt that particular message. The rest of the messages in the conversation will remain secure. Wire provides a simple, clean chat window and works much the same as any other chat app. As far as the basics go, Wire works like any other messaging app. Simply select a person and start a conversation. Wire gives you lots of control over each and every message that appears in a conversation. Select the three-dot icon next to any message and you'll see a menu with a range of options like these: Wire message options. Note the use of the new Dark Mode for the message window. What if you have something to say, but you don't want it preserved for all eternity on your own or someone else's device? Make it a timed message. Find the little stopwatch icon at the bottom of the Wire window (it is circled in red a couple of images back). Click it to see a menu of time delays. Select one of those delays, say 5 minutes. Every message you send while the timed message option is active will automatically disappear from every device where it appears after that amount of time. In addition to plain text messages, you can conduct voice and video chats, attach files, and so on. Everything is protected by end-to-end encryption, keeping your communications secure from outside snoops. To help you keep everything organized, you can: Create groups and communicate by text or voice with the entire group at once. Create folders to hold related contacts. Archive or delete conversations. If you are using the mobile apps you may have additional capabilities, such as creating voice memos, attaching animated GIFs to the conversation, location sharing, or drawing pictures with your finger on your device's touchscreen. Do you ever worry that the person you are talking to in a messaging app is actually an imposter? Wire has you covered there too. You can verify that the current conversation is secure for both messages and voice calls using key fingerprints. The exact steps to follow to verify key fingerprints are found here. Wire publishes mobile apps for both iOS and Android devices. At the time of this Wire review, these messenger apps were getting identical 3.6 out of 5 star ratings in both the Google Play Store and the Apple App Store. Why not a higher rating? Wire gets 3.6 stars on Google Play and 3.5 stars on the Apple App Store. From skimming through the comments at the app stores, it appears that many people are experiencing bugs of various kinds. I've used the Android app a lot and have only one complaint. When I look at key signatures on the phone, the signature text doesn't fit into the space the app gives it. As a result, the bottoms of every character in the keys is cut off. This isn't a major issue, but users in the app stores are reporting more serious bugs, such as the app failing to display alerts, crashing and freezing. Your best bet? Take advantage of the fact that the app is free, and give it a thorough test to see how it works with your device. You can reach the Wire Support & FAQ page from the Resources link at the top of the site. There is a good amount of information here for resolving problems. One drawback is that the information here is oriented toward the business versions of Wire, and not the personal version. Searching for information about a specific feature of the personal version is easy, but much of what you would find by browsing randomly through the topics here will turn up features that don't work on your version. Lots of info here, but most of it is for the paid versions, so may not apply to you. When it comes to support from a real, live human being, Wire (free version) users are pretty much out of luck. Here's the response I received when I sent a couple of questions related to this review: We currently offer limited support to our Wire Personal users. We are sorry for any inconvenience this may cause. Due to limited resources we can only fully serve Wire Pro users and help with very urgent or security-related tickets from Personal users. Please search our extensive Support site for frequently asked questions. Even though we cannot respond to every ticket, we take notice of all issues, feature requests, and any other feedback you share. The rest of the message consisted of links to articles from the Support site which might have been helpful. While I can understand the company's desire to focus on helping paying customers rather than those using a free version, it does illustrate how individual users are a low priority. Wire has strong security. The Proteus protocol they use to encrypt text and images is based on the encryption approach used in the Signal app. Without getting into the technical details, Proteus uses the Curve25519, ChaCha20, and HMAC-SHA256 algorithms. Voice and video communications use WebRTC with Perfect Forward Secrecy (PFS). All communications are end-to-end encrypted. Perhaps it is no coincidence that on September 21, 2019, Edward Snowden recommended people avoid using any email service and instead use Wire or Signal. Edward Snowden recommends abandoning email for any meaningful communication and using Wire or Signal instead. The privacy situation with Wire is a little less clear. The service collects some information in logs, which they says they keep for 72 hours (maximum). What exactly they collect isn't clear to me. According to a February 2018 report by the CrySP team at the University of Waterloo, Wire, "…does not attempt to hide metadata, other than the central server promising not to log very much information." As an update to that report, however, CrySP noted the following: After our original post, Wire updated their calling protocol to add end-to-end authentication and constant bitrate encoding. The server code was also released. This page now reflects the current state of the protocol. For our original post, including Wire's original response, see the archived version. – CrySP report on Wire A May 2017 article on Vice.com reported that Wire keeps an unencrypted list of everyone you have ever contacted using the service, along their email address or telephone number, for as long as your account exists. This isn't surprising for a service that focuses on the corporate market rather than individual users. Corporate buyers want security against outside threats, but also want some level of visibility into who their users are communicating with and access to their accounts when needed. These issues mean that you need to have a certain level of trust in Wire to protect your metadata and password. Paid Wire plans pack in a lot of features that aren't available in the free version of Wire: Group Messaging Video and audio calls with more users than the personal plan supports Guest Rooms Member roles On-premises and private cloud capabilities Wire is truly a team collaboration tool. For a full view of the features packed into the Wire business-oriented plans, see the Pricing page. As you've already seen, Wire is a free service. We have seen past rumors that Wire will be converting the personal plan to a freemium model at some point, but for now, it is 100% free of charge. The pricing page on the site addresses only Wire Pro (4 euros per user per month billed biennially), Wire Enterprise (8 euros per user per month billed biennially), and Wire Enterprise Technology. Having tested out the Pro and Personal versions, I can see that the free plan can likely meet most of your needs. While the team collaboration features are limited, you can always upgrade to Pro if necessary. The free version of Wire has a lot going for it as a secure messaging app. The messaging service is strong and secure, with the personal edition of Wire riding on the business-oriented paid services. In September of 2019, it even got mentioned by Edward Snowden as one of two secure messaging services that he recommends for meaningful communication. However, the future of Wire (as a free tool for the masses) is less clear. Beginning in late 2017, Wire Swiss GmbH started moving more and more toward a corporate focus, and away from worrying about individual users. Then it was announced (in November 2019) that in February 2019 Wire had raised $8.2 million from Morpheus Ventures and moved its holding company to the United States. This triggered outrage from many privacy advocates, including Mr. Snowden, who tweeted, "Wire was always for profit and planned to follow the typical venture backed route." [@Wire CEO] Brogger… describes individual consumers as "not part of our strategy." This is a grim turn for a once-promising app, and a window for@Signalapp to exploit. At the moment, Wire is a great secure messaging app for individuals. The Wire messaging service is secure, with independent reviews stating that the service is sound. While it does have some drawbacks, we do consider it to be one of the best alternatives to WhatsApp. While I like and regularly use Wire myself, you may want to think about the tradeoffs between security and privacy before settling on Wire as your messaging app of the future. Other secure messenger reviews on CyberInsider: This Wire messenger review was last updated on January 17, 2025. Stay informed with news, product updates, and thought leadership on privacy, security, and collaboration trends. Wire makes end-to-end encrypted messaging easy, with attractive, minimalistic free apps for all your devices. If you need a free and secure app with a pain-free setup for your family's group chat, Wire is worth considering. However, if you're seeking an audience or searching for new friends, Wire is not the app for you, as it lacks discoverability features. Signal is our Editors' Choice winner for private messaging apps because it blends trustworthy security with entertainment-focused group calling and chatting features.How Much Does Wire Cost?I tested the free version of the app, which includes calls, file sharing, and messaging for up to eight devices. You can create three accounts per device, which is very helpful, especially for people who (rightfully) want to separate their personal and work chats.There's also an unadvertised free tier called Teams, which Wire's in-app messaging says is intended for small businesses or personal use. A Teams account allows you to use some of the app's Discord-like features, such as creating public and private group chat channels and participating in large-scale group chats and calls. You can't initiate group calls, though. That's a feature reserved for paid customers.Wire is a business-first platform, so there are no paid personal account options. Wire for Enterprise is €7.45 (approximately $8.53 as of this writing) per person per month, paid annually. It adds audio and video conferencing capabilities for up to 150 participants, single sign-on integration, and admin controls that include call moderation tools.Can You Trust Wire?Wire isn't run by a not-for-profit organization like Signal, and it's not a community project like Briar. Instead, the app is from a company headquartered in Germany and a development team based in Switzerland. Wire uses decentralized servers for messages. Encryption is turned on by default, and the app collects and stores very little information about its customers. Wire stores your conversations, including any text, photos, and any files you share or receive, on your device, which is ideal. When you sign up, you need to provide an email address, and the app will access your contact list and store usage data, which isn't unusual. I do wish there were a way to sign up for the app anonymously, as you can with Briar.Download the app and choose to create a Personal account if you are not planning to sign up for Wire's paid plan. After signing up for a Wire account, you must click or tap to agree to the terms and conditions and note that you've read the privacy policy. We always recommend taking a few extra minutes to scan these documents to find out how companies collect, share, or store your personal data. I even put together a cheat sheet for quickly reading a privacy policy. (Credit: Wire/PCMag)Before you can use the app, Wire requires you to accept its terms of service (TOS). I appreciate that the company kept its privacy policy to just a few easy-to-read paragraphs, which clearly state that your conversations belong to you. The TOS is also presented in summary form and states that the messaging service is not ad-supported, so your personal conversations and other data will not be rented, sold, or used for third-party advertising. The company collects hashed contact information from your device's address book to find other people to chat with. You can read the full privacy policy here.Private Messaging With WireWire is available for Android, F-Droid, iOS, Linux, macOS, and Windows, and offers web apps for Chrome, Edge, and Firefox. I tested Wire using an iPhone 16, a Samsung A71 5G, a desktop computer running Windows 11, and the Google Chrome browser.As noted above, Wire requires an email address to sign up and asks you to provide a name. After providing these things, you can create a password and username for the account. If so inclined, you can always falsify your name, so that's not a big problem. The app also asks permission to share anonymized data with Wire during signup. You can decline this option without penalty.Unlike Briar and Session, Wire does not block in-app screenshots for all parties. In the Settings menu of the Android app, you can turn on an option to censor screenshots, but it only blocks your in-app screenshots on the Android device. In other words, the screenshot censor setting prevented me from taking screenshots of my own screen during a video call, but since the person I called, who was using an iPhone, could take screenshots of the call, the setting is not effective or particularly useful. A screenshot warning notification would be helpful here if blocking screenshots for all parties is impossible.(Credit: Wire/PCMag)I like that you can back up or restore conversations via the Settings menu. This is a good option if you regularly clear your conversations but still want to keep records of your discussions on your computer or a portable storage device. The Settings menu is also where you can remove devices you don't recognize from your account.SpamI didn't see obvious scam, spam, or troll accounts while using Wire. During the testing period, I received a few chat requests from strangers, but when I tapped the Ignore button, those requests disappeared without needing further engagement, which is ideal.TextingTo start chatting, tap the blue button at the bottom of the window and search for a friend's username. After the person accepts your connection request, you can begin chatting with them. Unlike Telegram or WhatsApp, which have location-based discoverability or semi-public interactivity areas for talking with strangers or cultivating an audience, Wire only lets you search for friends' usernames. It's a good way to ensure more privacy on the platform.The user interface is clean and minimal. Long-pressing on a message allows you to react using emoji, much like iMessage. Tapping on the plus sign reveals settings for text formatting, a sketch pad where you can draw pictures for your friends, a timer for creating self-deleting messages, and file-sharing options. You can also share your location and audio or videos from this menu. (Credit: Wire/PCMag)If you're someone whose friends and family are scattered across various messaging apps, Wire has a helpful feature to help you keep those conversations going. You can ping someone to get them to open the app and see your message. Ping carefully, because it sends a push notification to the person you're chatting with. If you get too many pings, tap on the offending chat partner's username. Android owners can change the types of notifications they receive from that conversation, and iOS users can mute the conversation completely.Group ChatsI had no difficulty establishing communication between an iPhone and a person chatting on Wire via the web app using Google Chrome. An Android to iOS connection also worked well. In a group chat with an Android user, a person on an iPhone, and me on the web app, our conversation was seamless between platforms. If you want to add more people to your group chat, there's plenty of room: Wire lets you include up to 500 people in a chat with a free plan and up to 2000 with the paid business plan. As mentioned earlier in the review, if you agree to convert your free personal account into a free Teams account, you can participate in large group calls and chats. Converting your account is irreversible; you'll lose your old username but keep your conversations. However, you cannot initiate group calls with a Teams account, which makes converting to a Teams account less appealing. (Credit: Wire/PCMag)To add more people to your chat, tap out of your current conversation. Start a new group chat by adding your friends' names to a new conversation. If a person joins the group a bit late, you'll need to catch them up on the topics discussed because Wire does not keep a log of the chat. Video CallsTo start a video call, tap the camera icon at the top right corner of your conversation window. Remember that you can't do this with a group chat unless you pay for the paid enterprise version of Wire. Almost every other messaging app I've reviewed with functioning video-calling features allows conference calls for free customers, so this is a surprising restriction. (Credit: Wire/PCMag)For this portion of the test, I staged a call between an Android phone and an iPhone. The video quality was clear, but the iOS version of the app indicated that the connection was poor, despite the devices being in the same room. Video calls are very straightforward, and you can minimize or hide the call to continue typing in chat windows on the app.