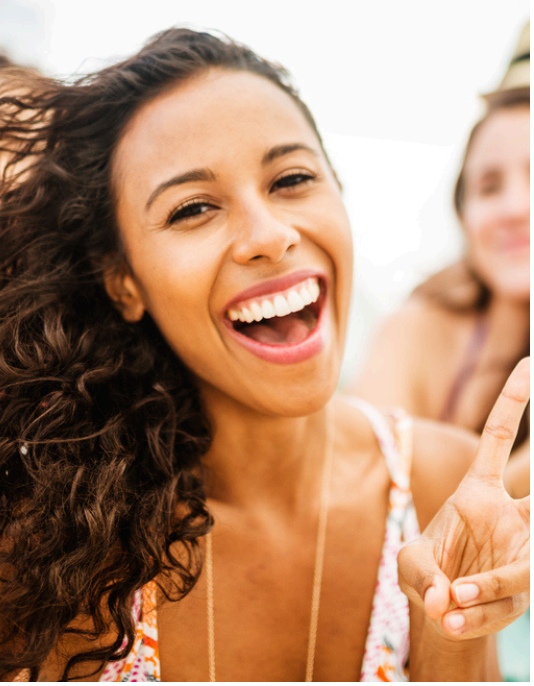
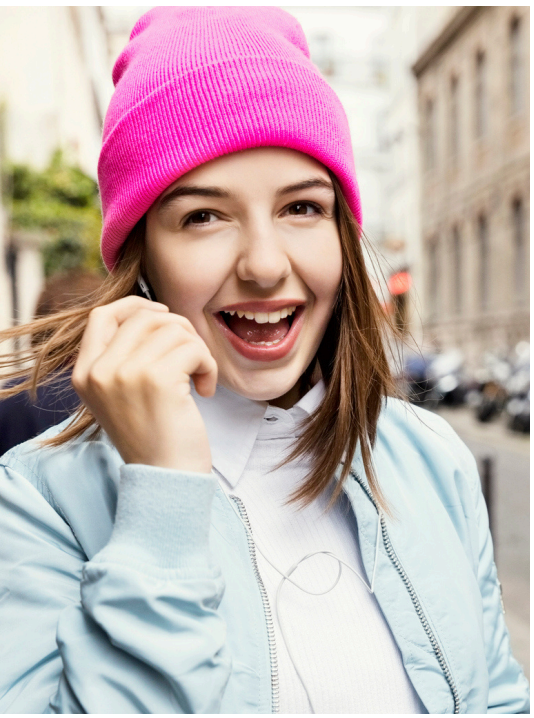
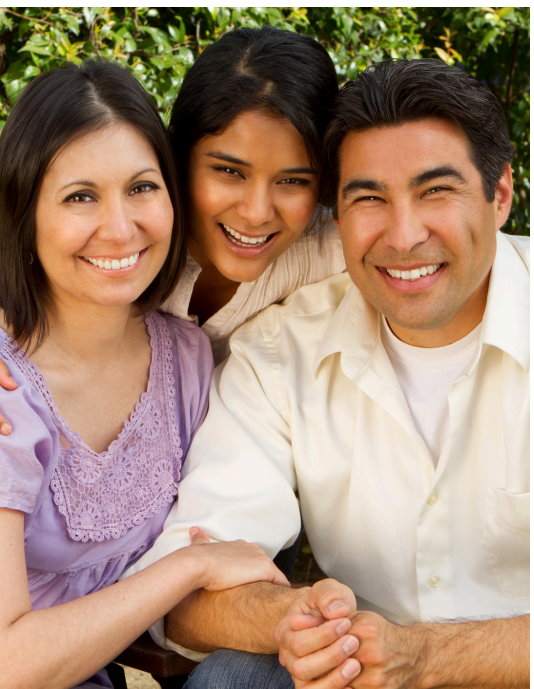






ConnectSafely

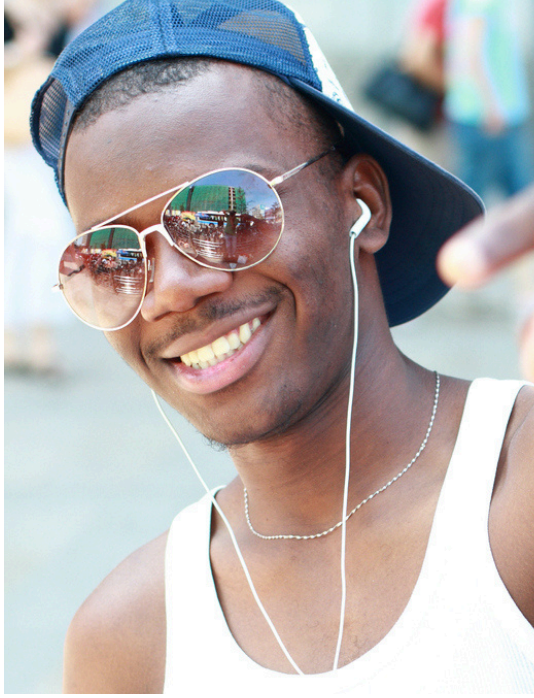
FAMILY GUIDE TO

Messenger

BY FACEBOOK

- Advice for Parents, by Parents
- Getting Started with Messenger
- How to Talk to Your Teens about Privacy
- Protections for Minors
- What You Should Know About Vanish Mode

What's Inside

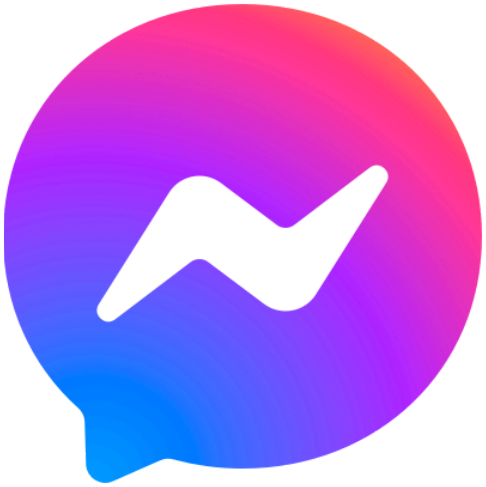


For more info, visit ConnectSafely.org/Messenger

GO

Join ConnectSafely on social

CONNECT



Messenger, which is both a mobile and desktop messaging app from Facebook and a feature built-into Facebook's desktop (web) platform,

allows you to exchange messages, watch videos with friends, and engage in group video or text chats complete with fun themes and animated effects. Messenger can also exchange messages, videos and images with Instagram and Facebook. This guide covers Messenger's safety and privacy features including those that apply when exchanging messages between Messenger and Instagram.

Safety & Privacy Features

Messenger has several features to put you in control of your privacy, safety and security. These include blocking, ignoring, reporting, media blurring in message requests, two-factor authentication, login alerts, vanishing messages, safety notices and opt-in "secret conversations" that offer end-to-end encryption.

Messaging vs. Posting

Messenger provides a more private alternative to social networking. Instead of posts that reach a potentially large audience, Messenger is a way for people to exchange ideas, videos and other media with friends, loved ones, classmates and colleagues in a way that encourages back and forth conversations without involving members of the public or friends that may not be appropriate for that conversation. It doesn't take the place of social networking but offers a more private way to interact.

Who Can Message You

You will only receive messages from people you're connected to. All other messages will appear in Message Requests, and any media in the message request folder will be blurred until you accept the message. Weblinks from unknown contacts are disabled for your protection.

Messenger Stories

Messenger Stories consist of photos and videos that appear at the top of both your Messenger Inbox and at the top of your Facebook News Feed for 24 hours. These stories can be shared with Facebook friends and Messenger connections.

Blocking

Blocking a person in the Messenger app means that they can no longer message you on either Messenger or Facebook. The person will not be notified that you've blocked them, and you can always unblock them.

Blocking messages is not the same as blocking profiles on Facebook. Blocking only affects another person's ability to message you on Messenger, Facebook or Instagram. For example, if you block someone's messages in Messenger but don't block their profile on Facebook, you may still see their Facebook profile and posts and, depending on their and your audience settings, they may still be able to see, react and comment on your posts.

Reporting

Messenger gives you the option to report a conversation that may be violating the company's community standards by harassing you, sending you inappropriate content or otherwise making you feel uncomfortable. The person will not be notified that they have been reported and Facebook will decide if it violates their rules. If so, they will take action that could include disabling the person's account or limiting their ability to send messages.

Prohibited activities include bullying, impersonation, serious threats of harm, and content that threatens or promotes sexual violence or exploitation.

For more info about reporting, visit Facebook.com/help

Blocking a person in Messenger means that they can no longer message you on either Messenger or Facebook.

Enhanced Protection for Minors

Messenger has additional protections for 13- to 17-year-olds, including limiting who can message them and how they can be found in search. The company says that it also uses “machine learning to detect and disable accounts who are engaging in inappropriate interactions with children.” Facebook also provides in-app education for users under 18 “to be cautious when interacting with an adult they may not know.” Minors and adults may see safety notices pop up to help people spot suspicious activity and “take action to block or ignore someone when something doesn’t seem right.”

Security Tools

Messenger has several important security tools to protect you and your information. Some of these, like Secret Conversations, two-factor authentication and App Lock, require opt-in by users, while others, like Facebook’s use of AI to detect and block phishing, scams and other harmful activities, run behind the scenes.

Secret Conversations

Messenger allows you to conduct one-on-one chats with another person through “Secret Conversations,” which are end-to-end encrypted so that even if they are intercepted, the content will be hidden from anyone besides you and the intended recipient. Secret Conversations can include messages, pictures, stickers, videos and voice recordings but can not be used for group messages, gifs, voice or video calls or payments.

Vanish Mode

Facebook now has a “vanish mode” on Messenger and Instagram, enabling users to send messages that disappear once they are viewed and the sender leaves the conversation.

For more on privacy, visit Messenger.com/privacy

GO

The feature, which only works on mobile devices (not the web), can be turned on by swiping up on your mobile device while in an existing chat thread. (To exit vanish mode, swipe up again.) If one person enters vanish mode, the recipient will be notified. Leaving a chat makes the messages you sent in vanish mode disappear, but if the other person hasn't viewed them yet, they'll be able to see them once they open the chat. If they never open the chat, the sent messages get deleted after 14 days. Vanish mode only works in one-to-one conversations, not group chats. And unlike regular (non-vanishing) chats, vanish mode does not work across apps so both of you have to be on Messenger or Instagram to access it. Vanishing conversations can be reported up to one hour after they disappear.

Two-Factor Authentication

Two-factor authentication is an added layer of security that can protect you even if a hacker has gotten access to your password. While there are no technologies that can protect you from 100% of all threats, dual-factor authentication can thwart most attackers.

Once it's turned on, you will be required to enter a code or take an additional action every time you log-in from a new device or browser. Two Factor Authentication works at the Facebook account level so you only need to turn it on once to cover anywhere you log in with Facebook, including Messenger.

Codes are typically sent as text messages but there are other options. Another may be to approve a login from a device that is already logged into Facebook and there are third-party apps and devices (such as physical keys) that can be used to authenticate you.

Vanish mode can be turned on by swiping up on your mobile device in an existing chat thread

For more info about kids & privacy, visit ConnectSafely.org/privacy

App Lock

App Lock, in privacy settings, requires you to use your PIN, fingerprint or facial recognition each time you use the app. It's a way to keep someone who is borrowing your phone (with or without permission) from reading your messages or sending messages in your name.

Messenger vs. Messenger Kids

Messenger, along with Facebook and Instagram, is for people 13 and older. Facebook also offers Messenger Kids, designed for younger children, with tools that give parents the ability to monitor and guide their child's experience, including who they can communicate with.

Closing Thoughts for Parents

Safety, security and privacy are shared responsibilities between companies, parents and — of course — our children. While companies like Facebook can build safety tools and try to enforce their rules, they can't guarantee safety any more than automakers can guarantee that air bags will prevent injuries in case of an accident. Children, and adults too, need to understand how to protect our own privacy, safety and security with good and secure passwords and other security practices as well as what we post — not being mean, not sharing false information and trying to avoid interacting with people who are mean or who have bad intentions. For families, it starts with conversations — not a lecture or an inquisition, but frank discussions about how we can all do our part to protect ourselves and our families and make these services better for everyone.

Facebook also offers Messenger Kids, designed for younger children, with tools for parents

For more info about Messenger Kids, visit messengerkids.com

About ConnectSafely

ConnectSafely is a Silicon Valley, California-based nonprofit organization dedicated to educating users of connected technology about safety, privacy and security. We publish research-based safety tips, parents' guidebooks, advice, news and commentary on all aspects of tech use and policy.