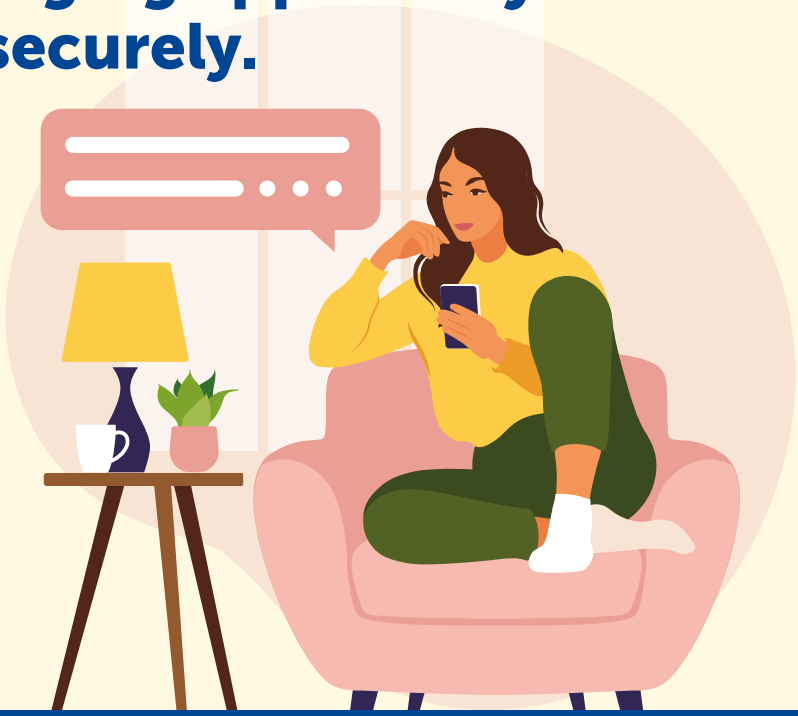
Using WhatsApp & other messaging apps safely and securely.



As well as being private spaces for chatting and sharing, messaging apps are widely used as social media platforms in their own right. But unlike Facebook, Instagram, X and LinkedIn, communications are completely 'closed' between senders and recipients, so they can be used to chat or share confidentially with individuals or groups. There are, however, risks to using any messaging app.

GET SAFE ONLINE .org ®

www.getsafeonline.org

We have listed information of some the most popular messaging apps below. They all enable secure messaging, voice calls, video calls and file sharing.

WhatsApp

- Requires your phone number to log in.
- Messages, voice and video calls are end-to-end encrypted, by default. If your message or call is confidential, confirm encryption via the 'Verify Security Code' screen (QR code and 60-digit number) in the contact info screen.
- Selectable two-factor authentication and session management for account security.
- Note that messages are not stored on WhatsApp servers after being delivered to the recipient. If undelivered, messages are automatically deleted from the server after 30 days.
- WhatsApp is owned by Meta, and allows data sharing between the two, in certain countries.

Snapchat

- Requires your username and password, or face/fingerprint, to log in.
- Provides end-to-end encryption for photos and videos ('snaps') but not for text messages or chat.
- Selectable two-factor authentication and session management for account security.
- Includes privacy and safety features for under-18s including reporting, blocking and the ability to turn off location.
- Direct chats vanish after viewing.
- Ghost Mode lets you appear to be offline, even when you are online.
- Automatically collects and shares user data with third parties.

Telegram

- Requires your phone number to log in.
- End-to-end encryption is not enabled by default. User has to select 'secret chat' feature to enable it. Secret Chat also ensures no forwarding of messages and that chat data is not saved on Telegram servers.
- Selectable two-factor authentication for account security.
- Self-destruct timer can delete confidential texts and media within a pre-set time limit.
- Choose to log out of other sessions from the device currently being used, ensuring security if any device on which the app is open is lost or stolen.
- Account can be set up to self-destruct after one, three, six or 12 months of inactivity.

Signal

- Requires your phone number to log in.
- Every message and call is end-to-end encrypted.
- Selectable two-factor authentication for account security.
- Messages may be viewed only by the sender and recipient and not by the company behind the Signal platform. Signal also enables voice calls, group messages and encrypted video calls.
- You can specify erasure of sent and received messages after a selected amount of time.
- Signal stores only the metadata required for the app's operation, such as phone number, random keys and profile info.
- Regarded by cybersecurity experts as one of the most secure messaging apps.

Wickr

- Requires your username and password, or face/fingerprint, to log in.
- Every message and call is end-to-end encrypted.
- No email address, device details or phone numbers are visible to the company behind the platform.
- If somebody takes a screenshot of your messages, you will be notified automatically. This also means that anybody *messaging you* will be notified if you have taken a screenshot.
- When using Wickr on iOS (Apple) devices, you can block third party keyboards to protect your information being recorded whilst being entered into the app.
- Wickr automatically periodically ensures that already-deleted files cannot be recovered. You may also do this manually if you choose to.
- Wickr is owned by Amazon Web Services, but claims that no user-identifying information related to the use of your Wickr app is shared.

Want to find out quickly and easily whether a messsage, email or website is an attempt to defraud you? Just Ask Silver, the clever new AI powered fraud detection tool. Find it on the Get Safe Online website.

Ask Silver

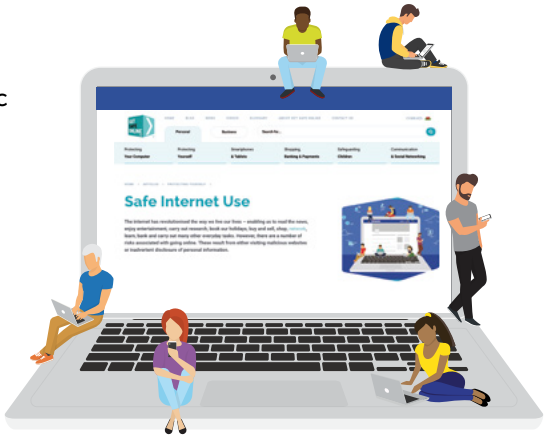
#MessagingApps

Your top safety tips for using messaging apps

- Use strong passwords that are unique to your messaging platform.
- Always enable 2FA (two-factor authentication) to add an extra layer of security.
- Avoid problems by always being careful to select individuals or groups you actually intend to chat, message or share with.
- Be aware of what you share, especially information or opinions which could prove harmful to others or yourself.
- Be wary of attempts at fraud, such as:
  - Requests for money or confidential information (like bank account details) from fraudsters posing as your family members or friends. They often gain your trust beforehand by claiming they've changed their phone number. Always call on the number you have stored to check in person.
  - Messages which contain malicious links to fraudulent websites or malware.
  - Messages claiming to be from the app's support team, requesting your login details or verification code.
- Be aware that the companies who own messaging apps store and can share your personal information and usage data.

Get Safe Online

Get Safe Online is the UK's leading source of information and advice on online safety and security, for the public and small businesses. It is a not-for-profit, public/private sector partnership backed by law enforcement agencies and leading organisations in internet security, banking and retail.



For more information and expert, easy-to-follow, impartial advice on safeguarding yourself, your family, finances, devices and workplace, visit **www.getsafeonline.org**

If you think you have been a victim of fraud, report it to **Action Fraud** at **actionfraud.police.uk** or by calling **0300 123 2040**. If you are in Scotland, contact **Police Scotland** on **101**.

GET SAFE ONLINE .org

www.getsafeonline.org

OFFICIAL PARTNERS

airbnb · BARCLAYS · barclaycard · UK International Development (Partnership | Progress | Prosperity) · ARMY BE THE BEST · LLOYDS · HALIFAX · BANK OF SCOTLAND · viagogo · Llywodraeth Cymru Welsh Government · CITY OF LONDON POLICE (National Policing Lead For Fraud) · NPCC (National Police Chiefs' Council) · NATIONAL TRADING STANDARDS (Protecting Consumers Safeguarding Businesses) · cifas (Fighting Economic Crime Together) · TAKE FIVE TO STOP FRAUD · neighbourhood ALERT · ActionFraud (National Fraud & Cyber Crime Reporting Centre actionfraud.police.uk) · METROPOLITAN POLICE · VS VICTIM SUPPORT · NEIGHBOURHOOD WATCH · Ofcom