

Testing checklist: dating app

Source: <https://howtotestaproduct.com/how-to-test/dating-app/>

Generated: 2026-10-07. Licence: CC BY 4.0.

☐ 1. release smoke tests

Done when: On the release build, a new member verifies a phone number, completes a profile with a photo, gets a match, sends a first message, and reports and blocks the match.

Risks: store-rejection. Tool class: mobile automation. Usually run by: QA engineer.

☐ 2. end-to-end functional tests

Done when: A profile reported by members for asking for money is hidden from discovery, and its pending likes and messages stop reaching other members.

Risks: fraud-abuse, store-rejection. Tool class: mobile automation. Usually run by: QA engineer.

☐ 3. penetration testing

Done when: A tester with a second account cannot read another member's private photos, exact location or messages, and cannot create profiles in bulk through the API.

Risks: data-breach, fraud-abuse. Tool class: proxy. Usually run by: security specialist.

☐ 4. exploratory testing

Done when: A tester posing as a scammer tries to move a match to an outside payment or chat channel, and the app warns the other member or blocks the attempt as the written rules say.

Risks: fraud-abuse. Tool class: test management. Usually run by: QA engineer.

☐ 5. payment and money-flow testing

Done when: A sandbox premium purchase, renewal, refund and bank dispute each leave the member's premium status and charge history matching the store receipt.

Risks: money-loss. Tool class: API client. Usually run by: QA engineer.

☐ 6. compliance checks

Done when: A reviewer confirms report and block exist on every profile and chat screen, and that no location or orientation data leaves the device before the consent screen is accepted.

Risks: store-rejection, regulatory-penalty. Tool class: test management. Usually run by: product manager.

☐ 7. analytics and event tracking tests

Done when: A network capture from first launch to first match shows no GPS coordinates, gender preference or orientation field sent to any ad or analytics domain before consent.

Risks: regulatory-penalty. Tool class: proxy. Usually run by: QA engineer.

☐ 8. security scanning

Done when: The scan report shows no open finding on profile, photo, location and message endpoints.

Risks: data-breach. Tool class: DAST scanner. Usually run by: security specialist.

☐ 9. data integrity and migration testing

Done when: After a member deletes the account, a support lookup finds no profile, photos or messages, and matched members no longer see the chat.

Risks: data-breach. Tool class: data validation. Usually run by: developer.