LOOK-ALIKE ICON AND SECURITY DISCLOSURE WARNING · AUTHENTICATION AND SECURITY

Google Authenticator's look. A different developer's password vault.

Authenticator:2FA Login Codes imitates Google Authenticator's multicolour, six-spoke icon while being sold by Mubashir Iqbal and linked to LowByte's Pakistan-based studio network. It invites users to store login codes and passwords, but links to broad policies with conflicting data claims; the investigation traces two related Google Play publisher identities and a website-linked Apple account.

By Alex Kleber · Published 2026-11-03 · Updated 2026-11-03

VISUAL EVIDENCE

Four store icons show the same borrowed visual identity

Original icons from both stores: the investigated Mac app and related LowByte Android app, beside official Google Authenticator on Apple's App Store and Google Play. The LowByte designs use the same four-colour, six-spoke motif with glossy arms and a white central star; the Mac version adds sparkles. Google's originals use flat colour shapes. The Mac and Android products have different publishers on their listings, linked by LowByte's legal/support infrastructure.

Investigated — Mac App Store



Original icon for Authenticator:2FA Login Codes, seller Mubashir Iqbal, app 6807766127. Apple CDN, retrieved 3 November 2026. E2/E6.

Related — Google Play



Original Google Play icon for Authenticator App: Secure OTP, LOWBYTE STUDIO (SMC-PRIVATE) LIMITED; com.lowbyte.authenticatorapp. Retrieved 3 November 2026. E12.

Official Google — App Store



Original Google Authenticator icon, seller Google LLC, app 388497605. Apple CDN, retrieved 3 November 2026. E7.

Official Google — Google Play

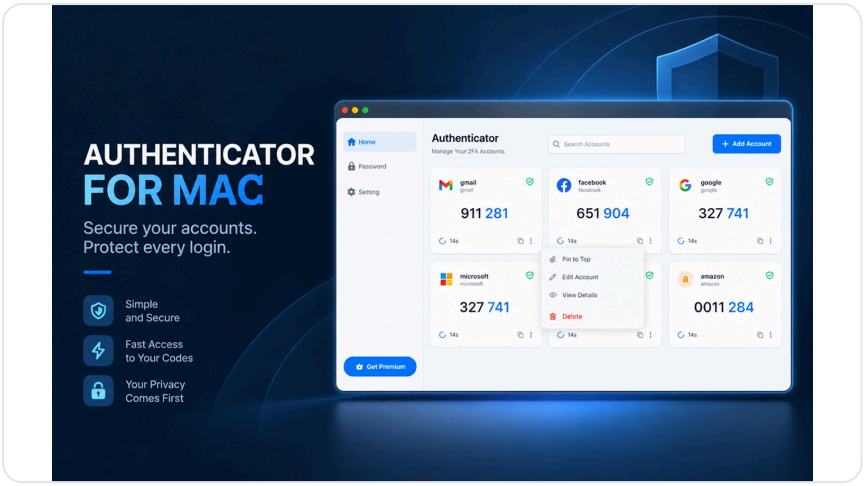


Original Google Play icon, Google LLC; com.google.android.apps.authenticator2. Retrieved 3 November 2026. E26.

LOOK FOR YOURSELF

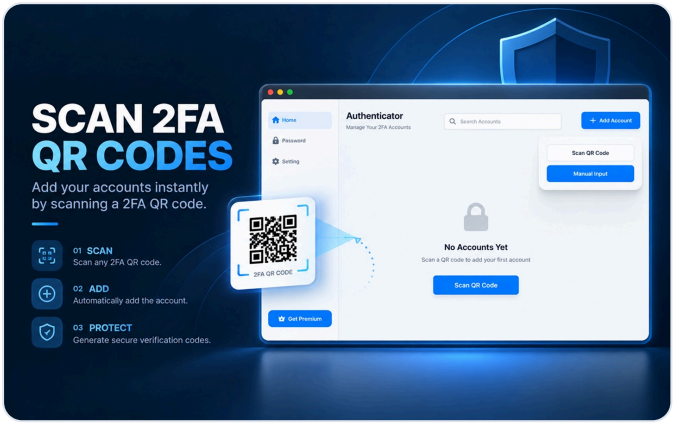
The screenshots tell the story.

All five original current Mac promotional images are preserved. The fifth advertises cloud backup but visibly describes launching when Windows starts. These are the seller's public claims and images, not results of installing or testing the software.

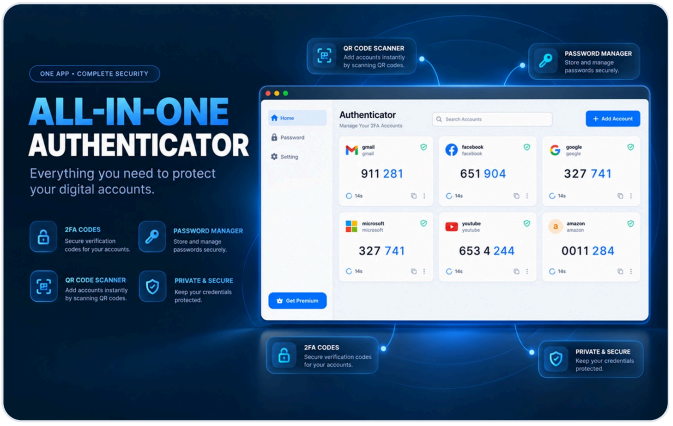


Original Apple-hosted Mac promotion 1. Authenticator for Mac: login-code dashboard and privacy/security claims. E2/E6; also source PDF page 4.

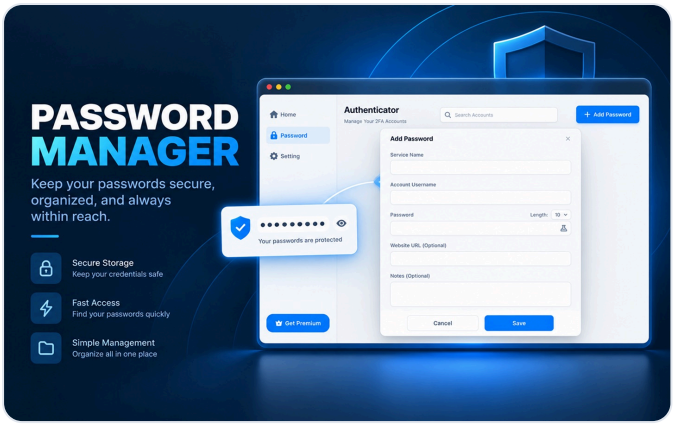
▼ See all 4 additional screenshots



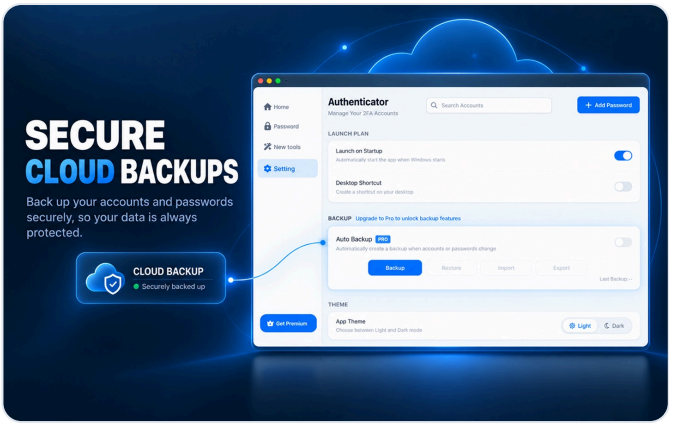
Original Apple-hosted Mac promotion 2. Scan 2FA QR Codes: advertised account setup. E2/E6; also source PDF page 4.



Original Apple-hosted Mac promotion 3. All-in-one Authenticator: advertised management controls. E2/E6; also source PDF page 4.



Original Apple-hosted Mac promotion 4. Password Manager: advertised credential vault. E2/E6; also source PDF page 4.



Original Apple-hosted Mac promotion 5. Secure Cloud Backups: advertised account/password backup; pictured startup setting refers to Windows. E2/E6; also source PDF page 4.

WHAT YOU NEED TO KNOW

A Google Authenticator look-alike is being used to market a separate security app whose linked policies do not clearly explain protection of login secrets and cloud backups.

01

The icon borrows Google Authenticator's recognisable design

The same six-spoke motif and four-colour palette are reworked with glossy arms, a central star and sparkles. Google's visual-identity guidance specifically addresses imitation of product icons and distinctive colour combinations.

Original source pages and independent public checks, 3 November 2026.

E2 E6 E7 E19

02

The app asks for especially sensitive trust

The listing promotes a password vault and cloud backup, while linked policies give broad, conflicting explanations and fail to describe protection of authentication secrets. The fifth Mac advertisement also contains Windows startup wording.

Original source pages and independent public checks, 3 November 2026.

E2 E8 E9 E10

03

The developer is connected to a wider studio network

Apple's Mubashir Iqbal listing links LowByte's company policy; a related Android authenticator uses that exact policy. Another Play publisher links the Google Sites policy, and the studio homepage points to its games and BAYBEEBRAIN Apple account.

Original source pages and independent public checks, 3 November 2026.

E5 E8 E9 E11 E12 E14 E16 E17

WHAT IT COSTS

A $99.99 lifetime offer and two unspecified premium periods

The US listing identifies one purchase as lifetime. The other two premium labels do not identify their billing periods in the public table. No weekly, monthly or yearly period is assigned to those two prices.

Prices displayed in the saved listing

Purchase option	United States	Germany / Ireland
Authenticator premium lifetime	$99.99	€99.99
Authenticator premium — higher price	$29.99	€34.99
Authenticator premium — lower price	$4.99	€5.99

WHO IS BEHIND IT?

The name on the listing.

App name

Authenticator:2FA Login Codes

Developer / seller

Mubashir Iqbal

Developer country · App ID 6807766127

Pakistan · Connected studio operating-country attribution. The Mac app links the same company privacy URL and support domain used by the Pakistan-declared Google Play company. This is not an Apple trader-country declaration or independent verification of the individual seller's residence. The website's Wyoming LLC identity is recorded separately.

Connected LowByte studio business sources, checked 3 November 2026: Google Play company panel declares Rawalpindi, Pakistan (E12); related publisher panel also declares Pakistan (E14); homepage-linked studio profile describes Islamabad operations (E22).

App Store listing ↗

▼ App ID, version and other identifiers

App Store ID

6807766127

Bundle identifier

com.lbs.macauthenticator

Version

1.0 — released 28 September 2026 (UTC)

First released

28 September 2026

A Google-like security identity, without Google as seller

The investigated icon closely imitates Google Authenticator's recognisable multicolour asterisk. Both have six rounded spokes arranged around a central crossing, with the green, yellow, blue and red palette on a white tile. The new design adds glossy bevels, a white central star and sparkles, while rotating the arrangement and changing how the colours overlap.

App Scam DB assesses the overall presentation as a look-alike branding warning. The app is called Authenticator:2FA Login Codes, not Google Authenticator, and its subtitle is Two Factor Authentication, OTP. Authenticator is a descriptive product term; the specific concern is the recognisable visual borrowing in the same security category. Service icons such as Gmail or Facebook inside account cards can identify supported accounts and do not by themselves prove impersonation.

Google's guidance prohibits imitation of its visual identity, including distinctive colour combinations and product icons, and forbids implying an affiliation that does not exist. The observed artwork raises an apparent brand-use concern under that guidance. No Google permission, affiliation, enforcement decision or legal infringement judgment was established.

The official comparison is Google LLC's iPhone/iPad app, ID 388497605. The investigated Mac product is sold by Mubashir Iqbal, ID 6807766127, with separate purchases. The icon comparison identifies whose brand is being evoked; it does not imply Google sells this Mac product or that different-platform feature sets are equivalent.

A Google-like security identity, without Google as seller

Feature	Investigated Mac icon	Official Google Authenticator
Basic motif	Six rounded spokes around a centre	Six rounded spokes around a centre
Palette	Green, yellow, blue and red	Green, yellow, blue and red
Rendering	Glossy raised arms; central white star; sparkles	Flat overlapping colour shapes
Seller	Mubashir Iqbal	Google LLC
Product / platform	Authenticator:2FA Login Codes / Mac	Google Authenticator / iPhone and iPad

A password vault deserves more than generic game policies

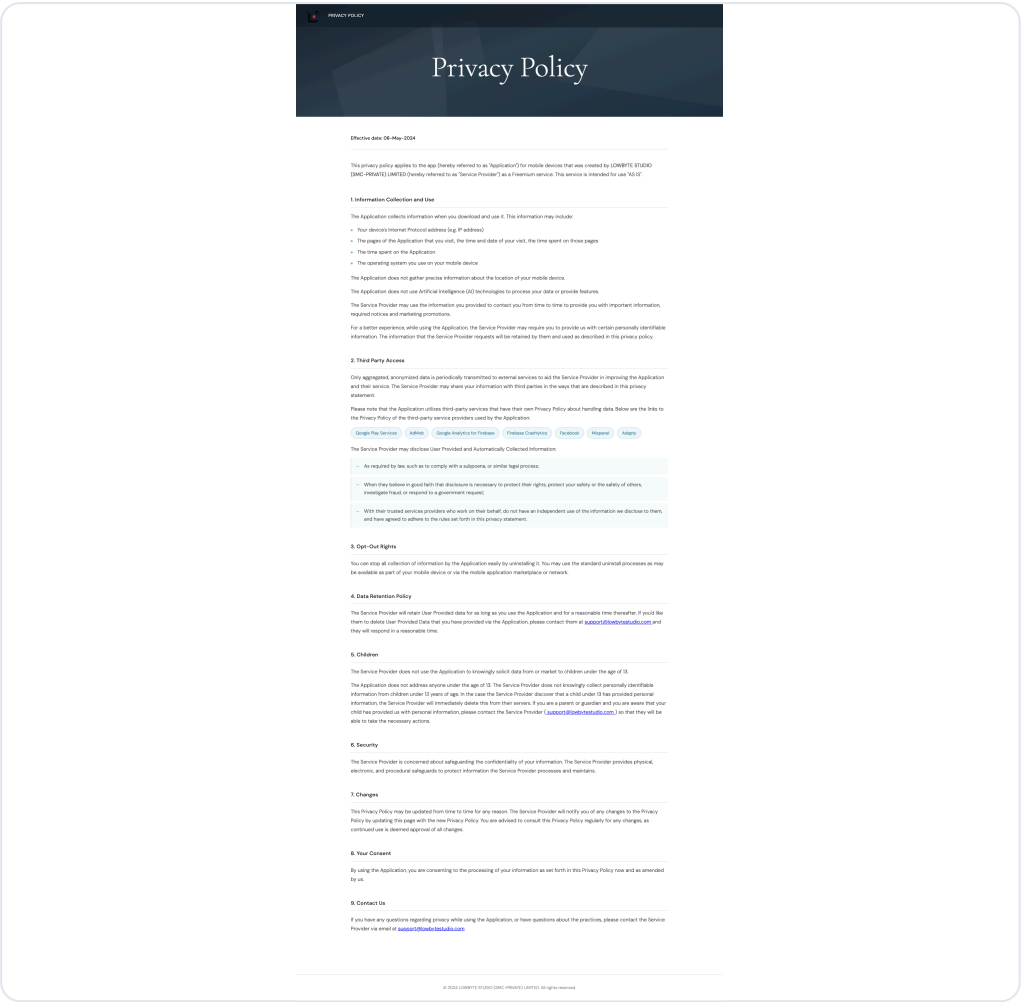
The App Store privacy button and the privacy URL inside the description lead to different documents. The first is a dedicated-domain policy naming LOWBYTE STUDIO (SMC-PRIVATE) LIMITED. The second is a long Google Sites document discussing games, children, visual communication and status content. They are both reachable, so the finding concerns their content rather

than broken links.

The Google Sites text asserts in one passage that no information is transmitted or stored online, but elsewhere describes personal information, advertising identifiers, analytics, marketing and retention. The Mac listing declares identity-linked purchases, contact information, user content, identifiers, usage data and diagnostics. The policy's sweeping no-collection/no-online-storage statements do not coherently explain those declarations or the advertised cloud backup.

Neither checked privacy document clearly explains storage of TOTP secrets and vault passwords, backup recipients, encryption/key custody, restore authorization or deletion of cloud copies. The dedicated-domain policy lists generic third-party services and broad data retention, but does not identify which apply to this Mac authenticator. A generic SDK list does not prove those SDKs run in the app.

This is a disclosure failure, not proof that passwords have leaked or that the Mac executable sends secrets to an attacker. An authentication app handles credentials capable of unlocking other accounts; the missing explanation is therefore central to assessing the product's security promises.


PRIVACY POLICY

Privacy Policy

Effective date: 06-May-2024

This privacy policy applies to the app (hereby referred to as "Application") for mobile devices that was created by LOWBYTE STUDIO (SMC-PRIVATE) LIMITED (hereby referred to as "Service Provider") as a Freemium service. This service is intended for use "AS IS".

1. Information Collection and Use

The Application collects information when you download and use it. This information may include:

- Your device's Internet Protocol address (e.g. IP address)
- The pages of the Application that you visit, the time and date of your visit, the time spent on those pages
- The time spent on the Application
- The operating system you use on your mobile device

The Application does not gather precise information about the location of your mobile device.

The Application does not use Artificial Intelligence (AI) technologies to process your data or provide features.

The Service Provider may use the information you provided to contact you from time to time to provide you with important information, required notices and marketing promotions.

For a better experience, while using the Application, the Service Provider may require you to provide us with certain personally identifiable information. The information that the Service Provider requests will be retained by them and used as described in this privacy policy.

2. Third Party Access

Only aggregated, anonymized data is periodically transmitted to external services to aid the Service Provider in improving the Application and their service. The Service Provider may share your information with third parties in the ways that are described in this privacy statement.

Please note that the Application utilizes third-party services that have their own Privacy Policy about handling data. Below are the links to the Privacy Policy of the third-party service providers used by the Application:

Google Play Services · AdMob · Google Analytics for Firebase · Firebase Crashlytics · Facebook · Mixpanel · Adapty

The Service Provider may disclose User Provided and Automatically Collected Information:

- As required by law, such as to comply with a subpoena, or similar legal process;
- When they believe in good faith that disclosure is necessary to protect their rights, protect your safety or the safety of others, investigate fraud, or respond to a government request;
- With their trusted services providers who work on their behalf, do not have an independent use of the information we disclose to them, and have agreed to adhere to the rules set forth in this privacy statement.

3. Opt-Out Rights

You can stop all collection of information by the Application easily by uninstalling it. You may use the standard uninstall processes as may be available as part of your mobile device or via the mobile application marketplace or network.

4. Data Retention Policy

The Service Provider will retain User Provided data for as long as you use the Application and for a reasonable time thereafter. If you'd like them to delete User Provided Data that you have provided via the Application, please contact them at support@lowbytestudio.com and they will respond in a reasonable time.

5. Children

The Service Provider does not use the Application to knowingly solicit data from or market to children under the age of 13.

The Application does not address anyone under the age of 13. The Service Provider does not knowingly collect personally identifiable information from children under 13 years of age. In the case the Service Provider discover that a child under 13 has provided personal information, the Service Provider will immediately delete this from their servers. If you are a parent or guardian and you are aware that your child has provided us with personal information, please contact the Service Provider (support@lowbytestudio.com) so that they will be able to take the necessary actions.

6. Security

The Service Provider is concerned about safeguarding the confidentiality of your information. The Service Provider provides physical, electronic, and procedural safeguards to protect information the Service Provider processes and maintains.

7. Changes

This Privacy Policy may be updated from time to time for any reason. The Service Provider will notify you of any changes to the Privacy Policy by updating this page with the new Privacy Policy. You are advised to consult this Privacy Policy regularly for any changes, as continued use is deemed approval of all changes.

8. Your Consent

By using the Application, you are consenting to the processing of your information as set forth in this Privacy Policy now and as amended by us.

9. Contact Us

If you have any questions regarding privacy while using the Application, or have questions about the practices, please contact the Service Provider via email at support@lowbytestudio.com

© 2024 LOWBYTE STUDIO (SMC-PRIVATE) LIMITED. All rights reserved.

Native public policy page, 3 November 2026. E8. Generic mobile-app disclosure linked by Apple's privacy button.

A password vault deserves more than generic game policies

Public claim / label	Disclosure problem
Password Vault and cloud backup	No app-specific secret protection, key custody or restore explanation
Identity-linked data in Apple label	Google Sites also contains broad no-personal-data assertions
Online backup and synchronization	Google Sites also says no information is sent/stored online
Generic external-service list	No clear mapping to the Mac app's actual processing

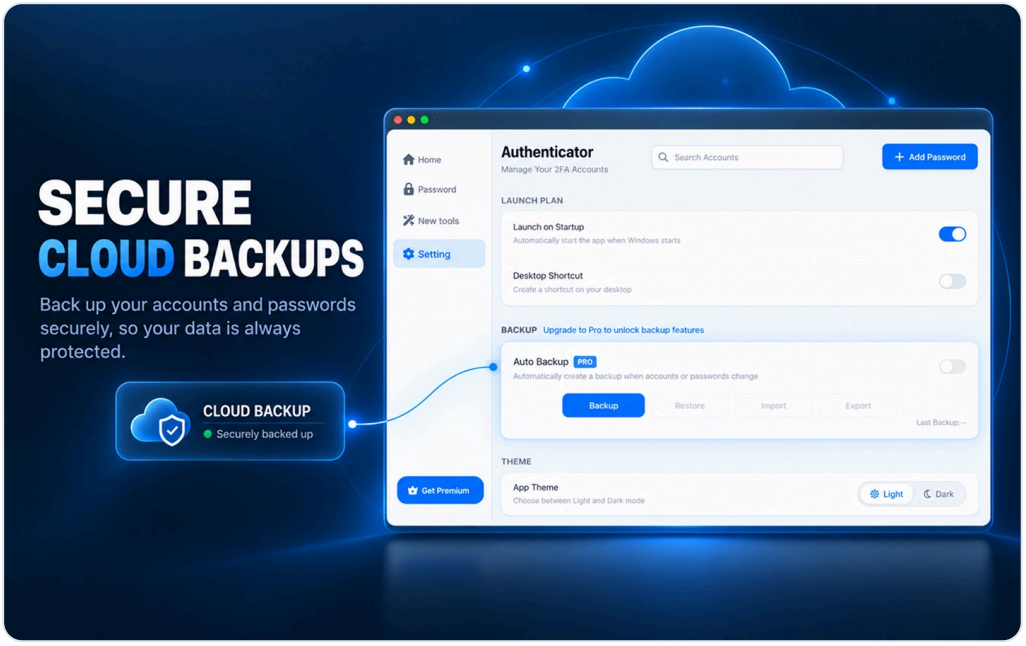
The Mac advertisement says Windows; Android shows a different product

The full Mac cloud-backup advertisement and its enlarged native-pixel detail below show a startup setting referring to Windows. This is the current Mac App Store promotion for a product requiring macOS 15.6. The mismatch is visible in the listing's own image; it does not establish what the installed executable actually does.

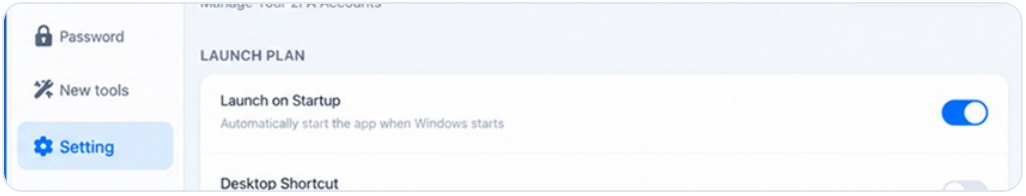
All seven original Android store screenshots were separately retrieved and inspected. They show a mobile dashboard, setup guidance and utility settings, without the Windows startup sentence. The Windows wording is therefore attributed only to the Mac promotion. The Android captures are reproduced in the next section so the two products can be compared directly.

The linked terms are also written around games: they discuss gaming behavior and describe a game developer as RG in the app-store section. They set a minimum user age of 16, while Apple rates the app 4+. The documents' different scopes and audience conditions are unresolved, rather than evidence of an observed child-data incident.

The Google Sites policy and terms print the malformed date 08-May-20245. The terms invoke Estonian intellectual-property laws and California law/courts in different passages. Neither phrase establishes a developer's actual country. Together with the gaming content, these details show why a dedicated security-product explanation is needed.



Complete original Mac App Store promotion 5, repeated here beside the platform-mismatch finding for context. E2/E6. No changes to the promotional pixels.

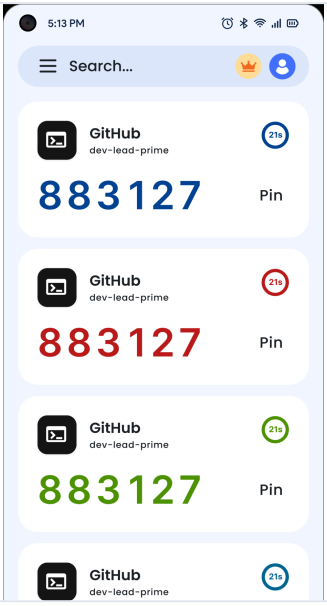


Native-pixel crop from Mac promotion 5, source rectangle x=540, y=235, width=850, height=155. Only cropping was applied; text was not reconstructed. E2/E6.

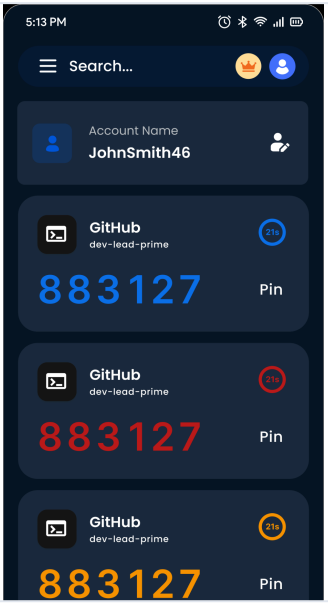
All seven original Android store screenshots

These are the seven unique original Google Play screenshots for LowByte's related Android authenticator. They are distinct from the five Mac promotional images preserved above. Captions identify the platform and visible feature, without treating simulated verification codes as real account credentials.

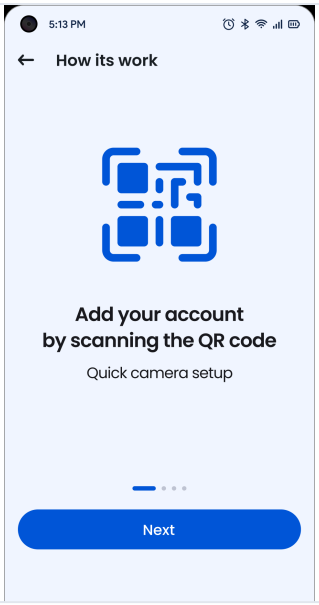
The fifth Android image advertises storing codes in a Google Account, while the seventh offers Google import and other utility controls. These are marketing claims; this investigation did not test a Google integration, cloud encryption or account recovery.



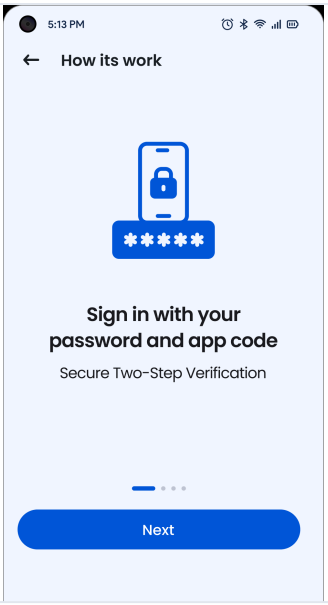
Original Google Play screenshot 1 for com.lowbyte.authenticatorapp. Light-theme Android authenticator dashboard with sample GitHub code cards. E12/E27.



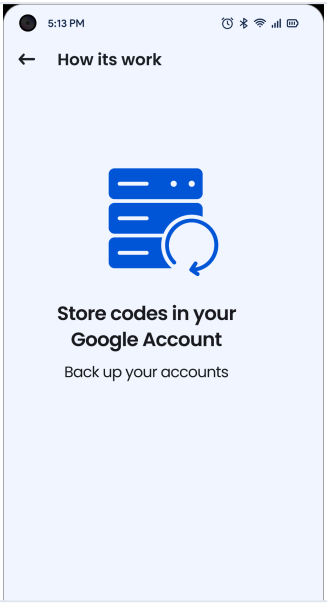
Original Google Play screenshot 2 for com.lowbyte.authenticatorapp. Dark-theme Android dashboard with account controls and sample code cards. E12/E27.



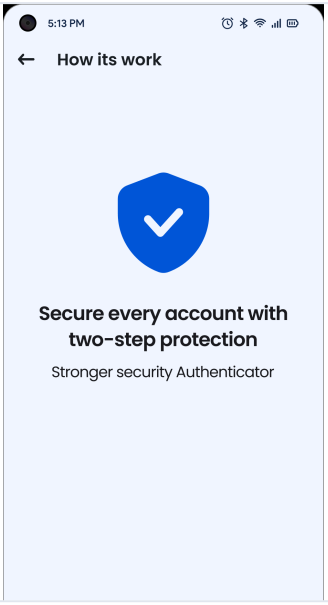
Original Google Play screenshot 3 for com.lowbyte.authenticatorapp. Android onboarding: account setup by scanning a QR code. E12/E27.



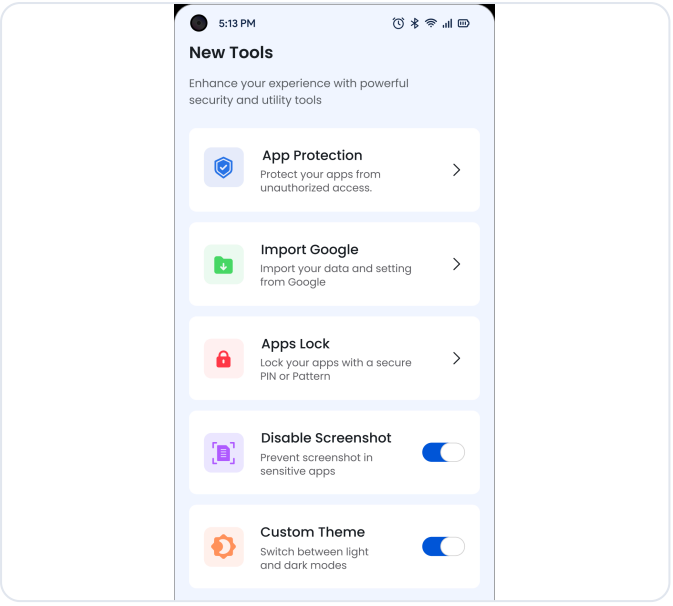
Original Google Play screenshot 4 for com.lowbyte.authenticatorapp. Android onboarding: sign-in with a password and app code. E12/E27.



Original Google Play screenshot 5 for com.lowbyte.authenticatorapp. Android onboarding advertises storing codes in a Google Account and backup. E12/E27.



Original Google Play screenshot 6 for com.lowbyte.authenticatorapp. Android onboarding promotes two-step account protection. E12/E27.



Original Google Play screenshot 7 for com.lowbyte.authenticatorapp. Android utility screen: app protection, Google import, app lock, screenshot control and theme. E12/E27.

The LowByte links are stronger than a matching surname

The Mac listing's support domain and privacy button directly connect it to LowByte's infrastructure. The dedicated-domain policy names LOWBYTE STUDIO (SMC-PRIVATE) LIMITED. The Android authenticator under that exact company name links the identical privacy URL and support domain. This is a direct shared legal/support infrastructure connection across stores.

A separate Google Play display publisher, LowByte Studio, discloses Rabia Aslam as its business identity on Category Sort: Puzzle Game. That app links the same custom-domain Google Sites privacy document named in the Mac description. The studio website additionally features Arrows & Screw using the exact package ID from this second publisher's catalog. The shared document plus first-party portfolio link support an operational studio association.

The studio website's public client bundle links Apple developer BAYBEEBRAIN, ID 1822542033, and a Real Strike game. The Apple developer page resolves, but the current US software lookup returns no apps for it. This establishes a website-published account link, not common legal ownership, an active portfolio or a ban-evasion history.

The network can be traced through explicit links, names and document URLs. Those records do not establish which individual controls every account, whether the people are related, or whether another app in the network is fraudulent. No prior Apple termination or deliberate account-circumvention sequence was verified.

The LowByte links are stronger than a matching surname

Publisher / identity	Bridge to the Mac app	Strength
Mubashir Iqbal — Apple 6781202819	Current Mac listing and studio legal/support domain	Direct
LOWBYTE STUDIO (SMC-PRIVATE) LIMITED — Google Play	Same dedicated-domain privacy URL and support domain	Direct shared infrastructure
LowByte Studio / Rabia Aslam — Google Play	Same Google Sites privacy URL; exact game package in studio portfolio	Corroborated operational association
BAYBEEBRAIN — Apple 1822542033	Explicit developer link in studio website code	Direct promotional link; control unverified
Other historical Apple listings	Indexed LowByte references; fresh pages unavailable	Historical leads only

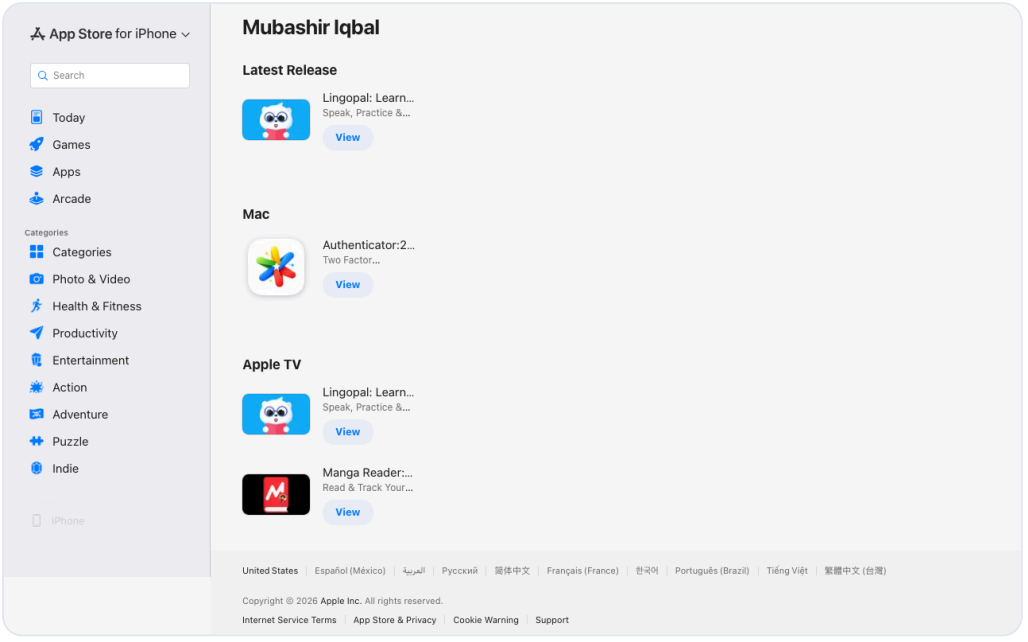
Mubashir Iqbal — current Apple account Related company Google Play account

Related LowByte Studio games account Website-linked BAYBEEBRAIN Apple account

What the connected accounts currently publish

Apple's current US catalog and software lookup return three apps under Mubashir Iqbal. Their numerical IDs and release dates are recorded below. The oldest app release is not the account-creation date. None of the other two Apple products is labelled fraudulent by association.

The company Google Play catalog displays five apps. The separate LowByte Studio game catalog displays nine games. These are current observed catalogs, not all-time release counts. The tables list titles and stable identifiers so readers can distinguish the accounts instead of treating the shared studio branding as one numerical account.



Native current US catalog, 3 November 2026. E5. All three apps are corroborated by the developer software lookup.

What the connected accounts currently publish

Platform / account	App	Stable identifier
Apple — Mubashir Iqbal	Manga Reader: Manga & Comics · 7 July 2026	6782316699
Apple — Mubashir Iqbal	Lingopal: Learn Languages · 26 August 2026	6803945678
Apple — Mubashir Iqbal	Authenticator:2FA Login Codes · 28 September 2026	6807766127
Google Play — company	Home Workout: Exercise at Home	com.homeworkout.noequipment.fitness
Google Play — company	Resume Builder - CV Maker App	com.lowbyte.cv.resume.maker.ai.new
Google Play — company	Authenticator App: Secure OTP	com.lowbyte.authenticatorapp
Google Play — company	Plant Identifier Scanner App	com.plant.identifier.flower.tree.leaf.myplantapp.plantscanner
Google Play — company	Football Live Score & News	com.football.soccer.worldcup.livescore

The second Google Play catalog

This account displays LowByte Studio while its developer details identify Rabia Aslam. The exact Arrows & Screw package is linked from the studio's own homepage portfolio. These games are included to document the account connection, without making an infringement or fraud finding about their titles or artwork.

The second Google Play catalog

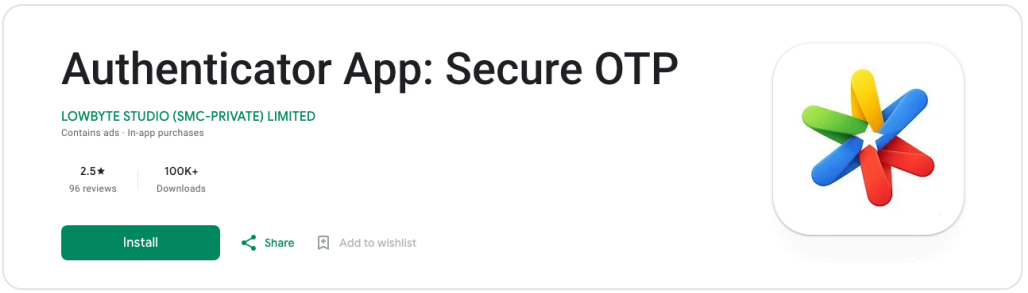
Observed game title	Package ID
Prism Arrow: Color Escape Game	com.lowbyte.prism.arrow.escape.puzzle
ASMR Drawing Coloring Games	com.lbs.coloring.drawing.paint.page.asmr.game
Brain Puzzle Games - IQ Test	braintest.games.puzzle.tricky.iqboost
Block Pic Jigsawcard Solitaire	com.lowbyte.studio.jigsaw.adults
Category Sort: Puzzle Game	com.lowbtye.category.sort.puzzle
Complete It - Draw One Part	com.dop.fun.draw.one.part.puzzle.games
Arrows & Screw - Puzzle Escape	com.lowbytestudio.screw.arrow.jam
Capital Theft Auto - CTA VI	com.lbs.gta.gangster.crime.mafia.city.game
Color Sort: Bus Point Out	com.lowbyte.men.sort.bus.jam

A related Android authenticator already attracts Google confusion

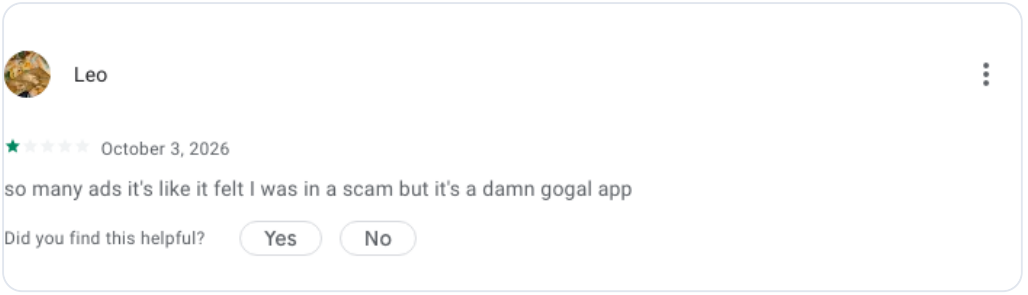
The related Android authenticator uses almost the same glossy four-colour spoke design, with a central star. Its publisher is the LowByte company, not Google. The current Android listing displays 100K+ downloads; this figure does not describe the Mac app. Its original icon is now shown in the four-store comparison at the top of the report.

A native review by Leo, dated 3 October 2026, complains about advertising and calls it a “gogal app”. That wording suggests the reviewer perceived it as a Google app. It is a consumer’s account on the related Android product, not a Mac buyer complaint or proof of a verified payment scam.

Google Play also displays a declaration that the Android app’s data is not encrypted. That is a developer-provided Android disclosure, not an independent security audit and not proof that the Mac app stores or transmits secrets unencrypted. The discrepancy deserves attention alongside the security marketing, while each product’s evidence remains separate.



Original public Google Play header crop. E12. The lower business-contact block and unrelated page footer are excluded; this is the Android app, not Mac download evidence.



Original native Google Play review card, 3 October 2026; captured 3 November 2026. E18. Android consumer allegation, not a Mac review.

Pakistan: the connected studio’s documented operating country

The connected company’s Google Play business panel declares Rawalpindi, Pakistan. The second Google Play publisher’s developer details identify Rabia Aslam in Pakistan. The studio’s own linked LinkedIn company profile describes Islamabad operations and Pakistan recruiting. These are direct business-source location statements, not an inference from the developers’ names.

The current studio website footer instead identifies Lowbyte Studio LLC in Sheridan, Wyoming, United States. A US entity and Pakistan operations can coexist. No incorporation record or ownership document was obtained to establish how the LLC, Pakistani company and individual Apple seller are legally related.

The report attributes Pakistan as the connected studio’s operating country, supported by the matching Mac/Android policy and support infrastructure plus the studio’s Pakistan business disclosures. Apple Germany and Ireland still list Mubashir Iqbal as a non-trader without a country. The attribution is therefore labelled as a studio association, not as an Apple trader declaration or proof of the individual’s residence. The Wyoming LLC website identity is recorded separately.

Pakistan: the connected studio's documented operating country

Source / identity	Observed location statement	What it establishes
Mac Apple seller Mubashir Iqbal	No country; non-trader in DE/IE	Apple supplies no country; connected-studio attribution used separately
Google Play company account	Rawalpindi, Pakistan	Company-provided business declaration
Google Play LowByte / Rabia Aslam	Pakistan	Separate publisher's business declaration
Linked studio LinkedIn	Islamabad, Pakistan operations	Company self-description
Studio website footer	Lowbyte Studio LLC · Sheridan, Wyoming, United States	Website legal identity claim; registry/control unverified

The lifetime label does not define the cloud promise

The lifetime offer is explicitly $99.99 in the US and €99.99 in Germany and Ireland. Two other premium prices are shown without billing intervals in the public table. The description gives auto-renewal/cancellation language but does not map those periods to the two generic purchase labels.

The linked game-oriented terms allow services to be discontinued and disclaim compensation in that context, but do not clearly define what lifetime means for this authenticator's cloud backup. The investigation did not obtain an in-app purchase screen or test a purchase. It therefore does not claim a hidden weekly charge, a completed payment or an observed loss of access.

The app also markets extended verification-code timers up to five hours, qualified by where supported. TOTP requires the generator and verifying service to share the time-step parameter; changing a local countdown cannot extend a website's acceptance window by itself. The listing does not explain compatible services or provisioning. No authentication-code test was performed.

The dates support a current warning, not a ban-evasion story

Apple records the first release of this Mac app and version 1.0 on 28 September 2026. The source capture is dated 3 November, 14:29:09 UTC. The exact source URL has a Wayback capture thirteen seconds later, and its replay opened. No earlier usable Apple icon or title sequence was established.

The indexed iOS authenticator 6792724838 and a Rabia Aslam Apple product 6768563654 contain LowByte-related leads in search results. Their fresh US pages returned 404 and current lookups returned no records. BAYBEEBRAIN's developer record still resolves but returned no current US software. These observations do not establish an Apple ban, its reason, who controls an absent app or deliberate review evasion.

Apple rules 2.3, 4.1 and 5.2.1 are relevant to accurate platform imagery and look-alike identity; privacy rule 5.1.1 is relevant to the app-specific explanation of sensitive data; subscription rule 3.1.2 is relevant to clear paid terms. The findings support review of those concrete issues. No additional proven fraud case, private account record or Apple enforcement notice was obtained.

▼ **View the dates and timeline**

2025-04-07

Studio domain registered

Verisign RDAP registration time 08:01:46 UTC; not Apple-account or company creation date.

2026-07-07

Oldest current app on the checked Apple account

Manga Reader: Manga & Comics; developer catalog/lookup.

2026-08-26

Lingopal released

Second current Apple portfolio app.

2026-09-28

Mac authenticator released

Apple version 1.0; exact-ID records.

2026-10-03

Related Android review references perceived Google identity

Leo’s public review; not Mac evidence.

2026-11-03

Source capture and independent investigation

All twelve source pages, original icon comparison, legal text and connected current publisher catalogs checked.

CHECK THE SOURCES

The records behind this report.

The entire supplied 12-page PDF is appended, including its original Mac store, promotion and policy captures. Source hash independently calculated. The written investigation adds current original Google Authenticator artwork, current LowByte infrastructure and publisher catalogs, a native related-Android review card and full linked policy text. No executable installed, purchase made, authentication secret imported or runtime data flow tested. Native screenshots are identified; cropping excludes irrelevant page furniture and business-contact details without changing the evidence shown. The updated report adds all seven original Android store screenshots, both store-specific official Google icon references and a clearly labelled native-pixel crop of the Windows text in the Mac advertisement.

▼ **Open source files, archive links and checksums**

E1 / Complete supplied 12-page analysis

Checked 3 November 2026. authenticator-2fa-login-codes_6807766127_2026-11-03_162909_analysis.pdf; capture 14:29:09 UTC. All 12 pages read and rendered. Information pages 1–3, promotions/description pages 4–5, source register page 6, full stores pages 7–10, policy pages 11–12. Hash independently calculated.

`SHA-256: 0056c0400b20e0c96ae2f3d67ed29202aec0ff50e330b81cd1c19d262e08838e`

E2 / Current US Mac listing

Retrieved 2026-11-03T14:34:02.646Z; HTTP 200. Exact name, subtitle, original icon and five promotions, three purchase amounts, linked-data label, privacy and terms routes.
Open source ↗

E3 / German Mac listing

Retrieved 2026-11-03T14:34:02.646Z; HTTP 200. Non-trader provider declaration, euro purchase amounts, no business-country record.
Open source ↗

E4 / Irish Mac listing

Retrieved 2026-11-03T14:34:02.643Z; HTTP 200. Matching non-trader declaration and euro purchase amounts, no business-country record.
Open source ↗

E5 / Mubashir Iqbal — Apple catalog

Retrieved 2026-11-03T14:34:10.513Z; HTTP 200. Developer 6781202819; three current US apps. Exact developer-software lookup corroborates their IDs, release dates and bundle IDs.
Open source ↗

E6 / Apple exact-ID lookup

Checked 3 November 2026. Both app/seller identities and original icon URLs; Mac release/version/bundle data. Separately queried developer 6781202819 with entity=software and limit=200.
Open source ↗

E7 / Official Google Authenticator

Retrieved 2026-11-03T14:34:18.705Z; HTTP 200. App 388497605, Google LLC, bundle com.google.Authenticator. Original icon independently downloaded. Official reference is the iPhone/iPad app, listed free; no equivalence of platform or paid entitlements asserted.
Open source ↗

E8 / App Store privacy button — dedicated-domain policy

Retrieved 2026-11-03T14:34:10.512Z; HTTP 200. Effective date 08-May-2024. Names LOWBYTE STUDIO (SMC-PRIVATE) LIMITED and studio-domain contact; generic mobile-app policy, IP/use collection, external services and retention; no authenticator-secret/vault-specific explanation.
Open source ↗

E9 / Description privacy link — Google Sites policy

Retrieved 2026-11-03T14:34:17.998Z; HTTP 200. Full rendered document read. Printed date 08-May-20245 preserved as malformed. Mixes games, children and status-content text with conflicting collection/transmission statements. No app-specific password, TOTP-secret, encryption or cloud-backup explanation found.
Open source ↗

E10 / Description terms — Google Sites

Retrieved 2026-11-03T14:34:18.227Z; HTTP 200. Full text read. Game-oriented license, minimum age 16, discontinuation/no-compensation clauses, RG developer reference, Estonia intellectual-property wording and California governing law; not country evidence.
Open source ↗

E11 / LowByte company website

Retrieved 2026-11-03T14:34:10.775Z; HTTP 200. Dedicated presentation website is functional; footer identifies Lowbyte Studio LLC in Sheridan, Wyoming, United States. Portfolio and public client script link to games and BAYBEEBRAIN Apple account. No company registry/control verification obtained. Direct /about and /team routes linked from the homepage returned 404 in fresh checks.
Open source ↗

E12 / Related Android Authenticator — company identity

Retrieved 2026-11-03T14:37:33.054Z; HTTP unknown. Separate Android app com.lowbyte.authenticatorapp, LOWBYTE STUDIO (SMC-PRIVATE) LIMITED; same domain privacy URL and support domain; business panel declares Rawalpindi, Pakistan. 100K+ downloads is Android-only. Current listing declares no data sharing, some collection and no encryption. This is not a measurement of Mac encryption.
Open source ↗

E13 / Related Google Play company catalog

Retrieved 2026-11-03T14:38:06.621Z; HTTP 200. Five displayed current apps, recorded with package IDs. Catalog scope is a current storefront observation, not an all-time total.
Open source ↗

E14 / Second Google Play publisher — LowByte Studio / Rabia Aslam

Retrieved 2026-11-03T14:37:37.718Z; HTTP unknown. Category Sort: Puzzle Game, com.lowbtye.category.sort.puzzle. LowByte Studio display publisher; public business identity Rabia Aslam, Pakistan. Links the same custom-domain Google Sites privacy page. Contact differs from the company account.
Open source ↗

E15 / LowByte Studio game catalog

Retrieved 2026-11-03T14:38:06.622Z; HTTP 200. Nine displayed current games; website portfolio links exactly to Arrows & Screw package in this catalog. No fraud inference made about those games.
Open source ↗

E16 / Website-published Apple account link and game links

Checked 3 November 2026. Public client bundle linked from the studio homepage. Contains explicit BAYBEEBRAIN developer URL 1822542033 and Real Strike game URL 6748994711, plus portfolio game package links. File read as public source, not executed as a research command. Hash independently calculated.
Open source ↗

`SHA-256: b57add05525e1ffe45eddb80cbfabf0a34d58baa7df17becd14be5aeb3b013ef`

E17 / BAYBEEBRAIN Apple account

Retrieved 2026-11-03T14:38:06.622Z; HTTP 200. Developer page resolves for 1822542033 and shows the publisher name but no app cards. Developer lookup returns artist record and zero software records. Website-linked game 6748994711 lookup returns zero; not evidence of a ban.
Open source ↗

E18 / Related Android native review card

Checked 3 November 2026. Reviewer Leo, 3 October 2026, complains about advertising and uses gogal app wording, suggesting perceived Google identity. Original native card captured separately. Consumer allegation about Android product; not a Mac review or independent proof of fraud.
Open source ↗

E19 / Google brand guidance

Retrieved 2026-11-03T14:35:45.199Z; HTTP 200. Official guidance prohibits imitating distinctive colour combinations, graphic designs and product icons, and implying nonexistent affiliation. Relevant to observed look-alike icon; no adjudicated infringement or Google enforcement decision obtained.
Open source ↗

E20 / Apple App Review Guidelines

Retrieved 2026-11-03T14:35:22.923Z; HTTP 200. 2.3 accurate metadata, 4.1 copycats, 5.2.1 intellectual property, 5.1.1 privacy and 3.1.2 subscriptions checked for the observed issues. No enforcement outcome obtained.
Open source ↗

E21 / Archive index and current replay

Retrieved 2026-11-03T14:38:14.368Z; HTTP 200. Exact US URL has capture 3 November 2026, 14:29:22 UTC; replay opened. Query-free and wildcard numeric-ID queries returned no additional captures. No earlier name/icon sequence verified.
Open source ↗

E22 / LowByte LinkedIn company profile

Retrieved 2026-11-03T14:35:15.690Z; HTTP 200. Homepage-linked corporate profile identifies Islamabad operations and Pakistan recruiting. Company self-description; headcount, founding-date inconsistencies and employee names are not treated as verified corporate ownership records.
Open source ↗

E23 / Domain registration RDAP

Checked 3 November 2026. Registration 7 April 2025, 08:01:46 UTC independently checked. Registration time does not prove who controls the Apple account or where they live.
Open source ↗

E24 / TOTP specification — RFC 6238

Checked 3 November 2026. Time-step is a shared prover/verifier system parameter; default 30 seconds. Longer steps affect exposure. Used only to assess the marketed extended timers, not as a test of this implementation.
Open source ↗

E25 / Additional historical/indexed leads and exact-identifier searches

Checked 3 November 2026. Indexed iOS authenticator 6792724838 shows LowByte legal URLs and a misspelled support domain, but live US page returns 404 and lookup zero records. Indexed Rabia Aslam Apple app 6768563654 shows Lowbyte copyright; live US page 404 and IE lookup zero. No current numerical Rabia Apple developer account established. Exact names/domain/support IDs checked against public search and existing local corpus; no prior ban, additional fraud case or account-evasion sequence verified. A secondary business directory lists a same-name executive; not used to prove seller identity/control.
Open source ↗

E26 / Official Google Authenticator — Google Play

Checked 3 November 2026. Original Google LLC Android listing and original Google-hosted icon retrieved. Package com.google.android.apps.authenticator2. This is the official Android reference alongside the separately verified official Apple app.
Open source ↗

E27 / Related Android app — seven original screenshot assets

Checked 3 November 2026. Seven unique Screenshot image assets read from the current Google Play listing, downloaded at available original aspect ratio, visually inspected. No Windows startup sentence appears in these seven images; the sentence is present in original Mac promotion 5. Source URLs and native Mac crop rectangle retained privately.
Open source ↗



Authenticator:2FA Login Codes

Two Factor Authentication, OTP

Mubashir Iqbal

ONE-OFF ANALYSIS · 03 Nov 2026, 16:29 (UTC+02:00)
a single reading of the public store page; the app is not monitored
Captured 2026-11-03 14:29:09 UTC · US App Store · App ID 6807766127

Risk indicators

- Brand terms mentioned in the description: google, apple, app store
- The developer account published its first app 119 days ago (2026-07-07)
- The provider has not identified itself as a trader on the EU (IE) App Store

App details (US App Store)

App name	Authenticator:2FA Login Codes
Subtitle	Two Factor Authentication, OTP
Developer	Mubashir Iqbal (ID 6781202819)
Seller	Mubashir Iqbal
Developer website	— (none listed on the App Store)
Privacy Policy	https://www.lowbytestudio.com/links/policy.html
Developer page	https://apps.apple.com/us/developer/mubashir-iqbal/id6781202819
Bundle ID	com.lbs.macauthenticator
Category	Productivity
Price	Free
Ratings	— (not enough ratings)
First released	2026-09-28
App Store link	https://apps.apple.com/us/app/authenticator-2fa-login-codes/id6807766127?mt=12
App ID	6807766127

Pages linked from the listing

Privacy Policy

Link	https://www.lowbytestudio.com/links/policy.html
Status	working · page title: Privacy Policy
Domain	lowbytestudio.com, registered 2025-04-07
Emails on the page	support@lowbytestudio.com

Latest update

Version	1.0
Released	2026-09-28

What's New

—

EU App Store (IE) — provider / trader

App name	Authenticator:2FA Login Codes
Provider	Mubashir Iqbal
Trader	No — not identified as a trader
Statement	Mubashir Iqbal has not identified itself as a trader for this app. If you are a consumer in the European Economic Area, consumer rights do not apply to agreements between you and the provider.
Store link	https://apps.apple.com/ie/app/authenticator-2fa-login-codes/id6807766127?mt=12

Information that differs on the IE store

In-App Purchases	Yes Authenticator premium lifetime: €99.99 Authenticator premium: €34.99 Authenticator premium: €5.99

Information

Seller	Mubashir Iqbal
Size	6.5 MB
Category	Productivity
Compatibility	Mac Requires macOS 15.6 or later.
Languages	English
Age Rating	4+
In-App Purchases	Yes Authenticator premium lifetime: $99.99 Authenticator premium: $29.99 Authenticator premium: $4.99
Copyright	© Authenticator 2026

App Privacy

Data Linked to You: Purchases, Contact Info, User Content, Identifiers, Usage Data, Diagnostics

Icon compared with the official apps of the brands it mentions

	**This app**	
	Google Drive by Google official google app · App ID 507874739	**39%** different
	Apple Music by Apple official apple app · App ID 1108187390	**2%** different

The brands are those named in the listing (name, subtitle, description, text in the screenshots); the official app of a brand is the App Store app with the brand in its name and the most ratings. Similarity is an automatic estimate; from 52% the icons count as similar.

Developer account

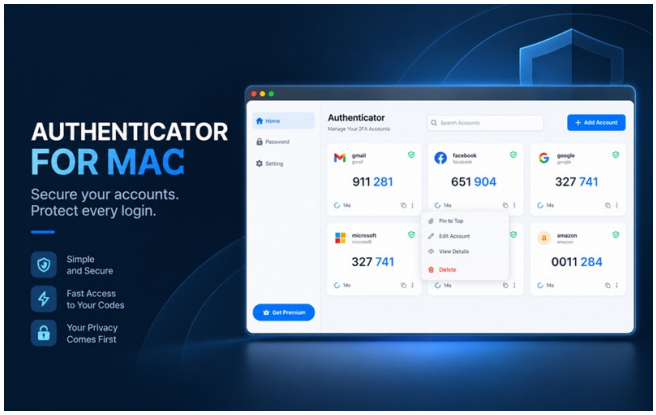
Developer	Mubashir Iqbal (ID 6781202819)
Apps on the US App Store	3
First app published	2026-07-07 (119 days ago)
Published in the last 90 days	2

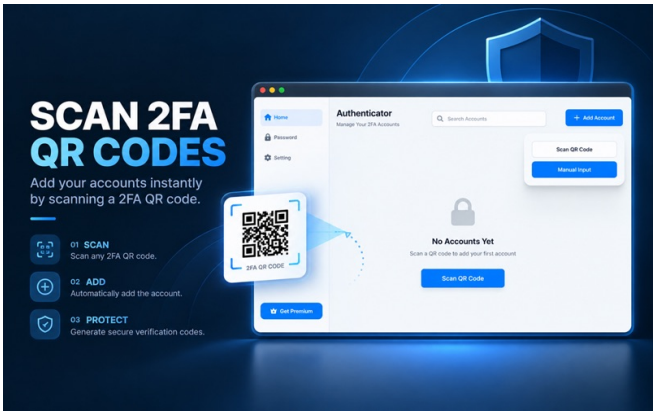
Apps of this developer account (oldest first)

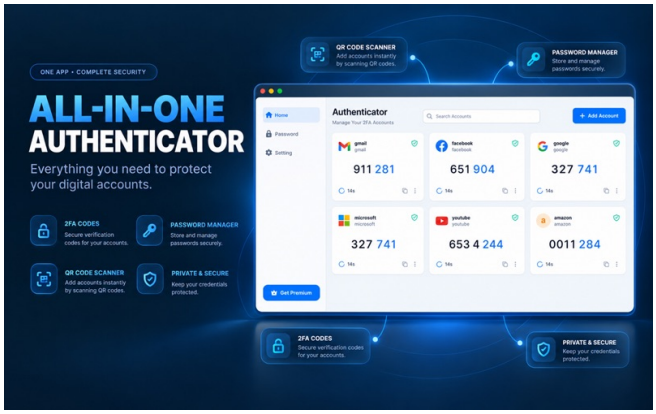
- Manga Reader: Manga & Comics · 2026-07-07 · 0 ratings · App ID 6782316699
- Lingopal: Learn Languages · 2026-08-26 · 0 ratings · App ID 6803945678
- Authenticator:2FA Login Codes · 2026-09-28 · 0 ratings · App ID 6807766127

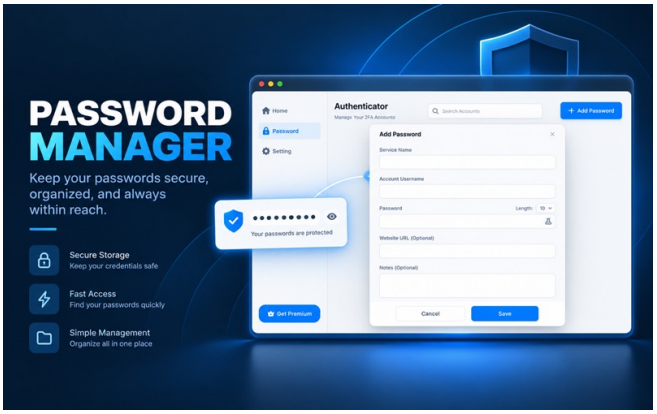
Screenshots

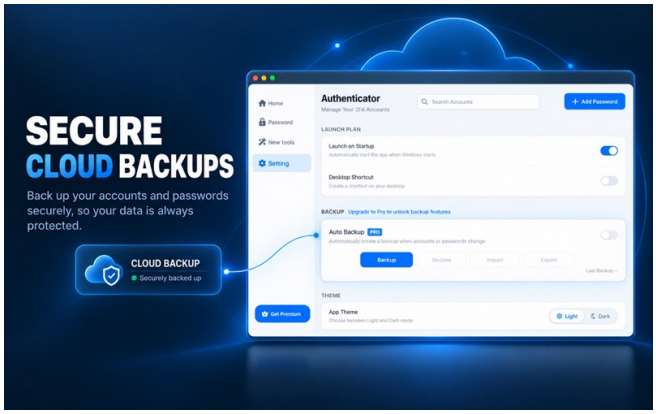
Mac (5)











Description

Protect your online accounts with Authenticator, a secure and easy-to-use authenticator app for Mac that generates time-based one-time passwords (TOTP) for your favorite websites and services. Whether you're securing email, social media, work accounts, banking, or cloud services, Authenticator helps you add an extra layer of security to your sign-in process.

Set up new accounts in seconds by scanning QR codes directly from your Mac screen, adding them manually, or importing accounts from other authenticator apps. Access your two-factor authentication (2FA) and verification codes directly from your Mac, even when you're offline.

Authenticator also includes a Password Vault to help you keep your important passwords and account information organized in one secure place. Manage your authentication codes and password credentials conveniently from your Mac.

Free Features
- Generate TOTP codes: Create secure time-based one-time password verification codes.
- Scan QR codes from your Mac screen: Set up supported accounts by scanning QR codes displayed on

your screen, including QR codes from other apps or your Dock.
- Add accounts manually: Enter account details whenever manual setup is needed.
- Import QR code images: Add accounts from QR code images, screenshots, or files stored on your Mac.
- Import from other authenticator apps: Migrate your supported accounts from other authenticator apps.
- Export accounts: Create secure local backups with optional encryption.
- Copy verification codes: Copy your 2FA codes with a single click.
- Search accounts instantly: Find the account you need quickly.
- Live countdown timer: See when your current verification code will refresh.
- Recently Deleted: Restore accidentally deleted accounts.
- PIN lock: Protect the app with a PIN and customizable auto-lock timer.
- Screenshot protection: Block screenshots for enhanced privacy and security.
- 2FA setup guides: Follow easy instructions for popular online services.
- Password Vault: Store and manage your passwords and account credentials.
- Multiple languages: Available in English, Arabic, Spanish, French, Hindi, Urdu, and more.

Premium Features
- Unlock additional security and convenience with Premium:
- Secure cloud backup and synchronization: Keep your supported authenticator accounts backed up and synchronized across your devices.
- Unlimited authenticator accounts: Store as many supported accounts as you need.
- Extended code timers: Customize verification code timers with options including 15-minute, 20-minute, and 5-hour timers where supported.
- Priority customer support: Get additional assistance when you need it.

Built for Your Mac
Authenticator is designed for users who want a dedicated Mac authenticator to manage their 2FA codes conveniently from their desktop. Whether you're protecting personal accounts, business logins, or developer services, Authenticator helps make two-factor authentication simple and accessible.
Your verification codes remain available even without an internet connection, helping you complete supported sign-ins wherever you are.

Subscription Information
Some features require a Premium subscription. Subscriptions automatically renew unless canceled at least 24 hours before the end of the current billing period. Payment is charged to your Apple ID account upon purchase, and you can manage or cancel your subscription anytime through your App Store account settings. Prices may vary by region. A free trial, if offered, will automatically convert to a paid subscription unless canceled before the trial ends.

Download Authenticator for Mac today and keep your digital accounts protected with secure, simple, and reliable two-factor authentication.

Contact Us: support@lowbytestudio.com
Privacy Policy: https://sites.google.com/lowbytestudio.com/privacypolicy/home
Terms of Service: https://sites.google.com/lowbytestudio.com/terms-of-service/home

Evidence and integrity

Captured (UTC)	2026-11-03 14:29:09 UTC
Source: US App Store page	https://apps.apple.com/us/app/authenticator-2fa-login-codes/id6807766127?mt=12
Source: IE App Store page	https://apps.apple.com/ie/app/authenticator-2fa-login-codes/id6807766127?mt=12
Source: privacy policy linked from the listing	https://www.lowbytestudio.com/links/policy.html
Web archive: US App Store page	https://web.archive.org/web/20261103142922/https://apps.apple.com/us/app/authenticator-2fa-login-codes/id6807766127?mt=12
Web archive: IE App Store page	https://web.archive.org/web/20261103142922/https://apps.apple.com/ie/app/authenticator-2fa-login-codes/id6807766127?mt=12
Web archive: privacy policy linked from the listing	not archived yet (web.archive.org was busy; the bot tries again later and lists the link in the dossier)

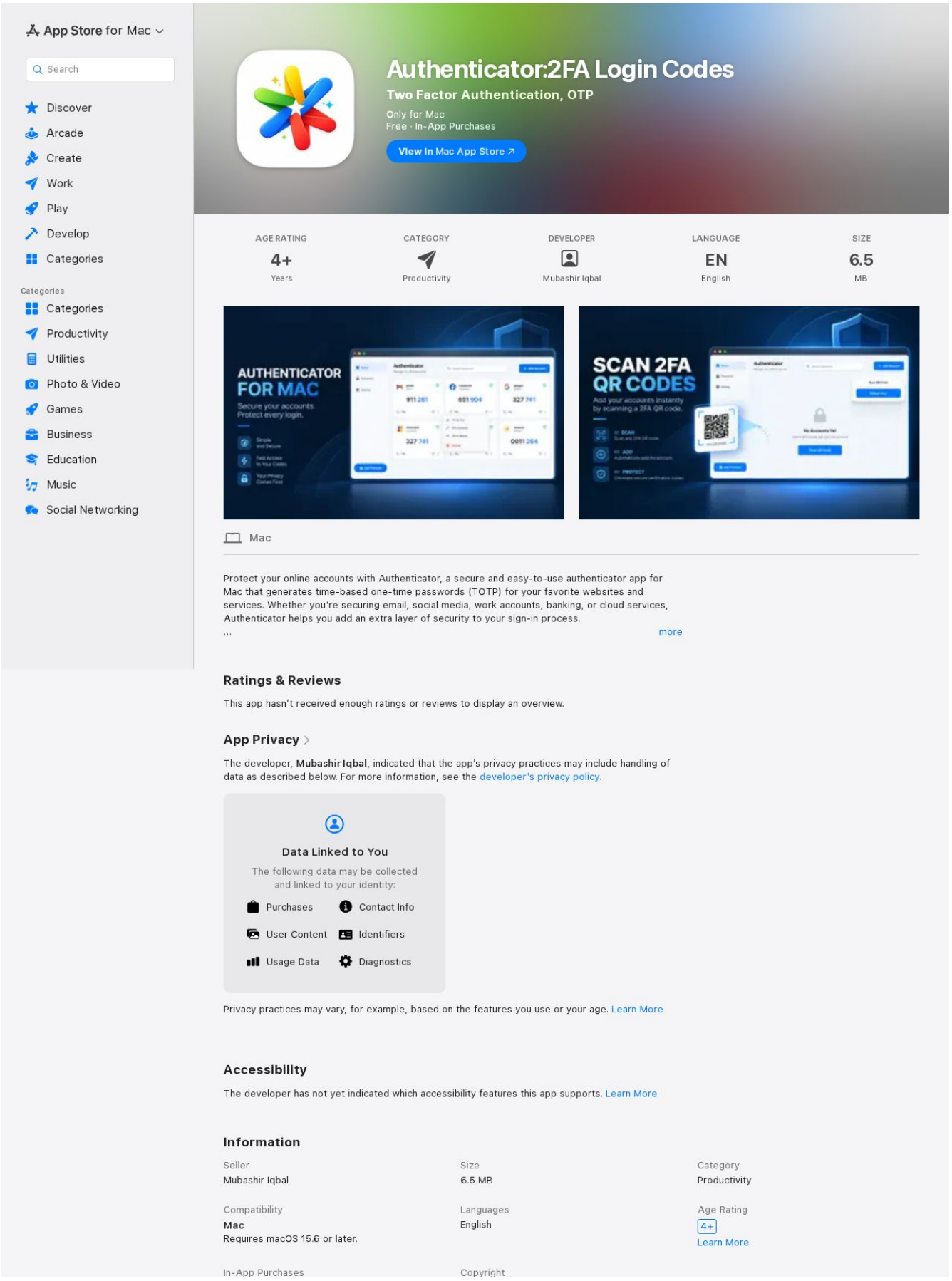
SHA-256 of the raw files captured for this snapshot

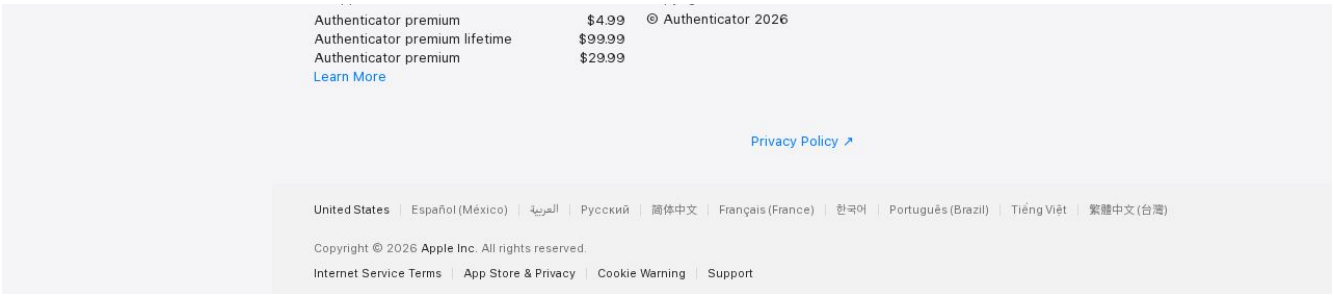
capture_ie.png	`5cb88894184a60ae1dd0c80f6bd2e149531835d7048681a60d3b4be25bacd782`
capture_site-privacy-policy.png	`c6d3815de00bf149a7859a81f20008882eeb1f5073078ea416c2f11b7a8d2dd6`
capture_us.png	`3e53afb59dce282e0292bd47fb6f09d14b717f4afec2f8e106d63750e9c83e2d`
lookup_ie.json	`4a70309fe17f88117af4a2d4f01acc5d94e0d329221de86849283980d3e97bb7`
lookup_us.json	`61eb8a778bb22e3a1c9c93ffcee2e2b8a7adcabf265df1b6a2db4c9ac88d40ef`
page_ie.html	`4020ac8355c0680b15740b67340a4d4472e36b5b18cd0af568e20d6b9075f7c9`
page_us.html	`bd8b4b0be52dae483198c9d76e018caab2648ac1d07224b1d5aba0f805fb1562`
site_privacy-policy.html	`89e0eebdb830274866be78f49bdce04a1e40e7aa0480db6781ab164e6eeb357c`

The raw answers from Apple, the page captures and the images are kept in the evidence archive that has the same name as this PDF. The SHA-256 of this PDF is written in that archive (SHA256SUMS.txt) and in the Telegram message that delivered it.

Appendix — the US App Store page as displayed

Full-page browser capture of https://apps.apple.com/us/app/authenticator-2fa-login-codes/id6807766127?mt=12, taken 2026-11-03 14:29:09 UTC.

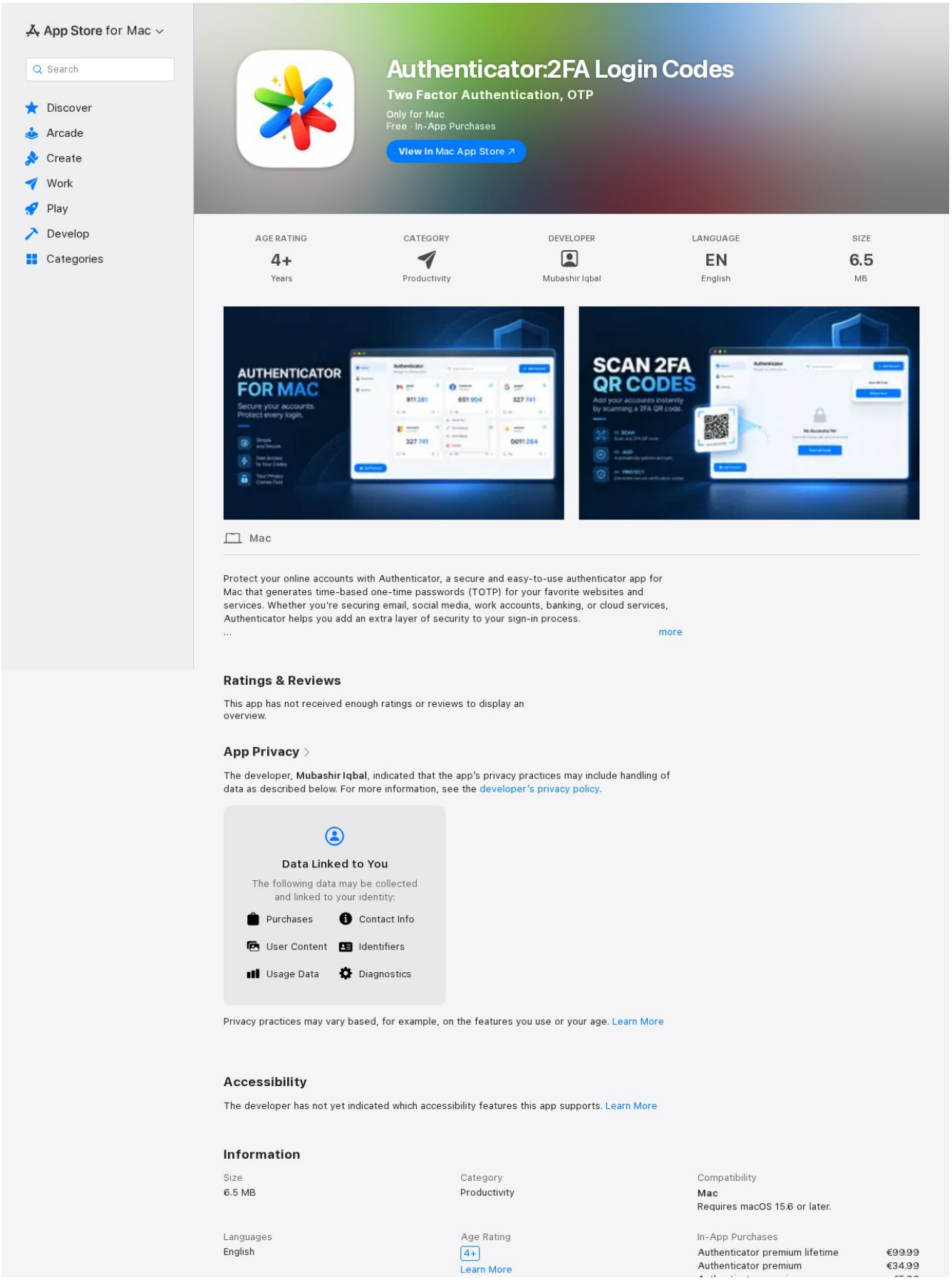


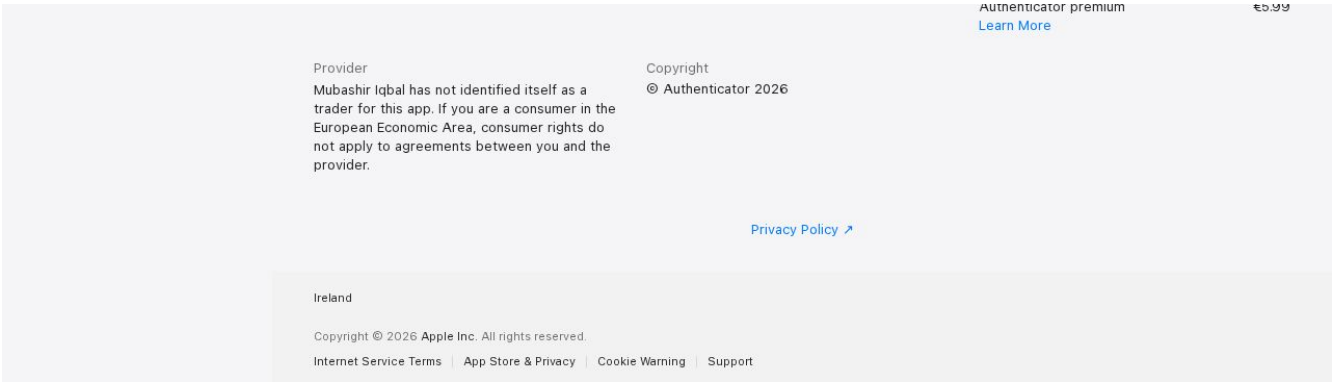


Privacy Policy ↗

Appendix — the IE App Store page as displayed

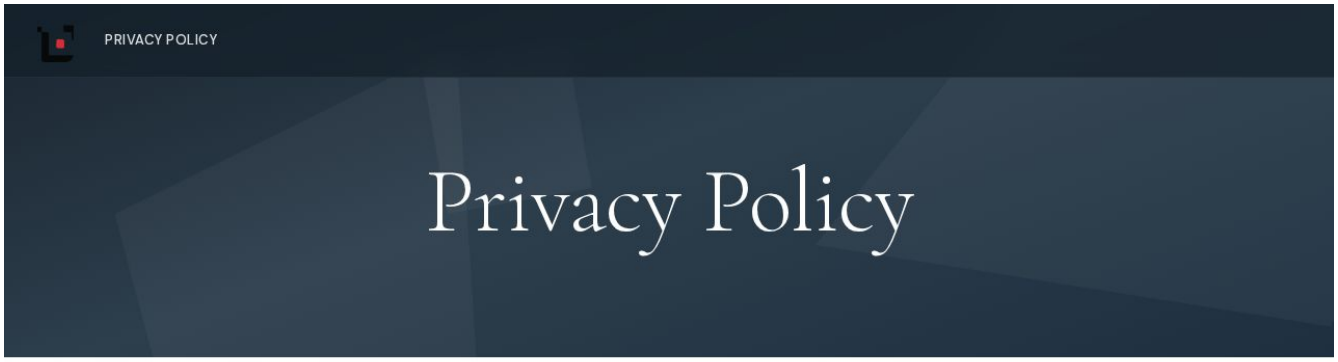
Full-page browser capture of https://apps.apple.com/ie/app/authenticator-2fa-login-codes/id6807766127?mt=12, taken 2026-11-03 14:29:09 UTC.




Authenticator premium
€5.99
Learn More
Provider
Mubashir Iqbal has not identified itself as a trader for this app. If you are a consumer in the European Economic Area, consumer rights do not apply to agreements between you and the provider.
Copyright
© Authenticator 2026
Privacy Policy ↗
Ireland
Copyright © 2026 Apple Inc. All rights reserved.
Internet Service Terms | App Store & Privacy | Cookie Warning | Support

Appendix — the privacy policy linked from the listing as displayed

Full-page browser capture of https://www.lowbytestudio.com/links/policy.html, taken 2026-11-03 14:29:09 UTC. Cookie-consent overlays (the host's, not the page's content) were hidden before the capture, and Google pages were opened in English.



Effective date: 08-May-2024

This privacy policy applies to the app (hereby referred to as "Application") for mobile devices that was created by LOWBYTE STUDIO (SMC-PRIVATE) LIMITED (hereby referred to as "Service Provider") as a Freemium service. This service is intended for use "AS IS".

1. Information Collection and Use

The Application collects information when you download and use it. This information may include:

- Your device's Internet Protocol address (e.g. IP address)
- The pages of the Application that you visit, the time and date of your visit, the time spent on those pages
- The time spent on the Application
- The operating system you use on your mobile device

The Application does not gather precise information about the location of your mobile device.

The Application does not use Artificial Intelligence (AI) technologies to process your data or provide features.

The Service Provider may use the information you provided to contact you from time to time to provide you with important information, required notices and marketing promotions.

For a better experience, while using the Application, the Service Provider may require you to provide us with certain personally identifiable information. The information that the Service Provider requests will be retained by them and used as described in this privacy policy.

2. Third Party Access

Only aggregated, anonymized data is periodically transmitted to external services to aid the Service Provider in improving the Application and their service. The Service Provider may share your information with third parties in the ways that are described in this privacy statement.

Please note that the Application utilizes third-party services that have their own Privacy Policy about handling data. Below are the links to the Privacy Policy of the third-party service providers used by the Application:

Google Play Services | AdMob | Google Analytics for Firebase | Firebase Crashlytics | Facebook | Mixpanel | Adapty

The Service Provider may disclose User Provided and Automatically Collected Information:

- As required by law, such as to comply with a subpoena, or similar legal process;
- When they believe in good faith that disclosure is necessary to protect their rights, protect your safety or the safety of others, investigate fraud, or respond to a government request;
- With their trusted services providers who work on their behalf, do not have an independent use of the information we disclose to them, and have agreed to adhere to the rules set forth in this privacy statement.

3. Opt-Out Rights

You can stop all collection of information by the Application easily by uninstalling it. You may use the standard uninstall processes as may be available as part of your mobile device or via the mobile application marketplace or network.

4. Data Retention Policy

The Service Provider will retain User Provided data for as long as you use the Application and for a reasonable time thereafter. If you'd like them to delete User Provided Data that you have provided via the Application, please contact them at support@lowbytestudio.com and they will respond in a reasonable time.

5. Children

The Service Provider does not use the Application to knowingly solicit data from or market to children under the age of 13.

The Application does not address anyone under the age of 13. The Service Provider does not knowingly collect personally identifiable information from children under 13 years of age. In the case the Service Provider discover that a child under 13 has provided personal information, the Service Provider will immediately delete this from their servers. If you are a parent or guardian and you are aware that your child has provided us with personal information, please contact the Service Provider (support@lowbytestudio.com) so that they will be able to take the necessary actions.

6. Security

The Service Provider is concerned about safeguarding the confidentiality of your information. The Service Provider provides physical, electronic, and procedural safeguards to protect information the Service Provider processes and maintains.

7. Changes

This Privacy Policy may be updated from time to time for any reason. The Service Provider will notify you of any changes to the Privacy Policy by updating this page with the new Privacy Policy. You are advised to consult this Privacy Policy regularly for any changes, as continued use is deemed approval of all changes.

8. Your Consent

By using the Application, you are consenting to the processing of your information as set forth in this Privacy Policy now and as amended by us.

9. Contact Us

If you have any questions regarding privacy while using the Application, or have questions about the practices, please contact the Service Provider via email at support@lowbytestudio.com

© 2024 LOWBYTE STUDIO (SMC-PRIVATE) LIMITED. All rights reserved.