PROPYLEUS

YOUR DIGITAL GUARDIAN

ANDROID / ENGLISH

BUSINESS

User manual



PROPYLEUS BUSINESS

For owners, administrators and employees. Organise members and departments, handle incidents and use optional Team wellbeing.

1.0.67 / NOVEMBER 2026

01 / START HERE

Your guide

Find what you need quickly. Select a section to jump straight to its instructions.

03 The home screen ›

04 Getting started and navigation ›

05 Checking messages and links ›

06 Photos and QR codes ›

07 Enabling Online Protection ›

08 Enabling call protection ›

09 Company workspace and departments ›

10 Incidents suppliers and training ›

11 Personal Wellness and SOS ›

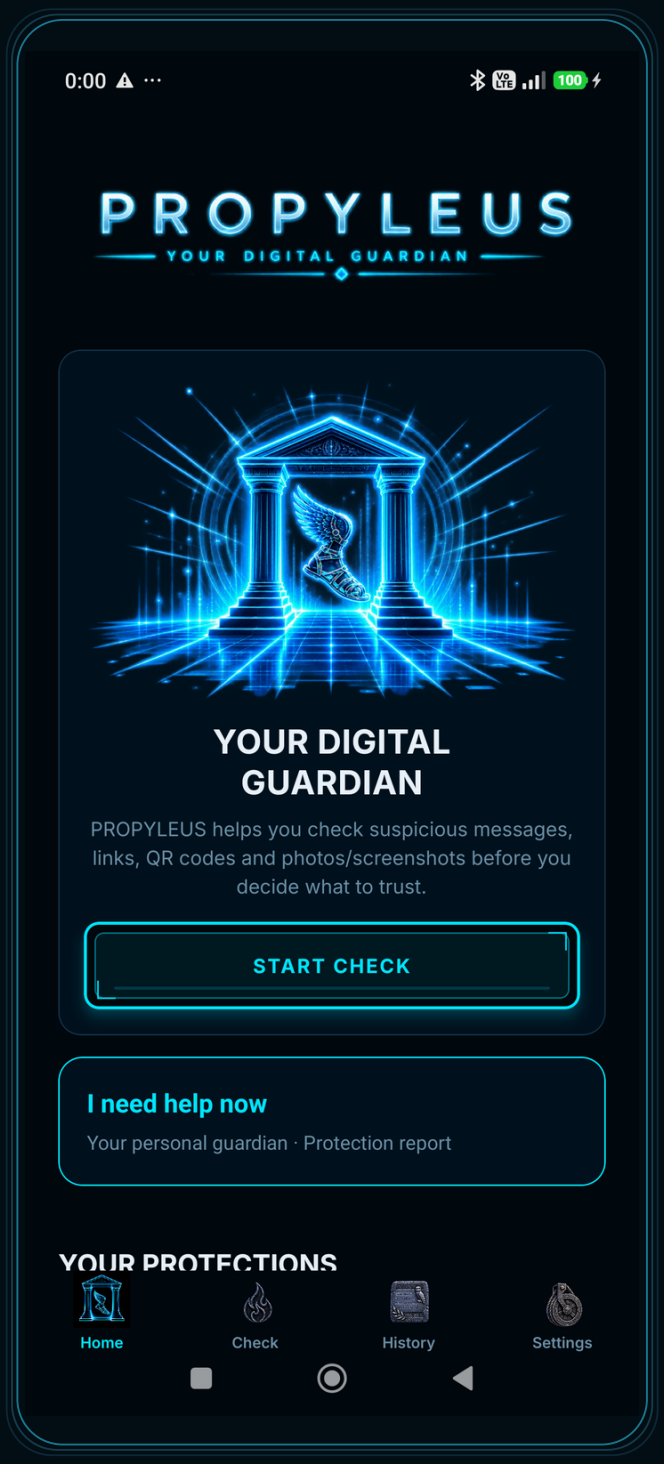
12 Team wellbeing by department ›

13 Subscription privacy and support ›

These instructions cover Android. Settings labels may vary by device.

02 / YOUR APP

Meet your home screen



Home

Start a check and see your protection cards.

Check

Choose a message, link, photo or QR.

History

Return to your saved personal checks.

Settings

Manage language, account, plan and permissions.

Example screen in English. Available cards depend on your plan and choices.

03 / BUSINESS

Getting started and navigation

Start with the app for your plan. FREE and SINGLE are in PERSONAL. FAMILY and BUSINESS have their own apps. These instructions cover Android and the 1.0.67 series. Phone settings may use different labels.

01 Open the app, choose EL or EN and read the introductory notices. Accept only if you agree.

02 Sign in to your PROPYLEUS account or use the account creation option. For a team invitation, use the email address that received it.

03 If asked, select your correct age category and role. This determines the available flows.

04 Open Settings and check your plan and sign-in status. Allow verification to finish before enabling additional features.

The four main tabs

- Home: start a check and view available protection cards.
- Check: choose a message, link, image or QR code.
- History: return to your saved personal checks.
- Settings: manage language, account and permissions. Family and business sections depend on the app and your access.

The question-mark help button explains the current section. An Android permission, enabling protection and sharing information with another person are separate choices.

04 / BUSINESS

Checking messages and links

Received a message asking for payment, a password or urgent action? Check it before opening its link or replying. Completing a manual analysis requires an internet connection.

Suspicious message

01 Tap Check and then “Suspicious message”.

02 Copy and paste the relevant text. Keep the context and suspicious link, but remove passwords, card details and unrelated personal data.

03 Tap “CHECK THIS” once and wait for the result.

04 Read the risk indication, explanation and suggested next steps. Choose “NEW CHECK” to examine different content.

Website address

01 Select “Website address”.

02 Paste the complete address, including http:// or https://. You do not need to visit the site before checking it.

03 Run the check and read the result before deciding what to do next.

Using the result

The result is guidance, not a safety certificate. If information is insufficient or the check is partial, do not treat the absence of a warning as approval. Confirm sensitive requests through a known, independent channel.

For example, a message saying “your account closes today” is not trustworthy simply because it displays a familiar logo. Open the service’s official app instead of following the link.



05 / BUSINESS

Photos and QR codes

Photo or screenshot

01 In Check, choose “Photo / Screenshot”.

02 Choose an image from your phone or use the camera option to photograph content on another screen. Grant the relevant permission only if you want to use it.

03 Keep the complete message, sender and links readable, without glare. Review the preview and remove unrelated private information before submitting.

04 Tap the photo/screenshot analysis button. The image is sent for text recognition as described in the privacy notice. Read the result.

Scan a QR before taking action

01 Select “QR code”, allow camera access and point the camera at the code.

02 Read the recognised content. For a website link, use the analysis option before opening its destination.

03 If the content is unsupported, do not assume it is safe. The app does not execute it or automatically connect you to Wi-Fi.

04 In a venue such as a café, ask staff to confirm the correct QR if you suspect tampering or a sticker placed over the original.

History and checking again

Open History to revisit a saved check. Its date matters: an old result does not establish the current situation. Personal history remains on the device; it is not a shared family or company dashboard.

06 / BUSINESS

Enabling Online Protection

Online Protection examines available text in new Android notifications for risk signals. It does not open your conversations or see text the operating system does not provide. Set it up separately on each device.

01 Open the Online Protection card on Home, or go to Settings → Online Protection.

02 Tap “ACTIVATE” and read which information is used.

03 Follow the notification-access guide. In Android, select PROPYLEUS and allow access if you agree.

04 Return to the app and also allow PROPYLEUS to display its own notifications so that you can see warnings.

05 Wait for the active and connected status. Use the screen’s test-warning option to check that a warning is displayed.

If you see App was denied access

Android may restrict sensitive permissions for apps installed from an APK file. Open phone Settings → Apps → PROPYLEUS → App info. If the menu offers “Allow restricted settings”, use it only for an installation you trust, then return to the guide. Do not disable Play Protect. Contact support if the option is missing.

Checking and stopping protection

If access is already enabled but the service is disconnected, follow the reset help: switch access off, wait two seconds and switch it on again. Then check the status in PROPYLEUS. A test warning checks notification display, not detection of every possible threat.

Use the protection switch to stop it. Stopping already active protection does not require a new online plan check. Sharing with a guardian or company is configured separately.

07 / BUSINESS

Enabling call protection

The card may be labelled Unknown Call Protection. It checks unknown numbers through a reputation service and displays available indications. It does not automatically block the call.

01 Open the call protection card on Home or its section in Settings.

02 Read the notice and follow the guide in order. Grant the permissions explained at each step.

03 At the call-app selection step, open settings and choose PROPYLEUS for caller identification and spam screening when Android offers that option. The exact label varies by device.

04 Return to PROPYLEUS and complete any remaining notification or warning-display steps.

05 Confirm that the card is active. If a step did not finish, reopen the guide rather than assuming protection is operating.

What a warning means

- Unknown number: there is not enough information for a reliable conclusion.
- Suspicious or reported as high risk: take care and verify independently. A report does not establish the caller’s identity.
- Caller-ID spoofing is possible. Do not disclose passwords or payment details. Hang up and call a known official number if needed.

If settings do not open

Check Android’s default apps for a caller-ID or call-screening option. If the required role is not offered, the feature may be unsupported on that device. Keep the guide’s message and contact support. Do not make emergency or premium-rate calls to test it.

08 / BUSINESS

Company workspace and departments

The base BUSINESS plan includes ten seats in total. Administrators organise the company workspace; each employee enables personal protection and selects permitted optional sharing on their own device.

Inviting an employee

01 Open Settings → “Business security centre”. Check the correct workspace and available seats.

02 Open the invitation and enter the employee’s email.

03 Select a permitted role. Only the owner can appoint administrators.

04 In “Department”, whose example is “e.g. Backoffice”, enter the actual department, such as Sales or Operations. Use a consistent name for everyone in the same department.

05 Review and send. The employee accepts in BUSINESS using the same invited email.

Managing members

In the members list, check each person’s name, role and department. Choose “Change department”, enter the correct name and tap “Save” to correct it. Role changes and member removal require the appropriate access and confirmation. Check the seat counter afterwards.

Employee first steps

- Accept the invitation and confirm that the correct company workspace appears.
- Enable Online Protection and call protection on your own phone.
- In company protection, read and separately choose any sharing of signals, text or location. Location also needs device permission.
- Do not include passwords, full card details or unrelated private conversations in an incident report.

Assigning an existing Wellness seat

As the add-on owner, open “Manage seats” from Wellness, load your seats and select an eligible member. Allocate a seat and confirm, then check the updated list. Releasing a seat is a separate action; it does not remove group membership or change billing. The member must enable their own Wellness permissions and consent.

09 / BUSINESS

Incidents suppliers and training

Reporting a suspicious incident

01 Open incidents in the Business security centre and choose a new report.

02 Describe what happened without access secrets. Select a category and priority.

03 Review and submit. Confirm that the report appears in the list permitted by your role.

04 The administrator reviews permitted reports, updates their status and records the resolution. Sharing a file, if needed, is a separate action.

Examples include a fake payment request from a manager, a supplier IBAN change, a link claiming to verify a bank account or theft of a business password. Pause a suspicious payment and confirm it through a known company channel.

Checking supplier details

01 Open suppliers and inspect the record and payment details available to your role.

02 If information is new or different, confirm it by calling an already known supplier number. Do not rely solely on contact details in the suspicious message.

03 Save a record change only if you have permission and independent verification has been completed.

A correctly formatted IBAN does not establish the beneficiary or legitimacy of a transaction. The company workspace is not a live view of all employees' private notifications.

Training and exercises

Open personal training or an available company exercise. Choose a lesson and answer one question at a time, reading the explanation. For campaigns, use only the tools displayed for your role. Completing a lesson is not a security certification.

10 / BUSINESS

Personal Wellness and SOS

Wellness uses real records from compatible Health Connect sources. Active Wellness access for your own seat is separate from the base subscription. A purchase does not automatically grant health-data permissions. This feature is for adult users.

Reading your own measurements

01 Synchronise your watch or supported device with its health app and Health Connect. Check there for recent records.

02 Open the Wellness card. Read the notice, confirm the measurements are yours and grant the requested permissions.

03 Request a reading and check its value, timestamp and source app. Available period views require the agreement shown on screen.

Automatic Wellness checks

01 Open “Automatic Wellness checks” → the step-by-step setup.

02 Choose available measurements, personal limits and a check interval. Follow a health professional’s guidance for limits.

03 For personal use choose “Only me, on this phone”. Grant health and background permissions and enable notifications.

04 Review the summary, confirm your agreement and enable the feature. Use the stop control to end automatic checks.

Checks use newly available records; they do not continuously measure from the watch. Blood-pressure or oxygen values are not created if absent from the source. Heart rate does not establish stress, and Wellness does not diagnose conditions.

Requesting help with SOS

Open SOS or “I need help now”, read what will be sent and select an available recipient. Include location only if you choose and have granted permission. Review and confirm sending. Options vary by edition. A recorded request does not mean it was read. In immediate danger, use emergency services without waiting for the app.

11 / BUSINESS

Team wellbeing by department

“Team wellbeing” uses optional stress and fatigue self-ratings with the appropriate Wellness access. Its chart shows a department-level aggregate. It does not display individual heart rates or infer stress automatically from a smartwatch.

For the employee

01 Open “Team wellbeing” in the company workspace. If no department is assigned, ask an administrator to add it.

02 Read the notice about optional participation and response retention.

03 Choose a rating from 1 to 5 for stress and fatigue, where 1 is low and 5 is high.

04 If you wish to participate, select the agreement and tap “Submit self-rating”. Wait for confirmation. The screen indicates if you have already responded for the period.

05 Use “Withdraw my responses” to withdraw.

For the administrator

Check that departments and the required Wellness access are configured. Read the usage notice before enabling the feature. Open the section and choose an available completed period. Periods last 14 days and require at least 10 distinct participants in the same department and period.

Averages are rounded to half-point steps. Names, individual responses and participant counts are not displayed. Ten purchased seats split into two departments of five are not sufficient to display a chart. Responses are deleted after 70 days.

Use the overview to discuss workload and support the team. Do not use it to rank individuals or make pay or disciplinary decisions. Refusal or withdrawal must not cause work-related disadvantage. An empty chart may simply mean that the requirements have not yet been met.

12 / BUSINESS

Subscription privacy and support

Plan and add-on access

Check the active plan in Settings. Before buying, read the term, final price and renewal conditions shown by Google Play. Do not repeat a purchase just because access did not appear immediately: check your PROPYLEUS account, Play account and connection, and use restore or purchase verification where offered.

For subscriptions purchased through Google Play, manage or cancel them in Play → profile → Payments and subscriptions → Subscriptions. Uninstalling the app or deleting an account does not cancel a subscription. Read the app's cancellation and refund section before proceeding.

Common difficulties

- Plan missing: check that you are in the correct app and account, and complete online verification.
- No notification: check notification permissions, active protection, connectivity and battery restrictions. For sharing, also check the recipient and consent.
- No measurements: first check the watch app and Health Connect. Missing data does not mean a normal condition.
- Invitation does not open: use the invited email and the private backup code. Request a new invitation if it expired.
- Check does not finish: check connectivity, input format and available allowance. Avoid repeated submissions.

Your choices remain yours

You can stop optional protection and sharing in their respective screens. Android permissions can also be withdrawn in phone settings. Leaving a group, deleting an account and cancelling a subscription are different actions. Read each confirmation before proceeding.

For help: propyleus@it-e.gr. Include your plan, app version, device model, Android version, exact message and the steps leading to it. Do not send passwords, health data or private messages. If a screenshot is needed, hide private details first.