A Guide to Bitdefender Scam Protection for Android

Scam Protection is a feature included in the paid version of Bitdefender Mobile Security for Android. This technology automatically detects link-based mobile attacks delivered through SMS, messaging apps, notifications and alerts you to emerging scam campaigns.

Scams, fraud, and malware campaigns often spread organically within the Android user community. In some cases, unsuspecting users share harmful links believing they are helping their contacts. Other times, malicious websites send deceptive notifications, or compromised devices distribute harmful messages without the owner's knowledge. Regardless of how these links spread, they pose a serious security risk. If you use Bitdefender Mobile Security for Android, the Web Protection module blocks phishing links as soon as you try to access them. Meanwhile, the Scam Protection module warns you that a link in a text message or notification is dangerous before you open it.

What is SMS phishing?

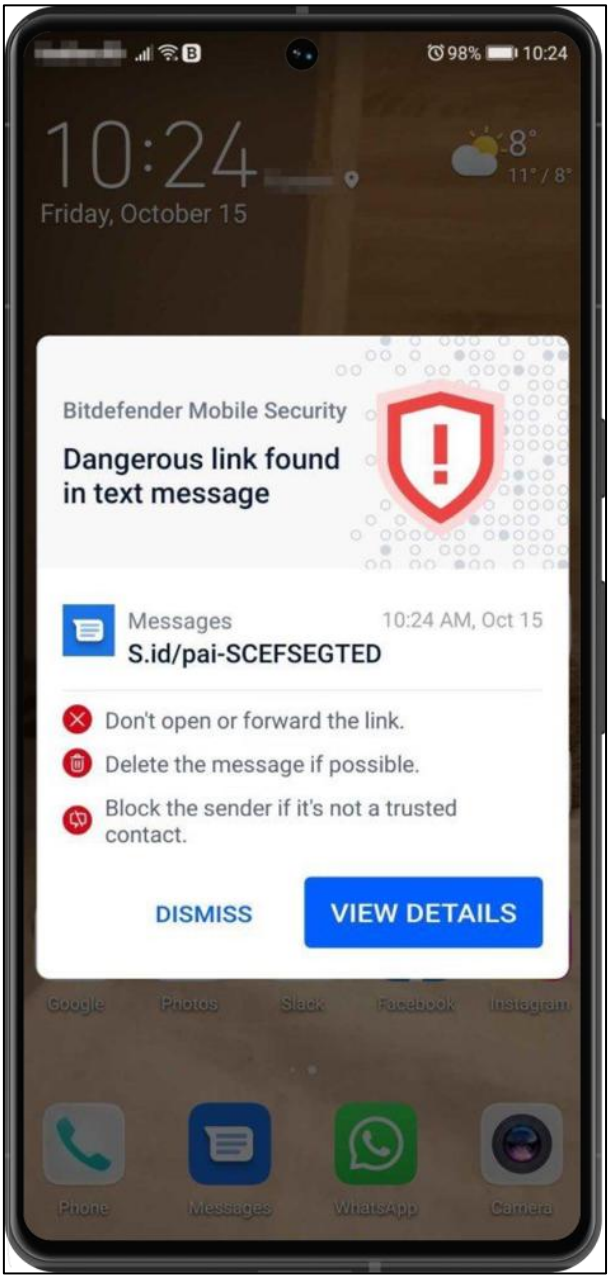
Phishing is a social engineering tactic that works across all platforms. Traditionally delivered via spam email, phishing campaigns use convincing messages to trick users into revealing sensitive information such as usernames, passwords, or credit card details. This tactic has evolved to include SMS, a method known as Smishing (SMS + phishing). These attacks often urge you to:

- Access a malicious link
- Reply with personal or financial information to claim a reward
- Call a premium-rate number

Some smishing attempts rely on scare tactics, warning that your personal data has been compromised and pressuring you to act immediately. Smishing messages are more common than many people realize, but malicious links spread through other channels as well. For example, websites frequently request permission to send notifications—a feature that can be abused. Users may receive harmful links through notifications that appear to come from the Android system itself. Additionally, malware campaigns often use SMS messages to distribute malicious payloads

Scam Protection features for Android

Chat Protection



The Chat Protection filter focuses on prevention, addressing potential threats before they escalate – including malware risks. Scam Protection monitors all incoming SMS messages and Android notifications in real time.

When a dangerous link is detected in a message, a warning appears on your device.

Bitdefender provides two options:

- Dismiss the alert
- View more details and receive practical advice, such as:
    - Don’t open or forward the detected link
    - Delete the text message (if possible)
    - Block the sender if they’re not a trusted contact
    - Uninstall the app that sends malicious notification links

ⓘ **Note**: Due to Android operating system limitations, Bitdefender cannot delete text messages or take direct action on SMS or notification sources. If you ignore the Scan Protection warning and attempt to open the link, the Web Protection feature will automatically block it and prevent infection.

Scam Radar

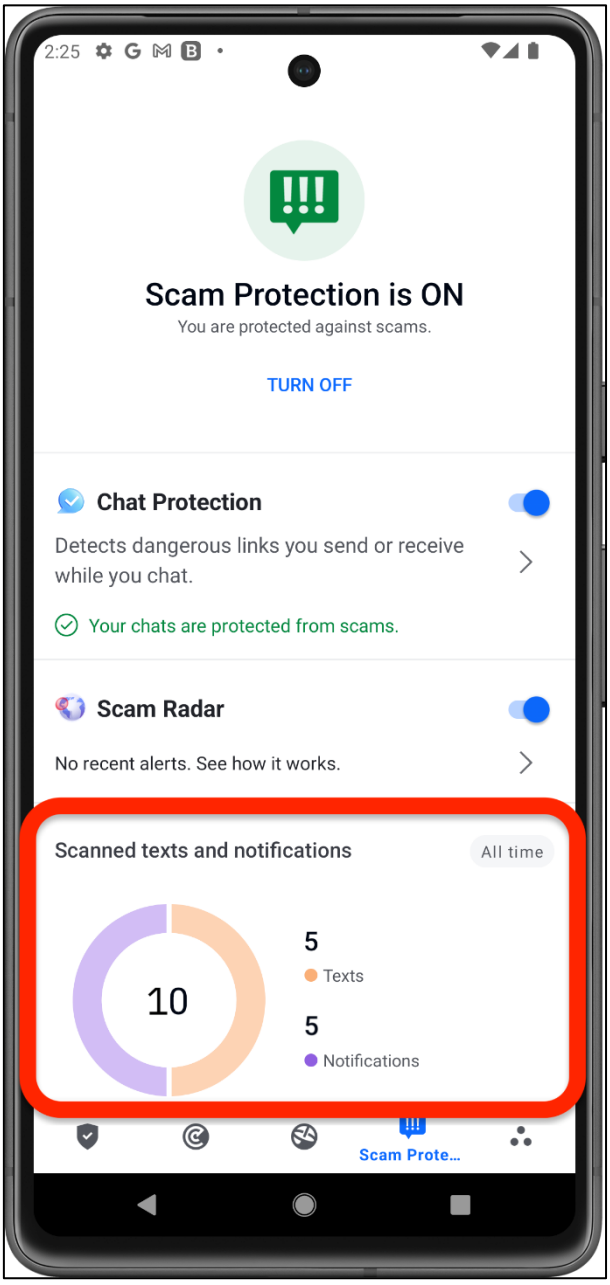
Scam Radar continuously monitors local scam activity. When a new scam wave begins to spread, you’re notified right away. Scam Radar provides AI-driven scam prevention:

- Early warnings about high-risk scam campaigns
- Examples of scam text messages or fake Facebook ads
- Highlighted key warning signs and suspicious keywords
- Practical tips to stay protected

Benefits:

- Helps you recognize scams before interacting with them
- Keeps you informed about local scams
- Improves awareness of evolving attack tactics

Scanned texts and notifications



Once Scam Protection is enabled, a donut chart displays the total number of scanned texts and notifications in the Scanned texts and notifications section. A legend below shows the exact number of:

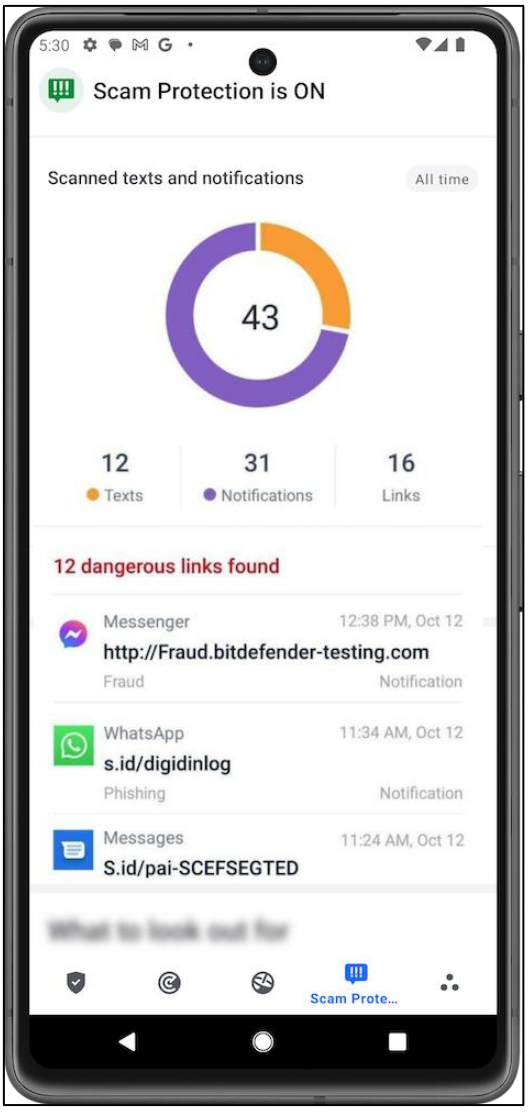
- Texts
- Notifications
- Links scanned

ⓘ **Note**: Links are not included in the chart total but are counted and displayed separately in the legend area.

The Scanned texts and notifications list will display the last 3 detections. To extend the list by 3 more, press LOAD MORE. Exiting the Scam Protection module will collapse this list.

When Scam Protection for Android detects a dangerous link, the following details are shown:

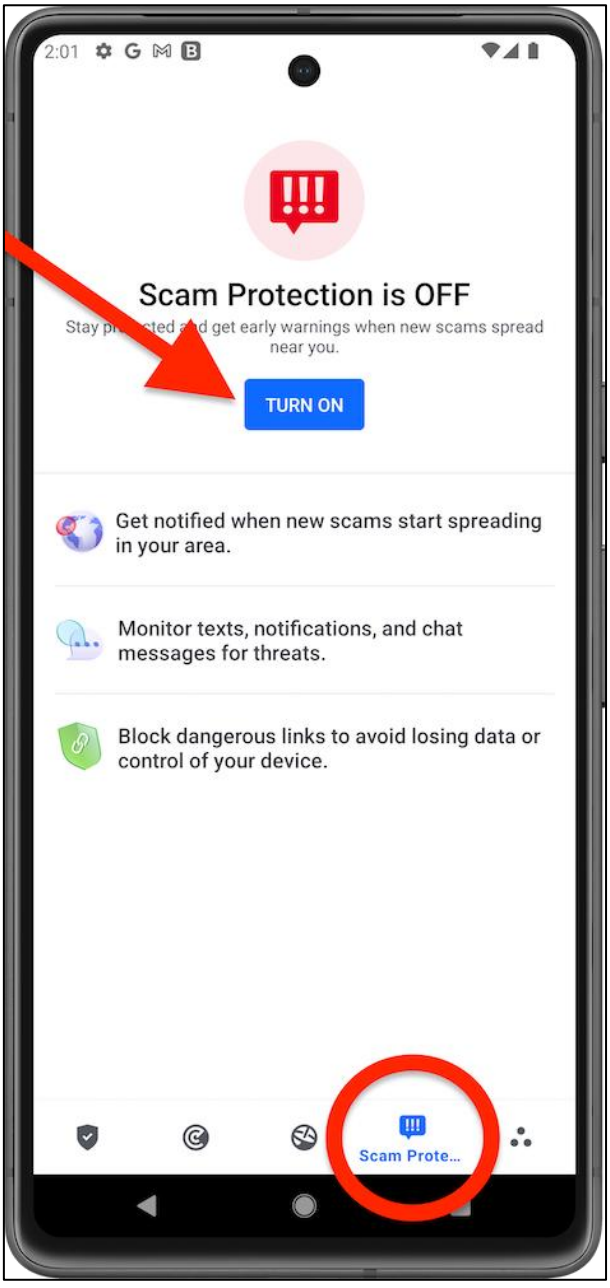
- Name of the app that generated the notification
- Timestamp (date and time)
- URL of the detected link (non-clickable)
- Threat type
- App category (text or notification)



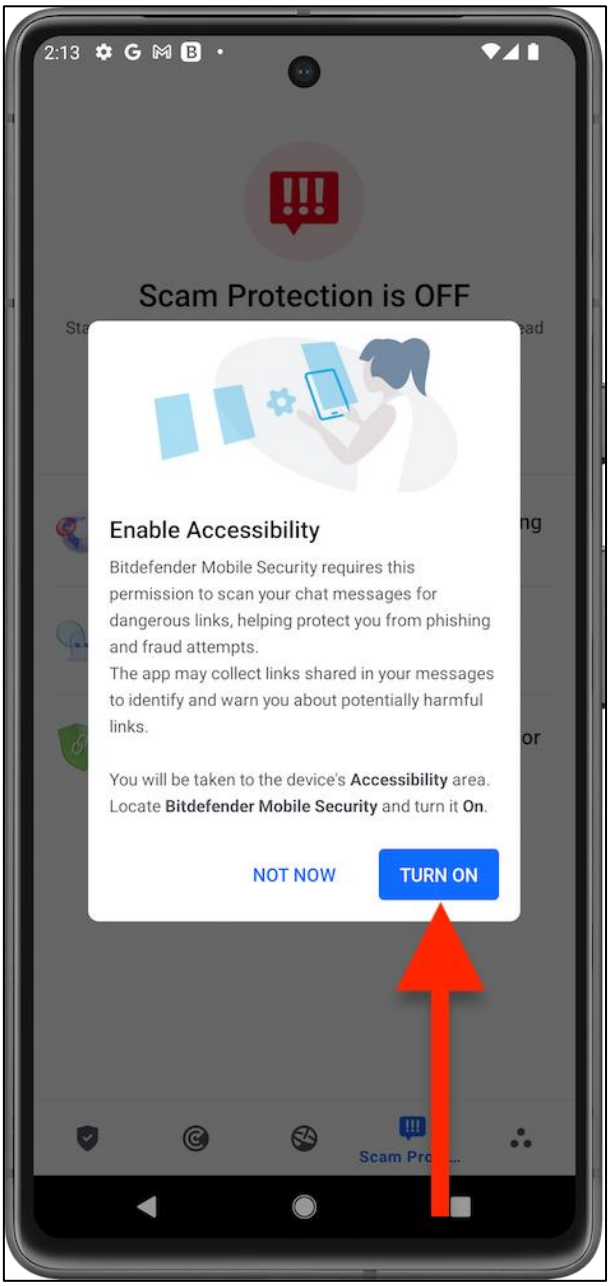
Set up Scam Protection in Bitdefender Mobile Security for Android

To set up Scam Protection on Android, you need to grant the Bitdefender Mobile Security app Accessibility, Notification and SMS permissions. Follow these steps:

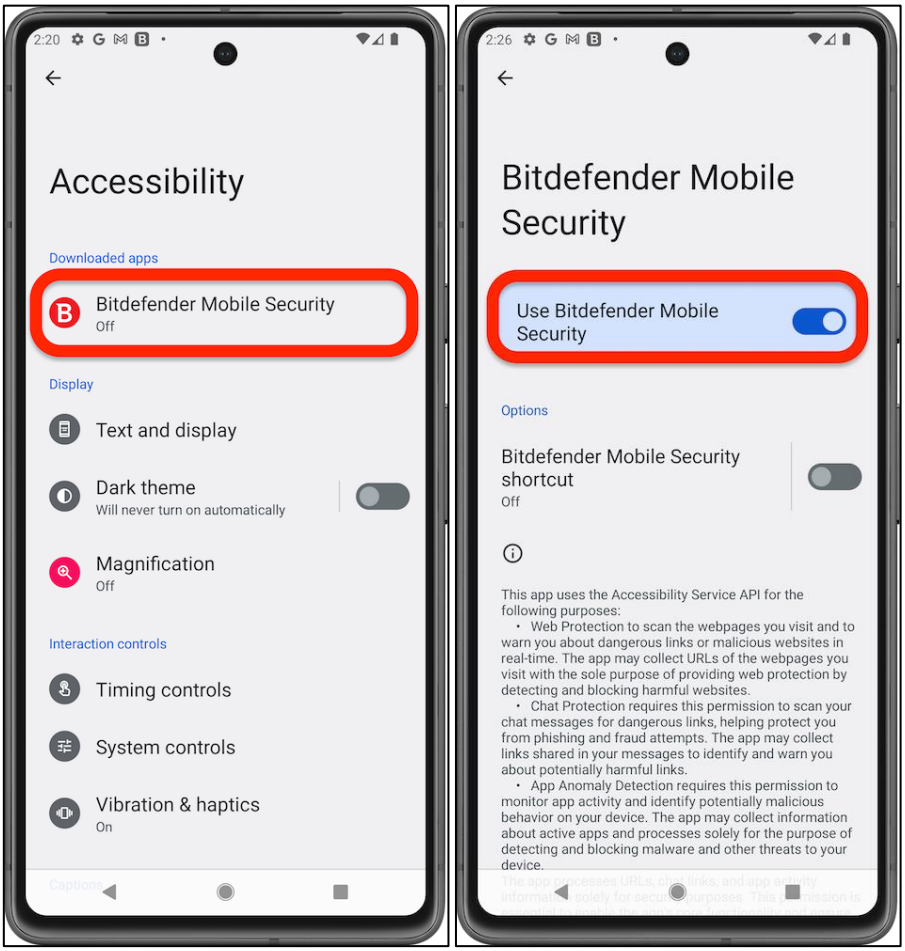
1. Open the Bitdefender Mobile Security app installed on your Android phone or tablet.
2. Tap the **Scam Protection** icon in the bottom navigation bar, then tap **Turn on**.



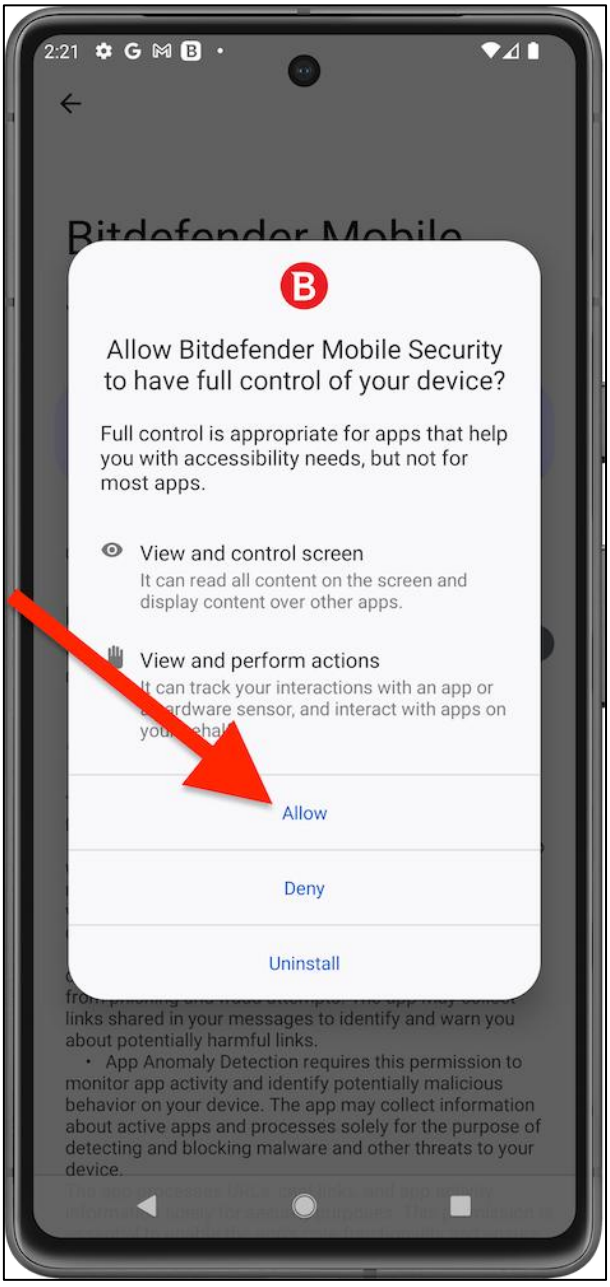
3. Tap **Turn on** again to allow the app to scan notifications and warn about phishing and fraud attempts.



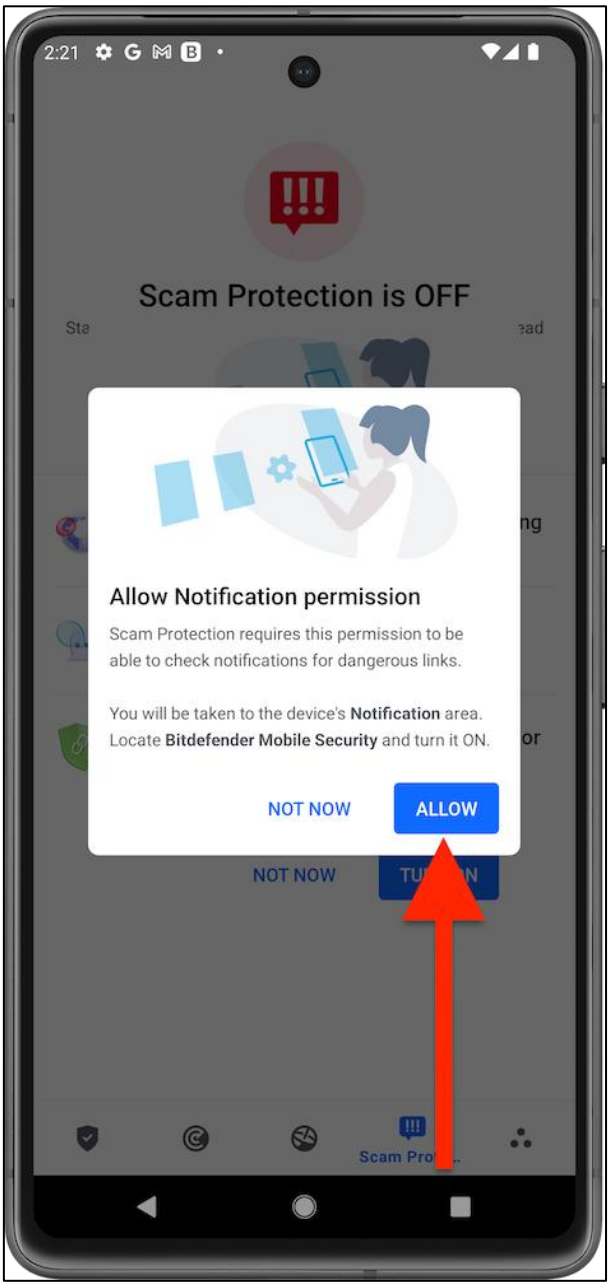
4. In the Accessibility list, enable Bitdefender Mobile Security.



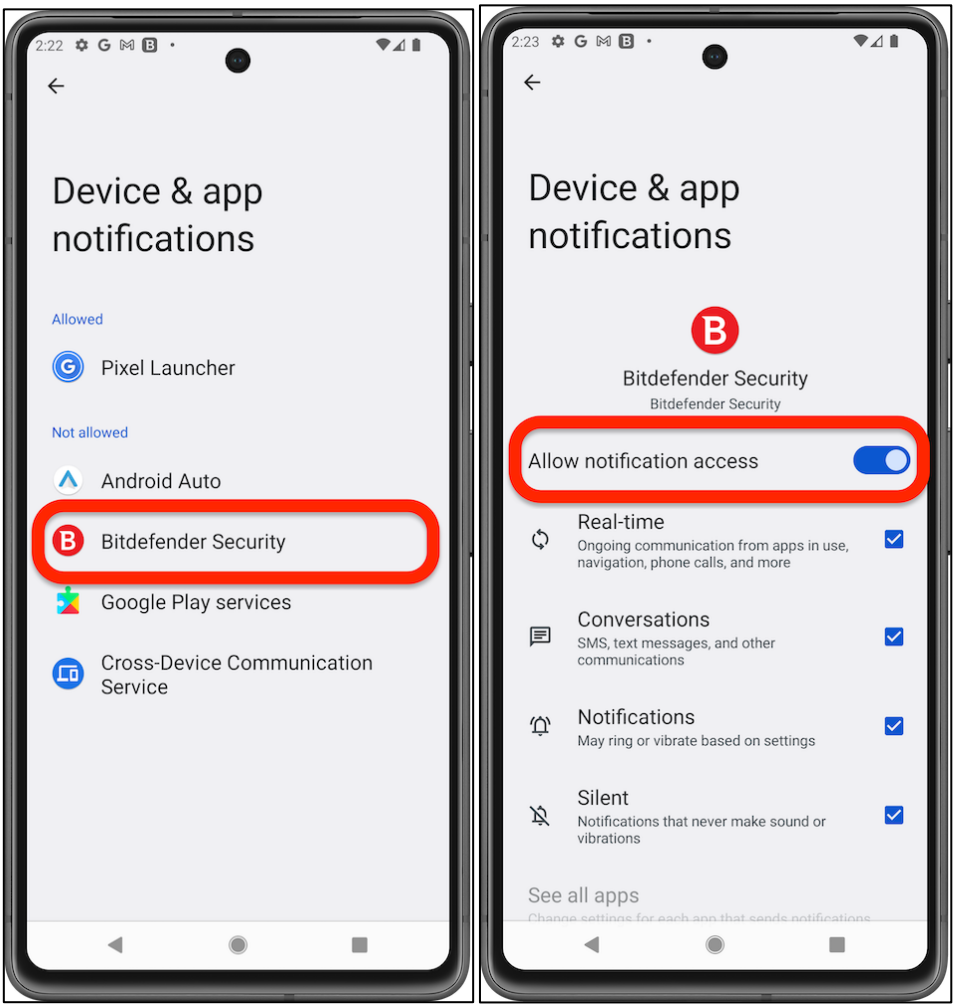
5. Choose **Allow** to confirm the action.



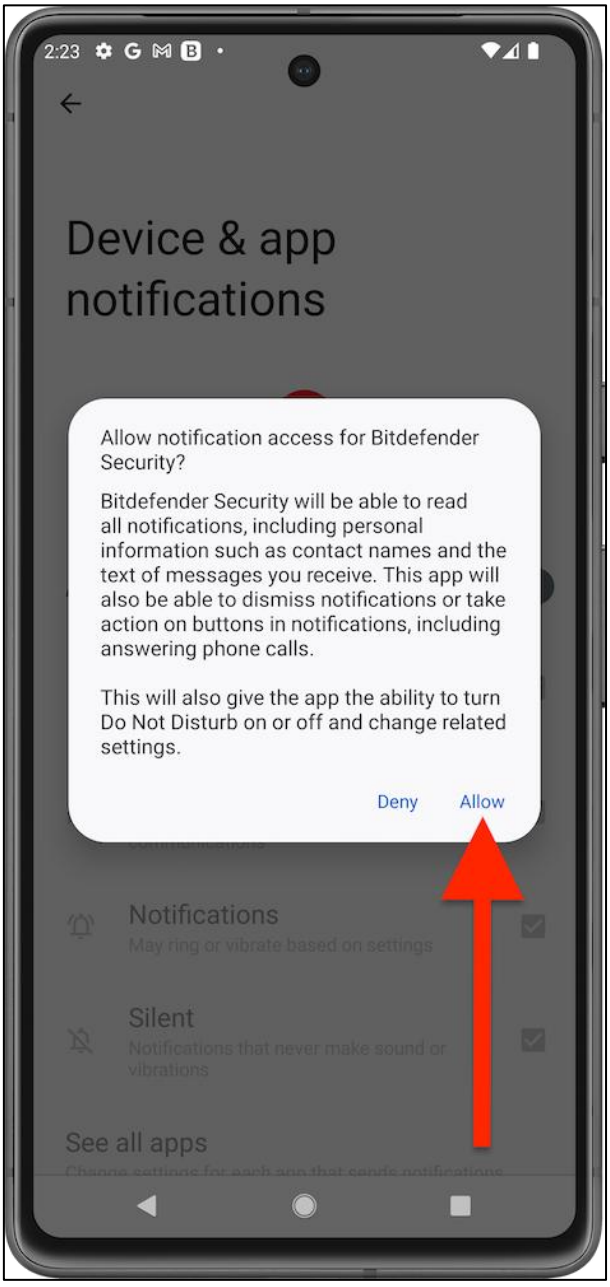
6. Return to the Scam Protection screen and tap **Allow** to enable SMS scanning.



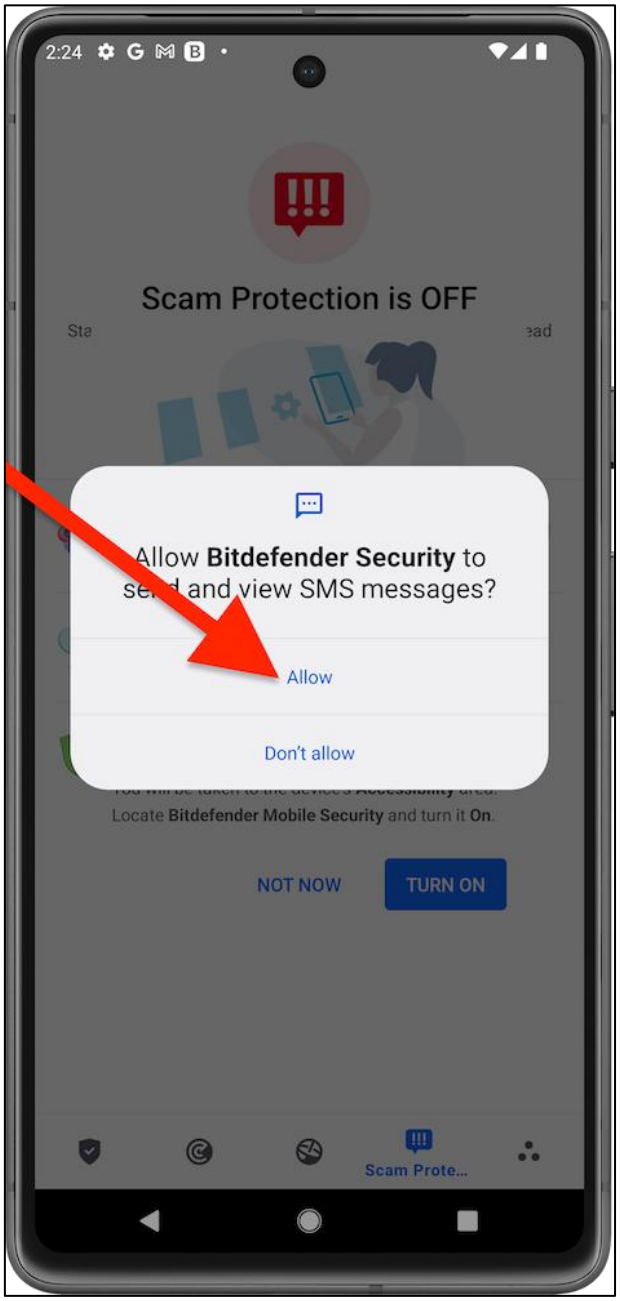
7. Allow notification access for Bitdefender Security.



8. Confirm by tapping **Allow**.



9. Return and allow the app to send and view SMS messages when prompted.



10. Tap **Turn on** in the Enable Accessibility screen.