C

Chargeware: Premium SMS, Toll Fraud, Unwanted Charges, and Recovery

Chargeware is mobile software associated with unwanted premium SMS, carrier-billing, or subscription charges. Learn how to identify the billing path, cancel it, remove the app, and dispute charges.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 How chargeware creates costs

02 Chargeware, toll fraud, SMS Trojan, and fleeceware

03 Warning signs

04 What to do after an unwanted charge

05 Android and iPhone checks

06 Prevention

07 Frequently asked questions

08 References

Chargeware is a loose term for mobile software that causes unwanted or insufficiently disclosed charges, commonly through premium SMS, carrier billing, paid subscriptions, or in-app payment flows. It may be outright malware that acts without consent or a deceptive app that obtains consent through confusing prompts and hidden terms.

The useful question is not only whether the app is called chargeware, but how the charge was authorized, which billing channel was used, and whether the device still has an active subscription or malicious app.

01 How chargeware creates costs

Billing path	How abuse works	Where the charge appears
Premium SMS	An app sends a message to a high-rate number or enrolls the number in an SMS service.	Mobile carrier bill or prepaid balance.
Wireless Application Protocol or carrier billing	Malware navigates a mobile subscription page and may intercept or hide confirmation messages.	Carrier account under third-party services or content.
App-store subscription	A misleading free trial converts to an expensive recurring plan or the cancellation terms are obscured.	Google Play, Apple, or another store purchase history.
Card or wallet payment	A deceptive app or page collects a payment method or starts a recurring merchant charge.	Bank, card, or digital-wallet statement.
In-app purchase	Weak device controls, social engineering, or account compromise enables unauthorized purchases.	App-store receipt and account history.

02 Chargeware, toll fraud, SMS Trojan, and fleeceware

- **Toll-fraud malware** subscribes a user to premium services without informed consent, often through a complex carrier-billing workflow.
- **SMS or call fraud** uses premium messages or calls to generate charges. Modern mobile operating systems add permission and confirmation barriers, but malware can still abuse vulnerabilities or deceive users.
- **Fleeceware** usually provides some advertised functionality but uses excessive subscription pricing, short trials, or confusing cancellation. It may violate store policy without using a hidden malware technique.
- **Chargeware** is an umbrella-style label used inconsistently for some or all of these unwanted billing behaviors.

A legitimate paid app is not chargeware merely because it has a subscription. Clear price disclosure, informed consent, accessible cancellation, and delivery of the promised service matter.

03 Warning signs

- Premium SMS or third-party content charges appear on the carrier bill.
- A subscription confirmation arrives for a service you did not request.
- A newly installed app asks for SMS, notification access, accessibility, phone, or browser permissions unrelated to its stated purpose.
- The app hides its icon, blocks removal, or was installed from an APK link rather than a trusted store.
- Verification screens repeatedly ask for a phone number or one-time code without explaining a price.
- Small recurring card or app-store charges use an unfamiliar merchant name.
- Confirmation messages disappear or notification history shows suppressed billing alerts.

04 What to do after an unwanted charge

1. **Preserve evidence.** Screenshot the app listing, permissions, receipt, subscription screen, messages, merchant descriptor, dates, and amounts before uninstalling anything.
2. **Identify the billing channel.** Check the carrier account, app-store subscriptions and purchase history, bank statement, and digital-wallet activity. Cancelling in one place does not cancel a different billing channel.
3. **Cancel the subscription through the official provider.** Use the carrier, store, or financial institution's own app or website, not a link sent by the suspicious service.
4. **Contact the billing provider promptly.** Ask the carrier to block premium SMS or third-party billing and the store or bank about its dispute process. Do not misstate a trial you intentionally accepted; explain exactly what was or was not disclosed.
5. **Remove the app.** Revoke device-administrator, accessibility, notification, SMS, and installation permissions first if Android will not allow normal uninstall.
6. **Run a mobile security scan and update the device.** Review all recently installed apps and profiles, not only the app whose icon you noticed.
7. **Secure accounts.** Change the app-store, email, and carrier-account passwords if their credentials or recovery codes may have been exposed. Sign out unknown sessions and enable MFA.
8. **Monitor for recurrence.** Review the next carrier and financial statements because cancellation and removal do not automatically reverse past charges.

05 Android and iPhone checks

Android	iPhone or iPad
Review Play subscriptions, Special app access, Accessibility, Device admin apps, notification access, SMS permissions, and apps installed from unknown sources.	Review Apple subscriptions, purchase history, profiles or device management, VPN configurations, calendar subscriptions, and unfamiliar apps.

Android	iPhone or iPad
Use Play Protect and a reputable mobile security product; install OS and security updates.	Install iOS updates and remove unrecognized configuration profiles. Traditional third-party scanners have more limited visibility on iOS.

Menu names vary by OS version and manufacturer. Search the device settings for the named permission if the path differs.

06 Prevention

- Install apps from a trusted store and verify the developer, recent reviews, permissions, and privacy information.
- Avoid sideloaded "premium unlocked" APKs and update prompts delivered by ads or messages.
- Read the price, renewal period, trial end date, and cancellation method before confirming.
- Require authentication for every purchase and use family purchase controls on shared devices.
- Ask the carrier whether premium messaging and third-party billing can be disabled or limited.
- Do not give an app accessibility, SMS, or notification access unless its core function clearly requires it.

07 Frequently asked questions

Will deleting the app cancel the subscription?

Usually not. Cancel through the carrier, app store, or merchant that controls the billing relationship, then remove the app.

Can an app charge a card stored for another app?

Apps normally cannot freely read another app's stored card. Charges may instead use the shared app-store account, carrier billing, a compromised account, or payment details entered into a deceptive screen.

Is every expensive subscription malware?

No. Excessive pricing and poor disclosure may be deceptive or violate store rules, but malware additionally performs unauthorized or harmful technical behavior. Preserve evidence and report both the billing and the app.

08 References

- NIST Mobile Threat Catalogue: Premium SMS Fraud
- Microsoft: Toll fraud malware on Android
- Malwarebytes: SMS Trojan

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com