

Download and Install ScamShield

STRONG PASSWORD

IhadKAYAtoastAT8am!

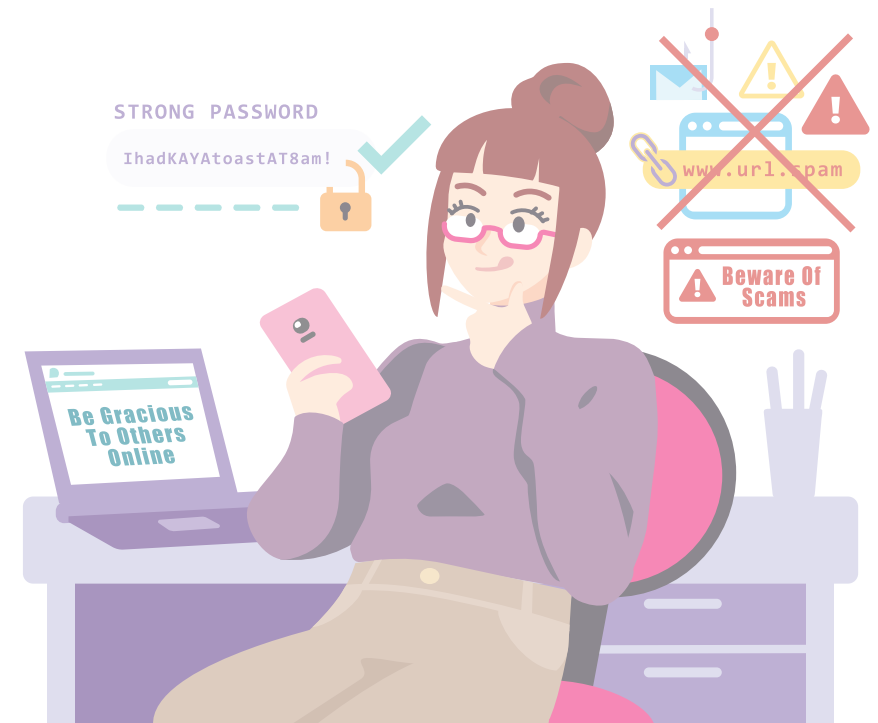


Scan the QR code below to learn more about Be Safe, Smart and Kind Online competency:



Content

Introduction	2
About ScamShield	3
Apple (iOS) - Set up the Scamshield App	4
Android - Set up the Scamshield App	9
Report Spam Calls and Messages	13
Check if it is a Scam Call, Message or Link	17



Introduction

The Digital Skills for Life (DSL) guide is a collection of booklets that is designed to help you learn essential digital skills for daily living. It offers step-by-step instructions and quick tips that empowers you to navigate the digital landscape confidently and safely.

It is designed for anyone who wants to pick up essential digital skills for daily living.

The DSL skills are grouped into 5 competency areas as shown in the diagram.

Learning Outcomes:

This guidebook focuses on the 'Be Safe, Smart and Kind Online' competency, where you will learn:



- Able to secure mobile device and accounts as well as identify and safeguard against malicious online content and scams.



The guidebook is based on common software icons and mobile device settings. Please note that certain features may differ across different mobile devices and models.



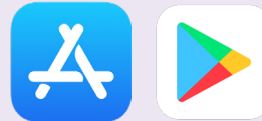
About ScamShield

ScamShield is an app developed by Open Government Products in collaboration with the National Crime Prevention Council and the Singapore Police Force. With the ScamShield app, you can expect to receive reduced numbers of scam calls and expect fewer malicious SMSes.

Why is it important to download ScamShield?

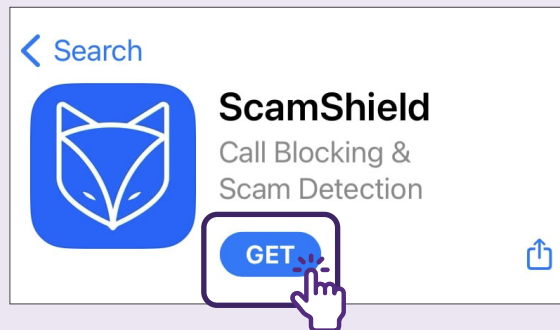
- **Blocks and filters** scam calls and SMSes
- **Check** if a suspicious call, message (SMS, WhatsApp, and Telegram) or link is a scam
- **Report** suspicious calls, messages (SMS, WhatsApp, and Telegram) or links

1 Select Apple App Store or Google Play Store



Find and tap "Apple App Store" or "Google Play Store" on your mobile device.

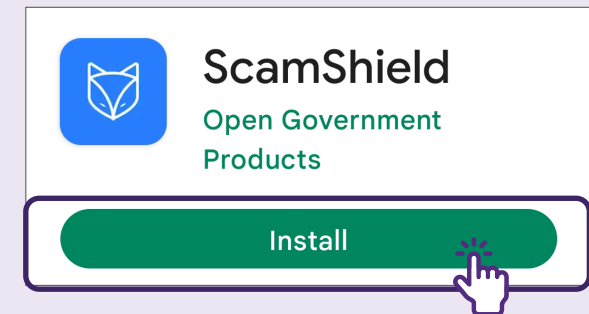
2 Search and Install ScamShield on iOS mobile device



Or scan the QR Code below.



2 Search and Install ScamShield on Android mobile device



Or scan the QR Code below.



Apple (iOS) - Set up the ScamShield App

1 Launch ScamShield



Find and tap "ScamShield" on your mobile device.

2 Select Set up

Set up your ScamShield app for better protection

The app requires permissions to detect scam calls and SMSes

- Scam call blocking not set up **Set up**
- Scam SMS filtering not set up **Set up**

Check for scams →

Know from trusted sources if something suspicious is a scam

3 Select Next to set up scam call blocking

Set up scam call blocking

This will let ScamShield block calls from numbers marked as scams by the authorities.

+1 480 896 1988

+62 857 7543 55

+65 8765 74

ScamShield respects your privacy, and cannot listen to any calls on your phone. [Learn more](#)

Next

4 Select Open Settings

Follow these steps to set up call blocking

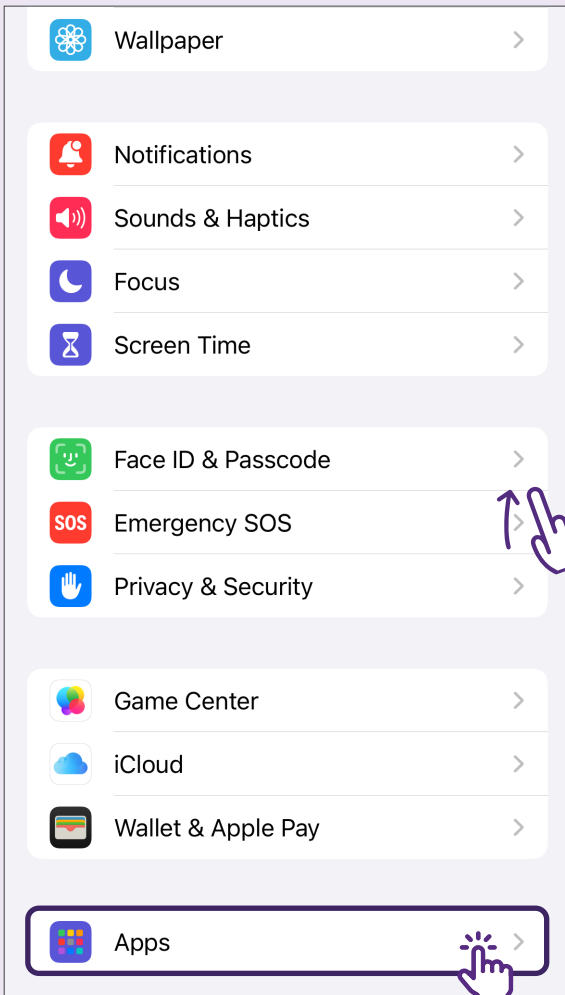
- Go to Settings and scroll down to **Apps**
- Search for **Phone**
- Scroll down and tap **Call blocking & identification**
- Tap ScamShield to turn it on
- Return to the ScamShield app, and tap **I've done this**

Open Settings

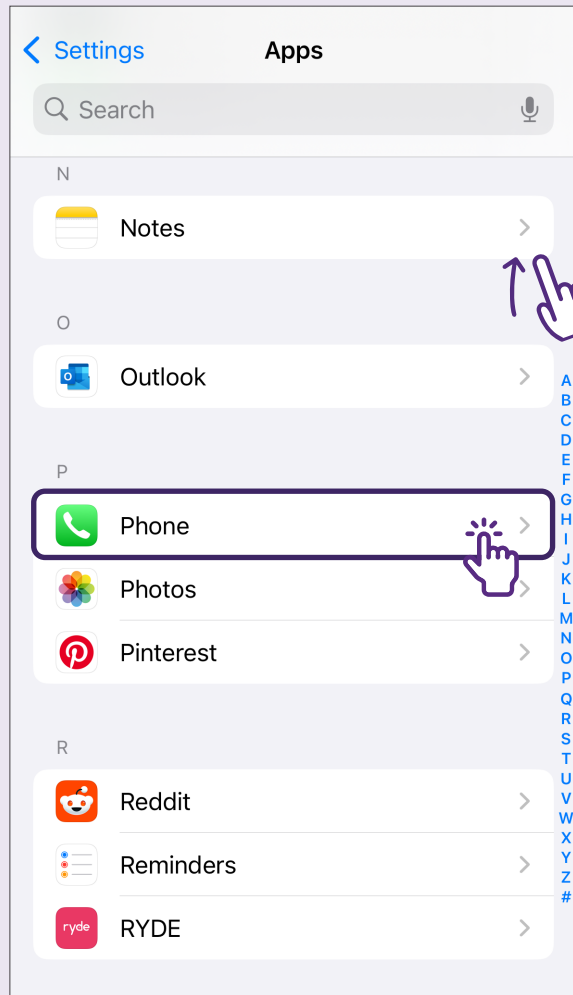
I've done this

Apple (iOS) - Set up the ScamShield App (Enable Call Blocking)

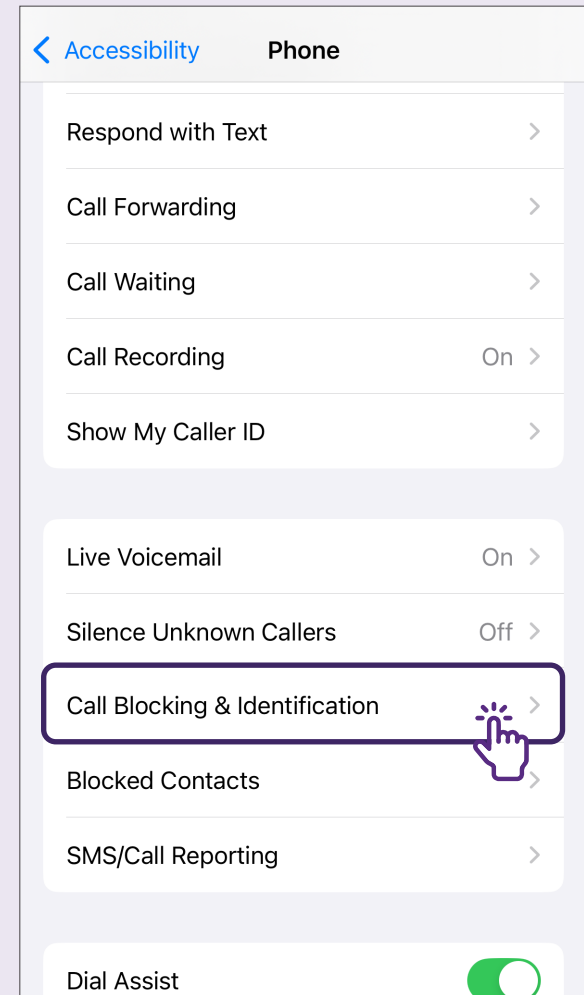
5 Select Apps



6 Select Phone



7 Select Call Blocking & Identification



8

Enable Call Blocking

[< Back](#) Call Blocking & Identification

CALL IDENTIFICATION



ScamShield



Allow Call blocking and identification apps to block calls and provide caller ID. These apps are not able to access any information about your incoming calls.

Turn on: Green

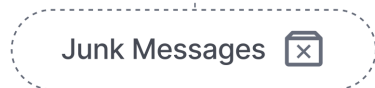
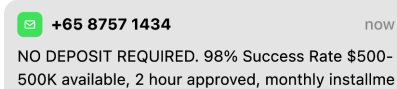
Turn off: Grey

Apple (iOS) - Set up the ScamShield App (Enable SMS Filtering)

3 Select Next to set up scam SMS filtering

Set up scam SMS filtering

This lets ScamShield detect suspicious SMSes from unknown numbers or known scammers, and send them to your Junk folder.



ScamShield respects your privacy, and will never read SMSes from numbers in your contact list.
[Learn more](#)

Next

4 Select Open Settings

Follow these steps to set up SMS filtering

- Go to Settings and scroll down to **Apps**
- Search for **Messages**
- Scroll down and tap **Unknown & Spam**
- Tap **Filter Unknown Senders**
- Tap **ScamShield**, and then **Enable**

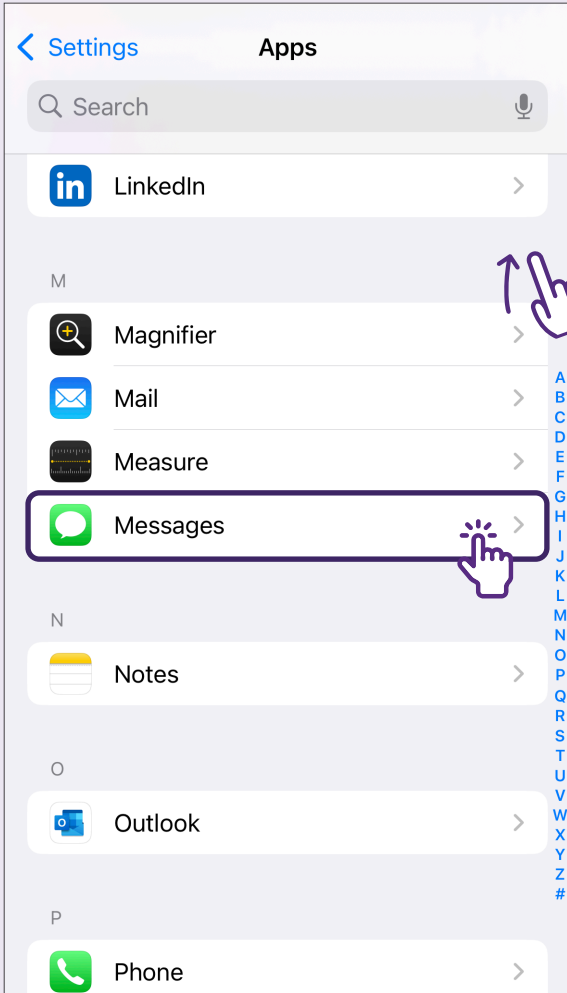
Open Settings

I've done this

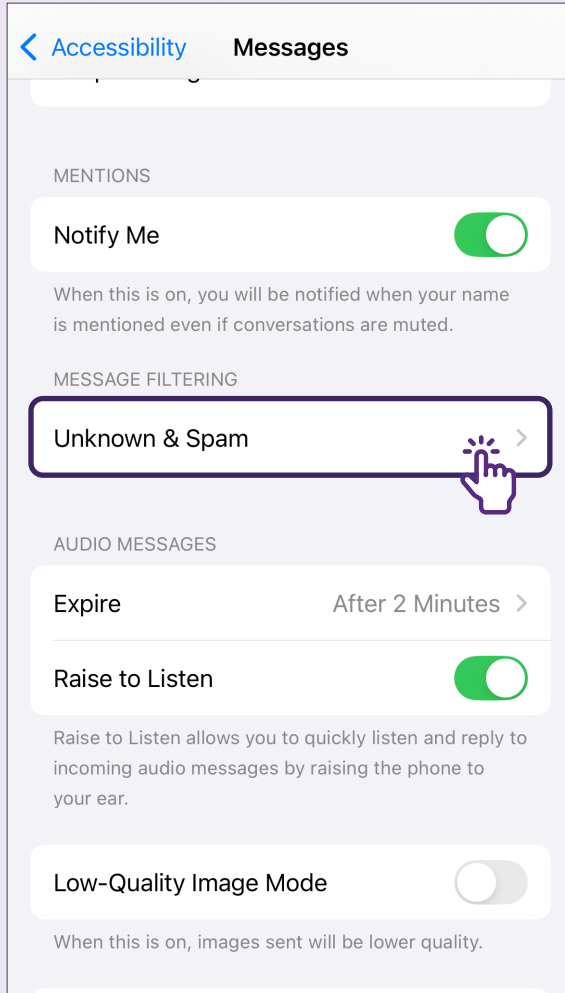
5 Select Apps

- Wallpaper
- Notifications
- Sounds & Haptics
- Focus
- Screen Time
- Face ID & Passcode
- Emergency SOS
- Privacy & Security
- Game Center
- iCloud
- Wallet & Apple Pay
- Apps

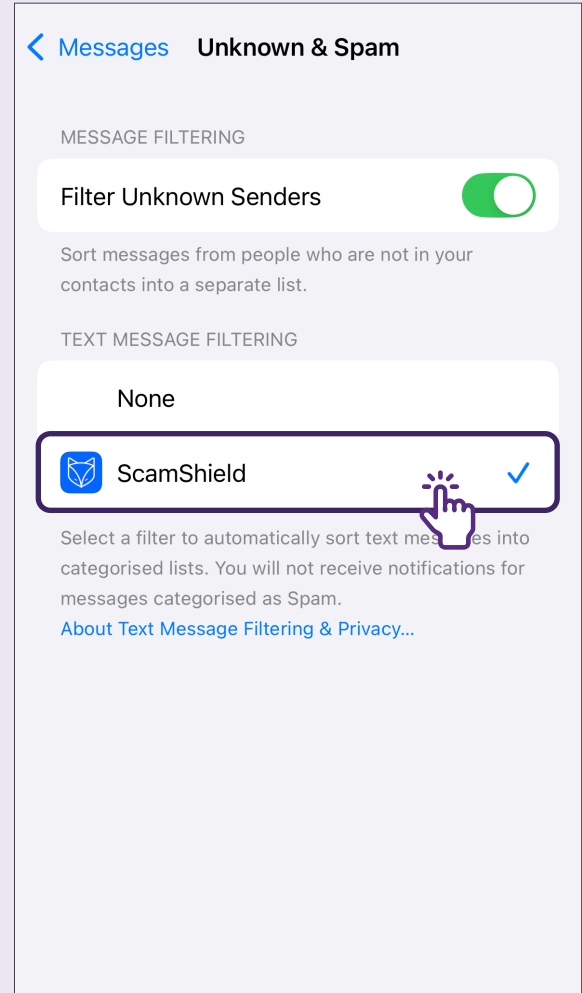
6 Select Messages



7 Select Unknown & Spam



8 Enable SMS Filtering



Android - Set up the ScamShield App

1 Launch ScamShield



Find and tap "ScamShield" on your mobile device.

2 Select Set up

The screenshot shows the ScamShield app's setup screen. At the top, there's a shield icon with a red exclamation mark. Below it, the text reads "Set up your ScamShield app for better protection" and "The app requires permissions to detect scam calls and SMSes". There are two red boxes with white text: "Scam call blocking not set up" and "Scam SMS filtering not set up", each with a red "Set up" button. A hand icon is shown clicking the "Set up" button for "Scam call blocking". At the bottom, there's a "Check for scams" button with a right arrow and a subtext: "Know from trusted sources if something suspicious is a scam".

3 Select Next to set up scam call blocking

The screenshot shows the "Set up scam call blocking" screen. The title is "Set up scam call blocking" with a subtitle: "This will let ScamShield block calls from numbers marked as scams by the authorities." Below the text is a large blue shield icon with the ScamShield logo. There are two red phone numbers: "8 1234 5467" and "+66 438". At the bottom, there's a blue "Next" button with a hand icon clicking it, and a link "I'll do this later".

4 Select Next

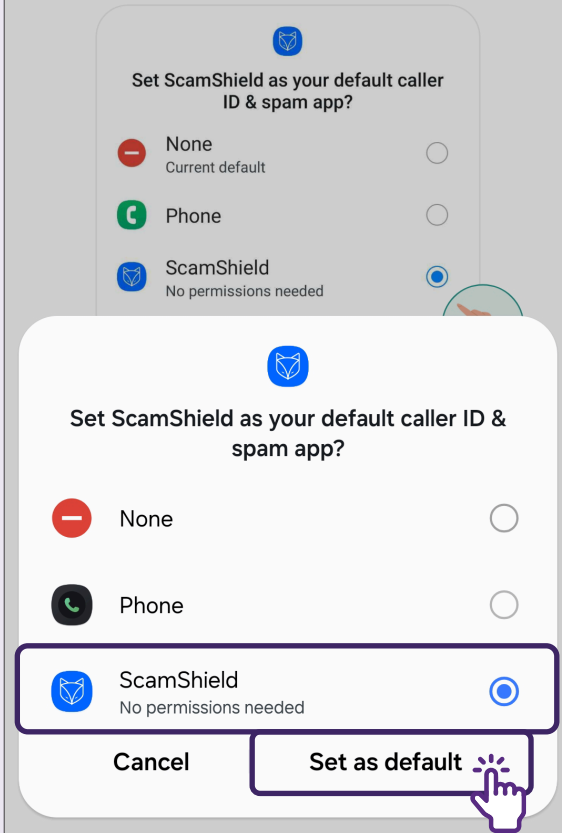
The screenshot shows the "Tap 'Set as default' at the next step" screen. The title is "Tap 'Set as default' at the next step" with a subtitle: "This will let ScamShield block calls from numbers marked as scams by the police." Below the text is a dialog box titled "Set ScamShield as your default caller ID & spam app?". It has three radio button options: "None" (Current default), "Phone", and "ScamShield" (No permissions needed). The "ScamShield" option is selected. There are "Cancel" and "Set as default" buttons. A hand icon is shown clicking the "Set as default" button. At the bottom, there's a blue "Next" button with a hand icon clicking it, and a link "I'll do this later".

Android - Set up the ScamShield App (Enable Call Blocking)

5 Select ScamShield and Set as default

step

This will let ScamShield block calls from numbers marked as scams by the authorities.



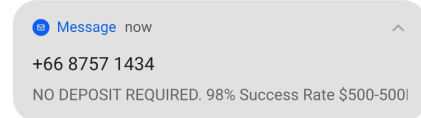
Android - Set up the ScamShield App (Enable SMS Filtering)

3 Select Next to set up scam SMS filtering

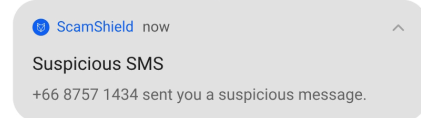
Set up scam SMS detection

This lets ScamShield notify you when you receive suspicious SMSes from unknown numbers or known scammers.

Suspicious SMS



Alert from ScamShield



ScamShield respects your privacy, and will never read SMSes from numbers in your contact list. [Learn more](#)

Next

4 Select Allow ScamShield to access your contacts

Tap 'Allow' at all steps to set up scam SMS detection

ScamShield needs all these permissions to work correctly.

Send Notifications
To alert you of scam SMSes

Access Contacts
To only screen numbers you haven't saved in your contacts

Send and view SMSes
To detect scam SMSes

Allow **ScamShield** to access your contacts?

Allow

Don't allow

5 Select Allow ScamShield to send and view SMS

Tap 'Allow' at all steps to set up scam SMS detection

ScamShield needs all these permissions to work correctly.

Send Notifications
To alert you of scam SMSes

Access Contacts
To only screen numbers you haven't saved in your contacts

Send and view SMSes
To detect scam SMSes

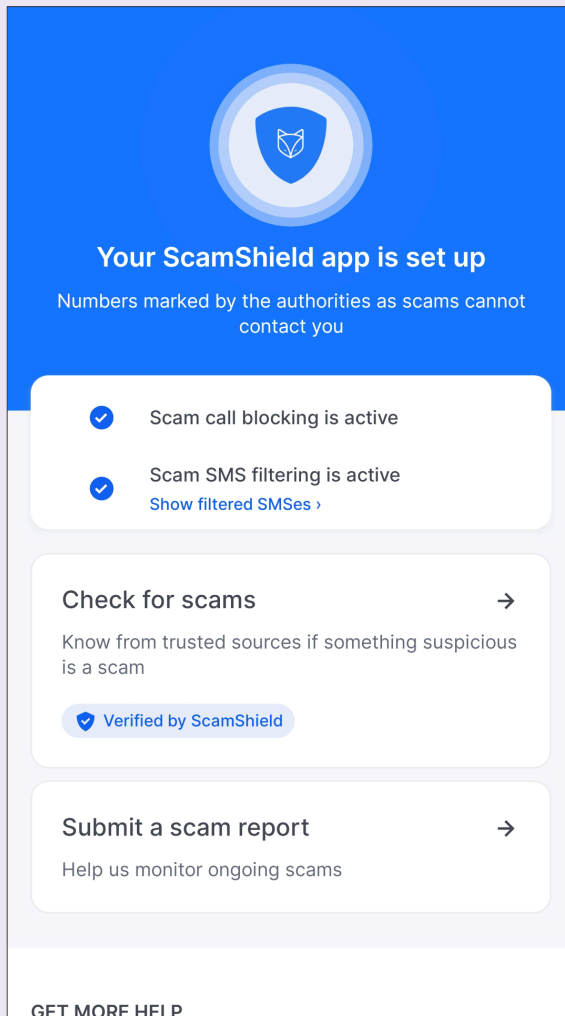
Allow **ScamShield** to send and view SMS messages?

Allow

Don't allow

Set up the ScamShield App (Completion)

1 Your ScamShield app is set up



Both Apple iOS or Android will show similar screen on the app's page to indicate successful set up.

Report Scam Calls and Messages

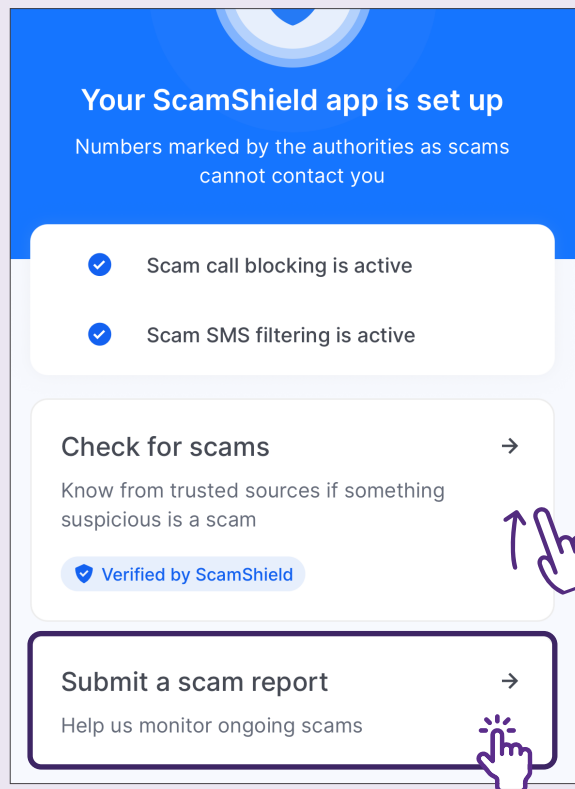
- All detected scam messages are automatically reported and sent to authorities for review.
- Scams are always evolving, with new types appearing all the time. ScamShield uses AI and learns from every report. If you spot a new scam number or message, report it on the ScamShield app to keep everyone safe!

1 Launch ScamShield

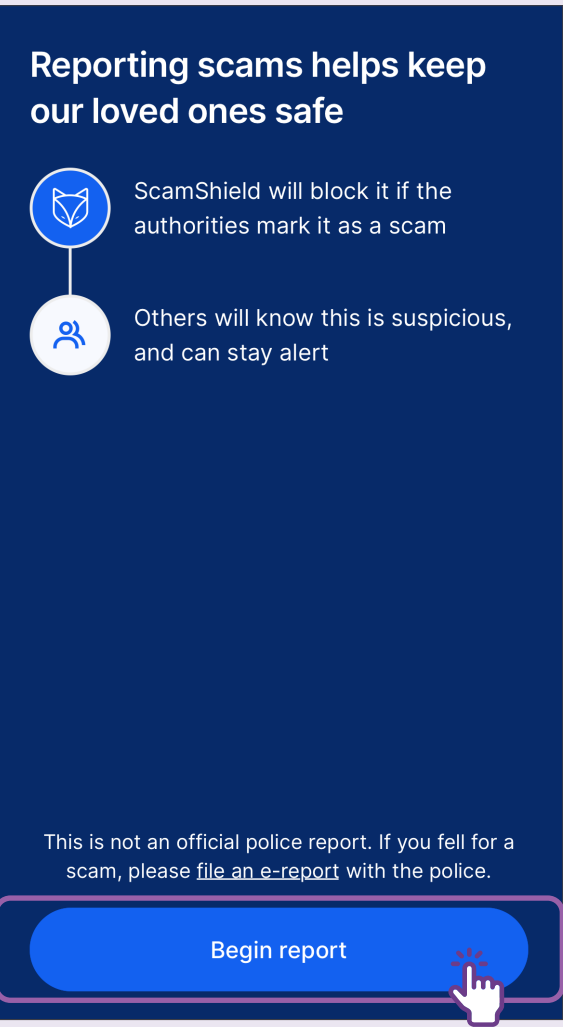


Find and tap "ScamShield" on your mobile device.

2 Select Submit a scam report



3 Select Begin report



4 Select Understood

Reporting scams helps keep our loved ones safe



ScamShield will block it if the authorities mark it as a scam



ABOUT YOUR PRIVACY

Choose what you want to share

Avoid sending personal details as we **may share these with third parties** for security checks. [Learn more](#)

- × NRIC and addresses
- × Passwords and login credentials
- × Confidential links to your personal accounts or documents

Understood

5 Select what you would like to report

What would you like to report?

A number that called you

A message you received

A website link

6 Select what type of call was it

What type of call was it?

Phone call

WhatsApp call

Telegram call

7 Enter the caller's number and select Next

What was the caller's number?
Enter the full number with the country code, if any (e.g. +6598765432)

+6598765432

Next

8 Select who was on the call

< [Progress bar] x

Who was on the call?

- A person
- A recorded voice
- I didn't pick up the call

9 Select who did they claim to be

< [Progress bar] x

Who did they claim to be?

- Bank representative
- Government official
- Phone company provider
- Hospital staff
- Others

10 Describe the call and select Review report

Please describe the call

Tell us what the caller said, or what information they asked for

Description of the call (optional)

Review report

11 Review your report and select Submit report

Does this look right?

Please make sure this information is correct and complete

Type of call

Call

Caller's number

+6598765432

Details

A person

Bank representative

Call description

Let us know any relevant details

Submit report

12 The number will be submitted for review



We have submitted a scam report for you

✓ You and other scam-spotters helped report this

● Awaiting review

✓ Numbers marked as scams will be added to ScamShield's blocklist

How was your experience?



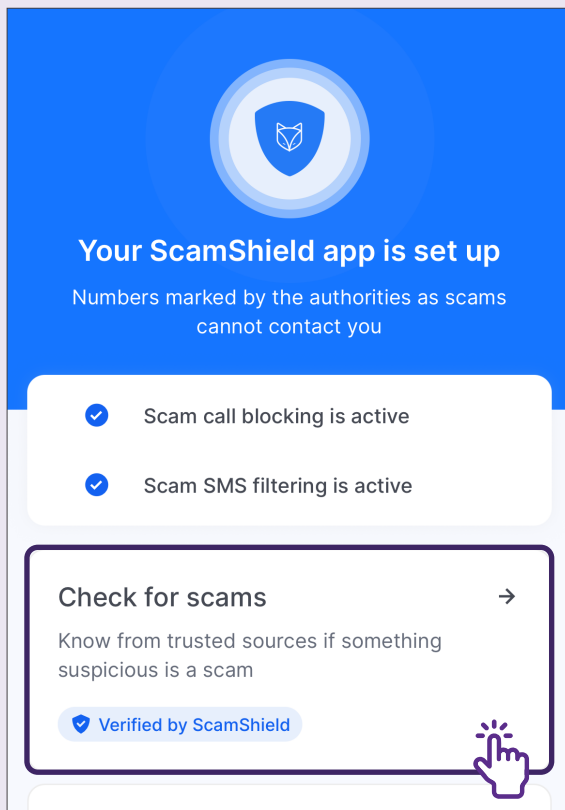
Check if it is a Scam Call, Message or Link

1 Launch ScamShield

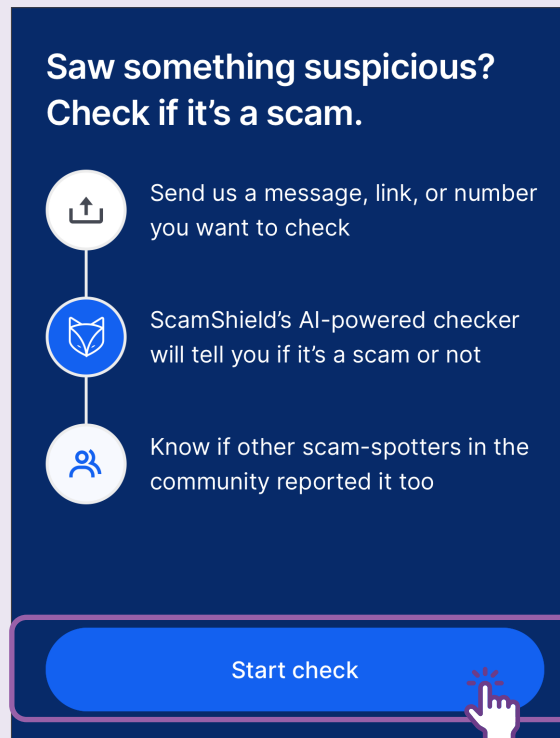


Find and tap "ScamShield" on your mobile device.

2 Select Check for scams



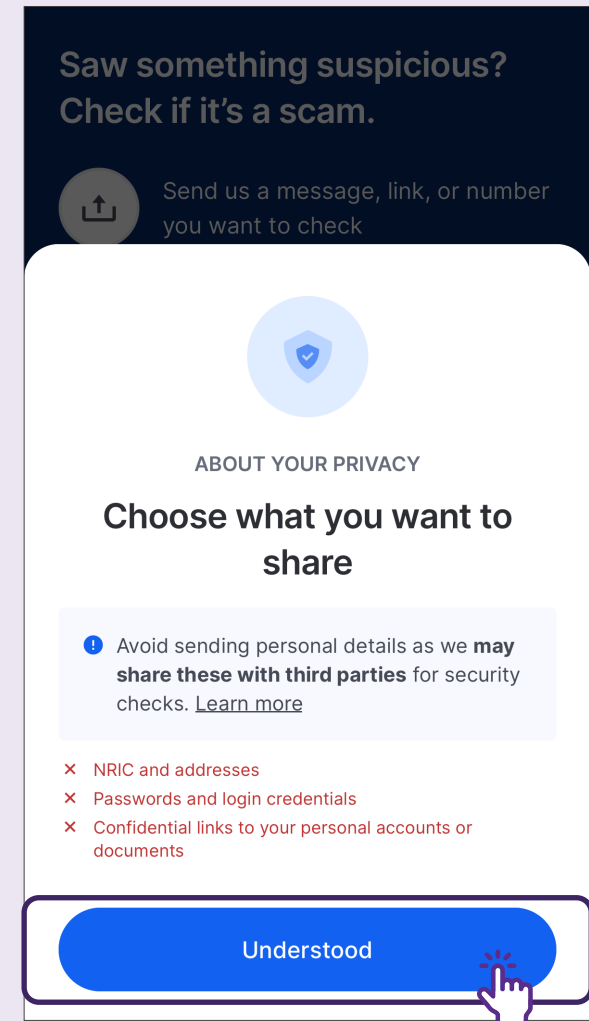
3 Select Start check



You can also call the anti-scam helpline for assistance at:
1799



4 Select Understood



5 Select what you would like to report

< [Progress bar] x

What would you like to report?

- A number that called you
- A message you received
- A website link

6 Select what type of message was it

< [Progress bar] x

What type of message was it?

- Text SMS
- WhatsApp message
- Telegram message

7 Upload a screenshot of the message or copy and paste the message in the open field

What is the message?

Upload a screenshot or paste the full text of the message you received

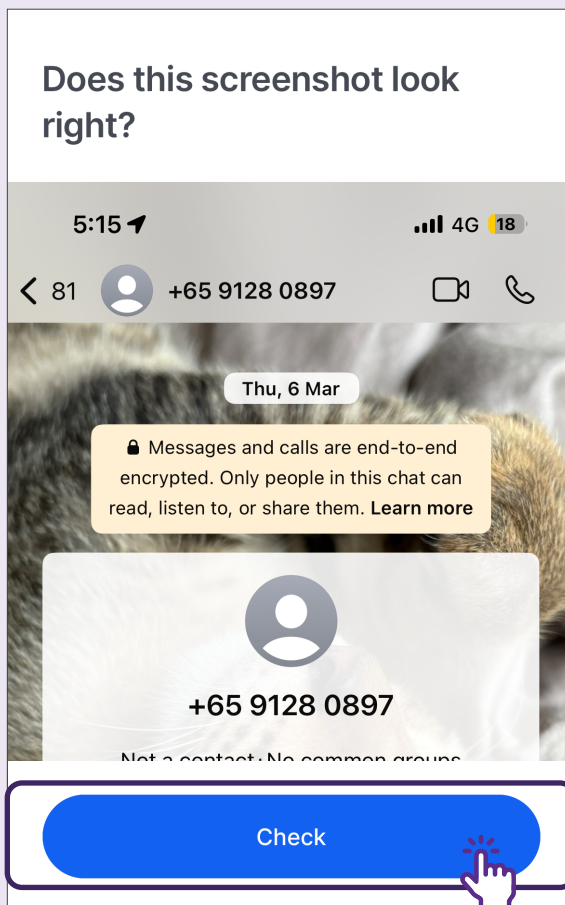
Upload message screenshot

OR

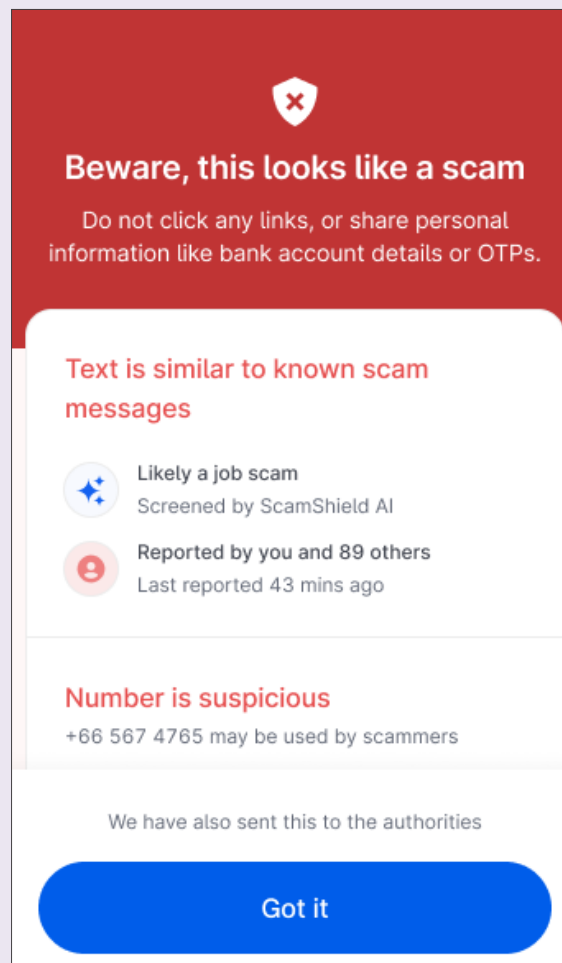
Paste message text

Check if it is a Scam Call, Message or Link

- 8** Confirm the screenshot (if you uploaded a screenshot). Select **Check to confirm**



- 9** If it is a scam, you will see a screen that looks like the one below



For more information on ScamShield App:

Visit ScamShield website:
<https://www.scamshield.gov.sg>

Notes



A large, light purple rounded rectangle containing 18 horizontal lines for writing notes.

**For more information and
to find your nearest SG
Digital community hubs:**

IMDA Contact Centre

Hotline: +65 6377 3800

Feedback: go.gov.sg/imda-feedback

Website: digitalforlife.gov.sg



Scan QR code to
visit the Digital for
Life Portal.

© 2026 Info-communications Media Development Authority. All rights reserved.
No part of this resource may be used or copied without explicit consent from IMDA.
Materials used in connection with this guide may also be subject to copyright protection.
These are not limited to: documents, slides, images, audio, and video. Unauthorized retention,
duplication, distribution, or modification of copyrighted materials is strictly prohibited.

*These resources take references from the National Crime Prevention Council, in collaboration with the
Singapore Police Force and Open Government Products.*