Your response

Introduction

At Google, we take seriously our responsibility to provide access to trustworthy information and content. We do this by protecting users and society from harm, delivering reliable information, and proactively partnering to create a safer web.

We combine safety efforts through product design and technological solutions, with a range of acceptable use policies and enforcement against fraud and scams, to protect users along their whole journey on our platforms.

Protection across the Android ecosystem
Building on decades (if not centuries) of letter-based fraud, fraudsters started using phone calls and text messages to commit their crimes, gradually adding online communications tools. This is why we have been developing a range of product features aimed at mitigating risks of fraud and scams for users when using Google-supported mobile devices running Android.

Android is an operating system (OS) that powers billions of devices worldwide. You can think of it like the software that runs your phone. This mobile operating system is based on a modified version of the Linux kernel and other open-source software, designed primarily for touchscreen mobile devices such as smartphones and tablets.

Android's top priority is the safety of its users – This responsibility is not taken lightly. We use industry-leading security practices and work closely with developers and device implementers across the entire ecosystem to ensure users are protected as soon as they power on their device.

No platform keeps more users safe on their devices – Android is incorporated on over 20,000 unique types of mobile devices, and Google Play Protect is active on 3 billion user devices. It stretches beyond the Play Store to protect users from malware in apps downloaded from the Play Store and third party stores/sites.

Android meets the toughest security standards in the world – we've attained the highest mobile industry certification standards, including the US Department of Defense and the Common Criteria recognized in 31 countries.

Android's approach to security focuses on three core pillars:

- **Multi-layered:** Each part of the Android ecosystem works together to build a strong defence that runs smoothly and effectively.
- **Transparency:** We work with the security research community to uncover, fix, and validate security issues. Once an issue is addressed, we share that with the world to ensure transparency and help others
- **Cross-Google technology:** We leverage Google's security expertise and incorporate leading security features into Android's OS, the Play Store, and apps on the device.

Our teams are dedicated to combating fraud, specifically focusing on cases where victims are targeted remotely through channels like email, phone calls, and messaging apps. Criminals exploit various attack vectors to carry out their schemes, including malware distribution, permission abuse, screen sharing, and social engineering tactics, such as phishing. We've built protections against these attack vectors into the core operating system and we layer on additional security services that continually scan devices for malware and other harmful behaviour.

Approach to tackling scams for Android phone and messaging

For its main communications-enabling features of phone and messaging, Android incorporates multiple layers of protections, including:

- Phone by Google helps protect against voice phishing and scams by blocking dangerous calls and warning you about suspicious callers with built-in caller ID, robust spam protection, and Call Screen. According to third party research, Android-powered phones utilising Phone by Google were able to identify and notify users about around 65% of potential spam or fraudulent calls, which is much higher than other mobile devices and operating systems not using Phone by Google. ('2023 Mobile Platform Scam and Phishing', Leviathan Security Group)
- Messages by Google provides built-in scam and phishing protection that warns users and automatically filters suspected spam and unsafe websites, using AI to spot suspicious messages by assessing the reputation of the sender and looking for known patterns and dangerous links.
- Chrome download warnings that alert you if you're about to download an Android (APK) file, ensuring you're aware a link is about to trigger a download of an app.
- Every **Pixel** device comes with caller ID and spam protection and we help users to identify potential scams with verified messages across all RCS enabled Android phones, which shows users the business name and logo as well as a verification badge in the message thread.
- We are also looking at leveraging AI tools to support enhanced scam call detection on Android.

RCS - Rich Communications Suite: improving on SMS especially to counter spam and scams

Traditional phone text messages, also known as 'SMS' (for 'short messaging service'), are not only an outdated form of communication, but also a flawed system – especially when it comes to phishing and scam detection. Because the SMS network is decentralised, there is no way that anyone can identify which networks are trustworthy and which aren't. This lack of trust along the journey of the message from creation to reception by the user limits the effectiveness of SMS fraud solutions, which is why users get so many phishing attacks and scam messages via SMS.

The SMS ecosystem has a number of known vulnerabilities that are exploited by those seeking to commit fraud and is in urgent need of modernisation. These vulnerabilities include:

- **Impersonation**: senders are typically unverified and only identified by a short code, alphanumeric, or long number, which may be shared across businesses, instead of by unique sender identification and verification.
- **Network bypass**: with its distributed, interconnected carrier topology, attackers can circumvent traffic and content firewalls to send malicious messages and exploit differences in carrier implementations.
- **Man in the middle attacks**: built on interconnected, and dated, SS7 signalling networks to transport messages, leaving SMS messages vulnerable to MITM attacks and weak security which allows devices to connect to fake network base stations and receive malicious messages.

To combat these abuse vectors, spam and abuse prevention methodologies include a combination of firewalls that block messages from suspicious sources, message content scanning by carrier / aggregator SMS platforms, and business commercial terms that require connected aggregator and interconnected carrier parties to operate lawfully. However, owing to its decentralised topology and reliance on SS7 signalling to transport messages across many entities involved in the message path between users, these methods cannot be applied with sufficient consistency and rigour to prevent fraud at scale. As a decentralised system, they are also inflexible and slow in addressing new threats.

The new messaging system, known as Rich Communications Suite (RCS), offers much better fraud detection: RCS, through carrier platform choice, has evolved to the point where it is now a centralised system, so we can implement these methodologies consistently and deploy new countermeasures quickly to address new threats. This converged system allows a single platform to authenticate users, police traffic and identify suspicious traffic patterns. For example: when a new user sends several international messages these are likely scam texts, and will be labelled as such for the end use.

RCS is the successor standard to SMS and is defined globally by the GSMA [GSMA | RCS - Future Networks]. It is supported by all major carriers in the UK and by numerous global telcos and manufacturers. RCS supports enhanced messaging features, such as chat, group chat, high-resolution photo and video sharing, and delivery and read receipts between users.

With broad adoption of RCS, we can address the key vulnerabilities that exist with SMS today, specifically:

- **No impersonation:** All senders delivering messages through this platform are uniquely identified and verified.
- **No network bypass:** In the UK, all carriers are converging on a single RBM platform that provides a single technical point of entry and policy enforcement. RBM is a messaging platform that businesses use to send One-Time Passwords (OTPs) and engage customers in dialog about transactions, customer service, promotions, and more.
- **Consistent and rigorous policy enforcement:** With UK carriers converging on a single shared
  platform, we can achieve consistent policy enforcement and malicious content detection and, at app level, develop more robust business rules for legacy SMS messages.

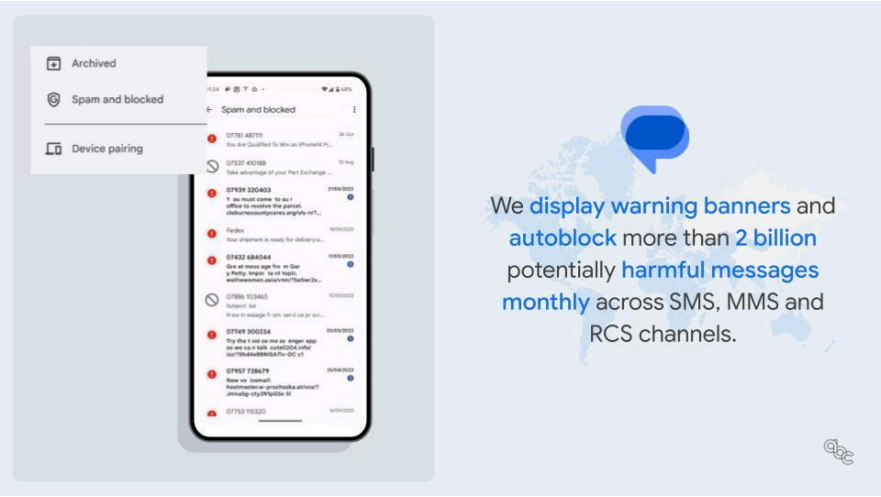
Crucially, RCS enables a safer messaging framework, comprising verified business to consumer messages, and interpersonal messaging with extensive platform and client malicious message detection and blocking features.

The combination of verified business messaging and interpersonal messaging protections greatly reduces the amount of scams and phishing attacks prevalent in SMS today through:

1. Interpersonal Messaging Scam Detection – RCS can detect unusual traffic and block it before it is delivered

- The common platform authenticates new users and their reputation
- The common platform is able to block messages in-transit and temporarily suspend abusive phone numbers due to spam.

- The common platform provides spam notices to connected clients based on user reputation and behaviour.
- Platform notices, and on device protections, may either result in messages being autoblocked or trigger a warning banner.
- RCS also allows for trusted parties to file spam texts into a spam folder, so they never reach the user's inbox
- In Google Messages, the scam detection feature works for both SMS and RCS messages.



Spam and blocked

07781 487111 — 24 Oct
You Are Qualified To Win an iPhone14 Pr...

07537 410188 — 25 Aug
Take advantage of your Part Exchange ...

07939 320403 — 21/05/2022
Y ou must come to ou r office to receive the parcel. cleburnecountycares.org/vb-n/?...

Fedex — 16/05/2022
Your shipment is ready for delivery:o...

07432 684044 — 11/05/2022
Gre at mess age fro m Gar y Petty. Impor ta nt topic. wethewomen.asia/vtm/?5e5er2x...

07886 103465 — 10/05/2022
Subject: ...
N ew m essage fr om servi ce pr ovi...

07749 300234 — 03/05/2022
Try tha t voi ce me ss enger app so we ca n talk cute0204.info/ izz/?5hd4eB8NiSA7iv-DC c1

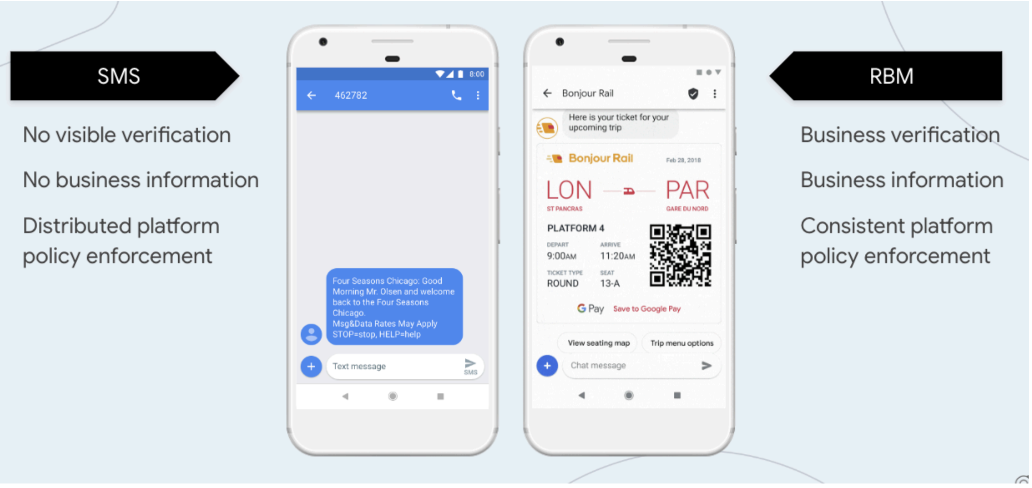
07957 728679 — 25/04/2022
New vo icemail: hostmaster.w-prochazka.at/vcs/?Jmna5g-cty2N1pG5c 5l

07753 115320 — 16/04/2022

We display warning banners and autoblock more than 2 billion potentially harmful messages monthly across SMS, MMS and RCS channels.

2. *Verified Business Messaging* – RCS can verify businesses, giving users trust in who they're messaging

- Over 2 trillion messages are sent from businesses to users every year (over 30% of global SMS traffic).
- Users are often tricked into responding to scam messages when they pose as businesses. Being able to ascertain that a business is genuine is therefore very important.
- RCS Business Messaging (RBM) requires businesses to be verified by the carrier service provider.
- Once verified, businesses will get a verified "check mark", instilling user confidence and trust in the sender.
- This allows users to distinguish between messages sent from unverified short codes over SMS, or long numbers over SMS or RCS, and legitimate businesses.
- RBM has the potential to transform how businesses communicate with their customers using messaging to build stronger, trusted relationships through brand verification, upstream business (agent) verification, content approval, active traffic management tools, and richer interactive experiences.



SMS

No visible verification

No business information

Distributed platform policy enforcement

462782

Four Seasons Chicago: Good Morning Mr. Olsen and welcome back to the Four Seasons Chicago.
Msg&Data Rates May Apply
STOP=stop, HELP=help

Bonjour Rail

Here is your ticket for your upcoming trip

RBM

Business verification

Business information

Consistent platform policy enforcement

In short, RCS offers a much safer and more effective messaging experience for users. While SMS is built on an outdated SS7 network, which allows bad actors to abuse the system, RCS is built on secure IP data connections and, as a converged system, offers a vast improvement for scam and phishing detection. RCS also serves as the foundation for key user safety features, like spam filtering and business verification. Going forwards, adopting the RCS standard would greatly reduce phishing attacks and scam text conversations.

We remain committed to addressing fraud in the UK and would welcome the opportunity to explore with the Government and Ofcom. We would also welcome greater collaboration with the broader mobile ecosystem (e.g., telcos, aggregators, mobile operators, manufacturers) and how we could realise these specific action points and modernise business messaging through RCS.

Question	Your response
Question 1: Do you agree that the routes described in this chapter cover all of the main methods that scammers use mobile messaging services to scam people? If not, please explain other methods.	
Question 2: Which routes do you think are the most important today and will be over the next 3 years for the perpetration of mobile messaging scams? Please provide evidence for your views.	Confidential? – N With RCS designed as the industry replacement to SMS, we fully expect scammers to shift their focus to this channel for both p2p and a2p traffic. However, unlike SMS, RCS benefits from robust identity management and sender verification for a2p traffic and, for p2p traffic, device and server-side spam protections, with both channels benefitting from a converged platform supporting carrier operations and consistent enforcement of policy. These combined countermeasures are globally delivering lower rates of scam

Question	Your response
	messages than SMS on the p2p channel, and no scam on the a2p RCS business messaging channel.
Question 3: Do you have any evidence specifically on what tactics scammers are using to access RCS messaging?	Confidential? – N As the industry replacement for SMS, scammers are applying similar approaches to RCS. This has allowed us to anticipate and preempt attacks in many cases, but some risks remain. Currently, the biggest challenge, especially in the UK, is that prepaid SIMs are very easy to acquire in bulk. This enables abusers to scale very quickly, even if they are only able to send a few messages for each phone number. This is highlighted as a priority area in our response to Q9.
Question 4: Are you aware of other relevant data sources on the scale or nature of scam messages sent over SMS and RCS?	
Question 5: What is your understanding of which channels are supporting the greatest harm (such as A2P or P2P SMS, or RCS)? Please provide any supporting evidence.	Confidential? – N Default, out of the box, mobile operator SMS messaging services were first launched in 1993 and built on an even older SS7 transport protocol first launched circa. 1975. The security vulnerabilities in this architecture, which also apply to voice, are now well documented and at the recent CEPT Workshop on combating fraudulent communications, the most common threats were presented by the ITU, highlighting the risks of *"man in the middle"* attacks and Caller Id spoofing for voice. ComReg in Ireland also reported a 40% drop in consumer confidence in SMS and, in the absence of modern features such as high quality media sharing, typing indicators, groups, and quoted replies, the shift to alternate OTT messaging channels is accelerating globally. The new messaging system, known as Rich Communications Suite (RCS), offers much better fraud detection. RCS, as deployed today, uses a converged cloud-based platform, which not only prevents man-in-the-middle attacks and identity spoofing (e.g., fake base stations or emulators), it also allows carriers to quickly identify scammers (e.g., sender clusters originated by SIM / Phone farms) and deploy countermeasures quickly.

Question	Your response
	RCS provides an unprecedented opportunity for the industry to tackle scams across carrier messaging and voice. Today, it is the only common, IP-based, secure platform across all carriers in all countries capable of solving identity spoofing, man-in-the-middle attacks, and misuse by bad actors. Operationally, this level of alignment allows new threats to be identified, regardless of where they originate, and effective counter measures to be deployed rapidly for the benefit of all users across every carrier in every country. In January, we outlined a series of measures that would harden our protections against RCS spam messages. These measures included: ● Making app attestation a requirement for messaging apps to connect to RCS. App attestation ensures the integrity of the device (e.g., preventing emulators) ● Improving the security of the standard through SIM-based authentication and public-private key service registration. These new capabilities will start to roll-out through 2025. ● Upgraded server-side traffic analysis to establish user reputation scores, supporting message blocking in-transit and server-to-client suspicious message notices. ● Temporary account suspensions. ● Reporting transparency with RCS service providers (carriers), enabling further account-level sanctions and / or SMS firewall updates. ● Improving on-device in Google Messages to detect content patterns linked to abuse. With these sanctions, early results show RCS is now performing significantly better than SMS. This common infrastructure has the potential to also support verified voice calls and, when combined with existing on-device capabilities, would provide a robust system to protect users against scam calls.
Question 6: What do you think will happen to RCS availability and adoption in the next few years? Please provide supporting evidence and or reasons for you views.	Confidential? – N RCS support has been a mandatory requirement for all Android phones for many years and, with Apple's recently announced adoption and roll-out, we expect accelerated adoption. With the switch away from SMS towards RCS user messaging, platform convergence has driven consistency, rigour, and rapid responses to

Question	Your response
	new existing and new threats. We expect the effectiveness of these solutions to deter bad actors over time. We also expect legitimate businesses to increasingly embrace RCS business messaging and adopt an ‘RBM first’ approach to a2p and p2a messaging. Unlike SMS, carriers in the UK share a common infrastructure, and will be able to maintain very high levels of integrity and commonality in their business onboarding and verification processes to guard against attackers as traffic scales, keeping the channel clean. Additionally, once a business has been verified and launched, the platform will provide AI-driven tools to ensure message content does not ‘drift’ beyond the approved purpose.
Question 7: Do you have views on the effectiveness of the measures discussed in this chapter? For measures where we have identified specific issues, please comment on these in your answer, providing reasoning and evidence if possible.	Confidential? – N Although this chapter provides a comprehensive set of measures, their effective implementation will be challenging in an ecosystem which comprises multiple service providers using multiple vendors, connected both nationally and internationally, using outdated foundational technology which is insecure and vulnerable to spoofing and man-in-the-middle attacks. RCS, as the intended successor to SMS, provides the technology modernisation and operational tooling necessary to deliver an effective implementation of these measures and, in many cases, these measures are already operational. As a system, RCS provides: ● Identity integrity for both users and brands ● Transmission path security against man-in-the-middle attacks ● Traffic quotas based on user reputation ● Message blocking in-transit based on sender reputation ● National and international scope ● SIM / phone farm intelligence based on traffic analysis and device intelligence ● Reporting transparency to enable service provider account / regulator criminal action ● The application of advanced AI technology to tackle new threats ● On-device best practices, ensuring consistency across Android and iOS ● User experiences which identify legitimate businesses and can help drive consumer awareness

Question	Your response
	- Extensibility and potential to support verified voice calls. These measures would be further enhanced by user SIM registration and a deeper connection with carrier SIM provisioning data e.g. activation country (HPLMN ye / no), phone pre-pay balance (credit / no credit).
Question 8: Are there other measures that we should include in our assessment of the measures that can address mobile messaging scams?	Confidential? – N We are open to discuss how we, together with our carrier partners in the UK, can collectively improve the capabilities of RCS, develop best practices for verified business messaging and their extension to voice.
Question 9: Within the options set out, what should be the priority areas, if any, to further disrupt mobile messaging scams?	Confidential? – N We have been working on supporting RCS rollout and enabling mobile operator partners to transition SMS to RBM. This will deliver safer, more helpful, business messages to users, through devices that support RCS served by the mobile operator's RBM service platform capabilities. In addition, the RBM service platform tools and operational processes are designed to enforce our RBM Acceptable Use Policy, which prohibits the use of the service for illegal and fraudulent activities. Violation of this policy may result in suspension of business accounts and/or reporting of illegal activities to authorities if required by law. While RCS messaging is now supported by device manufacturers and the 4 main UK operators, and serves over 1 billion global users, further action is required by regulators wanting to realise the RBM opportunity in tackling fraud, specifically: **RBM** 1. All mobile operators must support RCS verified business messaging. - In the UK, this is already the case, but an 'RBM first' approach is needed to drive scale business adoption. - While RBM is technically ready, mobile operators and aggregators should ensure they are operationally ready and the appropriate

Question	Your response
	commercial incentives are in place for businesses to register and drive RBM First e.g. an RBM message should not be more expensive than an equivalent SMS message, and aggregators have the technical switching capability. 2. All smartphones must support RCS business messaging. ● Today, most Android new handsets already support a default “out of the box” messaging app which supports RBM, but this feature has been delayed on Apple devices. 3. All mobile operators should support common operations and processes for business verification and approval. ● Mobile operators should define and operate to an agreed set of business principles and best practices, similar to that defined by the CTIA [CTIA - Messaging Principles & Best Practices] to minimise business adoption friction. 4. Build consumer and business awareness. ● Mobile operator and device manufacturer campaigns building consumer awareness to drive demand for safer messaging from businesses through RBM. **USER MESSAGING** 1. All mobile operators must support the latest RCS specifications to enable SIM-based authentication in 2025. 2. All devices must support the latest RCS specifications, specifically user RCS spam reports and ingest server notices, to enable Google Messages equivalent on-device protections to complement server-side traffic based countermeasures. 3. Mobile operator integration to determine user legitimacy e.g. SIM registration country, account balance. 4. User identity verification on mobile operator SIM registration.