

Your response

Question	Your response
<p>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.</p>	<p>Yes</p>
<p>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.</p>	<p>IT will be multi-factoral; the people most vulnerable to SMS scams will be those less tech savvy, so likely to stay on basic SMS, however the more sophisticated will move to richer media content, aided by AI-driven spoofs of trusted people recommending the scam service</p>
<p>Question 3: Do you have any evidence specifically on what tactics scammers are using to access RCS messaging?</p>	<p>Basic click-through links for SMishing approaches</p>
<p>Question 4: Are you aware of other relevant data sources on the scale or nature of scam messages sent over SMS and RCS?</p>	<p>There are multiple sources for spotting “dodgy” numbers, so if someone is not sure about an incoming message, then a basic search will bring up, e.g. https://who-called.co.uk/ and many others, however these rely on user reports, anchored to specific numbers, but if a number is used via an aggregation agency then sometimes it can be used for valid reasons, or it can be used for SMS Phishing (Smishing)</p> <p>I experienced a recent example from my employer where I was expecting an emergency response alert, however when checking the number before clicking on the offered link showed the number to be likely spam/smishing, even though on deeper checking it was entirely valid / trusted use.</p> <p>This shows up the issue, where Trusted numbers cannot be used via valid SMS agencies, if they cannot distinguish between valid and possibly criminal use cases.</p>
<p>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.</p>	

Question	Your response
<p>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.</p>	
<p>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.</p>	
<p>Question 8: Are there other measures that we should include in our assessment of the measures that can address mobile messaging scams?</p>	<p>Trusted Numbers need careful policing, and need vetting of the use cases from Agencies, or not to allow Agency-owned numbers unless they can prove use case policing</p>
<p>Question 9: Within the options set out, what should be the priority areas, if any, to further disrupt mobile messaging scams?</p>	<p>Legislation to distinguish the carriers from the Spammers, where Agencies & Carriers own some responsibility for validating the use cases</p>

Please complete this form in full and return to mobilemessagingcamsresponses@ofcom.org.uk.