Joint Online, Calls and Texts Fraud Research Questionnaire

Consent

Thank you for your interest in taking part in this research. YouGov is conducting this survey jointly with Ofcom who is the UK regulator for communications services such as mobile phone, broadband and landline services. Ofcom has a duty to ensure users of these services are treated fairly and are protected from harm. **This survey is about your experiences of receiving suspicious calls and texts on your mobile and landline and your experience of encountering suspicious activity online.**

The information we collect from this survey and other personal information you have already given us through your YouGov membership will help us better understand people's experiences. We respect that you might want to keep some of your information private, so there is no obligation to answer all the questions and you can choose 'prefer not to say' if so. However, if you are happy to share your honest answers, we would really appreciate it as it would help us build a fuller understanding on the subject at hand.

YouGov will only share anonymous data with Ofcom unless we ask for your permission otherwise. This means that Ofcom will not be able to identify you from the anonymous information they receive. All your personal data will strictly be used for research and analysis purposes only.

You have the right to withdraw your consent to process the information you have provided during or after the research. You may exit the survey at any time and your data will not be included in the results shared with Ofcom. If you would like to withdraw your consent after completing the survey, please contact YouGov at [email address].

For more information, please find our privacy policy here:

https://account.yougov.com/gb-en/account/privacy-policy

If you are happy to continue, please give your consent by clicking the button below to start the survey.

[START BUTTON TO PROCEED TO THE SURVEY]

[NEW SCREEN]

Please note: You will not be able to go back and change your answers so please take your time to read each question and the options available before moving to the next page. Thank you.

Comms activity and ownership of smartphone

ASK ALL [MULTI CODE]

Q1. Which, if any, of the following types of communication do you use? (Please select all that apply)

1. Making and/or receiving voice calls on a landline
2. Making and/or receiving voice calls on a mobile phone
3. Accessing the internet on a mobile phone*
4. Accessing the internet on a laptop, desktop or tablet*
5. None of these **[SCREEN OUT]**

6. Prefer not to say **[SCREEN OUT]**

*People access the internet for a variety of reasons, such as using social media and messaging, watching films, TV programmes and videos online, playing games online, video calls, checking emails, searching for information online and doing schoolwork or working from home.

ASK THOSE WITH A MOBILE PHONE [CODE 2 AND/OR 3 AT Q1] [SINGLE CODE]

Q2. Thinking about your personal mobile phone (i.e. not a phone provided by your workplace), which network are you on?

NOTE: If you use more than one personal mobile phone, please answer for the one you use MOST OFTEN.

1. EE/BT Mobile
2. giffgaff
3. iD Mobile
4. Lebara
5. Lycamobile
6. O2
7. Sky Mobile
8. Tesco Mobile
9. Three
10. Virgin Mobile
11. Vodafone
12. Other (please specify)
13. Don't know
14. Prefer not to say

ASK THOSE WITH A MOBILE PHONE [CODE 2 AND/OR 3 AT Q1] [SINGLE CODE]

Q3. Thinking about the personal mobile phone that you use most often, is it a smartphone?

A smartphone is a phone on which you can send and receive emails, download files, use apps, as well as view websites and generally go online on the internet.

1. Yes
2. No
3. Don't know

ASK THOSE WITH A MOBILE PHONE [CODE 2 AND/OR 3 AT Q1] [SINGLE CODE]

Q4. What is the make of the personal mobile phone that you use most often?

1. Google Pixel
2. Huawei
3. iPhone
4. Motorola
5. Nokia
6. OnePlus

7. Oppo
8. Samsung
9. Xiaomi
10. Other (please specify)
11. Don't know

Experience of suspicious calls, messages and online content

Introduction

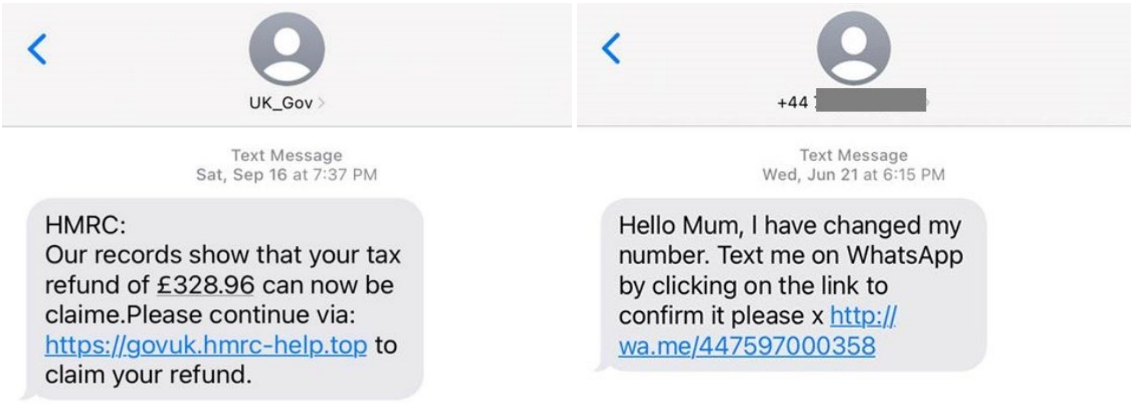
In the following set of questions, we will ask you about any experience you may have had receiving suspicious calls and texts on your mobile and/or landline, and your experience of suspicious activity online. Your input will help us understand the extent to which people are receiving these types of communications and the actions they take when they receive them.

We will specifically focus on the following types of calls and texts:

1) **Text messages** sent to your mobile
2) **Live voice calls** (when you answer your mobile or landline phone and there is a live person on the end of the line who you can have a conversation with)
3) **Recorded messages** (when you answer your mobile or landline phone and you hear a recorded message rather than a person on the end of the line)

By 'suspicious' we mean a call or text that made you suspect it was fraudulent.

Below are some examples of what could be a suspicious text message:



Examples of recent suspicious recorded and live voice messages are:

"I am calling from your bank to inform you that £600 has been paid out of your account. If this was not you, please press 1."

"This is your broadband supplier, your broadband account has been compromised and will be suspended."

[NEW SCREEN]

An online fraud or a scam involves someone wrongfully deceiving you with the intention of taking your money or other valuable possessions. It may involve them lying to you with made-up, false information, or deliberately hiding certain facts from you. They may promise to provide you with certain rewards, goods or services which they do not actually deliver, or something might be delivered but not as described.

Here are some examples of different types of online scam or fraud:

- **Impersonation fraud** – Fraudsters pretend to be from a legitimate organisation (e.g. a financial institution, the NHS, lottery institution, solicitors, government officials) and request a payment or information from you.
- **Counterfeit goods scam** – Goods such as fake designer brand clothes, accessories, perfumes, pirated copies of DVDs and computer games, often found at auctions and web marketplaces, where you can't check if the products are genuine until the item has been delivered.
- **Investment, pension or 'get rich quick' scam** – Fraudsters often present themselves as a trustworthy institution or advisor to pressurise you to invest money, or by luring with returns that are too good/quick to be true. They may present legitimate sounding investment opportunities such as energy firms, the foreign exchange market, or cryptocurrencies.
- **Romance or dating scam** – Fraudsters pretend to be someone else or lie to gain your affection and trust, and eventually ask for your money or financial information to purchase goods and services.

ASK ALL [SINGLE CODE PER ROW, RANDOMISE METHODS OF COMMUNICATION]

Q5) For this question, please think about your own experiences receiving suspicious content or activity. This can range from receiving contact from someone unknown or seeing an unusual link to click on, to instances when you were directly impacted (e.g. lost money, received sub-standard goods, spoken to a person you thought was someone else).

How often, if ever, have you experienced **suspicious content or activity** via each of the following methods of communication?

	Every day	At least once a week	At least once a month	About once every 3 months	About once every 6 months	Less than once every 6 months	Never	I don't use this service	Don't know
A text message on your mobile **[SHOW IF CODE 2 AND/OR 3 AT Q1]**	1	2	3	4	5	6	7	8	9
A phone call on your mobile **[SHOW IF CODE 2 AND/OR 3 AT Q1]**	1	2	3	4	5	6	7	8	9
A phone call on your landline **[SHOW IF CODE 1 AT Q1]**	1	2	3	4	5	6	7	8	9

A post on social media (e.g. Facebook, X (formerly Twitter), Instagram, Snapchat) **[SHOW IF CODE 3 AND/OR 4 AT Q1]**	1	2	3	4	5	6	7	8	9
A call on your instant messenger (e.g. Facebook Messenger, WhatsApp, Skype, Discord) **[SHOW IF CODE 3 AND/OR 4 AT Q1]**	1	2	3	4	5	6	7	8	9
A direct message on your social media or instant messenger **[SHOW IF CODE 3 AND/OR 4 AT Q1]**	1	2	3	4	5	6	7	8	9
Content and/or activity on a dating website or app (e.g. Match, Tinder, Bumble) **[SHOW IF CODE 3 AND/OR 4 AT Q1]**	1	2	3	4	5	6	7	8	9
Content and/or activity on a gaming website or app (e.g. PlayStation Network, Nintendo Online, Xbox Live, Roblox) **[SHOW IF CODE 3 AND/OR 4 AT Q1]**	1	2	3	4	5	6	7	8	9
A post on an online forum (e.g. Reddit, Mumsnet, The Student Room forum) **[SHOW IF CODE 3 AND/OR 4 AT Q1]**	1	2	3	4	5	6	7	8	9
Through an email **[SHOW IF CODE 3 AND/OR 4 AT Q1]**	1	2	3	4	5	6	7	8	9
Somewhere else **[SHOW ALL] [ANCHOR]**	1	2	3	4	5	6	7	8	9

ASK THOSE WHO SAID 'SOMEWHERE ELSE' [CODE 1-6] AT Q5 [OPEN END]

Q5b) You said you have experienced suspicious content or activity via other methods of communication not listed in the previous question.

Where else have you experienced suspicious content or activity? (Please type your answer in the bow below, giving as much detail as possible)

[ASK FOR EACH TYPE OF SUSPICIOUS ACTIVITY IF SHOWN AT Q5] [SINGLE CODE PER ROW]

Q6. Thinking back to this time last year, would you say you are experiencing more, about the same or less amount of each of the following types of suspicious activity?

	A lot more	A little more	About the same	A little les	A lot less	Not applicable as never experienced /don't use this service	Don't know	Can't remember
Suspicious text messages on your mobile	1	2	3	4	5	6	7	8
Suspicious calls on your mobile	1	2	3	4	5	6	7	8
Suspicious calls on your landline	1	2	3	4	5	6	7	8
Suspicious posts on social media (e.g. Facebook, X – formerly Twitter, Instagram, Snapchat)	1	2	3	4	5	6	7	8
Suspicious calls on your instant messenger (e.g. Facebook Messenger, WhatsApp, Skype, Discord)	1	2	3	4	5	6	7	8
Suspicious direct messages on your social media or instant messenger	1	2	3	4	5	6	7	8
Suspicious content and/or activity on a dating website or app (e.g. Match, Tinder, Bumble)	1	2	3	4	5	6	7	8
Suspicious content and/or activity on a gaming website or app (e.g. PlayStation Network, Nintendo Online, Xbox Live, Roblox)	1	2	3	4	5	6	7	8
Suspicious posts on an online forum (e.g. Reddit, Mumsnet, The Student Room forum)	1	2	3	4	5	6	7	8
Suspicious emails	1	2	3	4	5	6	7	8

[ASK FOR EACH TYPE OF SUSPICIOUS ACTIVITY IF ENCOUNTERED (CODES 1-6) AT Q5 ON INDIVIDUAL SCREENS] [MULTI CODE, RANDOMISE 1-10 (1-2 GROUPED)]

Q7. Thinking about when you've received suspicious content via **[INSERT COMMUNICATION METHOD]**…

Which, if any, of the following actions have you taken as a result? (Please select all that apply)

	Text messages on your mobile	Calls on your mobile	Calls on your landline	Posts on social media	Calls on your instant messenger	Direct messages on social media/instant messenger	On a dating website/app	On a gaming website/app	On an online forum	Emails
Clicked on the link but then realised it was suspicious and didn't do as instructed	1			1		1	1	1	1	1
Clicked on the link and then did as instructed by the message/person (e.g. called the number shown/provided bank details)	2			2		2	2	2	2	2
Engaged with the scammer (e.g. talked over a call/sent them a message)	3	3	3	3	3	3	3	3	3	3
Sent money/gifts	4	4	4	4	4	4	4	4	4	4
Arranged to meet the scammer	5	5	5	5	5	5	5	5	5	5
Invested money as recommended by the scammer	6	6	6	6	6	6	6	6	6	6
Reported it	7	7	7	7	7	7	7	7	7	7
Blocked the number/account	8	8	8	8	8	8	8	8	8	8
Told friends/family about it	9	9	9	9	9	9	9	9	9	9
Checked to see if the number/account is real (e.g. Google search/elsewhere)	10	10	10	10	10	10	10	10	10	10
Ignored/deleted it **[ANCHOR]**	11	11	11	11	11	11	11	11	11	11
Other (please specify) **[ANCHOR]**	12	12	12	12	12	12	12	12	12	12
Don't know **[ANCHOR]**	13	13	13	13	13	13	13	13	13	13
Can't remember **[ANCHOR]**	14	14	14	14	14	14	14	14	14	14
Prefer not to say **[ANCHOR]**	15	15	15	15	15	15	15	15	15	15

[ASK FOR EACH TYPE OF SUSPICIOUS ACTIVITY IF ENCOUNTERED (CODES 1-6) AT Q5 ON INDIVIDUAL SCREENS] [MULTI CODE, RANDOMISE 1-15 (7-8, 9-10 GROUPED)]

Q8. Still thinking about the suspicious content or activity you've experienced via [INSERT COMMUNICATION METHOD]…

Which of the following reasons made you think it was suspicious? (Please select all that apply)

	Text messages on your mobile	Calls on your mobile	Calls on your landline	Posts on your social media	Calls on your instant messenger	Direct messages on social media/instant messenger	On a dating website/app	On a gaming website/app	On an online forum	Email
Didn't recognise/know the number/sender/account who called/messaged/posted the content	1	1	1	1	1	1	1	1	1	1
The caller withheld their number		2	2		2					
The call/message was from an international number/abroad	3	3	3	3	3	3	3	3	3	3
No/poor-quality logo				4	4	4	4	4	4	4
Suspicious imagery (e.g. photos of a luxurious lifestyle/money)				5		5	5	5	5	5
Poorly written content (e.g. wrong spelling/grammar)/poor spoken English	6			6		6	6	6	6	6
Not endorsed by a credible person	7	7	7	7	7	7	7	7	7	7
Not endorsed by a credible organisation	8	8	8	8	8	8	8	8	8	8

No/few testimonials/reviews	9	9	9	9	9	9	9	9	9	9
Poor testimonials/reviews	10	10	10	10	10	10	10	10	10	10
The scammer expressed a strong personal/emotional attachment too soon	11	11	11	11	11	11	11	11	11	11
Inconsistent profile information (e.g. photos/bio of the supposedly same person didn't match)				12	12	12	12	12	12	12
Offered rewards which seemed 'too good to be true' (e.g. promise of free money/unrealistically high return on investment/extremely low price for a product/service)	13	13	13	13	13	13	13	13	13	13
Heard/saw warnings about it before	14	14	14	14	14	14	14	14	14	14
Other (please specify) **[ANCHOR]**	15	15	15	15	15	15	15	15	15	15
Don't know **[ANCHOR]**	16	16	16	16	16	16	16	16	16	16
Can't remember **[ANCHOR]**	17	17	17	17	17	17	17	17	17	17

[ASK THOSE WHO REPORTED THE INCIDENT (CODE 7) AT Q7 FOR EACH TYPE OF SUSPICIOUS CONTACT ON INDIVIDUAL SCREENS] [MULTI CODE, RANDOMISE 1-9]

Q9. You previously said that you have reported **[INSERT SUSPICIOUS CONTACT]** as suspicious.

Which of the following channels have you reported this to? (Please select all that apply)

	Text messages on your mobile	Calls on your mobile	Calls on your landline	Posts on your social media	Calls on your instant messenger	Direct messages on social media /instant messenger	On a dating website/app	On a gaming website/app	On an online forum	Email
Reported it to a special number for reporting suspicious messages/calls	1	1	1							
Reported it to my landline/mobile provider directly	2	2	2							
Reported it to Action Fraud	3	3	3	3	3	3	3	3	3	3
Reported it to Citizens' Advice	4	4	4	4	4	4	4	4	4	4
Reported it to the police	5	5	5	5	5	5	5	5	5	5
Reported it to Ofcom	6	6	6	6	6	6	6	6	6	6
Reported it to my bank, credit card company/building society	7	7	7	7	7	7	7	7	7	7
Reported it using the platform/app's reporting facility				8	8	8	8	8	8	8
Reported it using my mobile handset's reporting facility	9	9								
Reported to another organisation (please specify) **[ANCHOR]**	10	10	10	10	10	10	10	10	10	10
Did something else (please specify) **[ANCHOR]**	11	11	11	11	11	11	11	11	11	11
Don't know **[ANCHOR]**	12	12	12	12	12	12	12	12	12	12
Can't remember **[ANCHOR]**	13	13	13	13	13	13	13	13	13	13
Prefer not to say **[ANCHOR]**	14	14	14	14	14	14	14	14	14	14

[ASK THOSE WHO REPORTED THE INCIDENT TO A PARTY (CODE 1-11) AT Q11 FOR EACH TYPE OF SUSPICIOUS CONTACT ON INDIVIDUAL SCREENS**] [MULTI CODE, RANDOMISE 1-7]**

Q10. Still thinking about your experience reporting **[INSERT SUSPICIOUS CONTACT]**…

How did you know where to report this? (Please select all that apply)

	Text messages on your mobile	Calls on your mobile	Calls on your landline	Posts on your social media	Calls on your instant messenger	Messages on your instant messenger	On a dating website/app	On a gaming website/app	On an online forum	Email
I'd fallen victim this way before	1	1	1	1	1	1	1	1	1	1
From friends/family	2	2	2	2	2	2	2	2	2	2
Searched for where to report it (e.g. Google search)	3	3	3	3	3	3	3	3	3	3
From the media (e.g. TV/radio/magazine/newspaper)	4	4	4	4	4	4	4	4	4	4
From social media	5	5	5	5	5	5	5	5	5	5
From information from my landline, mobile/internet service provider	6	6	6	6	6	6	6	6	6	6
From information from another organisation (please specify) **[ANCHOR]**	7	7	7	7	7	7	7	7	7	7
From somewhere else (please specify) **[ANCHOR]**	8	8	8	8	8	8	8	8	8	8
Don't know **[ANCHOR]**	9	9	9	9	9	9	9	9	9	9
Can't remember **[ANCHOR]**	10	10	10	10	10	10	10	10	10	10
Prefer not to say **[ANCHOR]**	11	11	11	11	11	11	11	11	11	11

[ASK IF ENGAGED WITH SUSPICIOUS CONTACT (CODES 1-11) AT Q7] [SINGLE CODE]

Q11. Now please specifically think about the **most recent experience** you have with suspicious content or activity among the different communication methods you have used…

Which of the following best describes the nature of your most recently experienced suspicious content or activity?

1. Suspicious text messages on your mobile
2. Suspicious calls on your mobile
3. Suspicious calls on your landline
4. Suspicious posts on social media (e.g. Facebook, X – formerly Twitter, Instagram, Snapchat)
5. Suspicious calls on your instant messenger (e.g. Facebook Messenger, WhatsApp, Skype, Discord)
6. Suspicious direct messages on your social media or instant messenger
7. Suspicious content and/or activity on a dating website or app (e.g. Match, Tinder, Bumble)
8. Suspicious content and/or activity on a gaming website or app (e.g. PlayStation Network, Nintendo Online, Xbox Live, Roblox)
9. Suspicious posts on an online forum (e.g. Reddit, Mumsnet, The Student Room forum)
10. Suspicious emails
11. Other (please specify)
12. Don't know
13. Can't remember
14. Prefer not to say

[ASK IF ENGAGED WITH SUSPICIOUS CONTACT (CODES 1-11) AT Q7] [SINGLE CODE, RANDOMISE 1-14]

Q12. Still thinking about your most recently experienced suspicious content or activity…

Which of the following best describes the moment when you realised something was wrong?

1. When I saw the first message/post/got the first call
2. When I was asked to provide my bank account details
3. When I was asked to read out a code sent to my mobile
4. When I tried to contact the scammer and couldn't
5. When I called my bank to check whether the call/request was genuine
6. When I realised money had been taken from my bank
7. When the scammer kept asking me for more and more money
8. When I went to meet the scammer and they didn't turn up
9. When I met the scammer and realised they were not who I thought they were
10. When I couldn't log into my computer
11. When I didn't receive the goods I had ordered
12. When I received goods that were different from/poorer quality than what I had expected
13. When I read about other peoples' experiences and realised the same thing had happened to me
14. After I had asked a friend/family member about the message/call/post
15. Other (please specify) **[ANCHOR]**
16. Don't know **[ANCHOR]**
17. Can't remember **[ANCHOR]**
18. Prefer not to say **[ANCHOR]**

[ASK IF ENGAGED WITH SUSPICIOUS CONTACT (CODES 1-11) AT Q7] [SINGLE CODE]

Q13. Last time when you experienced suspicious content or activity, approximately how long did it take you to realise that someone was attempting to scam you?

1. Immediately
2. Within an hour
3. A few hours
4. A few days

5. About a week
6. About two weeks
7. About a month
8. About three months
9. About six months
10. About a year
11. Over a year
12. Don't' know
13. Can't remember
14. Prefer not to say

[ASK THOSE WHO REPORTED THE INCIDENT (ANY CODE 7) AT Q7] [MULTICODE, RANDOMISE 1-5]

Q14. You previously said that you have reported some types of suspicious content or activity.

Which of the following are reasons for why you decided to report it? (Please select all that apply)

1. To stop the same contact/see the same content again
2. Didn't want the same to happen to others
3. To feel like I am helping to tackle scams
4. Encouraged to do so by family/friends
5. Encouraged to do so by a campaign
6. Other (please specify) **[ANCHOR]**
7. Don't know **[ANCHOR]**
8. Can't remember **[ANCHOR]**
9. Prefer not to say **[ANCHOR]**

[ASK THOSE WHO DID NOT REPORT THE INCIDENT (IF CODE 7 IS <u>NOT</u> SELECTED FOR ANY COMMUNICATION METHODS) AT Q7] [MULTICODE, RANDOMISE 1-10]

Q15. You previously said that for some types of suspicious content or activity you encountered, you did not report it.

Which of the following are reasons for not doing so? (Please select all that apply)

1. I didn't think any action would be taken
2. I didn't know how to report it
3. I didn't know who to report it to
4. I didn't think it was serious enough
5. I thought it would be too time consuming
6. I received conflicting advice on what to do
7. I was embarrassed that I had fallen for the scam
8. I wasn't directly impacted
9. I thought somebody else would report it
10. I didn't see the need to report it
11. Other (please specify) **[ANCHOR]**
12. Don't know **[ANCHOR]**
13. Can't remember **[ANCHOR]**
14. Prefer not to say **[ANCHOR]**