.YONDER

16TH MARCH 2023

Executive Summary Report: Online Scams & Fraud Research

PREPARED FOR: OFCOM

PREPARED BY: YONDER CONSULTING

Ofcom foreword

Ofcom has statutory duties under the Communications Act 2003 to promote, and carry out research into, media literacy. A key way we seek to fulfil this duty is through our *Making Sense of Media* programme, which aims to help improve the online skills, knowledge and understanding of children and adults in the UK. In December 2020, the Government confirmed its intention to nominate Ofcom as the regulator for online safety in the UK, under the Online Safety Bill, which is currently in Parliament.

As referenced in our Roadmap to Online Safety Regulation, this summary report is one in a series of research studies into online safety that will inform our preparations for implementing the new online safety laws. As part of these preparations, we are building a robust evidence base, bringing together internal and external data, collected using different methods, from a variety of different sources.

In this context, this programme of research further develops our understanding of online harms and how we can help to promote a safer user experience. The findings should not be considered a reflection of any policy position that Ofcom may adopt when we take up our role as the online safety regulator. We will use this research alongside other relevant evidence as we design the relevant parts of the regulatory regime, including the draft code for illegal content, which we will publish for consultation within 100 days of the Online Safety Bill becoming law.

This **Online Scams and Fraud Research** was commissioned to enable Ofcom to extend and enrich its understanding of UK internet users' attitudes and perceptions towards different online fraud and scams, the experiences of those who encountered such incidents, and the practical as well as emotional impact such incidents had on users. This report summarises findings from a mixed-method (quantitative and qualitative) study conducted in 2022.

Table of Contents

Introduction

This **Online Scams and Fraud Research** was undertaken by Yonder Consulting on behalf of Ofcom. For the purposes of the research we define an experience of an online scam or fraud as one which originated online (e.g. saw an advertisement online, received a message on social media), even if it involved offline activity after. There were five core objectives of this mixed-method (quantitative and qualitative) study, as follows:

- To understand users' **attitudes** and **perceptions** towards online frauds/scams (qualitative);
- To gauge **prevalence of online fraud or scams based on self-reports from UK internet users**, including different types (quantitative);
- To explore the **key characteristics of various types of online scams, and the respective user journeys**, including the various communication channels that may be used to target victims (qualitative and quantitative);
- To understand **how victims responded, and the reported outcomes** of the experience (qualitative and quantitative);
- To investigate **the practical and emotional impact** of online fraud or scams on victims who took part in this research (qualitative and quantitative).

This report combines the findings from both the qualitative and quantitative phases of research. The insights drawn from this research will further develop Ofcom's understanding of online harms, and of how Ofcom can help to promote a safer user experience. **All views expressed in this report are those of the participants who took part in the research rather than the views of Ofcom.**

Methodology

The **Online Scams and Fraud Research** was a mixed-method quantitative and qualitative study, conducted with a sample of internet users aged 18+ in the UK. The quantitative phase was conducted via an online survey which took place between 5th and 17th May 2022, among a sample of 2,097 UK residents. The qualitative phase ran from 12th October to 11th November 2022, consisting of online in-depth interviews with 32 victims of online scams or fraud (to explore their experiences and the resultant impact on their lives in greater detail), and 5 online in-depth interviews with experts who support victims of online scams and fraud.

In the quantitative research, respondents were recruited to be nationally representative of the UK internet user population, using a quota-based sampling approach with quotas set on gender, age, socio-economic group and region. Sample boosts were applied to achieve at least 100 respondents who had experienced each of the eleven examples of scam or fraud that were tested during research. Due to the low incidence among the population of some of these harms this was not always possible, and wherever base sizes are below 100 they have been excluded from the analysis, with a note to explain which examples have been excluded. Data was weighted to be representative of the UK internet user population on age within gender, and overall to region and socioeconomic grade profiles. This approach counteracted any effect that boost oversampling would have on the data.

Qualitative research participants were recruited if they had been victim of one of a number of types of scams or fraud, with 5 interviews each among victims of money laundering scams[1], romance scams, investment scams, counterfeit goods scams, ransomware scams, and impersonation scams, and 2 interviews among victims of cryptocurrency scams[2]. The qualitative research also involved speaking to 5 experts who have supported victims of online scams and fraud.

For a detailed breakdown of the sample design, weighting, net definitions and methodology for both quantitative and qualitative research phases, please refer to the accompanying technical report[3].

[1] Victims of money laundering scams were recruited based on self-reports of their past experiences and they would have qualified if they believed they may have been involved in this type of scam or fraud, even if there was no evidence of 'classic' money laundering (e.g. people were not asked to accept money into their account or move it).
[2] Information on how these examples of scams or fraud were defined can be found in Section 2 of this report.
[3] The accompanying technical report is available on the Ofcom website.

Key takeaways

- **Nearly nine in ten adult internet users (87%) have encountered content** online which they believed to be a scam or fraud.
- **Nearly half (46%) of adult internet users reported having personally been drawn into engaging in an online scam or fraud**, while four in ten (39%) reported knowing someone who has fallen victim to an online scam or fraud.
    - Qualitative research reflected a broad awareness of scams online in today's society, with scams believed to be gaining in prevalence due to the increasing amount of activities carried out online, and the specific dynamics of some social media platforms which were considered by participants to be facilitating scammers' operations.
    - Respondents believed scammers exploit a number of factors, such as:
        - A lack of account verification, meaning scammers can operate with anonymity;
        - A tendency for users to reveal personal details which can be used to manipulate potential victims;
        - The fact that social media has become a common channel for brands to interact with the customers, and a sense of aspiration and envy cultivated by platforms.
- Of the eleven examples of scams or fraud tested during the quantitative research, **impersonation fraud (51%)** was the most common type ever experienced, followed by **counterfeit goods scams (42%)**, **investment, pension or 'get rich quick' scams (40%)** and **computer software service fraud or ransomware scams (37%)**.
- Scam or fraud victims were most likely to be using either their **computer (43%)** or **smartphone (43%)** when they first encountered an online scam or fraud.
    - The most likely channel or type of online service to encounter a potential scam or instance of fraud was on **email (30%)**, followed by **social media newsfeed (12%)**.
    - The most common type of content which fraudsters use to reach potential victims was through a **direct message (41%)**.
- **Just under two in ten (17%) who encountered a potential scam or fraud online did not take any action at all.**
    - Among those who did not take action (17%) on experiencing a scam or fraud, uncertainty around the outcome, not knowing who to tell, and not being directly impacted, were the main reasons for not doing so.
- **The platform or service itself was most likely to be considered by participants to bear some responsibility in acting against scams or fraud (61%).**
    - A warning from the platform that content or messages come from an unverified source (53%) was most likely to be considered by participants as a helpful method to prevent people from engaging with fraud or scams.
- **A quarter (25%) of those who encountered an online scam or fraud lost money as a result**, while a third (34%) reported that the experience had had an immediate negative effect on their mental health.

Section 1: Attitudes and perceptions towards, and experiences with, online scams or fraud

- **The overwhelming majority of internet users (87%) have encountered something online which they believed to be a scam or fraud.**
  - Reported experience of scams and fraud is significantly higher among men (89%), users aged 18-34 (92%) and those with children in the household (93%). (Figure 1)

Figure 1. Reported experience of having encountered suspicious content online

Source: Ofcom Online Scams or Fraud Research, May 2022

Q.1 Have you ever encountered or seen anything suspicious online which you thought might be a fraud or scam?

Base: All respondents (2,097), Men (1,122), Women (964), 18-34 (546), 35-54 (767), 55+ (784), Children in the household (577), No children in the household (1,518)

- **One in four (25%) have *frequently* experienced something online they suspect to be a scam or fraud.**
  - Men (28%), users aged 18-34 (30%) or 35-54 (28%), or those with children in the household (33%) are significantly more likely to report seeing suspicious content on a frequent basis.

- **The most common way to identify suspicious content was that it was badly designed or poorly written.**
  - Just under two thirds (65%) of internet users identified content as suspicious because it contained poorly written content, over half (54%) because the rewards offered seemed 'too good to be true', and over four in ten (44%) because they didn't know the person who posted the content/contacted them.

- **Nearly half (46%) of adult internet users reported having personally been drawn into engaging with online scams or fraud, while four in ten (39%) reported knowing someone who has fallen victim to an online scam or fraud.**

- Qualitative research provided context around the fact that reported experience of online scams or fraud is high. Participants' perceptions are that online scams are currently a widespread threat, as most reported experiencing multiple suspected scams, as well as knowing friends and family who have been affected.
    - Some participants felt that online scams had become more prevalent as an increasing amount of consumer financial transactions take place online; thus opportunities to be scammed have increased, while regulation is perceived not to have kept up.

"Regular internet users are always online and most of my activity is also online. I'm aware of scams and people I know have been scammed." ***Female, 30yrs, ransomware scam, lost £1,400 but was refunded***

"[Before his current experience he thought it wouldn't happen to him] Everyone is a potential victim no-one is immune." ***Male, 38yrs, counterfeit goods scam, lost £150 but was refunded***

"Online scams are something you are aware of, they've always been around…. You need to be street savvy online" ***Male, 30yrs, cryptocurrency scam, lost £1,000***

- Among qualitative research participants, the specific dynamics of some social media platforms were also felt to facilitate scammers. These included:
    - Social media platforms allowing users to set up multiple profiles and accounts with no identity verification, thus allowing scammers to create false identities to dupe potential victims.
    - Social media users often revealing details of their personal lives which scammers can use to manipulate their victims.
    - Social media has become a common way for companies and brands to communicate with potential customers, and scammers are taking advantage of that to make contact with potential victims.
    - Scammers exploiting the sense of aspiration and envy social media platforms cultivate i.e. scammers often showing images or videos of lavish lifestyles and offering their victims a chance of this life if they take part in their scam.

"Scammers trawl through your [social media] profiles and see if you are vulnerable and play on those insecurities i.e. death of loved ones." ***Female, 40yrs, investment scam, no money lost but was asked for £500***

"Social media allows scammers access to your life." ***Female, 47yrs, money laundering scam, lost £5,000***

"I saw a wicked looking product… it was an advert on [an online marketplace] for a remote-control aero plane." ***Male, 56yrs, counterfeit goods scam, lost £50***

Section 2: Types of online scam or fraud experienced

During the online survey, respondents were shown a randomised list of descriptions for each type of scam or fraud tested. A full list of definitions used is in the call-out box below[4]:

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 - *Counterfeit goods (e.g. 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.*
Computer software service fraud or ransomware scam - *Fraudsters use computer techniques to disable your computer's normal functioning, sometimes unknowingly to you, to steal your money or personal information.*
Fake employment scam - *Job advertisements that claim you can make a lot of money with little time and effort. You may be required to buy a starter kit, tools or goods that are worthless.*
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.*
Health or medical scam - *Health products or medication that are described as alternative forms of medical cures, or you believe are exactly the same as another legitimate brand of medication at a lower price. You may have seen advertisements promising miracle results, or you are allowed to make a purchase without a valid prescription.*
Identity fraud - *Fraudsters pretend to be you by accessing information about your identity (e.g. name, date of birth, current or previous addresses) and use it to obtain goods or services without your permission.*
Psychic or clairvoyant scam - *Fraudsters approach you to say they have seen something special in your future and ask for money in order to provide you with a full report about it. They may ask forcefully or may threaten to invoke bad luck if you refuse.*
Holiday scam - *Holidays advertised online (e.g. using social media) that are fake or misrepresented.*
Money mule recruitment or money laundering - *Fraudsters recruit people as money mules to transfer illegally obtained money between different bank accounts, sometimes internationally.*

- Of the eleven examples of scams or fraud tested during the quantitative research, **impersonation fraud** (51%) is the most common type ever experienced, followed by **counterfeit goods scams** (42%), **investment**, **pension or 'get rich quick' scams** (40%) and **computer software service fraud or ransomware scams** (37%). (Table 1)

[4] During the survey, respondents were shown each definition individually, and were given time to absorb the information, before being shown the next so as not to overwhelm them with text.

Table 1. Experience of eleven types of online scam or fraud tested

Type of scam or fraud	Ever experienced	Last experienced
Impersonation fraud	51%	12%
Counterfeit goods scam	42%	16%
Investment, pension or 'get rich quick' scam	40%	15%
Computer software service fraud or ransomware scam	37%	13%
Fake employment scam	30%	5%
Romance or dating scam	29%	12%
Health or medical scam	24%	5%
Identity fraud	24%	8%
Psychic or clairvoyant scam	18%	4%
Holiday scam	17%	4%
Money laundering	14%	3%

Source: Ofcom Spotlight Online Scams/Fraud Survey May 2022
Q.6a Have you ever experienced the following type of online fraud or scam in your lifetime?
Base: All respondents who have engaged with fraud/scams (958)
Q.6b Which of the following best describes your last experience?
Base: All respondents who have engaged with two or more fraud/scams (893)

- Participants in the qualitative interviews felt that counterfeit goods scams are common because online purchasing of goods is one of the main uses of the internet in today's society, and so opportunities to encounter this type of scam are higher.

- Qualitative research also provided context to the perceived high prevalence of financial scams. According to participants, these were particularly common in the midst of a cost-of-living crisis, as people look for a variety of ways to make extra money.

- When asked about the type of the last scam or fraud participants experienced in the survey, the most common is counterfeit goods scams (16%), closely followed by investment, pension or 'get rich quick' scams (15%).
  - Of those who have last experienced an investment, pension or 'get rich quick' scam, one in three (34%) fell victim to a pyramid or Ponzi scheme[5], a quarter (26%) experienced a money flipping scam[6], one in ten (11%) experienced a pension scam[7], and just under one in ten (8%) experienced a 'boiler room' scam.[8]

[5] The following definition of a pyramid or Ponzi scheme was provided to respondents in the survey: "Fraudsters offer great-sounding profits with little or no risk and asks you to pay a fee to join the scheme."
[6] The following definition of a money flipping scam was provided to respondents in the survey: "Fraudsters reach out on social media offering a quick way to double or triple your money in a small investment. Once you have transferred the money, the scammer never responds. They often lure victims with images of money or adverts with language such as 'double or triple your £20 investment in minutes!'"
[7] The following definition of a pension scam was provided to respondents in the survey: "Fraudsters make false claims to gain your trust (e.g. claiming they are FCA-authorised or are not subject to FCA's approval because they are not providing the advice themselves) and typically design attractive offers to persuade you to transfer your pension to them, or to release funds from it. Once the funds are released and transferred, your money is stolen and no investment is made."
[8] The following definition of a 'boiler room' scam was provided to respondents in the survey: "Share and bond scams are often run from 'boiler rooms' where fraudsters cold-call investors offering you worthless, overpriced or even non-existent shares or bonds. Boiler rooms use increasingly sophisticated tactics to approach investors, offering to buy or sell shares in a way that will bring you a huge return."

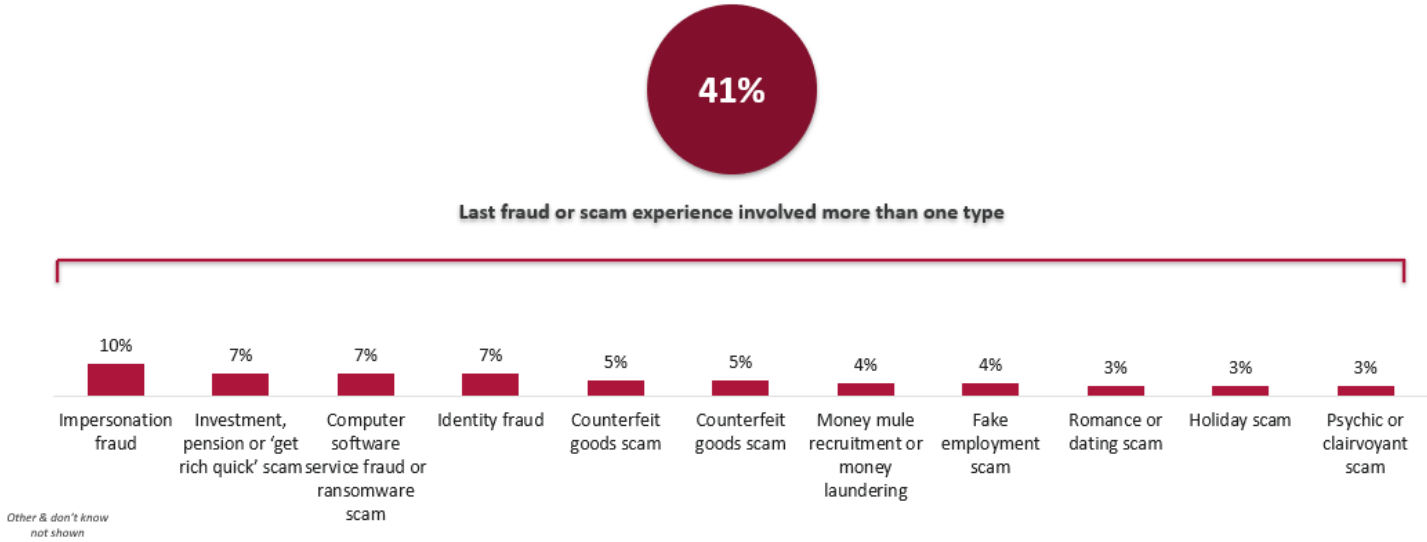
- In the qualitative research, one participant had experienced a Ponzi scheme where she initially invested £12,000 in investment bonds. The fraudulent investment company felt legitimate as they had a professional looking website and a responsive customer service team. She only realised she was involved in a scam when the company went into administration, and it was exposed in the media.

"I was looking for a place to get interest on my savings and saw a lovely website and dashboard [of investment results]. The company was responsive, [the person I spoke to was] charming and they had great customer service…seemed too good to be true…sucked into it so put all my savings into it."

"Even we don't understand what happened to us!" ***Female, 38yrs, investment scam, lost £12,000***

- **The quantitative research reveals that different types of scams or fraud may be experienced together.** Those who had experienced scams or fraud were asked whether their last experience involved any other type(s) of scam or fraud, after they had chosen one category that best described their experience. We found that two in five (41%) selected more than one type of scams or fraud to describe their last experience, suggesting that many incidents had inflicted issues of different nature (Figure 2).
  - Of the eleven types of online scam or fraud tested during the quantitative research, survey participants were most likely to encounter impersonation fraud in conjunction with another scam or fraud (10%) at the same time.

Figure 2. Combined experience of scams or fraud: last scam or fraud experienced

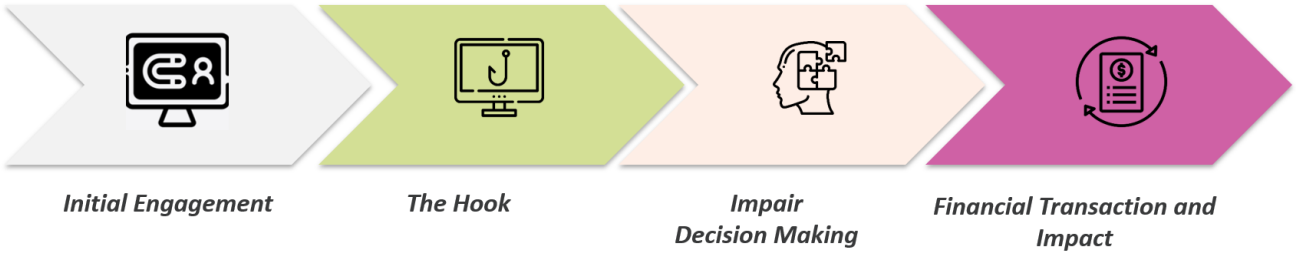


Source: Ofcom Spotlight Online Scams/Fraud Survey May 2022
Q8. Did your last experience involve any other type(s) of fraud or scam apart from [CODE 6b]? Please select all that apply.
Base: All respondents who have experienced fraud/scams (893)

Section 3: The online fraud or scams journey

Our qualitative research found that while scams and fraud experiences are varied, there is a pattern of four key phases that frequently appears, as illustrated in Figure 3:

Figure 3. Four key phases of scams or fraud experience



Source: Ofcom Spotlight Online Scams/Fraud Qualitative Interviews, November 2022

(i) There was an **initial engagement** phase where there was **direct** (victim engaged directly with scamming communication, e.g. direct message sent through social media platforms), or **indirect** (e.g. link to fake website sent via social media platform as 'suggested for you').

(ii) The next phase of the scam was the **hook** used to **attract** the victim. This was where the scam offered a clear **benefit to the victim** such as the opportunity to make money or make a connection.

(iii) In order to gain victims' trust, the scammer often employed **one or more engagement techniques** which **impairs the rational decision-making process** such as: constant contact and messaging victims, telling hardship tales, giving victims a return on their initial investment, being charming, or emphasising time sensitivity (i.e. to get this price you need to sign up in the next 24hrs).

(iv) And finally, the **financial transaction phase** which, after completing phases 1-3, was where the victim gives the scammer their money. Often the victim only realises it was a scam after they have given over their money. This was also where victims start to process the emotional and financial impact of being scammed.

"The minute after I transferred the money I couldn't get hold of anyone…then it hit me [I'd been scammed]." ***Male, 42yrs, investment scam, lost £1,000***

"Not a single alarm bell through the whole phone call [with the scammer]. If I had an inkling I would have cut the call….10 minutes after the call I realised I'd been scammed." ***Female, 30yrs, ransomware scam, lost £1,400 but was refunded***

- For the most part, qualitative research participants felt that, nowadays, anyone could be a potential victim of scams or fraud. However, participants revealed a number of underlying vulnerabilities on which scammers may be able to play, ranging from a desire to become rich quickly to seeking a connection due to loneliness.

- Interviews with experts supporting the victims of scams or fraud confirmed these findings. From their combined experiences, there were some common themes/traits amongst victims of scams. The following themes were given by experts as evidence of so-called 'unmet needs' which tend to leave victims vulnerable to exploitation by scammers:
    - Lack of a sense of belonging or community, leading to low self-esteem;
    - A desire to seek love and connection;
    - A desire to be financially successful.

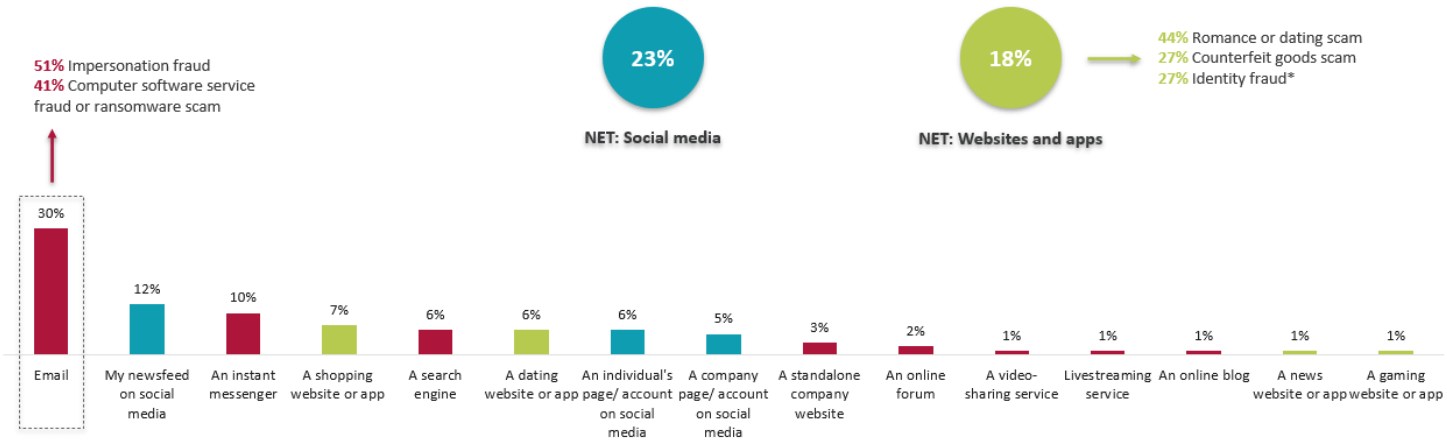
- Alongside 'unmet needs', experts also identified a number of underlying conditions or experiences which may make individuals more susceptible to being scammed:
    - Cognitive difficulties, such as dementia, or neurodiversity leading to challenges reading social cues;
    - A background of having grown up with insecure attachments, leading to a lack of experience of healthy, reciprocal, relationships.

"You are more likely to be scammed if there are unmet needs such as seeking love and connection or if there are cognitive difficulties." ***Expert, clinical psychologist working with victims of online scams***

- **The quantitative research revealed that victims were most likely to be using either their computer or smartphone when they encountered an online scam or fraud.**
    - Over four in ten (43%) victims were using a computer when they last experienced a scam or fraud, the same proportion (43%) were using a smartphone, followed by one in ten (10%) were using a tablet.

- **The most likely channel to encounter a potential scam or instance of fraud is on email. (Figure 4)**
    - Three in ten (30%) of those surveyed experienced a potential instance of scam or fraud through email, just under a quarter (23%) through social media, and just under two in ten (18%) through specific websites and apps.
    - Users were more likely to encounter different scams depending on the channel. Impersonation fraud (51%), and computer software service fraud/ransomware scams (41%) were more likely to be experienced through email, and romance/dating scams (44%), counterfeit goods scams (27%) were more likely to be experienced through websites and apps.

Figure 4. Platforms where scams or fraud were first encountered[9]



Source: Ofcom Spotlight Online Scams/Fraud Survey, May 2022
Q9. Which of the following best describes the type of online service or platform you were using when you first encountered the fraud or scam you last experienced?
Base: All respondents who have experienced fraud/scams (893), Experienced Romance or dating scam (103), Investment, pension or 'get rich quick' scam (131), Impersonation fraud (112), Identity fraud (75), Computer software service fraud or ransomware scam (118), Counterfeit goods scams (139) *Caution low base size*

- **The majority of fraudsters use a single channel to interact with potential victims.**
  - 77% of those who had experienced an online scam or fraud reported that fraudsters had made contact through one channel (e.g. email), while 15% reported fraudsters had used multiple channels.
  - Among the fraudsters who used multiple channels, victims reported that instant messenger (25%), email (23%), and social media (22%) were the most popular secondary channels.

- **The most common type of content used by fraudsters to reach potential victims is a targeted message.**
  - Four in ten (41%) scam or fraud victims were contacted by a potential fraudster through a targeted message such as a direct message or a mass message posted to a group, a fifth (20%) through advertisements they saw on websites/apps, social media sites or video-sharing platforms, and less than a tenth (6%) were targeted through user-generated content (posts or videos) or (4%) influencer-generated content (posts or videos).

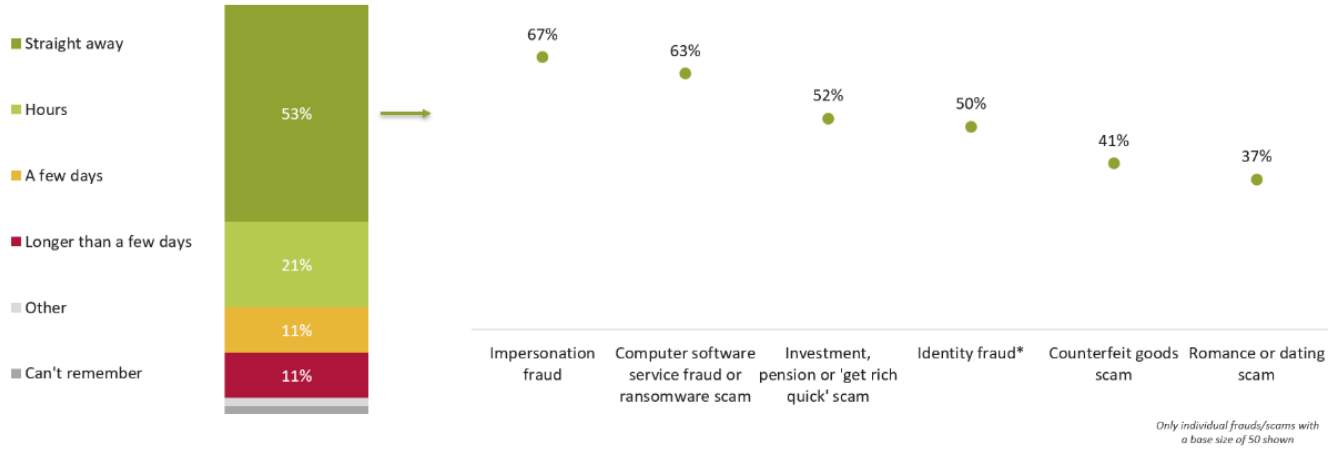
- **Most of those who encountered malicious content via user/influencer-generated content, or a search result, reported that it came from a user/source they did not know.**
  - Over eight in ten (82%) scams or fraud victims received malicious content from a user/source they did not know, while just over one in ten (12%) received malicious content from a friend or connection.

[9] Health or medical scams were significantly more likely to be experienced through social media, but as the base <50 they have been excluded from the analysis.

- One in four (25%) who first encountered malicious content via user/influencer-generated content (posts and videos), or a search result/listing, recalled the content being promoted.

- **Over a fifth of victims took longer than a day to realise they had been scammed.**
  - Over half (53%) realised it was a scam straight away, while one in five (21%) realised within a few hours. However, one in ten (11%) took a few days, and a further one in ten (11%) took longer than that.
  - Those who encountered an impersonation fraud (67%) or a computer software service/ransomware fraud (63%) were more likely than the average to realise straight away, while those who encountered a counterfeit goods scam (41%) or romance scam (37%) were less likely than the average to realise straight away.

Figure 5. Length of time taken to realise they were a victim of a scam or fraud; proportion realising straight away by scam type



Source: Ofcom Spotlight Online Scams/Fraud Survey, May 2022
Q18. How long did it take from engaging with the content (e.g. clicked on the advertisement, followed specific instructions, replied to a message) for you to realise it was a fraud or scam?
Base: All respondents who have experienced fraud/scam (893), Experienced Romance or dating scam (103), Investment, pension or 'get rich quick' scam (131), Impersonation fraud (112), Identity fraud (75), Computer software service fraud or ransomware scam (118), Counterfeit goods scams (139) *Caution low base size*

Section 4: Reporting of online scams or fraud

- **Just under two in ten (17%) who encountered a potential scam or fraud online did not take any action at all.**
  - The proportion of those experiencing a potential scam or fraud who took action varied by type of encounter. Those who encountered potential identity fraud (89%) were most likely to take some action[10], while 85% took action on encountering impersonation fraud, 82% on encountering computer software service fraud/ransomware scam, 80% on encountering a romance or investment scam, and 76% on encountering a counterfeit goods scam.

Figure 6. Reporting of online scams or fraud[11]

Source: Ofcom Spotlight Online Scams/Fraud Survey May 2022
Q21. When you realised you had experienced a scam or fraud, which of the following action(s) did you take, if any?
Base: All respondents who have ever experienced fraud/scam (893), Experienced Romance or dating scam (103), Investment, pension or 'get rich quick' scam (131), Impersonation fraud (112), Identity fraud (75), Computer software service fraud or ransomware scam (118), Counterfeit goods scams (139) *Caution low base size*

- In the qualitative research most participants who had lost money reported the scam to their bank first, as recovering any lost money was said to be the priority. Once money had been refunded, most said they did not take any further action. However, if the scam took place on a social media platform, some reported alerting the platform.

"After all my suspicions confirmed [it was a scam] I called my credit card company straight away and they put me through to the fraud department who said don't worry we'll refund you." ***Male, 38yrs, counterfeit goods scam, lost £150 but was refunded***

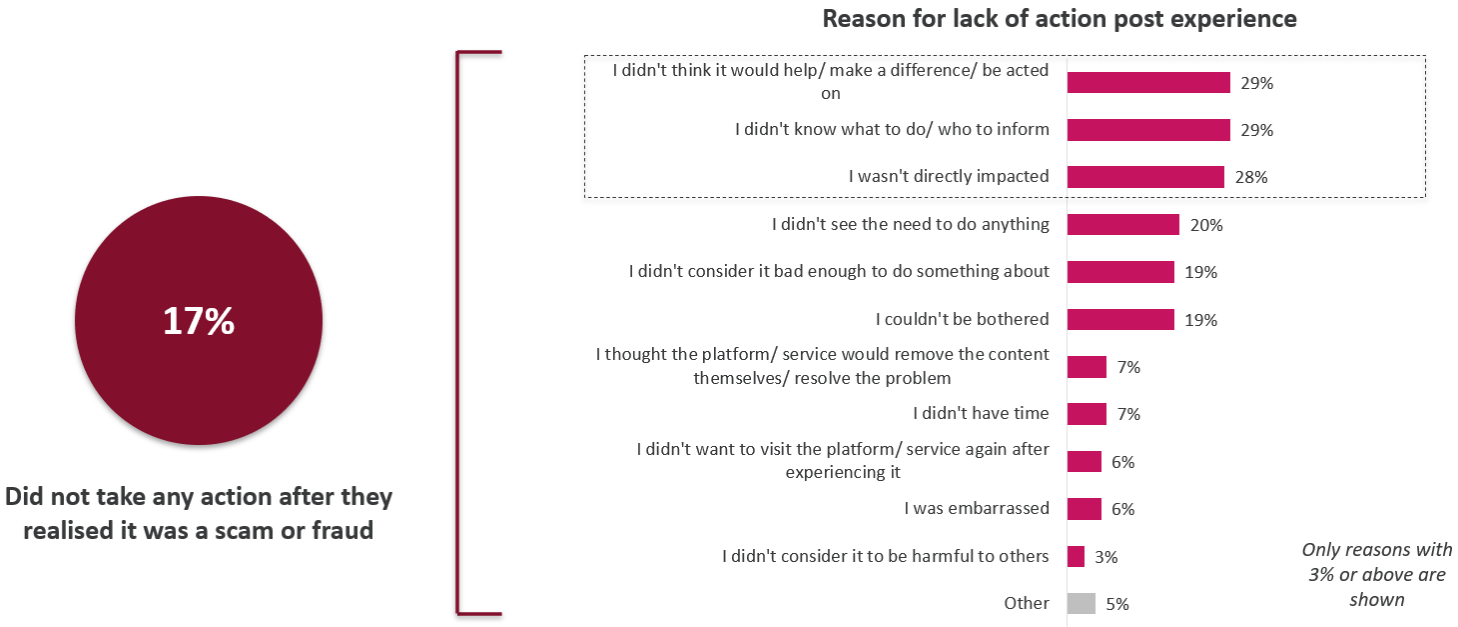
- Where participants became more emotionally involved with their scammer over a longer period of time, they reported being more likely to alert the police as well as their bank. For example, one participant who was a victim of an impersonation scam (during which the scammer stayed at her house over a period of weeks) used social media to track down her scammer and, with the help of fellow victims, have him arrested.

[10] Findings here are indicative given the low base size (n=75)
[11] N.B. only examples of scams/fraud with a base size >50 are shown; 'Can't remember' has not been shown

"[The scammer had posted the scam on] 19 selling groups so to expose him I posted a message saying this person is not who he says he is…I wanted to prove to him that he wasn't getting away and I that I wouldn't let it go….The police put out a Crimestoppers advert out to find him, with a reward of £1,000…..with the help of two other victims the scammer was arrested." ***Female, 55yrs, impersonation scam, lost £1,400-£1,500***

- **Among those who did not take action (17%) on experiencing a potential scam or fraud, uncertainty around the outcome, not knowing who to tell, and not being directly impacted were the main reasons for not doing so.**
  - The most common reasons for choosing not to take action were that victims did not think it would help/make a difference/be acted upon (29%), they did not know what to do/who to inform (29%), or they did not feel they were directly impacted (28%).

Figure 7. Reasons for lack of action after experiencing a scam or fraud



Source: Ofcom Spotlight Online Scams/Fraud Survey, May 2022
Q21. When you realised you had experienced a scam or fraud, which of the following action(s) did you take, if any?
Base: All respondents who have ever experienced fraud/scam (893)
Q22. You mentioned you did not take any action, why not?
Base: All respondents who have not taken any action post-experience (153)

- Qualitative research revealed that some participants were reluctant to take action because they felt it was their own fault for falling for the scam, suggesting that they felt shame and embarrassment.

"I felt disappointed with myself…shouldn't be rushing into things [signing up to the fraudulent website]…in the end I had to own it so didn't report." ***Male, 30yrs, cryptocurrency scam, lost £1,000***

"I felt it was my fault so didn't go to the police" ***Female, 23yrs, romance scam, lost £500***

- **Among those who did act (82%), the most popular type of action taken was to report the fraud or scam.**
  - 56% reported the encounter (either to the platform/service on which they encountered it, their bank, Action Fraud, Citizens Advice, the police or a regulator), 30% avoided future contact (such as blocking the contact or closing their account), and 21% shared their experience (with friends/family, publicly on social media, or on a ratings site).
  - Two in five participants (43%) who reported the incident claim nothing happened as result, whereas just under a quarter received a response (23%).

"I reported the username and account of scammer [to the online marketplace]…it was quite easy to report but I didn't hear [from the online marketplace]." ***Female, 29yrs, investment scam, lost £210***

- **Over half of users think the platform/service itself should bear some responsibility in acting against scams or fraud online, slightly more than the proportion who feel that users themselves should bear some responsibility.**
  - Of a multiple choice list of different parties and authorities, around six in ten (61%) of internet users believe the platform itself should bear some responsibility, while just over half (54%) selected users themselves, the same proportion (54%) believe it is the police, and half (50%) believe it is Action Fraud; three in ten (31%) believe Ofcom should be responsible.
  - 18-34 year olds are most likely to be unsure of whose responsibility it is to take action against fraud and scams online, with 13% responding 'Don't know' when asked who should take responsibility (compared to 8% on average).

- **A warning from the platform that content or messages come from an unverified source is most likely to be considered as a helpful method to prevent people from engaging with fraud or scams. (Table 2)**
  - When asked which measures, from a list provided, could stop people engaging with scams or fraud, over half (53%) of internet users surveyed believe that online alerts from the platform warning of an unverified user would be helpful, followed by a warning/pop-up message from the platform that a link will take them to another site (48%), a warning about a message having been forwarded multiple times (47%), and a warning from an authority that content may be suspicious (46%).

Table 2. Actions to prevent engagement with online scams or fraud

Action	%
A warning from the platform that the content or message came from an unverified user	53%
A warning/pop-up message from the platform to notify me when a link will take me to another site or service	48%
A warning from the platform that the same direct message has been forwarded many times	47%

A warning from an authority that the content may be suspicious	46%
Advice about keeping safe online on television documentaries/factual programmes (e.g. Rip-off Britain)	38%
Online advice about keeping safe online, specifically when I search for such information	36%
An occasional pop-up warning on the platform to remain alert for fraudulent content	35%
Social media posts on advice about keeping safe online	34%
Emails from my bank, credit card company, building society or pension provider	34%
Texts from my bank, credit card company, building society or pension provider	29%
Make the content more obvious that it was promoted/sponsored	27%
Articles in newspapers on advice about keeping safe online	26%
Online video advice about keeping safe online	24%
Posters in bus shelters and on billboards etc. on advice about keeping safe online	24%
Advertisements in newspapers on advice about keeping safe online	23%
Articles in magazines on advice about keeping safe online	22%
Advertisements in magazines on advice about keeping safe online	19%
Printed leaflets on advice about keeping safe online	17%

Source: Ofcom Spotlight Online Scams/Fraud Survey, May 2022
Q26. Which of the following measure(s) do you think could stop people from engaging with the fraud or scam you last experienced?
Base: All respondents (2,097)

Section 5: Impact of online fraud or scams

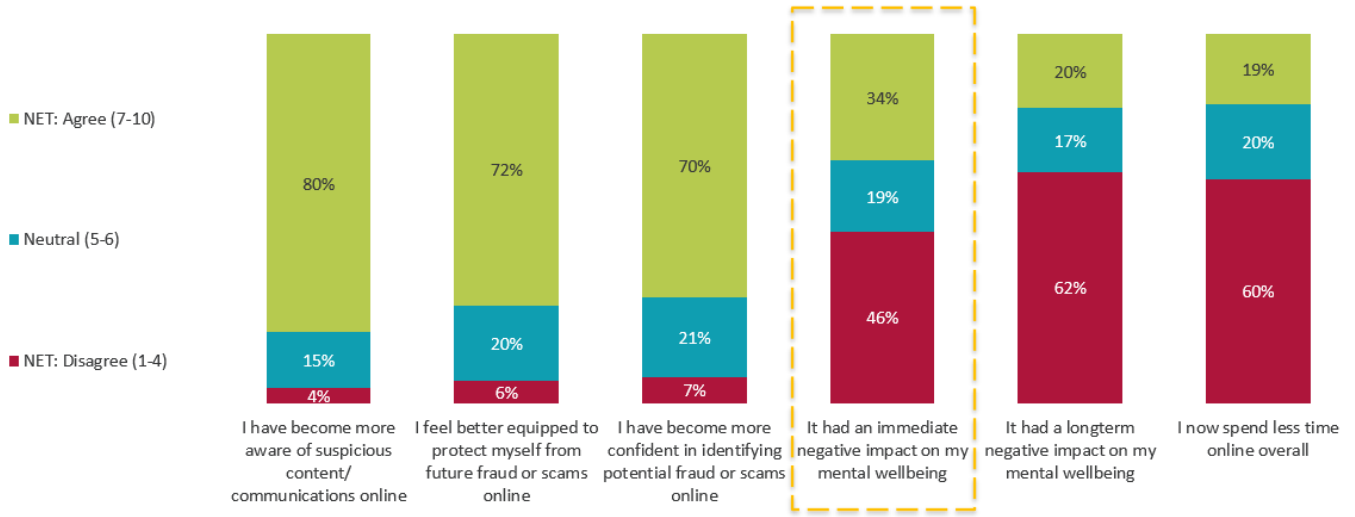
- **A quarter (25%) of those who encountered an online scam or fraud lost money as a result.**
  - The likelihood of losing money varied according to the type of scam encountered. Those encountering a counterfeit goods scam (40%) were most likely to have lost money.
  - Amongst those who had lost money as a result of a scam, one in five (21%) lost £1,000 or more, while the most common amount of money to be lost (42%) was between £1-£99.

- **A cash transfer is the most common way for fraudsters to be paid, either digitally or physically, through single or multiple payments, or through direct debit.**
  - Of those who lost money as a result of a scam, two thirds (67%) made payment to a fraudster by cash transfer. This includes just under four in ten (38%) who made a single digital transfer, a fifth (20%) who made a series of digital payments, one in ten (11%) who made a single physical transfer, one in twenty (5%) who made a series of physical transfers, and one in fifty (2%) who set up a direct debit.
  - Just under a fifth (19%) of those who lost money made a debit card payment to the fraudster, while less than one in ten (8%) made a credit card payment.

- **Among those who have experienced an online scam or fraud, four in ten (38%) have noticed a higher than usual amount of suspicious content, since their scam/fraud experience, on the sites they visit and the services they use.**
  - Three in ten (29%) report being contacted by strangers more often since their experience.

- **A third (34%) of those who have encountered an online scam or fraud claim that the experience has had an immediate negative impact on their mental wellbeing. (Figure 8)**
  - Those aged 18-34 (45%) or with children in the household (42%) are more likely to have had their mental wellbeing negatively affected by their experience of an online fraud or scam (compared to 34% average).
  - A high proportion (80%) of those who have encountered an online scam or fraud agree that they have become more aware of suspicious content/communications online; similarly, high proportions feel better equipped to protect themselves in the future (72%) and consider that they have become more confident in identifying potential scams/fraud (70%).

Figure 8. The impacts of scam or fraud experience



Source: Ofcom Spotlight Online Scams/Fraud Survey, May 2022

Q27. On a scale of 1 to 10, where 1 means 'Strongly disagree' and 10 means 'Strongly agree', to what extent do you agree with each of the following statements?

NET: Agree (7-10), Neutral (5-6), Disagree (1-4)

Base: All respondents who have experienced fraud/scam (893)

- **Those who lost money as a result of an online scam are more likely to have been negatively affected in both the short and long term compared to the average (of those reporting any experience).**
  - The scale of the negative impact on mental health corresponds to the amount of money that is lost - those who lost £100-£999 were more likely to agree (45%) that this experience has had a long-term negative impact on their mental wellbeing than those who lost £1-99 (29%) and those who did not lose any money (13%)[12].

"I was really upset…I couldn't buy food or use the leccy [electricity]." ***Male, 41yrs, counterfeit goods scam, lost £800***

- In the qualitative study, most participants described the scams or fraud experience as emotionally turbulent, with victims starting on an initial high emotionally when engaging with the scammer, and ending on an emotional low after realising they had been scammed, experiencing emotional peaks and troughs in between.

"I was happy as I saw an offer [on a baby carrier], so I was excited waiting for it. But when it didn't arrive, I was worried and thinking 'what I have done?'. I felt fear and worry as I had not had this experience before." ***Male, 38years, counterfeit goods scam, lost £150 but was refunded***

"I went through an emotional rollercoaster…I was depressed, frustrated…when payments went out of my account I felt stressed and anxious. I was crying." ***Female, 47yrs, money laundering scam, lost £4,000***

[12] The base size for those who lost £1,000 or more is too small to report on.

- For most qualitative participants, the key driver to emotional distress was the amount of money lost due to the scam. If the money was subsequently recovered, the emotional impact was reported to be markedly less. (Figure 8)

"Reality dawned the next day and I'd lost £31k….depressed for a couple of days and didn't go to work…it's like losing a loved one…you don't get over it but learn to live with it." ***Male, 29yrs, cryptocurrency scam, lost £31,000***

"Noticed small amounts of money going out so called bank and reported and bank refunded the money. The impact was inconvenience as was without a bank account for a couple of days. Reassuring to know bank refunds money quite quickly." ***Female, 40yrs, impersonation scam, lost £1,000 but was refunded***

- However, there were a range of other emotional reactions that victims described during qualitative interviews: these included shame and embarrassment at having fallen for a scam, and a **sense of loss** for the relationship they had developed with the scammer.

"I kept it to myself because in the end I was stupid and it was my fault." ***Female, 24yrs, romance scam, lost £600***

Section 6: Key learnings and recommendations based on participants' views[13]

1. While online users are generally aware of online scams, there needs to be greater awareness of the current online scams in circulation. Scammers use a range of techniques to draw their victims in; and if online users are aware of the popular scam scenarios this can help them, possibly, avoid falling for them[14].

2. Online users would benefit from an improved understanding of the key characteristics of scams, such as initial engagement (how scammers establish communication with potential victims), the 'hook' (how they draw potential victims into engagement with a scam or fraud), techniques used to sustain engagement (e.g. frequent/overwhelming communication, tales of hardship), the financial transaction phase (how scammers defraud potential victims into handing over their money)[15] and potential impacts associated with scam or fraud (financial or otherwise), so they can identify a scam earlier in the process rather than when it is too late.

3. Being scammed has the potential to trigger mental health issues, so it is important victims recognise that they need support and therefore talk to friends and family about their experiences, and to report the incident as well.

4. From the qualitative interviews, participants feel there are steps that online users can take before engaging with users or content from unknown backgrounds or sources to avoid falling victim to fraud or a scam. For example, on accessing websites, stop and think before clicking on a link that is sent to you, check the website such as its contact and T&C pages to see if it is genuine, or find the website over a search engine yourself if in doubt rather than accessing it from the received link. When paying online, pay securely through websites that have a padlock, pay with a credit card and take screenshots of any payments before hitting send.

[13] Please note the learnings and recommendations presented in this report are based on the views of participants in this research, and should not be considered a reflection of any policy position that Ofcom may adopt when we take up our role as the online safety regulator.
[14] For example, one participant had signed up for a scams alert from a major search engine service, which made them aware of the current popular delivery scams, where a 'delivery company' requests a payment before they can deliver an item. However, the requested payment is not from the purported delivery company but from a scammer.
[15] These are identified in Figure 3 of the report.