Online Paid-for Advertisements Research

Produced by: YouGov & Ofcom

Published 10 July 2026

Contents

Section 1:

Research Background and Objectives

Background and Objectives

Research objectives:

The overarching aim of this research was to investigate consumer experiences and perceptions of online paid-for advertisements across search engines, social media and video-sharing platforms. The quantitative survey provided nationally representative data on user engagement, consequences and identification strategies of non-genuine advertisements, while the qualitative study offered deeper insights into how users assess trustworthiness and respond to potentially fraudulent online paid-for advertisements.

Definition of 'Paid-for Advertisements' in the context of this research:

As part of this research, Ofcom provided a clear definition of online paid-for advertisements to respondents prior to the start of the study to gather more relevant data. 'Paid-for advertisements' are defined as

'advertisements that appear on search services, social media platforms, and video-sharing platforms. Advertisements on other websites or in emails are excluded. Examples include sponsored search results, promoted social media posts, and video advertisements.'

Key research questions:

1. What are users' overall experiences and levels of engagement with potentially fraudulent online paid-for advertisements?

2. How do users interact with potentially fraudulent online paid-for advertisements, and what are the subsequent consequences of these interactions?

3. What methods or strategies do users employ to identify fraudulent online paid-for advertisements?

4. How do users evaluate and determine the trustworthiness of online content, particularly in relation to paid-for advertisements?

5. What specific visual or contextual elements do users recognise as indicators or cues of fraudulent online paid-for advertisements?

6. What levels of financial losses or psychological impacts have users experienced as a result of engaging with fraudulent online paid-for advertisements?

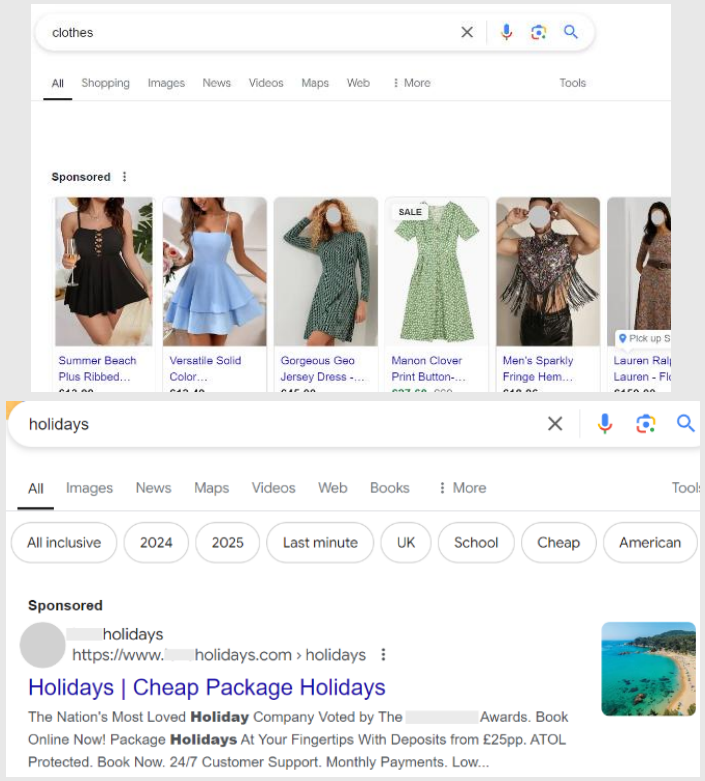
Note: Section 236 of the Online Safety Act 2023 defines a "paid-for advertisement" in relation to an internet service as an advertisement where (i) the service provider receives some form of consideration for the advertisement (either financial or non-financial), whether directly from the advertiser or indirectly through another person; and (ii) the placement of the advertisement is determined by systems or processes agreed upon by the parties under the advertising contract. This legal definition was not used in the research.

Examples of online paid-for advertisements in the context of this research

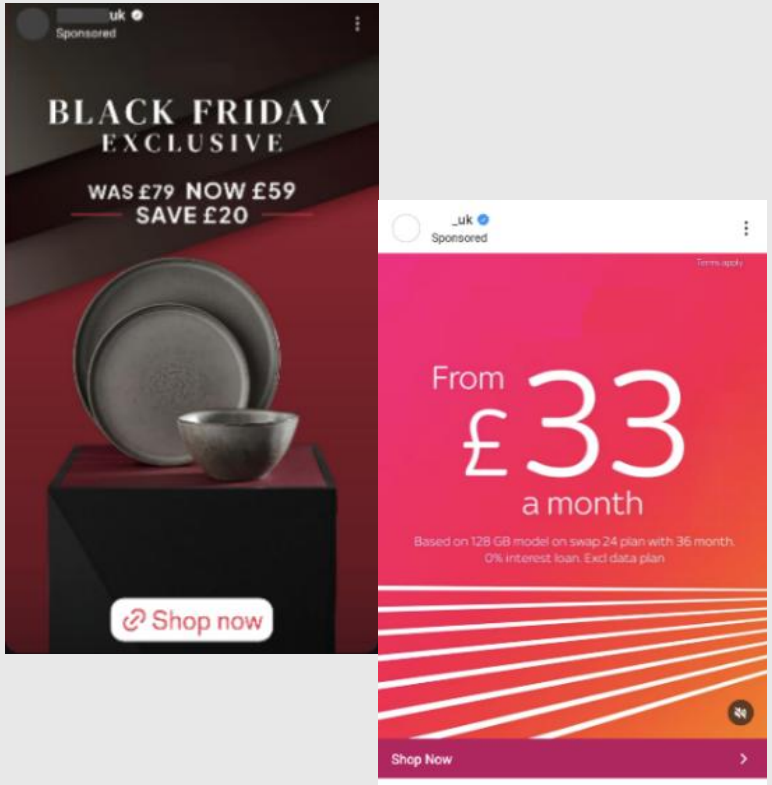
The definition and examples below were provided to participants to aid understanding of online paid-for advertisements in the context of this research:

'Paid-for advertisements' are defined as 'advertisements that appear on search services (e.g., Google, Bing), social media platforms (e.g., Facebook, Instagram, Twitter), and video-sharing platforms (e.g., YouTube, TikTok). Advertisements on other websites or in emails are excluded. Examples include sponsored search results, promoted social media posts, and video advertisements on platforms (parts of images or logos may be redacted)'.

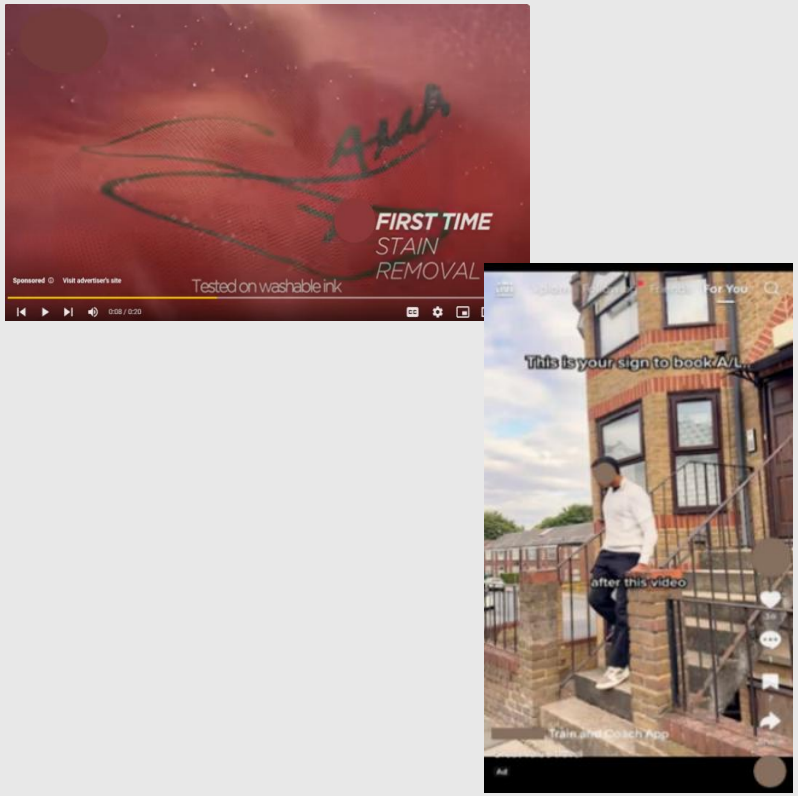
A display ad on a page of search results, possibly labelled as 'ad' or 'sponsored'



A post on their social media newsfeed that is not from accounts they follow, possibly labelled as 'sponsored'



An ad on a video-sharing service before their chosen video plays which is usually labelled 'sponsored' or 'ad'



Source: Search advertisement: Search results for "clothes" (top) and "holidays" (bottom) from Google, accessed October 2024

Source: ProCook advertisement from Instagram (left), accessed November 2024; Sky advertisement from Facebook (right), accessed October 2024

Source: Persil advertisement from YouTube (left), accessed November 2024; Trainline advertisement from TikTok (right), accessed October 2024

Methodology

Phase 1 – Quantitative Survey

- Fieldwork from 12 to 18 December 2024, carried out online by YouGov, with respondents recruited from YouGov's online panel
- Sample included 4,285 online users aged 18+ in the UK, with quotas set on region, gender, age, and social grade according to the national census
- Results were weighted to be nationally representative of the UK population (aged 18+)
- Significance testing was applied at the 95% confidence level between subgroups as well as against the total in data reporting

Phase 2 – Qualitative Follow-up

Fieldwork:

Stage 1 (2 to 6 June 2025): A 5-Day Passive Observation Diary Study
Participants uploaded up to 10 online paid-for advertisement screenshots that they came across in their day-to-day online activities (on social media, video sharing platforms or search services) and answered some related questions per day.

Stage 2 (24 to 26 June 2025): A 3-Day Online Community
Participants answered a series of deliberative questions about their perceptions of online paid-for advertisements, their assessments on a selected set of advertisements, and their thoughts on preventing fraud on each day, respectively.

Sample:
- 30 adults aged 18+ from a mix of backgrounds (e.g. different gender, region, ethnicity, digital confidence, social media usage)
- Half had previously experienced fraud as a result of fraudulent online paid-for advertisements and the other half had not

Analysis: Undertaken by researchers who conducted the fieldwork in multiple analysis sessions. Data was analysed using thematic analysis and key recruitment criteria – demographics, level of digital confidence and experiences of fraud.

Note: Since December 2024 when the quantitative research was conducted, the online environment – including advertising – has continued to change, with AI-generated content becoming more prominent. Further qualitative research conducted in June 2025 highlighted concerns about AI-generated images and increasingly sophisticated fraudulent advertisements. This suggests that AI has made existing challenges more intense rather than introducing entirely new ones. Overall, the findings are still relevant, but this context and the increasing prevalence of AI on user experiences and perceptions should be kept in mind when interpreting the quantitative findings.

Section 2:

Summary of Key Findings

Summary of key findings (1 of 2)

Fraudulent online paid-for advertisements are perceived to be a notable issue

The quantitative data shows that 51% of all respondents had encountered potentially fraudulent online paid-for advertisements, with 36% reporting they see them frequently online. **30% of UK adults have interacted with potentially fraudulent online paid-for advertisements** (e.g. clicking on them or following specific instructions), with younger adults (aged 18–24 and 25-34) being particularly susceptible to this behaviour (39% and 33% interacted respectively).

Users' judgement on the legitimacy and trustworthiness of an advertisement is influenced by a range of different factors

Qualitative insights show that consumers use a **combination of visual and contextual cues** to judge whether an advertisement is genuine. Indicators of trust include familiar branding, professional design, verified account badges and realistic offers.

Brand familiarity plays an influential role in eliciting trust. Consumers are more likely to engage with advertisements from brands they recognise, especially when the advertisement's design and language align with their expectations of the brand. However, that familiarity can also be leveraged to build false trust as the potentially fraudulent online paid-for advertisements encountered often feature **brands or public bodies (43%)** or **well-known individuals (24%)**.

Suspicion triggers include poor grammar, low-quality production, exaggerated claims, urgency-driven language, unfamiliar URLs and AI-generated imagery.

Some users feel vulnerable as fraudulent online advertisements become more sophisticated

Both the quantitative and qualitative research show that when legitimate cues outweigh suspicious ones, people can still be misled. This highlights the increasing **sophistication of fraudulent online paid-for advertisements**, especially those using **AI-generated content**.

Summary of key findings (2 of 2)

A notable proportion of users choose not to report potentially fraudulent online paid-for advertisements

Our qualitative research found that many participants expressed that they generally do not report potentially fraudulent online paid-for advertisements citing **lack of time, unclear processes and perceived ineffectiveness,** as barriers. A few said there was **no follow-up or resolution after reporting** in the past.

If users realised they had interacted with a fraudulent online paid-for advertisement, **43% said they reported the advertisement in some way** (of which 3% started to report but failed to finish the process). Around a third (34%) shared their experience with others, while 19% used the service less or stopped using it altogether, and **23% took no action** at all.

Online users have a strong desire for online platforms and services to implement stronger safeguards

Participants perceived online platforms as **profit-driven**, prioritising advertisement revenue over user safety. Some participants believed that platforms avoid strict vetting as a result. **Verified badges have lost credibility for some**, as participants noted they can be purchased or perceived them as being inconsistently awarded across platforms.

To improve this, participants suggested potential solutions such as **stricter verification for advertisers** (e.g. identity and business registration checks), **clearer warning systems** to flag suspicious advertisements and **clear labelling and disclosures of AI-generated content**.

The survey shows that **66% of those who interacted with fraudulent online paid-for advertisements (e.g. having clicked on them or followed specific instructions) found the advertisement attention-catching**.

Section 3: Engagement with Potentially Fraudulent Online Paid-for Advertisements

Half of respondents said they had encountered potentially fraudulent online paid-for advertisements, with a third reporting they see them frequently

Half (**51%**) of all respondents **had encountered potentially fraudulent online paid-for advertisements**, with a third (**36%**) reporting they see them **frequently** (i.e. almost every time or more than half the time when they go online) and another third (**35%**) seeing them **sometimes** (i.e. about half the time). Around a quarter (**27%**) said they **rarely** see such advertisements, indicating a widespread presence online.

Amongst the **C2DE** social group, participants **frequently** encountering potentially fraudulent online paid-for advertisements rose to **41%**.

Just under a third (**30%**) of respondents reported having **interacted with potentially fraudulent online paid-for advertisements**, such as clicking on it or following specific instructions. Among **18 to 24-year-olds**, engagement with potentially fraudulent online paid-for advertisements rose to nearly two-fifths (**39%**).

Two thirds of respondents (**66%**) who had interacted with a potentially fraudulent online paid-for advertisement found the advertisement **attention-catching**, with a third of respondents (**31%**) rating the advertisement as **extremely attention-catching**.

Among those who had interacted with a potentially fraudulent online paid-for advertisement, **two-fifths said the advertisement featured a well-known organisation**, while a quarter said the advertisement featured a well-known individual

Of those respondents who had interacted with a potentially fraudulent online paid-for advertisement, **24%** recalled that the advertisement had **featured a well-known individual**, and **43%** recalled it had **featured a well-known organisation**. Overall, **57%** reported that the advertisement had **featured either a well-known individual or a well-known organisation**.

Among those who had interacted with potentially fraudulent online paid-for advertisements, people aged **55 and over** were more likely than average to report having seen **a well-known organisation** in the last such advertisement they interacted with (**50%** vs 43%). By contrast, those **aged 25 to 34 years old** were more likely to have seen **a well-known individual** (**30%** vs 24%) featured.

Of interactions with a potentially fraudulent online paid-for advertisement that resulted in **monetary loss**, **35% featured a well-known influencer or social media personality** within the advertisement.

When participants were asked to name, unprompted, who or what was featured in the last fraudulent online paid-for advertisement they encountered, **Martin Lewis** was the most frequent answer. This represents an intentional misuse of his likeness, without his permission, given that Martin Lewis does not associate with advertisements*.

Those who interacted with a fraudulent online paid-for advertisement that featured **a well-known brand** were more likely than average to say that the advertisement was **extremely attention-catching** (**37%** vs 31%).

*Source: Money Saving Expert https://www.moneysavingexpert.com/shopping/fake-martin-lewis-ads/

A **single click** could open the door to fraud and lead to **unexpected risks**

Just under a third (**30%**) of respondents reported having ever **interacted with one or more potentially fraudulent online paid-for advertisements**, such as clicking on them or following specific instructions.

Of those respondents who had interacted with a potentially fraudulent online paid-for advertisement, many (**62%**) reported **clicking on it**. In particular, older adults aged **55 and over** or **those who saw a well-known brand featured** in the advertisement were more likely to click on it than average (both at **68%**).

Among those who clicked, over half (**52%**) said they were **taken to a page with a different product, service, or content than what was expected** from the advertisement, while **12%** reported that **an unexpected file was downloaded** onto their device.

Of those who experienced an unexpected file download, which was a small subset of the wider sample*, nearly half (**46%**) said they **later found a virus** on their device.

*The small base was n=94 or equivalent to around 2% of the total sample (n=4285)

The qualitative phase found that **health and financial service industries were felt to be most prone to fraudulent advertising**, with participants concerned about targeting those who are most vulnerable

- **Participants were concerned about advertisements in health and weight loss industries**, particularly those making **misleading** or **exaggerated claims** and **promising 'quick fixes'**. There was worry that they target those experiencing health issues or those struggling to lose weight, making them more likely to fall for these claims.

- Participants felt that **advertisements in the financial industry were prone to fraud**, such as those offering credit cards, loans, investments, debt help and insurance claims. They also noted being **concerned about gambling product advertisements** and schemes that promise to make money quickly. Participants expressed extra concern about these advertisements which were perceived to be targeting people in financial need or other vulnerable positions, making them more susceptible to fraud.

- Other products and services that participants felt were prone to fraudulent advertisements based on their own experience and knowledge included **solar panels, job postings, online dating, electricals** (particularly smartphones), as well as **fashion items** from famous brands offering large discounts.

"I think any product that promises a quick fix in terms of weight or health, as people are highly emotional about that and more likely to engage with a solution." – Female, 18-34, Not experienced fraud, High digital confidence

"Those offering easy ways to make money, e.g., gambling, competition organisers. I think this is because people are likely to be tempted, especially if the initial outlay is small and the potential win is big." – Female, 55+, Experienced fraud, Low digital confidence

"Life insurance scams that target the elderly who are most likely to take up these offers that the company promises." – Male, 55+, Experienced fraud, Low digital confidence

"Trying to recruit people into pyramid schemes through get rich quick scams. Also so many adverts for vitamins and weight loss products which may be dangerous." – Female, 55+, Not experienced fraud, Medium digital confidence

Section 4:
Interactions with and Consequences of Potentially Fraudulent Online Paid-for Advertisements

Among respondents who interacted with potentially fraudulent online paid-for advertisements, a majority realised it was fraudulent straight away, while **just under a quarter** were contacted by a scammer afterwards

Around a quarter (**24%**) of respondents who had interacted with a potentially fraudulent online paid-for advertisement were **contacted by a scammer afterwards**. Email (42%) was most common, followed by phone (33%), SMS/text or social media (both 26%), then instant messenger (23%).

Many respondents (**61%**) who interacted with potentially fraudulent online paid-for advertisements reported they **realised the advertisement was fraudulent straight away**, while nearly one in ten (**9%**) reported it taking them **between a week and a month**. Overall, the majority (**83%**) realised in **less than a week**.

After interacting with a potentially fraudulent online paid-for advertisement, around two in five (**43%**) of respondents said they **reported the advertisement** to some form of official body such as the platform or their bank (20%) and Action Fraud* (8%). A notable **23% took no action** at at all.

Reporting the potentially fraudulent online paid-for advertisement was more common among those aged 55 and over than average (**49%** vs 43%). Around a third (**34%**) of respondents **shared their experience** in some way, including discussing with family and friends, or on social media. Sharing was **more common among 18 to 24-year-olds** (**43%**).

<u>Why participants did not take action after interacting with potentially fraudulent online paid-for advertisements:</u>

Of the 23% who took no action, the most frequently shared reasons included **not knowing what to do or who to inform** or **not feeling they were directly impacted** (both at **27%**), followed by believing that **reporting would not make a difference** (**23%**).

Overall, the most common reason for not reporting was a **lack of motivation or time (50%)**, followed by **perceived ineffectiveness of reporting (45%)**, **perceived lack of harm or severity (30%)** and **fear of reporting (14%)** such as feeling embarrassed.

*Action Fraud was renamed to Report Fraud from 4 December 2025 following this research.

Those who had been a **victim of fraud disregarded their suspicions when legitimate advertisement indicators outweighed suspicious ones**

Those who had experienced fraud because of online paid-for advertisements **felt they were acting with vigilance before being scammed**.

Trust was built early on in their experience with advertisements having high-quality images, numerous likes/followers and low prices but still **realistic**. Where the advertisement was linked to a working website, this increased perceptions of authenticity.

As they perceived most **cues pointed to a legitimate advertisement early on**, the participants were less suspicious towards the end of the process, disregarding suspicious factors, unconventional payment process or asking for extensive details.

It was not until **after the initial transaction that they discovered they had been scammed** (e.g. no items materialising, unwillingly looped into a subscription, money being taken).

A few **lost faith** in the ability of platforms and services to help victims of fraud as there was **no follow-up after reporting** and had to turn to their credit card companies to recoup losses.

*"I saw this ad for some shirts that looked really nice and were kinda cheap. The **website looked proper**, and they had a [social media] page too with lots of followers and good pics, so I thought it was safe. I ordered but never got anything. Tried messaging them, but no reply. The page was gone after some days. I felt so stupid. Since then, I don't trust small brands easily even if they look fancy."*
– Male, 18-34, Experienced Fraud, Medium digital confidence

*"I got suckered into purchasing 24 multipack of [a snack] flavoured ginger... living close to the factory, I could believe this was to get rid of excess stock. The **ad looked legitimate, the web address looked correct, the website I clicked to from the advertisement looked proper, had working links**... But when I went to purchase and pay, it took me to [an e-commerce platform] and asked for bank details - probably should have been a red flag, but I continued with the purchase."*
– Female, 35-54, Experienced Fraud, Medium digital confidence

*"I **won a competition** for some tools from a [social media] advertisement from a **branded company but had to pay postage** of £4.95. I foolishly paid via my credit card and **somehow got signed up for a subscription** to a financial advisor service, and they tried taking money every 2 weeks. I contacted the credit card company, and they blocked the account, said it was a common scam, and luckily, I got my money refunded."*
– Male, 35-54, Experienced Fraud, Medium digital confidence

Although the majority of users did not suffer monetary loss, interactions with potentially fraudulent online paid-for advertisements can have significant effects, with **over half of affected respondents** reporting an **immediate negative impact on their mental health**

The majority of interactions (**71%**) with potentially fraudulent online paid-for advertisements did **not result in monetary loss** for the user.

A quarter of respondents (**26%**) who interacted with a fraudulent online paid-for advertisement reported **financial loss**, with a significantly **higher likelihood** if they were **contacted by scammers afterwards** (**41%**), **among 18–24s** (**36%**), or if the advertisement **featured influencers/social media personalities** (**35%**).

In terms of the amount of money lost, the largest proportion (**18%**) of those who interacted with a fraudulent online paid-for advertisement lost **between £1 and £99**. Around one in fifteen (**6%**) lost **between £100 and £999**, one in fifty (**2%**) lost **between £1,000 and £9,999** and one in a hundred (**1%**) lost **between £10,000 and £19,999**.

Over half of respondents (**54%**) who lost money to a fraudulent online paid-for advertisement reported an **immediate negative impact** on their mental health, with a third (**33%**) saying that the impact was **long-term**.

Section 5:
Perception of Authenticity in Online Paid-for Advertisements

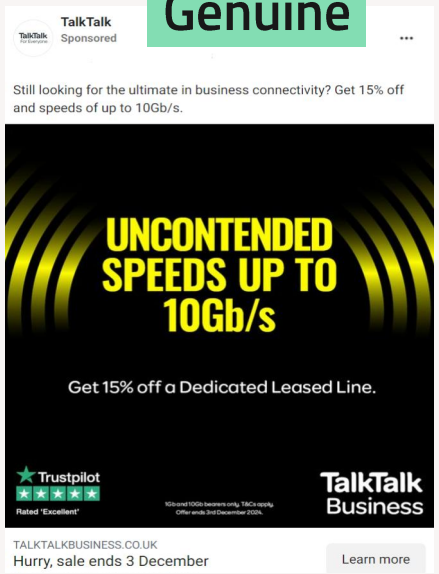
Exploring **perceptions of authenticity** in online paid-for advertisements

Participants were shown five online paid-for advertisements, some genuine and some potentially fraudulent. They were asked to determine **whether they believed the advertisement was genuine or not**, and **what factors influenced their perceptions**.

This section of the research was focused on understanding what factors create trust or distrust amongst users, and the ability of users to distinguish potentially fraudulent from genuine online paid-for advertisements. Heatmap analysis is used to demonstrate which specific features of the advertisement were identified by the participants as characteristics indicating authenticity or inauthenticity.

The examples used were retrieved from publicly available sources.

Genuine

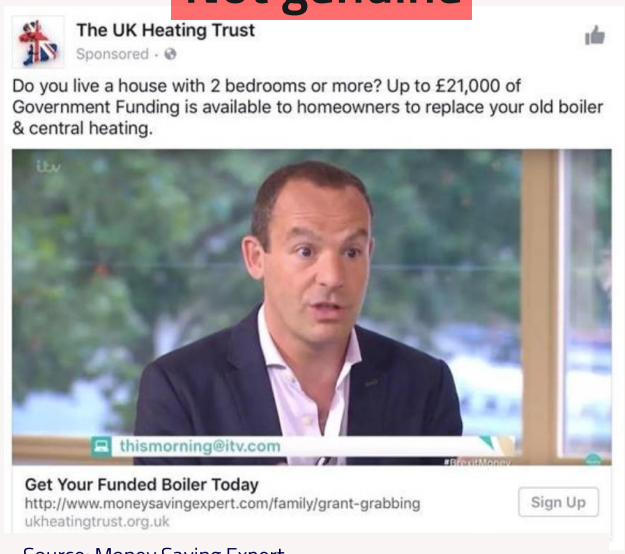


Source: TalkTalk Business advertisement from Facebook, accessed November 2024

Not genuine

Source: Which? https://www.which.co.uk/news/article/how-our-fake-scam-ad-breezed-through-facebooks-approvals-process-a5zzC7j1n3BN, accessed November 2024

Not genuine

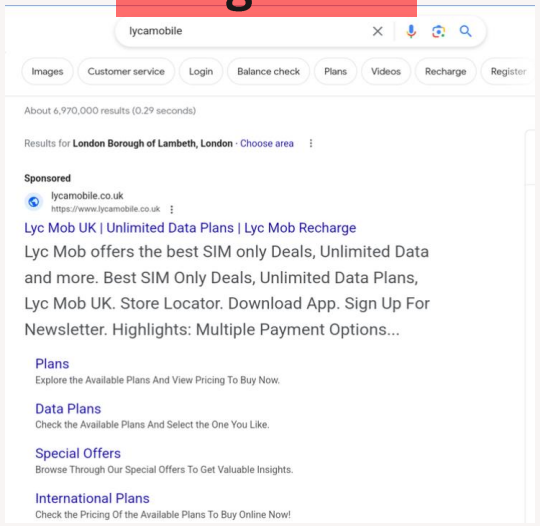


Source: Money Saving Expert https://www.moneysavingexpert.com/shopping/fake-martin-lewis-ads/, accessed November 2024

Not genuine

Source: Mirror https://www.mirror.co.uk/news/uk-news/elon-must-act-stop-tide-30451315, accessed November 2024

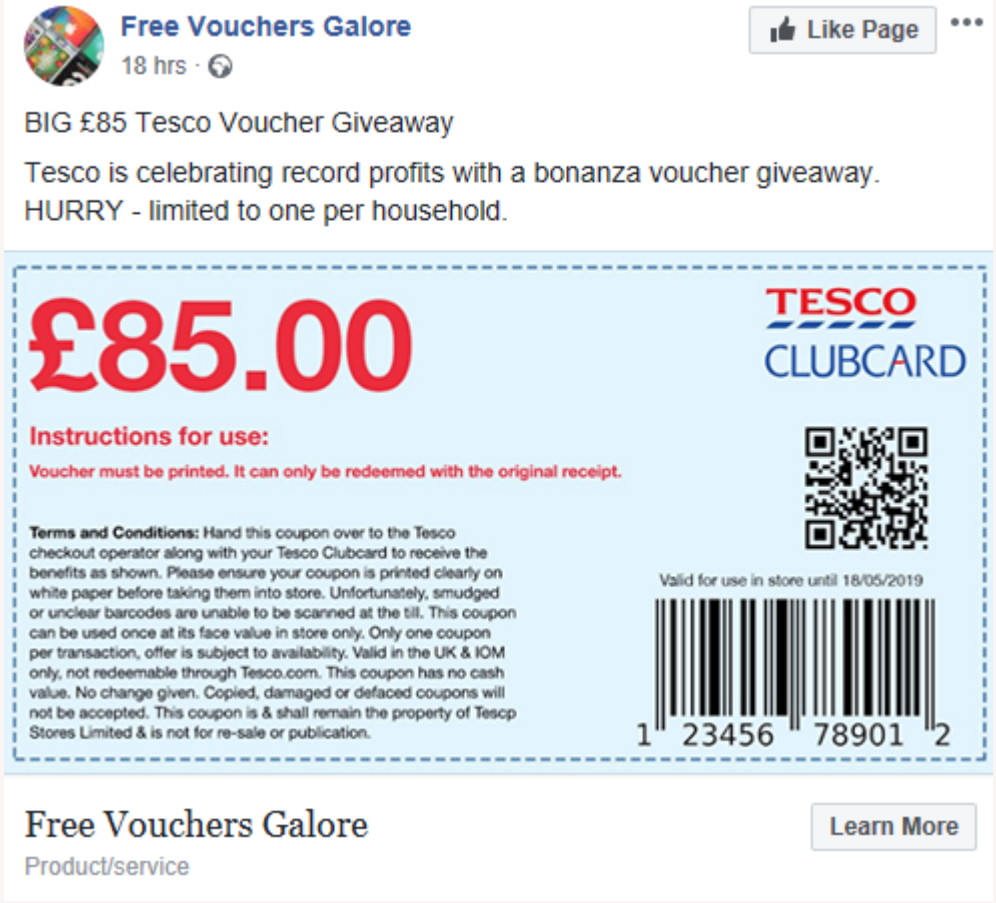
Not genuine



Source: Which? https://www.which.co.uk/news/article/scammer-bypasses-google-search-as-verified-advertisementiser-alCjw4y3pz7b, accessed November 2024

Those who perceived the advertisement as a scam said the offer seemed unreasonable, while half of those who **believed it was genuine trusted its association with a well-known brand**

Scam



Do you think this is a genuine advertisement or a scam?

Genuine	8%
Scam	85%
Don't know	7%

Why do you think that?

Genuine

1. It's a well-known brand – 47%
2. The logo is familiar – 42%
3. There's a QR code – 41%

Scam

1. The offer doesn't seem reasonable – 69%
2. It doesn't look professionally put together – 36%
3. The promoter's name is unfamiliar – 30%

Note: This advertisement is not genuine; Tesco has no association with or involvement in the scam.

Source: Which? https://www.which.co.uk/news/article/how-our-fake-scam-ad-breezed-through-facebooks-approvals-process-a5zzC7j1n3BN, accessed November 2024

The unknown account, coupled with the high voucher amount, made nearly all the participants feel this was not a legitimate advertisement

Inauthentic indicators

The account name raised suspicions as to why the advertisement was not coming from the official page, along with the name being generic and having 'free' in it.

'**HURRY**' **Created a sense of urgency** as well as a belief that big brands do not use capitals.

The amount of money being advertised was unusual compared to typical offers.

Many believed **an advertisement from an established brand would not include spelling and grammar mistakes ('Tescp')**

A minority highlighted that the **barcode was not realistic and unlikely to have consecutive numbers.**

Inauthentic advertisement

Trust indicators

A very small number felt the advertisement could potentially be legitimate.

The inclusion of the 'genuine looking' **branding/logo added legitimacy** to the advertisement.

A small number of participants believed the use of the **QR in the vouchers made it appear professional** and therefore, more credible.

The **requirement to print the voucher and present it in-store**, rather than clicking a link or making an immediate purchase, **increased participants' trust of the advertisement**.

"Offer is far too good to be true, big companies will maybe give £10 off a hundred-pound shop, never mind free money." – Male, 35-54, Experienced fraud, Medium digital confidence

"This is an unknown website offering Tesco vouchers. I would expect Tesco to be offering their own vouchers." – Female, 55+, Experienced fraud, Low digital confidence

"As it's redeemable only with your Clubcard and you have to take it to the checkout, it seems legitimate. If it required the customer to part with money, then I would be suspicious." – Male, 55+, Experienced fraud, Low digital confidence

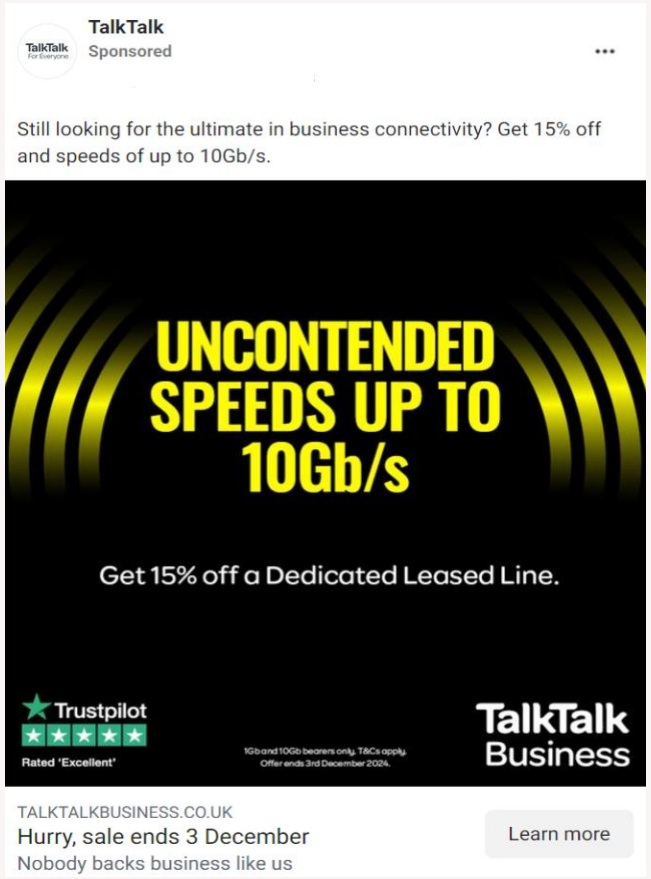
***Colours on the heatmap indicate the areas that participants labelled as raising trust or suspicion – red=most annotated areas**

Note: This advertisement is not genuine; Tesco has no association with or involvement in the scam.

Source: Which? https://www.which.co.uk/news/article/how-our-fake-scam-ad-breezed-through-facebooks-approvals-process-a5zzC7j1n3BN, accessed November 2024

Familiarity with the promoter, logo, professionalism and trusted consumer review ratings helped respondents to judge the advertisement as genuine, while those who saw it as a scam pointed to the urgency in language and an unprofessional appearance, though **no single factor was dominant**

Genuine



Do you think this is a genuine advertisement or a scam?

Genuine	66%
Scam	15%
Don't know	19%

Why do you think that?

Reasons it is genuine:

1. The promoter is familiar – 55%
2. There's a Trustpilot rating – 53%
3. The logo is familiar – 49%

Reasons it is a scam:

1. There's language that expresses urgency – 31%
2. It doesn't look professionally put together – 28%
3. The offer doesn't seem reasonable – 25%

Source: TalkTalk advertisement from Facebook, accessed November 2024

The recognisable branding, reasonable offer, and inclusion of trusted consumer review ratings made the advertisement appear more trustworthy to the majority

Inauthentic indicators

A minority noted **the post did not come from a verified account** and placed no value in it being sponsored.

A minority felt **the advertisement used strange terminology, such as 'uncontended'** and believed the brand would use simpler language.

Participants who had experienced fraud noted **'Hurry, sale ends' created a sense of urgency to purchase, which felt suspicious** given the long period of time left on the offer.
Others, however, felt it was standard language for big companies which are promoting deals to include in their advertisement.

Some noted **the date was written as '3 December'** rather than '3rd December [Year]', which was counter to their expectations and caused concern.

Legitimate advertisement

Trust indicators

The account which posted the advertisement matched the official branding, as it included the recognisable, correct logo and spelling.

Participants felt '15% off' was a believable discount for a company like this to offer its customers.

The subject seemed appropriate and expected of the brand, and therefore the advertisement was considered authentic.

The inclusion of a Trustpilot ('an independent trust body') score was **a major indicator of legitimacy,** as ratings can be verified through individual research.

"Not promising me money but instead trying to draw me in with subtle discounts, as a big trustworthy organisation normally would." – Male, 18-34, Not experienced fraud, High digital confidence

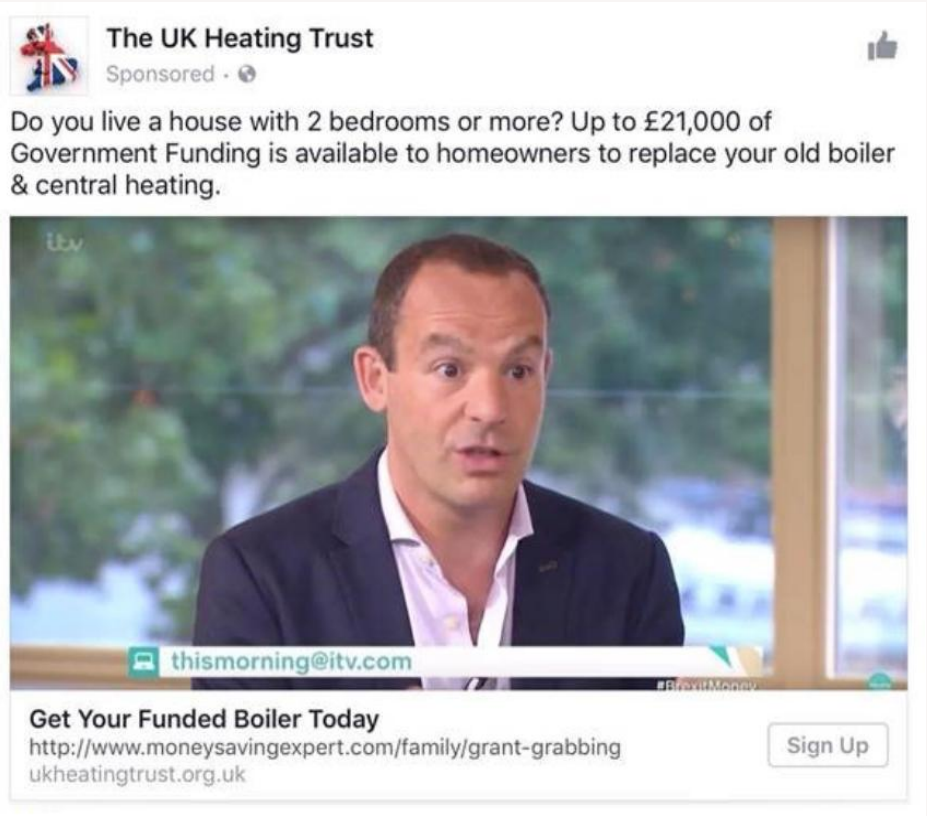
"The trust pilot rating makes this ad more trustworthy because it is an external reviewer approving them, but also because it is a fact that can be cross referenced with Trustpilot's own site as part of a strategy to check the legitimacy of the advertisement." – Female, 18-34, Not experienced fraud, Medium digital confidence

***Colours on the heatmap indicate the areas that participants labelled as raising trust or suspicion – red=most annotated areas**

Source: TalkTalk advertisement from Facebook, accessed November 2024

Knowing that the public figure doesn't advertise helped some respondents to correctly identify the advertisement as not genuine, **while those who didn't know would have viewed the public figure as a cue to legitimacy**, further enhanced by a realistic-looking web link

Not Genuine



Do you think this is a genuine advertisement or not genuine?

Genuine	23%
Not Genuine	59%
Don't know	18%

Why do you think that?

1. The web links seem legitimate – 45%
2. There's a well-known public figure – 38%
3. The content is labelled as "Sponsored" – 29%

1. I think this public figure doesn't do advertisements – 56%
2. The offer doesn't seem reasonable – 32%
3. The web links seem suspicious – 27%

Note: This advertisement is referred to as not genuine rather than a scam because there is a possibility that The UK Heating Trust could be a legitimate company, although its legitimacy could not be verified. This advertisement was "falsely trading off Martin Lewis's name" according to Money Saving Expert.

Source: Money Saving Expert https://www.moneysavingexpert.com/shopping/fake-martin-lewis-ads/, accessed November 2024

The majority thought the advertisement was not genuine, but the combination of official bodies increased trust, with a significant minority believing it to be legitimate

Inauthentic indicators

For the majority, they perceived the advertisement to be fraudulent as they were aware that this public figure **does not endorse third-party advertisements**.

The firm named in the advertisement was not believed by some to be a legitimate provider of government grants. This suspicion was heightened due to the high value of the offer and the urgent call to action.

The **inclusion of two different links raised suspicion**. The link that included '**http', not 'https**' was **treated with caution**.

Inauthentic advertisement

Trust indicators

The use of the word 'trust' in the account name and relevant logo **added legitimacy** to the source of the advertisement for a minority. **The mention of the government** in the advertisement description also made the advertisement more trustworthy.

The image gave a further **indicator of trust as it appeared this public figure had endorsed the advertisement,** coupled with his website appearing at the bottom.

The association with an established organisation suggested a trusted source of information had approved the advertisement. Those who thought the advertisement was true believed this organisation **would not allow fraudulent advertisements to use their name**.

"I know Martin Lewis has previously fought against his face being used on advertisements without his permission. He is a trusted person, and I am aware that lots of scam adverts will use his likeness to try and instil trust." – Male, 35-54, Not experienced fraud, Medium digital confidence

"The word 'trust' makes people think right away that it's a charity and can be trusted, 'government' - making the advertisement seem reliable as you're not getting money from a company but the government." – Female, 35-54, Has experienced fraud, Medium digital confidence

"I trust Martin Lewis, so if he was saying this on a TV programme like this morning, then I would trust what he had to say." – Female, 35-54, Not experienced fraud, Low digital confidence

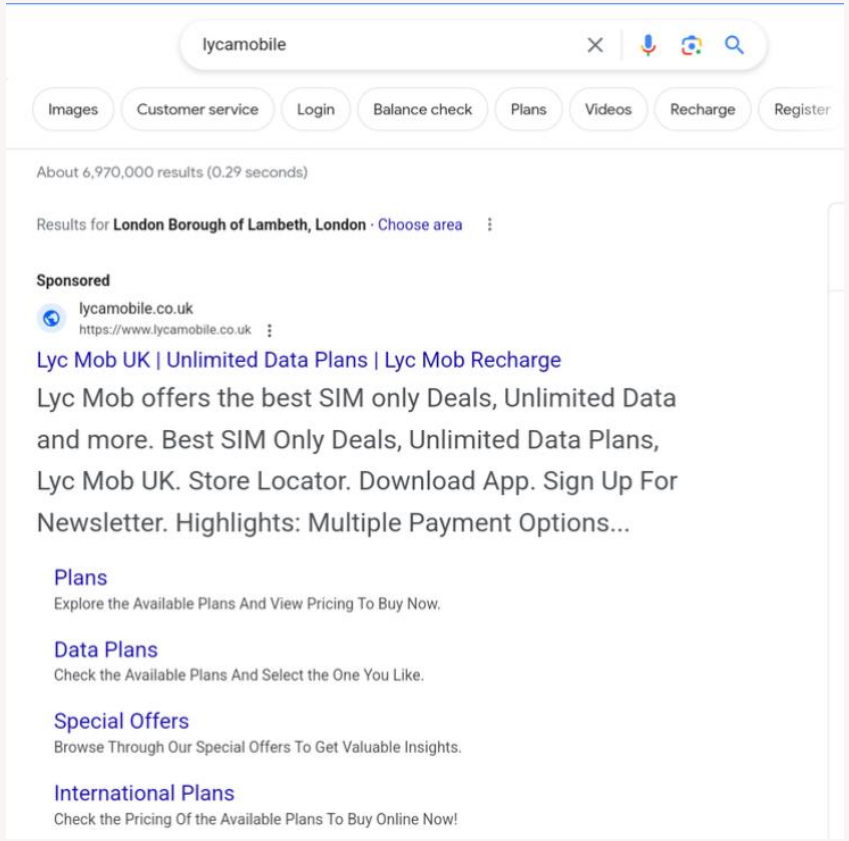
***Colours on the heatmap indicate the areas that participants labelled as raising trust or suspicion – red=most annotated areas**

Note: This advertisement is referred to as not genuine rather than a scam because there is a possibility that The UK Heating Trust could be a legitimate company, although its legitimacy could not be verified. This advertisement was "falsely trading off Martin Lewis's name" according to Money Saving Expert.

Source: Money Saving Expert https://www.moneysavingexpert.com/shopping/fake-martin-lewis-ads/, accessed November 2024

This advertisement divided opinion, with around two-fifths considering it genuine and the same proportion seeing it as a scam, while a quarter were unable to decide - those who thought the advertisement was a scam identified **issues with the brand name**, while those who believed it was genuine pointed to its links and suggested webpages which appeared legitimate

Scam



Do you think this is a genuine advertisement or a scam?

Genuine	38%
Scam	37%
Don't know	24%

Why do you think that?

Genuine:
1. The web links seem legitimate – 67%
2. The suggested web pages (e.g. Plans, Data Plans) seem legitimate – 50%
3. The content is labelled as sponsored – 38%

Scam:
1. Something wrong with the brand name – 49%
2. The web links seem suspicious – 32%
3. Something wrong with the blurb – 31%

Note: This advertisement is not genuine; Lycamobile has no association with or involvement in the scam.

Source: Which? https://www.which.co.uk/news/article/scammer-bypasses-google-search-as-verified-advertisementiser-alCjw4y3pz7b, accessed November 2024

There was no consensus on the legitimacy of this advertisement – poor spelling and grammar were the main tip-off for those who felt the advertisement was inauthentic

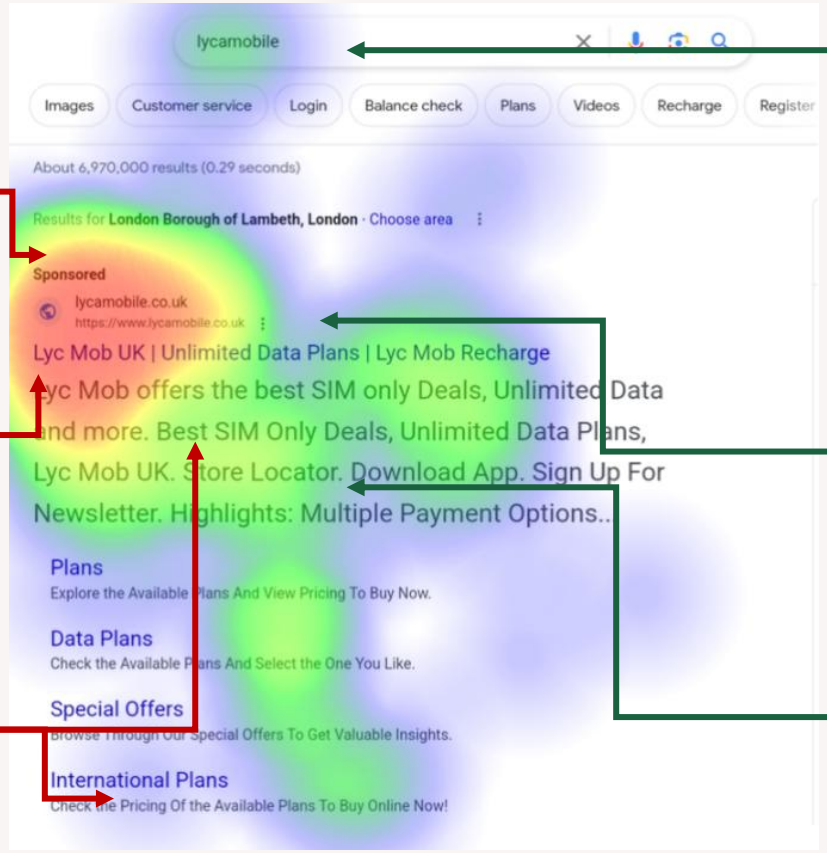
Inauthentic indicators

Being a **sponsored advertisement automatically created suspicions,** as many participants felt anyone can pay to post.

Participants **noticed the inconsistent spelling between 'Lyca Mobile' and 'Lyc Mob',** which raised suspicion and caused participants to stop engaging with the advertisement.

The **random capitalisation of letters didn't feel in line with a legitimate company**. The repetition of 'best sim' throughout the advertisement made it feel inauthentic.

Inauthentic advertisement



Trust indicators

Although the majority were suspicious of sponsored advertisements, a minority felt the opposite and assumed that the search service would have a vetting process.

Many noted that **the link included 'https' and/or '.co.uk', therefore it appeared secure and genuine**. They felt the **URL was spelt correctly** for the company advertised.

The **reference to the store location** and the app **increased the advertisement's authenticity** as participants noted fraudulent advertisements usually do not promote these.

"Someone has paid to put it there rather than it being an organic listing. Anyone can pay to advertise on [a search service] so I am always suspicious of sponsored links." – Male, 35-54, Not experienced fraud, Medium digital confidence

"I spotted the spelling mistake straight away, the fact that there are so many instances of the mistake would stop me in my tracks and make me not engage." – Male, 35-54, Experienced fraud, High digital confidence

"The way this is set out … just a list that from store locator looks like the tabs you usually find at the top of a web page….the blurb does look suspicious as it does not flow and is disjointed." – Female, 55+, Experienced fraud, Low digital confidence

***Colours on the heatmap indicate the areas that participants labelled as raising trust or suspicion – red=most annotated areas**

Note: This advertisement is not genuine; Lycamobile has no association with or involvement in the scam.

Source: Which? https://www.which.co.uk/news/article/scammer-bypasses-google-search-as-verified-advertisementiser-alCjw4y3pz7b, accessed November 2024

Those who perceived the advertisement to be not genuine cited **issues with the photo** and its lack of professionalism, while those who saw it as genuine mainly attributed it to the blue tick

Not Genuine

Do you think this is a genuine advertisement or not genuine?

Genuine	7%
Not Genuine	83%
Don't know	10%

Why do you think that?

1. The promoter's account is verified/has a blue tick – 37%
2. The web link seems legitimate – 25%
3. The content is labelled as "promoted" – 21%

1. Something wrong with the photo – 61%
2. It doesn't look professionally put together – 49%
3. The web link seems suspicious – 29%

*This advertisement is referred to as not genuine rather than a scam because its legitimacy could not be verified. The deepfake image may have been used to attract attention. Lambros Law Office has no association with or involvement in the scam.

Source: Mirror https://www.mirror.co.uk/news/uk-news/elon-must-act-stop-tide-30451315, accessed November 2024

The majority easily identified this advertisement as inauthentic due to the apparent use of AI and the unrealistic situation depicted

Inauthentic advertisement

Inauthentic indicators

The **'Law office',** which was advertising the celebrity's website **was suspicious as they are seemingly unrelated to one another**.

The sensationalist language used, such as 'astonishing' and 'prepare yourself', **felt like 'clickbait'.**

The image was felt to be **clearly AI-generated, and it was considered highly unrealistic for the celebrity to behave or be involved in a situation like this.**

"This looks like an AI-generated image of a celebrity. It is quite click-baity as he is depicted being arrested, which would pique the viewer's curiosity." – Female, 35-54, Not experienced fraud, Medium digital confidence

Trust indicators

A very small number of participants (from both those who had experienced fraud and hadn't) felt the advertisement was legitimate. Those who did, felt the **verification tick meant that the account posting the advertisement was trustworthy**.

However, a couple of participants noted the account may have been hacked and **that this advertisement is most likely spam due to its unrealistic nature.**

A small number of participants believed **the link to the celebrity's website appeared to be legitimate and trustworthy due to the correct spelling**.

"A verified account indicates trustworthiness; however, it appears that if this is a genuine account, it has been hacked and is now posting spam content." – Female, 35-54, Not experienced fraud, Medium digital confidence

***Colours on the heatmap indicate the areas that participants labelled as raising trust or suspicion – red=most annotated areas**

*This advertisement is referred to as not genuine rather than a scam because its legitimacy could not be verified. The deepfake image may have been used to attract attention. Lambros Law Office has no association with or involvement in the scam.

Source: Mirror https://www.mirror.co.uk/news/uk-news/elon-must-act-stop-tide-30451315, accessed November 2024

Section 6: Determining Trustworthiness in Online Paid-for Advertisements

Participants tended to look out for **a range of factors to help them identify potentially fraudulent online paid-for advertisements**

Checking if the URLs appear to be legitimate and if there is a **padlock sign**. A minority preferred to go directly to the official company website, as opposed to clicking on the link provided in the online paid-for advertisement.

Researching the company, looking at the comments under the advertisement and **customer reviews across trusted, independent platforms**, particularly if they were unfamiliar with the brand or the advertiser.

Checking for 'verified' labels next to the account name can help validate the advertisement.

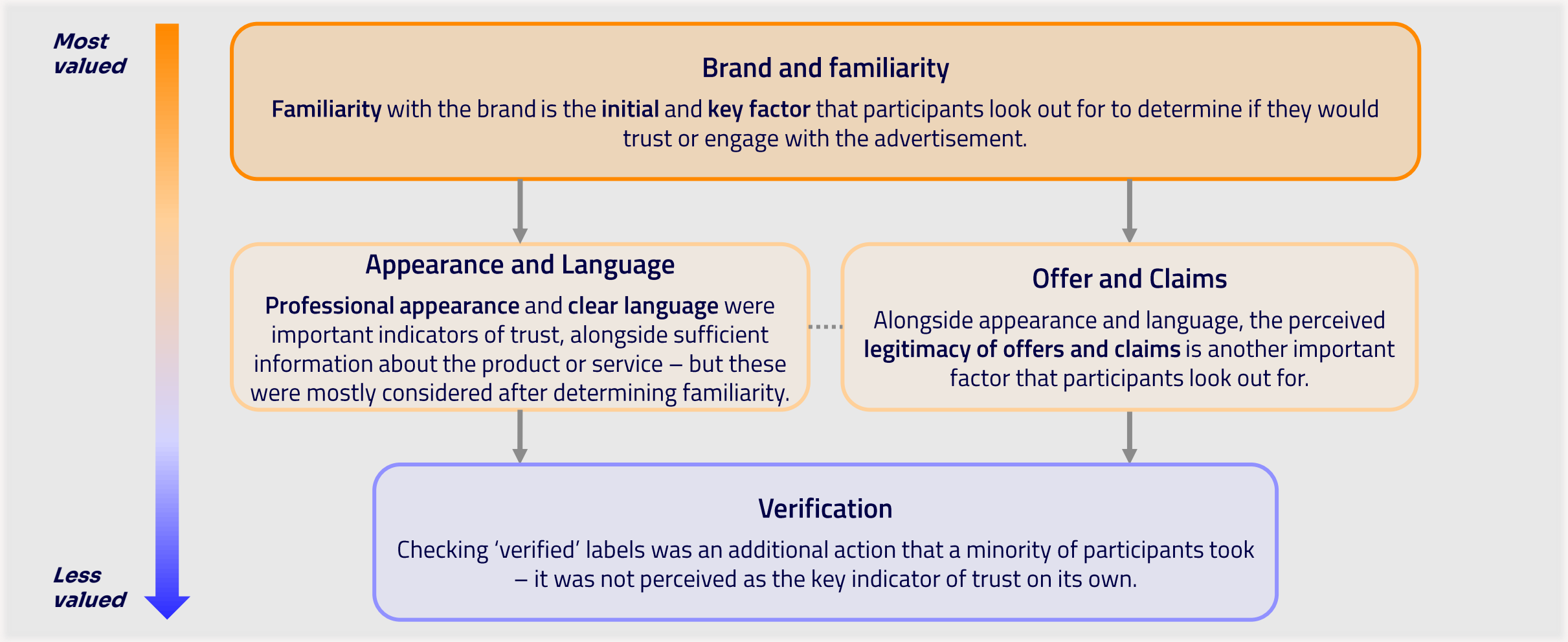
Paying attention to language of the advertisement, such as click-bait titles, phrasing that indicates a sense of urgency, alongside poor grammar and spelling mistakes.

Being cautious about offers that are perceived as 'too good to be true', such as very low prices or exaggerated claims.

Being cautious about advertisements that include public figures, particularly for unknown brands, or where the values of the public figure do not tie in with the product advertised. This also includes looking out for signs of the advertisement being AI-generated.

Being cautious about engaging with advertisements from industries that are prone to scams, such as insurance claims or weight loss.

In summary, the **perception of trustworthiness in online paid-for advertisements is dependent on a number of interconnected factors**, where some hold more value than others:



Participants were **more likely to trust advertisements from well-known, established brands that they were familiar with**

Familiarity with the brand or the company was the most important factor in determining trustworthiness:

- ✓ **Advertisements from well-known brands generally inspired trust**, particularly if the advertisement was coming from a brand's own verified account. This was further reinforced if the advertisement was **consistent with the perceptions or expectations of the brand**. This included having high-quality video or images, as well as prices, offers, style and language that felt align with the brand.
- ✓ Participants pointed out that **well-known brands were easily recognisable** through prominent logos, distinctive colours, unique fonts and consistent use of slogans throughout.
- ✓ Participants were **more likely to trust** an advertisement if they or someone they knew had previously used the company and had a **positive experience**. Seeing friends or family engage with the advertisement, for example, by liking the post or following the advertiser's account, also increased their trust.

"[Greeting cards advertisement – from search] I am familiar with the advertiser. I recognised the website address and branding within the image… the branding are as I would expect from this company. The advertised price is also about what I would expect to pay ." – Male, 35-54, Not experienced fraud, Medium digital confidence

"[Investment trading service advertisement – from video-sharing platform] The ad seemed trustworthy. It highlighted clear features, mentioned regulatory compliance, and referenced high ratings [from a trusted consumer review platform], matching [the trading service]'s reputation for transparency and reliability." – Male, 18-34, Not experienced fraud, Medium digital confidence

"Sometimes I will trust a brand because I know it and have heard of it. Or I am aware of their values and or practices as a company and the ad might reinforce or remind me to look at their products/services." – Female, 18-34, Experienced fraud, Medium digital confidence

Whilst brand familiarity was important, and participants were more likely to trust advertisements from established brands, **participants tended to look out for a range of indicators of trust**

Lack of familiarity with the advertiser, or absence of a clear logo, name and branding, tended to reduce participants' trust in the advertisement. However, even if they were familiar with the brand, they tended to look out for other factors to determine trust:

- × Participants were more **sceptical of advertisements that appeared manipulated or out of character** for the brand they were familiar with (e.g., poor-quality images, offers or language that does not align with the usual brand communications).
- × **Brand reputation** played a role in determining trustworthiness – participants noted they would be **unlikely to engage with an advertisement if the brand had a poor reputation** (e.g., e-commerce platforms that were perceived to have poor-quality items and ethical concerns).
- × A minority of those who had previously experienced fraud noted that, despite familiarity with the advertiser, they would still be cautious and would go to the website directly (e.g., via a link in search services), rather than clicking on the social media advertisement, due to **concerns about fake URLs**.

"I trust ads for established brands more than unfamiliar or unknown brands… I have seen a lot of ads for sites such as [certain e-commerce platform] which I do not click on as I do not trust the brands themselves (due to poor product quality, ethical/supply chain concerns and poor security around financial/payment information)." – Female, 35-54, Not experienced fraud, Medium digital confidence

"[Haircare advertisement – from social media] Not at all familiar with the advertiser. Not sure whether trustworthy. Says it's an award-winning product but never heard of it." – Female, 55+, Not experienced fraud, Low digital confidence

"[Trainer's advertisement – from social media] It's an unknown shoe seller, selling expensive shoes that could easily be fake. The link title looks iffy, but it somehow takes you to the [trainers' brand] website." – Female, 18-34, Experienced fraud, High digital confidence

Whilst high-profile, familiar celebrities increased trust in the advertisement, there were **significant concerns about the misleading use of celebrity images and videos, particularly those generated by AI**

- ✓ **The presence of a high-profile celebrity** was felt **to increase the legitimacy of the advertisement**. This was because participants felt that a company would need a large marketing budget to hire a celebrity, therefore indicating its legitimacy. It was also felt that the celebrity endorsing the product would be unlikely to do so if there was a risk of reputational damage (e.g., if they endorsed potentially unsafe products).
- ✓ The presence of a celebrity, particularly **enhanced trust** if the individual was perceived as an **expert** in the field (e.g., renowned chef recommending a restaurant).

- × However, there were concerns about the **prevalence of AI-generated celebrity endorsements**. Participants were worried about the potential for AI-generated advertisements featuring celebrity likenesses to target people in a deceptive manner, without the celebrity's consent. Many were also concerned about the increasing difficulty in distinguishing real from fake or manipulated celebrity endorsements, especially online, as the technology advances. Participants expressed uncertainty about whether they had been fooled by such content in the past.
- × A minority noted coming across or hearing about AI-generated advertisements using well-known public figures' images/videos to promote financial products.

"[A very subtle luxury fashion brand advertisement – from video-sharing platform] [This actress] is a rep for [this luxury fashion brand], so I identified that that advertisement was [from this luxury fashion brand]... I find the advert very trustworthy due to the use of celebrities and also how big the brand itself is." – Female, 18-34, Experienced fraud, Medium digital confidence

"[An advertisement featuring an online influencer – from social media] Very untrustworthy. It was not clear what the topic was about - the statement was vague and clickbait. They used a well-known celebrity to make people think it is about him." – Female, 35-54, Not experienced fraud, High digital confidence

"I have recently been seeing ads for a gambling app on my [video sharing platform's] for you page featuring videos of high-profile celebrities endorsing the product, when I know realistically that these celebrities would not do that and AI has been used." – Female, 35-54, Not experienced fraud, Medium digital confidence

Advertisements that appeared professional and of high production value elicited trust, particularly if the design aligned with brand perceptions

- ✓ Participants tended to have **higher trust** in advertisements that had **visually appealing product presentation**, included **high-quality footage** and **graphics**, alongside a **clear product or service display and messaging**. Higher production quality often indicated a legitimate company investing in the advertisement, therefore making it appear more **credible**.
- ✓ **Professional look and design quality** were particularly important for advertisements that promoted products or services that required them to trust the advertiser with their financial and personal information (e.g., insurance, investment products).
- ✓ Participants also considered the overall aesthetic of the advertisement and whether they **aligned with the brand's image**. They paid attention to style elements, such as whether the **advertisement matched the usual style or colours of the brand**.

"[A beverage advertisement – from video-sharing platform] I recognised [this beverage brand] from its branding, the focus on flavours, and its disruptive tone… The ad seemed trustworthy. It was professionally produced, clearly branded, and highlighted real product features and new flavours." – Male, 18-34, Not experienced fraud, Medium digital confidence

"[A train service advertisement – from social media] I find this ad trustworthy as it is a high-quality video which shows the customer experience of [this train company's] services." – Female, 18-34, Not experienced fraud, Medium digital confidence

"I trust video advertisement (higher quality) the most because it seems like there's been a legitimate company putting legitimate money behind a project." – Male, 18-34, Not experienced fraud, High digital confidence

Poor-quality production, lack of clarity about the product or the service advertised and the **use of AI raised suspicions**

- Advertisements with **poor-quality production** and **amateur style** (e.g., videos that were visibly created using a domestic standard camera) were judged as **less credible**. Seeing such advertisements led participants to doubt the quality and credibility of the brand, product or service, as it was felt they would be easy for anyone to create, including potentially illegitimate companies.
- Similarly, if participants spotted **advertisements clearly using AI-generated visuals or videos (not necessarily deepfake content)**, they perceived them as **untrustworthy**, as they wanted to see real images or videos, to establish trust in what they are purchasing.
- Participants noted that video advertisements featuring individuals they are not familiar with (i.e., not public figures, celebrities or experts) who talk about the product or service **reduced the perceived trustworthiness** of the advertisement, as there was no obvious legitimacy to back up their statements.
- Participants were **suspicious** of advertisements that were **generic, lacked details** or had images/videos that were **unrelated** to the product or service advertised. Such advertisements were felt to be purposefully misleading, in order to capture attention and direct to the advertiser's website.

"[E-commerce platform advertisement – from social media] The ad is not trustworthy, it [wants] you to engage by putting random pictures on it without words so you're likely to click on it." – Female, 18-34, Experienced fraud, Medium digital confidence

"[Nutrition and meal-planning advertisement – from social media] I don't trust this Instagram ad. It looks cheaply made, and weight loss advice from the internet can be dangerous." – Female, 55+, Not experienced fraud, Medium digital confidence

"Usually, if it's a very good quality advertisement with high-quality filming and production would give it a lot more trust than something that's been thrown together quickly and looks unprofessional." – Female, 35-54, Experienced fraud, High digital confidence

Clear and simple language was a strong indicator of trust, with participants being **cautious about advertisements that use emotive phrases or poor grammar**

- ✓ Advertisements with **clear, simple** and **straightforward language** that provided **sufficient details** about the product or service were generally felt to **inspire trust**.
- ✓ When coming across advertisements from well-known companies, participants also paid attention to the **style of messaging**. Slogans, wording or an overall style of communication that was felt to be **authentic** and **consistent** with the brand often created a sense of **familiarity and trust**.

- × Advertisements containing **vague language**, providing **limited information** about the advertiser, product or service, whilst also using **emotive language** to create a sense of urgency (e.g., phrases that indicate that sales end soon or limited products are available), were mostly perceived as **untrustworthy**. Those who had previously experienced fraud mentioned this more frequently.
- × **Poor grammar, spelling mistakes** or punctuation in the account name (e.g. underscores) were judged as **unprofessional**, making participants question the legitimacy of the advertisement.

"I find this ad [theatre advertisement – from social media] trustworthy as it is entertaining and gives good insight into the type of show which is being promoted. The ad is just as humorous as the musical, showing a good knowledge of their audience which gains my trust." – Female, 18-34, Not experienced fraud, Medium digital confidence

"[Debt removal advertisement – from social media] I didn't find it trustworthy. It felt too dramatic and vague, and I don't know or trust the company." – Male, 18-34, Not experienced fraud, Medium digital confidence

"The content needs to be clear and informative for it to be trusted. I don't trust when the content has generic language, vague offers or sometimes poor grammar." – Male, 35-54, Not experienced fraud, Medium digital confidence

Participants were **concerned about advertisements with offers that felt 'too good to be true'**

- ✓ In general, **pricing** or **offers** that seemed **aligned with what was expected from the brand or other similar brands** in the market created a sense of **trust**.
- ✓ Advertisements that contained **detailed information** about the product/service and the company behind it, **without making exaggerated claims or creating a strong sense of urgency,** were perceived as more **trustworthy**.

- × In contrast, participants were **suspicious** of **very low prices**, **large discounts** and **free gifts**, particularly if the advertisement indicated a **sense of urgency**, such as there being limited time to claim the offer or sales ending soon.
- × Participants were also **sceptical** about offers that required **upfront payments, sign-ups**, or **personal/financial information** in exchange for an offer.
- × **Exaggerated claims** or **benefits** of using a product or service (e.g., losing weight in a short amount of time; getting very high returns on investment) were perceived as **untrustworthy.** Participants were particularly concerned about the advertisements that target those who may be **vulnerable** to such messaging, such as those struggling with health issues or those in a financially vulnerable position.

"[Experience days advertisement – from search] The ad seems trustworthy - it is just promoting general services and doesn't seem to be offering any deals that are too good to be true." – Male, 35-54, Not experienced fraud, Medium digital confidence

"[Coffee box gift advertisement – from social media] They hook people on an offer of freebies and urge people to register quickly whilst they are looking. They capture people's data and even ask for people to pay money to get the box posted." – Male, 55+, Experienced fraud, High digital confidence

"Any [advertisement] that offer you something for nothing or suggest you are missing out on something, I approach with scepticism. Adverts that say you need to take immediate action or are aimed at a specific age group are also suspicious." – Female, 55+, Experienced fraud, Low digital confidence

A verified account badge added a layer of trust in the advertisement, although it was not the key factor determining trust

✓ Participants, particularly those who had previously experienced fraud, commonly checked whether an advertisement belonged to a **verified account**, as it indicated that they could trust it being genuine and legitimate.

× Whilst participants **paid attention** to whether the advertiser's account is **verified**, this was **not the key determinant** in how **trustworthy** they perceived the advertisement to be, particularly if they had never heard of the advertiser. As a result, they still looked out for other indicators of trust, such as if the advertiser's name, logo and URLs looked legitimate and if the claim or offer was felt to be credible.

× **Absence of the verification icon** next to a brand that participants **recognised and trusted** made them **more likely to doubt** whether the advertisement was **genuine**.

× A small minority of participants assumed that the 'promoted' or 'sponsored' labels meant that the account or the advertisement had been **verified** by the platform and can therefore be trusted.

"[A messaging service advertisement – from social media] The colour scheme used in the ad is in keeping with the logo. The account is verified on the site and looks how I expect it to. The fonts are similar as well." – Female, 18-34, Experienced fraud, High digital confidence

"[A money management app advertisement – from video-sharing platform] The ad came across as untrustworthy. When dealing with money and financial services, it's crucial that the ad clearly shows the company is verified by both the [video-sharing] platform and by relevant financial authorities. This wasn't evident, which made me cautious." – Male, 35-54, Experienced fraud, High digital confidence

"I don't really click on ads. Or if I do, I go to the verified account on social media and navigate following the links they have provided. I am anxious about being scammed or hacked." – Male, 18-34, Not experienced fraud, High digital confidence

There were concerns about **fraudulent online paid-for advertisements becoming more sophisticated, particularly with the prevalence of AI**, making it more difficult to spot

Most concerning types of fraudulent online paid-for advertisements

AI-generated advertisements that feature trusted public figures or celebrities – participants were concerned that it might be easy to mistake them for real and legitimate advertisements.

Advertisements that require users to enter personal information to redeem an 'offer'.

Advertisements that imitate legitimate brands, making it difficult for individuals to distinguish a real website from a fraudulent one.

Advertisements from industries that were felt to be most prone to fraud, such as finance and health.

Whilst there was **some concern about legitimate advertiser accounts being taken over by criminals**, awareness about such instances was low. A few participants mentioned that they would expect to be able to spot changes from typical company or brand advertising.

Changes in fraudulent online paid-for advertisements over time

Participants felt that **fraudulent online paid-for advertisements have become more widespread** and **sophisticated**, with there being increasingly more ways of scamming people and obtaining customer details.

There was a worry that with the use of **AI** and **advanced technologies**, it would become increasingly **harder** to spot the difference between real and fake advertisements.

"My main concerns are primarily crypto scams that appear to be endorsed by wealthy individuals. What worries me most is how they [are] clearly targeting financially vulnerable people." – Male, 18-34, Experienced fraud, High digital confidence

"[Fraudulent advertising] has changed over time. You knew if a site was dodgy ten years ago, because of the 'You won a new iPhone' signs and bright lights. Now, the scam sites look realistic and mimic the real sites." – Male, 18-34, Not experienced fraud, Medium digital confidence

"In my opinion, the most harmful scams involve financial ads. Any ad promoting financial services or crypto should require approval from an independent regulatory body (at the cost of these platforms). Similar to how ABTA oversees travel companies... AI-generated ads must clearly be labelled as such, with let's say a 5-second disclosure at the beginning of the video." – Male, 18-34, Experienced fraud, High digital confidence

Section 7:
Solution Development

Many participants said they would **generally do nothing when they encounter a suspected fraudulent online paid-for advertisement**

The **majority of participants generally ignore any advertisements**, including those they considered potentially fraudulent, due to the high prevalence of advertisements online.

Only a **minority expressed any intention to report** an advertisement, and several were **unsure how to report advertisements.** This was a general sentiment across platforms **believing it to be overly time-consuming or complicated**.

There was a sense of **personal apathy towards taking action**, feeling it wouldn't make a difference.

A minority who had previously reported (especially those who had experienced fraud), no longer did so as they felt there was **no action taken or acknowledgement from the platform that the report had been noted (this was particularly noted of social media platforms)**.

In a small number of cases, if they were interested in the advertisement, they would research the company to decide if it was legitimate, e.g. looking at its site, going on review sites.

"Fake and fraudulent ads are so common now that I have just accepted them."
– Male, 35-54, Not experienced fraud, Medium digital confidence

"If I come across a fraudulent ad, I tend to ignore it and not take any action. I like to think I'm fairly good at spotting fake ads (and don't click many ads to begin with) and assume most other people would be. Fake and fraudulent ads are so common now that I have just accepted them."
– Male, 35-54, Not experienced fraud, Medium digital confidence

"I actually just scroll past most paid-for ads… I wouldn't know how to actually report a fraudulent ad, though. As a general rule, I just avoid sponsored or paid-for posts and ads."
– Female, 35-54, Not experienced fraud, Medium digital confidence

"In the past, I used to report these issues to social media companies via the report function on the post, but it reached a point where even when feedback was provided on my report, nothing was ever done."
– Male, 18-34, Experienced fraud, High digital confidence

"Mostly, I would just ignore it. If I were interested in the product or service, I would check the web address, and [search] for further information."
– Male, 18-34, Experienced fraud, Medium digital confidence

Participants felt that **platforms and services are currently not doing enough** to tackle fraudulent online paid-for advertisements

The majority **lacked faith** in online platforms and services, as participants felt that they were profit-driven and therefore the safety of their users was not a priority. A minority of participants believed that, by regulating advertisements on the sites of these online platforms and services, it would make them legally liable should a user become a victim of fraudulent online paid-for advertisements.

Participants were not knowledgeable or certain of what measures were in place. They felt that **any measures that were currently deployed were ineffective** due to the high number of perceived fraudulent online paid-for advertisements they encountered.

Verified markers were not considered to be very effective, as some participants mentioned they are available to anyone for a fee. Platforms are inconsistent in their awarding criteria making it hard to judge how easy it was to attain a verified marker and therefore eroding trust.

"I do not think online platform providers are doing enough to keep people safe. If we as consumers, are able to see signs of fraudulent activity, then with teams of people, these sites should be able to easily identify fraud and only approve ads that meet guidelines. It seems they prioritise profits over keeping people safe."
– Female, 18-34, Not experienced fraud, Medium digital confidence

"I have no faith in online platforms providing safety"
– Male, 55+, Experienced fraud, Low digital confidence

"I would expect a better vetting process in order to prevent these ads from being published. I would also expect that each platform to be clear about the correct process for removal of these ads as well as stating their strategies to stop them re-appearing."
– Male, 35-54, Not experienced fraud, Medium digital confidence

"The verified markers used to mean something, but they don't anymore. Especially on [certain social media platform] as you can pay for a verification. This has taken away a lot of trust for me, personally."
– Male, 18-34, Not experienced fraud, High digital confidence

Participants were asked about their perceptions of the following potential ideas to tackle fraudulent online paid-for advertisements

When applying to place an advertisement, the advertiser would have to verify their identity and would be prevented from having their advertisement posted if they failed the verification process

This idea was **welcomed by all**, with broad agreement that it should be implemented.

However, some had concerns about potential loopholes e.g., fraudsters using AI to dupe the verification process.

To strengthen the verification process there were calls that passports, or business registration details should be manually checked in order to provide certainty.

"I think this is a great idea as it prevents any fraudulent adverts from being posted in the first place. However, scammers might be able to fake the verification process through modern technology like AI." – Male, 18-34, Not experienced fraud, High digital confidence

"This should be a minimum requirement [verification]. I think that a business should also have to give its business registration details. I do think that there needs to be a body to check that the platforms are checking the information provided. They seem to hide behind data protection, when the legislation is designed to protect the individual and not fraudulent businesses" – Female, 55+, Experienced fraud, Low digital confidence

Stronger security to prevent advertisers' accounts from being hacked and having fraudsters take over their accounts/advertisement

Although the majority **felt it was a good potential solution**, there were concerns about the effectiveness of the security.

Given that large companies have recently been hacked, a minority feel that fraudsters will find a way to bypass security measures.

"This should be a given, although we know the skills of hackers may circumvent this. Ignoring adverts, many friends have had their email or [social media] accounts hacked." – Male, 65, Experienced fraud, Digital confidence – Medium

Services using their technology to detect and remove fraudulent online paid-for advertisements from their platforms before they are posted and seen by users

Most felt this **should already be the case but agreed it would be a good preventative potential solution**.

Concerns were raised about whether platforms would be able to keep up with the quantity of advertisements. A few are also concerned that it may block legitimate advertisements by mistake e.g., if it is from a smaller new brand.

"I would question what technology is being used, and is it biased or not. Anything automatic or using AI to detect certain things has a bias, and you wouldn't want minority communities to be impacted." – Female, 18-34, Experienced fraud, Medium digital confidence

Participants expressed **a desire for a variety of safeguards**, with **financial penalties** applied to platforms and services to hold them accountable and encourage them to be more proactive

Stricter advertiser verification: Identity and business registration checks.

"[Verification] should be a minimum requirement. I think that a business should also have to give its business registration details. I do think that there needs to be a body to check that the platforms are checking the information provided. They seem to hide behind data protection, when the legislation is designed to protect the individual and not fraudulent businesses"
– Female, 55+, Experienced fraud, Low digital confidence

Clearer labelling and warning systems: Red flags or alerts for suspicious advertisements.

"When dealing with financial services, it's crucial that the ad clearly shows the company is verified by both the platform and by relevant financial authorities."
– Male, 35-54, Experienced fraud, High digital confidence

"I saw ads for a gambling app on my [video-sharing platform's] page with videos of high-profile celebrities, whom I know realistically would not [endorse such products]." – Female, 35-54, Not experienced fraud, Medium digital confidence

Industry-specific checks: Extra scrutiny for finance, health, and medical advertisements.

"The most harmful scams involve financial ads. Any ad promoting financial services or crypto should require approval from an independent regulatory body (at the cost of platforms)."
– Male, 18-34, Experienced fraud, High digital confidence

"I don't trust this [social media] ad... weight loss advice from the internet can be dangerous." – Female, 55+, Not experienced fraud, Medium digital confidence

AI transparency: Labels for AI-generated advertisements; tools to help users spot synthetic content.

"AI-generated ads must clearly be labelled as such, with let's say a 5-second disclosure at the beginning of the video."
– Male, 18-34, Experienced fraud, High digital confidence

"[Fraudulent advertising] has changed over time... Now, the scam sites look realistic and mimic the real sites."
– Male, 18-34, Not experienced fraud, Medium digital confidence

Platform accountability: Financial penalties for allowing fraudulent advertisements; stronger security to prevent account takeovers.

"[Stronger security is] good in theory, yes, but if even bigger companies are getting hacked, then I don't know what tech would be strong enough to protect a small advertiser."
– Female, 35-54, Not experienced fraud, Medium digital confidence

"I feel there should be a regulatory body that could fine the online providers if they allow fraudulent content on their platforms" – Male, 55+, Experienced Fraud, Low digital confidence