Which?

POLICY RESEARCH REPORT OCTOBER 2020

Connecting the world to fraudsters?

Protecting social media users from scams

Executive Summary

Fake ads. Fake products. Fake celebrity endorsements. Lottery scams. Job scams. Investment scams. A staggering variety of scams can be found on social media. They can lead to the loss of personal data and severe financial loss, but they also cause substantial emotional harm. Victims can be left embarrassed, upset and angry, and can experience stress, worry, loneliness and depression as a result of becoming a victim.

Given the severity of these harms, it is essential that social media users are appropriately protected, but the best way to do this is yet to be determined. Recent measures have tended to place more responsibility on users to protect themselves from criminals. For example, information to make users more aware of scams and Facebook's introduction of a scam reporting tool. However, user behaviour and attitudes towards scams on social media are not well understood and so it's not clear that people are sufficiently capable of protecting themselves.

To better understand the best way to protect social media users from being scammed, Which? undertook a two-stage, mixed-method research project. First, we conducted qualitative research using **a 10-day online community of 50 Facebook users** to explore in detail what they thought about scams on social media and their understanding and expectations of what Facebook does to protect them from scams. We also examined whether concerns varied across certain types of scam content and what actions people took in response to seeing scam content.

Next, we conducted **a short, 15-question online survey with a larger sample (c. 1,700) of Facebook users**. This was a nationally representative survey that we reweighted to be representative of Facebook users. The purpose of the survey was to see how prevalent certain attitudes and behaviours are among Facebook users, and to establish whether certain groups within the general population are more susceptible to social media scams than others. The research was conducted with a focus on Facebook due to its size and market power, which enabled us to achieve appropriate numbers of research participants. However, we believe that the findings and implications of this research could reasonably be extended to apply similarly to other social networking platforms.

Research findings

Our survey found that **65% of Facebook users were fairly or greatly concerned about scams**. Among these people, **the most popular main reason for the concern was a lack of confidence in Facebook's systems and processes** (28% of those who are concerned said this), while 23% said their concern was mainly because scams can be very hard to identify. Around one in eight said their main concern was for other people who might not know about scams (13%). This altruistic concern also came across strongly in our qualitative research where people often thought that scams are something which happen to other people, or that they represent a greater risk to less seasoned social media users, for example older people who may be less familiar with the online environment. The third of Facebook users who are not concerned about scams tend to believe that they have the knowledge and ability to keep themselves safe. We also found in the qualitative research, that while people are concerned about scams, content that could enable a scam is not

viewed as immediately harmful. This is a consequence of the platform primarily being seen as a social space, but it suggests that the risk of being scammed is not top of mind when using the platform.

We also found that **people have only partial awareness of the breadth, range and sophistication of types of scams that can be found on social media**. For example, we asked participants in our qualitative research to identify types of scams and found that none of the participants were aware of all of them. Awareness tended to be lowest for the types of scams that are likely to lead to the theft of personal data, but substantial numbers of participants failed to identify even some of the more obvious scam types. About a third of participants did not know that fake products might be advertised, while a quarter did not recognise an investment scam using a fake celebrity endorsement.

Alongside this limited awareness, **people often exhibit overconfidence in their ability to recognise scam content**. We asked participants in our online community to self-assess their ability to identify a scam and then we tested them with a scam-spotting exercise. We found participants with varying levels of self-assessed confidence (high, medium and low) misidentified scam content as legitimate in similar numbers and at similar rates. This is concerning as overconfidence in one's judgment has been linked to increased susceptibility to scams.

So that we could examine whether susceptibility to being scammed might vary across demographic groups, we used the quantitative survey to investigate which types of Facebook users are most likely to have characteristics that make them more persuadable, and to explore whether these users are more or less likely to engage in riskier behaviours on Facebook.

We found that younger Facebook users identified as both more persuadable and more likely to engage in riskier behaviours. This implies that, despite older people stating they are more concerned about the risk of scams, **younger social media users may be more susceptible to falling victim**.

Our research specifically explored knowledge and use of Facebook's scam ad reporting tool and our findings question its effectiveness. We found that awareness of the tool was low among respondents to our survey - **with just 30% saying that they were aware of the scam reporting tool. Only a third of these (10% of the total sample) said they had used the tool themselves**. Users also lacked motivation to use the tool for reasons including doubts about the usefulness of reporting suspicious content due to a lack of confidence that reports would be acted upon and concerns about the consequences of reporting a scam, such as being identified or getting involved in a subsequent confrontation.

Participants in the qualitative research expected Facebook to have systems and processes in place to protect them from scams and criminals, but specific knowledge of what these systems are and how effectively they worked was extremely limited. In some cases there was a misalignment between users' high expectations and the processes that actually exist, and this could lead to users doing less than they might to protect themselves from scams. **As people gained knowledge of the systems and processes Facebook have in place, many became sceptical of their effectiveness** particularly in relation to stopping scam content appearing on the platform.

Recommendations to social media platforms

Which? believes that social media platforms are best placed to tackle scams and the research suggests a number of recommendations to reduce the risk of social media users falling victim to scams. Since the recommendations follow from our research, these are mostly made to Facebook, but we think they could apply more broadly to other social media platforms.

First, the findings have implications for what social media platforms should do to raise awareness of scams among social media users. It is clear from the research that there is much scope to increase awareness, but the limited relationship between confidence and scam-spotting ability indicated by this research suggests that if heightened awareness leads to overconfidence then it may not be helpful. Given this, we think it is important to challenge peoples' perceptions about the risk from scams and we recommend that **Facebook should do more to raise user awareness of the wide and varied range of scams and understanding of the harm from scams.**

We also recommend that **Facebook takes actions to raise user awareness of the scam reporting tool.** To build confidence in the efficacy of the tool we recommend **that Facebook considers how it can report back on what happened next to users of the tool.** However, while these are important actions to support users, the research has demonstrated that it is unreasonable and implausible to expect users to be able to protect themselves from sophisticated scams and so Facebook needs to take greater responsibility to protect its community. In particular, **Facebook must have effective systems and processes** to tackle illegal and fraudulent content and reduce consumers' exposure to it. Which? would like to see Facebook introduce both proactive and reactive measures to deal with illegal content as part of these effective systems and processes.

- **Monitoring, blocking and removal**
  Facebook must work to improve the effectiveness of existing systems for identification, removal and prevention of harmful content through effective automated monitoring systems, clear site conduct policies, and blocking bad actors from accessing and re-accessing their sites. Where harmful content slips through despite these proactive measures, Facebook must remove the content as quickly as possible, ideally within a defined timeframe.

- **Targeted alerts and warnings**
  Facebook, with the amount of information it holds about its users and what they engage with, is in a unique position to be able to help notify its users if they have engaged with harmful or fraudulent content. We recommend that **when fraudulent content is identified on the site, Facebook should use the information it already holds to alert the users who have engaged with the content** (for example, those who have clicked on an ad that is later found to be a scam or have shared content that links to phishing domains or malware).

- **Advertiser verification**
  Facebook should have systems and processes in place to prevent fraudulent ads from being listed on its platform. Facebook has Advertising Policies setting out what is and is not allowed and operates a review process against these, but it is clear that many fraudulent ads still make it through these checks. **There should be a requirement for Facebook to verify the identity of its advertisers**. This would prevent many scammers being able to operate anonymously via social media platforms. We acknowledge that the steps required to verify all advertisers may be onerous for Facebook, but we believe this is a process that could be rolled out incrementally over a period as long as, in the interim, **Facebook is clear which ads have and have not been verified**. This should be displayed clearly on each ad so consumers can judge for themselves the risks involved with engaging with that ad.

Recommendations to government

The detriment to social media users caused by harmful content, including scams and fraud, has been well known for some time, but platforms have not made sufficient changes to their systems to tackle these harms. While most platforms can show that they have taken steps towards blocking bad actors and taking down suspicious content or introducing reporting tools, these have been piecemeal and we do not think these changes have been sufficiently effective.

Given the limited measures introduced voluntarily by platforms to date, we believe it is unlikely that platforms will take sufficient steps without bringing in a strong regulatory framework that requires it. Unless online platforms are required to tackle this problem, the incidence of scams will continue to grow and cause financial and emotional harm for social media users. For this reason, and to make sure the responsibilities of platforms are brought more in line with the expectations of consumers for social media platforms, we have recommendations to the government:

- **Social media platforms should be given a legal responsibility for preventing scam content from appearing on their sites**, as well as more responsibility for taking quick action to remove harmful content when it is reported. **Legislation should set out the requirement for the proactive and reactive measures** discussed above and require platforms to demonstrate how they are implementing measures to protect their users.
- In addition to a requirement for effective systems and processes (including both proactive and reactive measures), **platforms should also be made legally responsible for the design of their systems to prevent illegal activities, including scams and fraud**. This could include efforts to be transparent about the potential risks users may face on social media and that not all content has been moderated; for example, clear labelling of verified and unverified ads.
- To support the actions of other agencies in tackling scams, **a legal requirement for transparency about illegal activity on their sites and to report to relevant regulators and law enforcement bodies should also be applied to platforms**. This should require platforms to have processes in place for reporting illegal activity to appropriate bodies, while the transparency requirements should call for reporting on the number of complaints, response times and resolutions, the amount of content removed, and the number of bad actor accounts disabled.

1. Introduction

There is growing concern about the number of scams that are perpetrated using social media and the substantial harm that this causes to victims. UK Finance notes that scammers are increasingly using social media to reach and entice victims[1] and Action Fraud states the use of social media is increasing in all aspects of fraud,[2] while a high profile legal dispute between Martin Lewis and Facebook drew attention to one of the ways in which criminals attempt to defraud social media users.

The types of scams perpetrated on social media are varied. These include traditional fraud offences, such as investment scams, in which criminals use social media to increase the reach of their scam and target new potential victims. This is an example of 'cyber-enabled' fraud and Action Fraud estimates that 85% of the 822,276 fraud reports it received in the year to June 2020 were cyber-enabled.[3] Other types of scams on social media are more novel, such as hacking and spreading viruses or malware, and these are 'cyber-dependent' crimes as they can only be committed using a computer, computer networks or other forms of information communications technology (ICT).

The harm from these scams could be financial loss, the loss of personal data (which might lead to future harm) or emotional harm. The emotional harm may be particularly large. Common responses to being scammed include embarrassment, distress and anger, but victims can also experience stress, worry, loneliness and depression.[4] The experience of becoming a victim of fraud can also lead to a loss of trust in others[5] and loss of self-esteem,[6] and there is evidence across a range of fraud types that the emotional impact can be more severe than the financial impact.[7] People can also experience physical illness and harmful health consequences, such as insomnia, nausea and/or weight loss after falling victim to fraud.[8]

Efforts have been made to try to reduce the incidence of social media scams. Most notably, as part of its settlement with Martin Lewis, Facebook launched a scam advertising reporting tool and a dedicated team to handle these complaints, and it donated £3 million to Citizens Advice to deliver a new UK Scams Action project. However, these measures tend to place more responsibility on users to protect themselves from criminals.

However, user behaviour and attitudes towards scams on social media are not well understood and so it's not clear that users are sufficiently capable of protecting themselves. The likelihood of being scammed will vary across social media users and it may be that this likelihood is affected by the social media environment itself. It is also not known how likely people will be to suspect content or to report this. The answers to such questions are critical to understanding the best way to protect social media users from being scammed.

This research project seeks to shed light on these issues. Using a mixture of qualitative and quantitative research methods we examine, among other things, consumers' awareness of the risks, whether or not they can protect themselves, their expectations of protections that social media companies provide and how this compares to the protections that actually exist.

The report is structured as follows. The next chapter sets out the context for the research by identifying the types of scams that can be found on social media and knowledge about the susceptibility of individuals to being scammed from previous research that was focused on non-social media settings. Chapter 3 sets out our research methodology. This involved both qualitative and quantitative research, but in both cases focused on Facebook users. As the largest social media platform in the UK, the proportional impact of interventions on this platform will be substantially greater than on other social media platforms. However, our focus also reflects a pragmatic research decision in that we were more able to engage research participants that broadly reflect this platforms' users. Although the research is focused on Facebook, we expect that the findings might similarly apply to other social media platforms.

Chapters 4 to 7 present our research findings. Chapter 4 focuses on how users experience the social environment and their concerns about scams, while chapter 5 explores issues of awareness, confidence in spotting scams and overall susceptibility to being scammed. Chapter 6 investigates people's knowledge and use of Facebook's systems for protecting them from scams, and in particular explores usage of the scam ad reporting tool. Chapter 7 considers what users would like to happen to improve the current situation.

The final chapter draws together these research findings and their implications. On the basis of these, we set out Which?'s recommendations for improving social media to better protect users from scams.

2. Scams on social media

Scams have long been the cause of significant harm to consumers, but social media has enabled criminals to develop new types of scams and to increase the reach of existing methods.

2.1 Types of social media scams

Many scams that take place over social media can be grouped into UK Finance's fraud categories of:

- 'malicious payee' – in which the victim makes a payment to someone they believe is legitimate but who later turns out to be a criminal, and
- 'malicious redirection' – in which the victim believes they are making a payment to a known and legitimate payee but are instead tricked into paying a criminal.

However, other types of scams may not lead directly to financial loss and are not covered by these terms. These include scams that seek to install malware on victims' devices and phishing scams that harvest victims' personal data that can later be used to carry out more convincing scams or sold onwards to other criminals. Table 1 provides examples of these different types of scams and sets out the different types of harm that are commonly associated with each of these.

Table 1: Scams and fraud on social media

Types of scams on social media	Examples	The harm
Malicious payee – investment scams; purchase scams; advance fee scams	Fake adverts and celebrity endorsements	• Significant financial loss (esp. investment scams) • Time, significant emotional toll
	Fake products	• Financial loss but often less severe • Hassle, time, stress
	Loan scams, lottery scams, job scams	• Loss of personal information and sometimes monetary loss • Stress, particularly in relation to loans and jobs
Malicious redirection - impersonation	Requests from hacked accounts of friends to send money	• Financial loss • Emotional harm from both the financial loss and emotions associated with being tricked, such as shame or anger. Worries that a scammer had access to personal communications
Phishing	Shopping vouchers; job scams; 'friend' requests; phoney quizzes.	• Loss of personal data • Increased risk of being scammed later • Likely to be minimal emotional harm at the time as the victim may not be aware they've been scammed
Malware scams	Free shopping vouchers; fake ads; sensational news; "See who's blocked you" tools	• Loss of personal data/privacy or loss of access to own devices • Increased risk of being scammed later • Hassle/stress

2.2 Susceptibility to scams

Who is more or less likely to be a victim of a scam is subject to debate, given the profile of scam victims is obscured as a result of underreporting. However, it is known that behavioural and

psychological characteristics can increase people's likelihood of falling victim to scams, including the extent to which people are open to persuasion and the influence of others.[9] Scams and fraud involving psychological persuasion usually involve one or more of the 'six principles of persuasion' outlined by Cialdini.[10] These techniques are:

1. **Reciprocity** – The psychological need to 'repay' a perceived favour to the individual who is believed to have behaved selflessly, generously or in some other way altruistically.
2. **Consistency** – The need to behave in such a way that one's current behaviour can be perceived as consistent with one's past behaviour.
3. **Social proof and norms** – The tendency to believe something or behave in a specific way if other people seem to believe the same thing or behave in a similar manner.
4. **Liking** – The tendency to trust those individuals who are perceived likable and similar to oneself.
5. **Authority** – The tendency to trust and comply to the requests of those who are perceived to be in a position of authority.
6. **Scarcity** – The tendency to believe that scarce goods, services and opportunities are better than those that are not scarce.

Additional psychological methods used by scammers identified in literature include:

7. **Small 'investment', enormous 'possibility'** – Psychological research indicates that people often place too much weight on low probability events when making decisions.[11, 12] Scammers can take advantage of this by promising huge pay-offs for small 'investments'.
8. **Visceral influences** – Fraudsters will try to trigger emotions in victims that are related to basic human needs and desires, such as appeals to greed, fear, avoidance of physical pain, or the desire to be liked.[13] This can activate automatic and intuitive thinking and suppress rationality in the victim, which may enable the fraudster to manipulate the victim's behaviour more easily.[14]

These persuasive techniques used by scammers mean that people with certain behavioural attributes are likely to be at greater risk of falling victim to scams that involve some aspect of psychological persuasion. For example, several factors have been found to influence 'scam compliance', or the actions taken by victims that enable the scam to succeed. These include susceptibility to social influence, compliance with authority, the need for consistency and lack of self-control.[15] Overconfidence in one's judgments has also been linked to increased susceptibility to scams.[16] Previous research conducted by Which? found no correlation between confidence and ability in spotting scams and a substantial overconfidence bias in people's assessments about the accuracy of their judgments.[17]

Those most at risk of scams through their behavioural characteristics are not necessarily those typically thought of as being vulnerable to scams, such as older people. In fact, some literature finds that older people are no more likely to fall victim to fraud compared to the rest of the population.[18, 19] This appears to be supported by Action Fraud and the National Fraud Intelligence Bureau data in which the highest volume of fraud reports come from people aged 20–39, although those aged 50–69 are more at risk of losing larger sums.[20, 21]

Overall, while there is a large body of research that examines behavioural and psychological factors determining an individual's susceptibility to be scammed, little of this has focused on social media. It seems likely that many of the findings above will also hold in the context of social media; for example, users may be overconfident in their ability to spot scams on social media. However, we do not know how the diversity of scam types influences awareness of scams or how behaviour might be influenced by the social nature of the environment, and these questions are explored in this research.

3. Research methodology

To develop a deep understanding of the behaviours and attitudes of users towards social media scams, we adopted a two-stage, mixed-method approach. In the first phase, we created an online community of 50 Facebook users and worked with them over 10 days using deliberative but asynchronous research methods. We explored in detail what they thought about scams on social media and their understanding and expectations of what Facebook does to protect them from criminals. We also examined whether concerns varied across certain types of scam content and what actions people took in response to seeing scam content.

Facebook users were chosen due to Facebook's enduring dominance of the social media landscape (almost nine in ten (88%) social media users have a Facebook profile and over half (56%) consider it to be their main social media site/app) and our ability to engage research participants that broadly reflect this platforms' users.[22] While the research was conducted specifically using Facebook, we believe that the consumer attitudes and sentiment found in this research will apply to other social media platforms.

The moderating team split the participants between themselves so that they could more easily track their journey throughout the 10 days. The electronic records from the online community platform, hosted by Recollective, acted as virtual transcripts which were reviewed and used as a basis to populate an analytical coding framework.

Following this, we used what we had learnt from the online community to design a short, 15-question online survey to see how prevalent certain attitudes and behaviours are among a larger sample of Facebook users, and to establish whether certain groups within the general population are more susceptible to social media scams than others.

Figure 3.1: Overview of research approach

Phase 1: Qualitative online community taking a deliberative approach	Phase 2: Quantitative online survey
• 10-day long online community incorporating deliberative research principles • 50 participants recruited to quotas broadly reflective of Facebook's users • Additional quotas for type of online behaviour engaged in and confidence in spotting scams	• 2,000 nationally representative UK sample • 15 questions • Data weighted to be representative of Facebook users

3.1 Phase 1: Online community

3.1.1 Method

We embedded deliberative research principles into the design of the 10-day online community and used immersive activities to try to understand social media users' awareness of and ability to identify scam content, and to observe responses to scam content. The content and structure of the online community is outlined below:

- **Days 1–3: Consumption of content and exposure to scams:** The first three days of the online community focused on understanding how participants use Facebook, their views on different types of content and their awareness, perceptions and knowledge of scams. We took a staged approach to understanding participants' concerns around different types of content by first asking unprompted questions about a wide range of content and how safe or unsafe they feel on Facebook before raising the issue of scams in particular.
- **Days 3–7: Views on Facebook's systems and processes:** Half way through the third day of the online community and across days four to six we explored participants' expectations for and reactions to the systems and processes Facebook has in place to mitigate the risks posed by scams to its users.[23]
- **Days 8-10: How to treat social media users and mitigate risks:** The final days of the community focused on how people scammed on Facebook could be supported and how social media users could be better protected. We developed scam scenarios to understand how participants feel victims of scams should be treated and tested potential new interventions developed by Which? with users.

A complete set of the research materials can be found in the report annex.

3.1.2 Sample

We recruited study participants to provide a balanced cross section of users by demographic, behavioural and attitudinal characteristics, and to be inclusive in our approach. All research participants were members of the general public who use Facebook at least once a month. A full breakdown of the sample by these characteristics is provided in the report annex.

Additional quotas were set to ensure:

- A spread of the extent to which users engage in different activities on Facebook to act as a possible proxy for exposure to risky content.
- A spread of self-perceived confidence in spotting scams online.

The quota related to confidence was included as wider research suggests confidence (or rather overconfidence) is related to scam susceptibility.

All demographic and usage quotas were informed by profile data from a general public survey, although some of these quotas were relaxed to meet fieldwork timings. Minimum quotas were set for users who engage in types of activities which may increase risk of exposure to certain types of scams (completing quizzes, buying products through ads seen on Facebook, buying and/or selling products through Facebook marketplace). Similarly, we recruited a spread of participants with high, medium and low self-assessed confidence in their abilities to identify scams online.

3.2 Phase 2: Representative survey

3.2.1 Method

Following the completion of Phase 1, Which? designed a short online survey to understand the prevalence of certain views, attitudes and behaviours amongst Facebook users. We incorporated the scale of susceptibility to persuasion developed by Modic (2012).[24] A copy of the survey can be found in the annex accompanying this report.

3.2.2 Sample

Which? surveyed 2,080 UK adults, of whom 1,691 were Facebook users, between 10 and 12 July 2020. The fieldwork was carried out online by Populus who weighted the data to be representative of the UK population (aged 18+). Analysis of the survey data used in this report was conducted by

Which?. This entailed re-weighting that data to be representative of Facebook users based on a profile of Facebook users that was developed from a previous survey (see the annex accompanying this report).

4. Participants' use of Facebook and views of content

Key insights

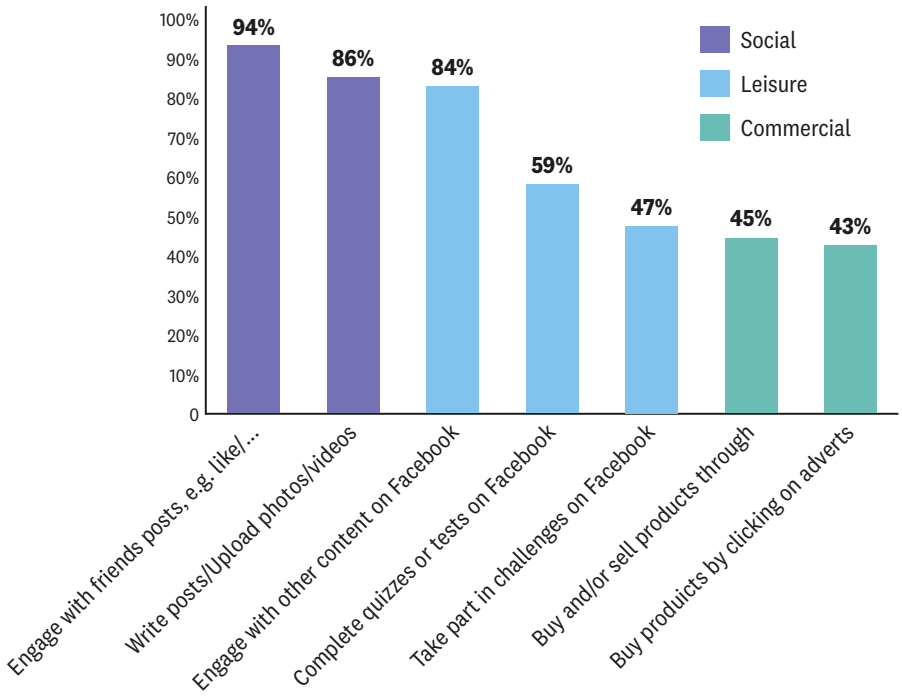
- Content that could enable a scam is not viewed as immediately harmful and is certainly not top of mind as risky. This is a consequence of the platform primarily being seen and used as a social space.
- Two-thirds of users are concerned about scams on Facebook, but these concerns result from low confidence in Facebook's systems and processes to protect users or altruistic concerns for other users perceived as more vulnerable. Relatively few users are concerned that they are unable to keep themselves safe.
- By contrast, those who are not concerned about scams tend to believe that they have the knowledge and ability to keep themselves safe.
- There are a variety of views as to whether social media platforms such as Facebook can be trusted to protect users from harmful content voluntarily. Some of the lack of trust comes from the resigned acceptance that social media platforms provide a free service to users by selling space to organisations that could result in publishing harmful content.

In this chapter we examine how Facebook users experience Facebook's online environment. This is important context as it indicates to what extent consumers are conscious and concerned about the risk of being scammed, and this will frame users' behaviour on the platform. Throughout the chapter, we draw on insight from the early stages of the qualitative, online community research that was conducted before participants had been presented with information regarding online scams or the systems and processes Facebook uses to deal with scams. We also refer to findings from our online survey of Facebook users.

4.1 User attitudes to Facebook as an online environment

Facebook users were broadly positive about their experiences using the platform. They see it as a largely social space and this is reflected in their behaviours (see Figure 4.1) and the types of content they like (and dislike) encountering. While a fairly high proportion of users engage in commercial activities such as clicking on ads (43%) or buying or selling products (45%) while on the platform, this is far less common than using it for social and networking activities or engaging in other leisure activities such as consuming news stories or videos, completing quizzes or taking part in challenges.

Figure 4.1: Facebook users behaviour on Facebook.



Base: All Facebook users: Effective sample sizes 1,375–1,378

The fact that Facebook is overwhelmingly seen and used as a social space and the social nature of Facebook appears to frame the way users view content on the platform. This is demonstrated by the responses given by participants to questions about what they dislike or find concerning on social media. The aspects of social media which they disliked sometimes focused on specific content (for instance, politically extremist content), behaviours of other users (oversharing, rows, trolling) or were related to more generic aspects of social media and its funding model. Participants' expressed dislike for content they considered 'irrelevant' (e.g. badly targeted ads), or which triggered concerns over their data privacy and online security (e.g. seeing ads that were very tailored and specific).

Unless the users had previously been a victim of a scam, then scams and criminals were rarely spontaneously mentioned during more general discussions of disliked content or disadvantages to being on Facebook, which indicates that the risk of fraudulent content and scams are not a top-of-mind concern. However, many participants stated that they disliked activities, practices and behaviours that are potentially scam-enabling. For instance, a handful of participants described encountering fake ads or seeing fake accounts.

Concerns around data privacy, data sharing outside of Facebook and data security tended to be generalised and not specifically connected to scam-enabling content. More broadly, users do not often connect the sharing of personal data in a quiz or challenge with the possibility of potential misuse of personal data by a criminal.

Regularly encountering content they dislike has been normalised, becoming viewed as part and parcel of using social media. As such, users often meet it with resigned acceptance and there is some evidence to suggest that exposure to suspect content builds a sense of complacency. When shown an image of a scam sponsored post or quiz in our survey, a sizeable proportion indicated they would simply keep scrolling past that content and few would engage critically with it.

This could have implications both for individuals' own susceptibility to being scammed and their likelihood of taking action to report suspicious content, which would protect others. We explore this latter point in Chapter 6.

4.2 Concerns about scams

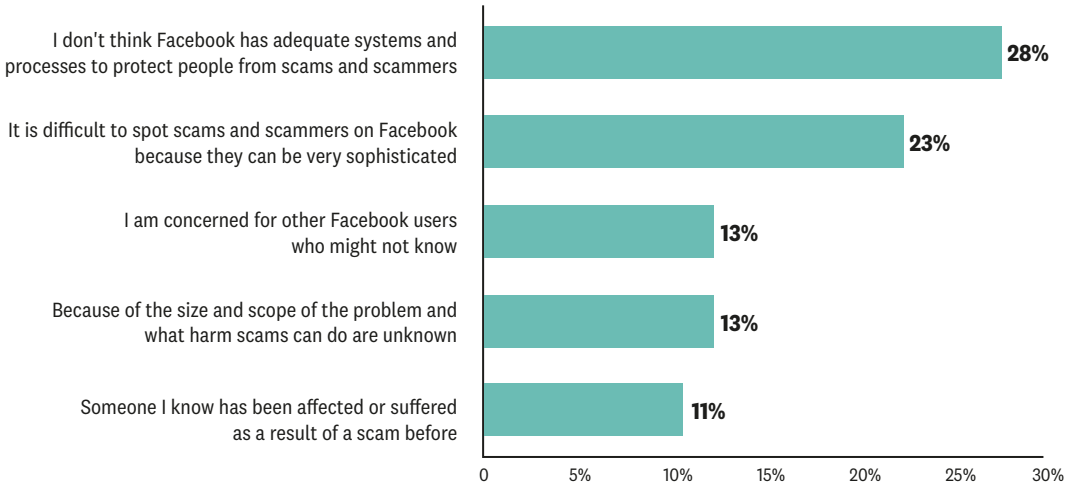
When Facebook users in our online survey were asked directly about whether they are concerned about exposure to scams, almost two-thirds (65%) said that they had a great deal or a fair amount of concern. This was greatest amongst older respondents to our survey (70% and 68% of 55–64 year olds and 65+ respectively) and lowest amongst the youngest respondents to our survey (53%), but over half of all age groups expressed some concern, with this concern increasing with age (53% ~ 70%).

Exploring what lies beneath this headline statistic on level of concern, we find a more nuanced story about what users are concerned about and who their concerns are focused on. Although the main concern of some people is that scams can be very hard to identify, and 23% of survey respondents said this, people were more commonly concerned because of a lack of confidence in Facebook's systems and processes (28%), which we explore further below. Around one in eight said their main concern was for other people who might not know about scams (13%), and our qualitative research found that those that are more mindful of the full range of risks associated with scams tended to think they are something that happens to other people, or that they represent a greater risk to less seasoned social media users, for example older people who may be less familiar with the online environment.

> *"Personally, I have little concern due to the diligence I practice. But I am very concerned that others, such as my mother, would fall victim to these sorts of scam"*

Overall, this indicates that concerns about one's own ability to protect oneself from scams did not feature strongly. Those that did express such concerns were likely to have already been a victim of a scam or to know someone who had been and these people were more likely to recognise the potential that scams could happen to anyone.

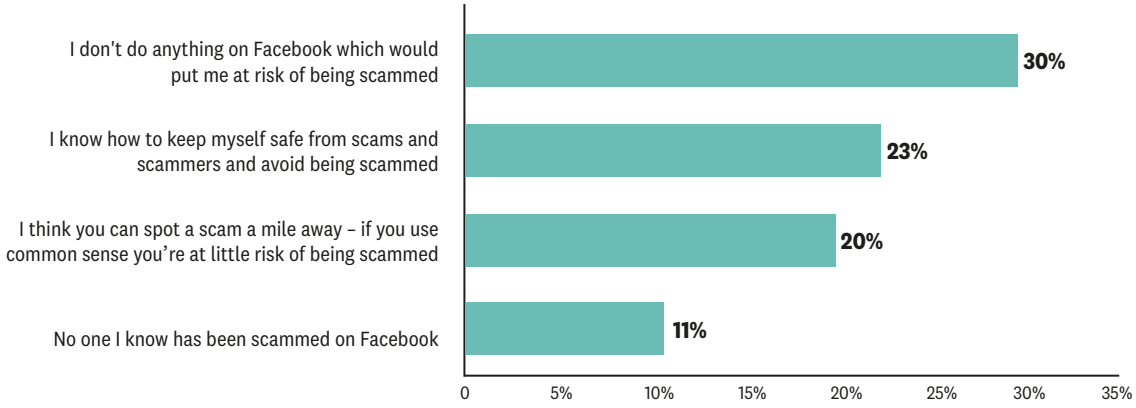
Figure 4.2: Main reasons Facebook users are concerned about being exposed to scams on Facebook.



Base: All Facebook users who are concerned about being exposed to scams/fraud on Facebook: Effective sample size 876

By contrast, those users who said that they are not concerned about scams were inclined to believe that their behaviours or abilities did not make them vulnerable. 30% said they did not engage in risky behaviours, while almost a quarter (23%) said they knew how to keep themselves safe and a fifth (20%) thought that you can "spot a scam a mile away" and could use your common sense to stay safe. We explore in the next chapter whether individuals are likely to have the skills necessary to keep themselves safe from scams and criminals.

Figure 4.3: Main reasons Facebook users are not concerned about being exposed to scams on Facebook.



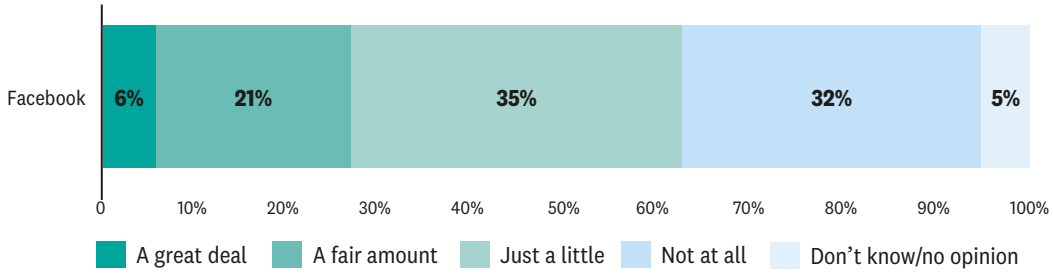
Base: All Facebook users who are not concerned about being exposed to scams/fraud on Facebook: Effective sample size 463

4.3 Attitudes to Facebook as a company

As indicated above, attitudes to Facebook also framed concerns about scams. These related to general perceptions of trust, Facebook as a commercial entity, and beliefs about the efficacy of Facebook's systems to tackle the issue.

Some participants held concerns over whether social media platforms can be trusted to do more to keep people safe in the absence of clear guidelines set and monitored by an effective regulator. The survey research found that among the general public trust that Facebook would protect users from exposure to online harms was low. We found opinion to be divided with 28% trusting Facebook 'a great deal' or 'a fair amount' to protect them from exposure to online harms, and 32% not trusting Facebook to do this at all (see Figure 4.4).

Figure 4.4: Trust in Facebook to protect users from exposure to online harms.



Base: All respondents: General Population: Sample Size 2080

Facebook users commonly understood, if only at a relatively superficial level, that it is a commercial business and that its business model relies on using personal data to sell advertising. Participants' understanding that Facebook is a commercial organisation informed how much they thought Facebook would do to keep users safe, although this led to conflicting assumptions among participants. Some had a feeling of being commoditised because of how social media platforms use their personal data and this made them cynical about Facebook's ultimate motives – believing it would prioritise delivering value to their shareholders rather than users. Others assumed that Facebook has a commercial imperative to keep users safe from harm and felt reassured by this. The following two verbatim quotes illustrate these contrasting views.

> *"I think Facebook sees it's user/customers as a commodity, as the amount of data that is available is a great resource for commercial purposes. Data shared by facebook would be of great use for organisation for targeted marketing."*

> *"I think Facebook needs its customers and users, I think it is aware that if people stopped using the platform, they would cease to exist in the same way. I think as far as such a massive company can, it does try to do the right thing when it comes to users but the scale of social media makes this hard and causes mistakes – especially when it comes to the protection of people's data and selling this on."*

Finally, there were some concerns expressed over Facebook's infrastructure and security measures. Approximately half (54%) of Facebook users were concerned about their or their friends' Facebook account being hacked or taken over, suggesting doubts are fairly widespread. Participants in our online community recognised that Facebook faces a significant challenge from cyber criminals, and some participants felt Facebook's size and scale mean it would be difficult to monitor content across markets and channels. These participants did not feel that Facebook should be absolved of responsibility simply because acting on issues may be difficult or expensive, but moderated their expectations of Facebook and what they believed was feasible for Facebook to achieve in stopping harmful content. In recognising the challenges Facebook faced, they expected that Facebook would make some genuine mistakes, for instance in relation to the prevention of scam content appearing on their site.

Overall, these attitudes to Facebook reflect that users have varying expectations of how much Facebook will do to protect them. Some believe Facebook will take action to protect users, either through benevolence or a commercial imperative, but many others are sceptical that Facebook can or will effectively protect them.

4.4 Summary

Facebook users visit the site expecting to connect with friends and family, and to see and consume enjoyable content. They are not primed to think about scams or other risks and the salience of the threat of scams might be reduced by seeing the platform as a social space. However, when asked explicitly about scams, two-thirds of Facebook users said they are concerned. This concern stems from a variety of factors, but fears were often driven by low confidence in Facebook's systems and process or concern for other users, and not so commonly by the difficulty in identifying scam content. Those who are not concerned tended to be confident they could protect themselves.

Despite seeing strong social and hedonic benefits to being on Facebook, users' views on Facebook as a company were complicated and sometimes conflicted. While participants hoped Facebook would act in users' interests and believed there are commercial pressures to incentivise this,

some did not trust that Facebook would always act responsibly or that Facebook would have effective systems and processes in place to keep them safe from online harms.

Ultimately, participants' general behaviours and views on Facebook hold a number of implications for their expectations in relation to scams. While these will be explored in greater detail in subsequent chapters, they suggest that even prior to being presented with information about scams, Facebook's systems and processes and the potential risks users face, participants support Facebook intervening to support users' safety.

5. Awareness, overconfidence and susceptibility to scams

Key insights

- People have only partial awareness of the breadth, range and sophistication of types of scams that can be found on social media.
- Alongside this limited awareness, people often exhibit overconfidence in their ability to recognise scam content.
- Younger people are more predisposed to being a victim of a scam: they are more persuadable and more likely to engage in riskier behaviours.

Having established in the previous chapter that Facebook users have fairly low levels of concern that they will personally be scammed, we now explore to what extent this is reasonable by examining the awareness and ability of users to identify scams. We do this by first establishing users' subjective beliefs about their own level of awareness of scams and ability to spot these, and then testing this with various activities. Following this we examine how susceptibility to scams might vary across demographic groups.

5.1 Awareness of scams

Participants in our online community typically believed they had a good awareness of scams. Most participants (41 out of 48) claimed that they were aware "a great deal" or "a fair amount" that they could be exposed to scams on Facebook. However, we found substantial evidence that awareness was in fact more limited. For example, participants' descriptions of scams suggest that their awareness is superficial and one-dimensional, and indicated that the participants have a somewhat narrow notion of scams and may not be aware of the associated risks:

- Most participants' descriptions of scams focused exclusively on losing money (for instance, buying a product that never arrives or buying a fake good). Data loss was less commonly mentioned.
- Participants also typically only focused on one type of loss, mentioning either losing money or data but not both.
- Those who provided examples of scams as a part of their definition typically only provided a single example or examples from a single category of scams.
- Most participants that reported seeing suspicious content rarely described it as being a "scam" despite the content arguably having the features of a scam (e.g. an element of deception, a price for a branded product that is too good to be true).

To further examine participants' awareness, we asked participants to undertake an immersive activity that used examples of scams which have appeared on Facebook before exploring awareness of two types of content that can enable scams: quizzes and ads/sponsored content.

First, we presented participants with a "scams bingo card" and asked them to indicate whether they were familiar with each of the scams. None of the participants were aware of all of the scams. Awareness tended to be lowest for the types of scams that are likely to lead to the theft of personal data, but substantial numbers of participants failed to identify even some of the more obvious

scam types, see Figure 5.1 where "thumbs down" markers represent a participant that claimed not to be aware of that particular type of scam. About a third of participants did not know that fake products might be advertised, while a quarter did not recognise an investment scam using a fake celebrity endorsement.

Figure 5.1: Scams Bingo: which scams are you aware of?

Second, we presented users with examples of two types of potentially scam-enabling content, interactive quizzes/challenges and sponsored content/ads, and elicited their thoughts about these. Online community participants typically described them as innocuous. While some felt they were distracting, irrelevant or uninteresting, awareness that they could be a means of stealing data or lead to scams was limited.

Low awareness of the risks associated with certain types of content is worrisome given the frequency with which participants are exposed to content that may be inauthentic. The lack of implicit association of scams with data loss is especially troublesome given the potential risk of data loss on social media is vast. In our online survey we found that most Facebook users always or sometimes see quizzes (67%) and sponsored content (75%), but less than a third of respondents

(29%) ignore this content because they find it suspicious. We found that when shown an image of a specific scam quiz (about Disney princesses) more than one in ten (12%) said they would click on the link, while 9% said they would click the link on an image of a sponsored post for an investment scam.

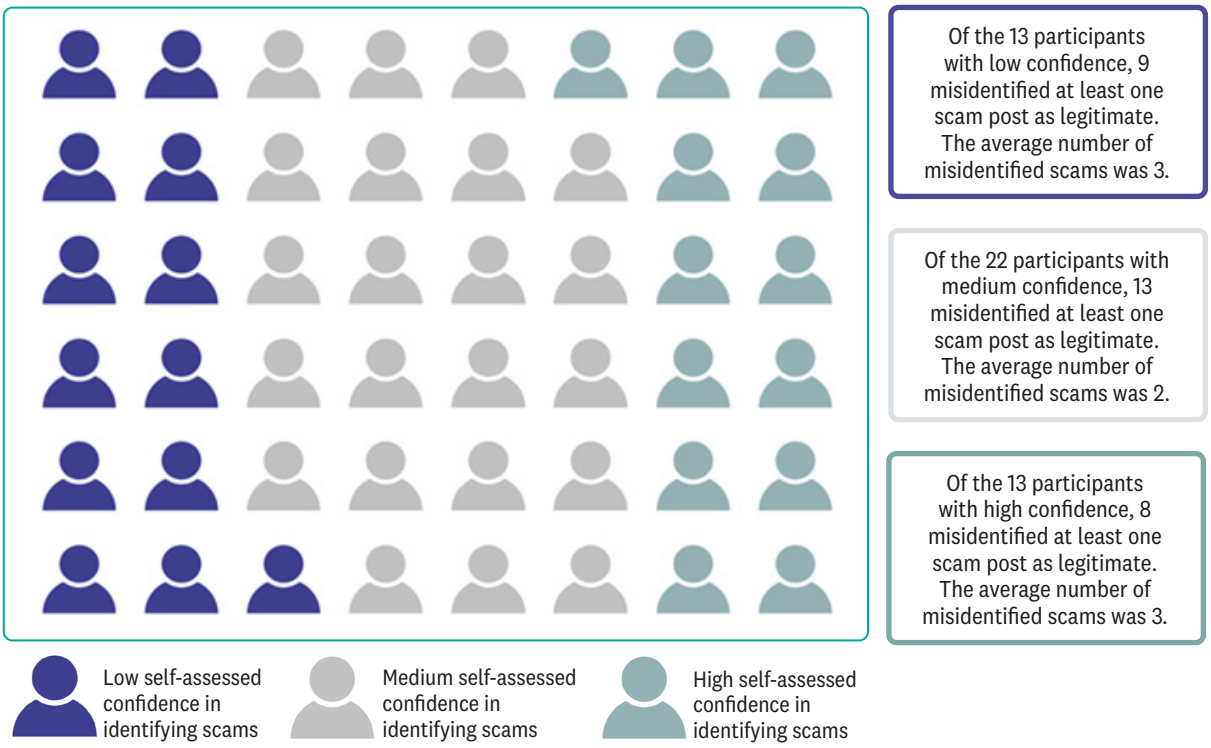
5.2 Confidence identifying scams

Participants' lack of awareness of types of scams may not necessarily increase their susceptibility to being scammed, providing they recognise their awareness of scams is incomplete. To examine this we asked participants in the online community to give a self-assessment of their ability to spot scams on Facebook.[25] We then used an immersive task to assess participants' actual abilities to recognise different types of scams by getting them to sort images of Facebook content into three groups: scams, not scams and unsure. The purpose of this task was to understand how confidence relates to ability, but not to make claims about how confidence varies amongst Facebook users or to make generalisable claims around variations in confidence outside of the context of the online community.

A plurality of the community identified themselves as having a middling ability to spot scams on Facebook, while equal numbers identified themselves as having high or low ability (see Figure 5.2). However, the scam-spotting task showed that participants commonly overstate their ability to identify scams. We found participants in all three confidence groups (high, medium and low) misidentified scam content as legitimate in similar numbers and at similar rates (see Figure 5.2).

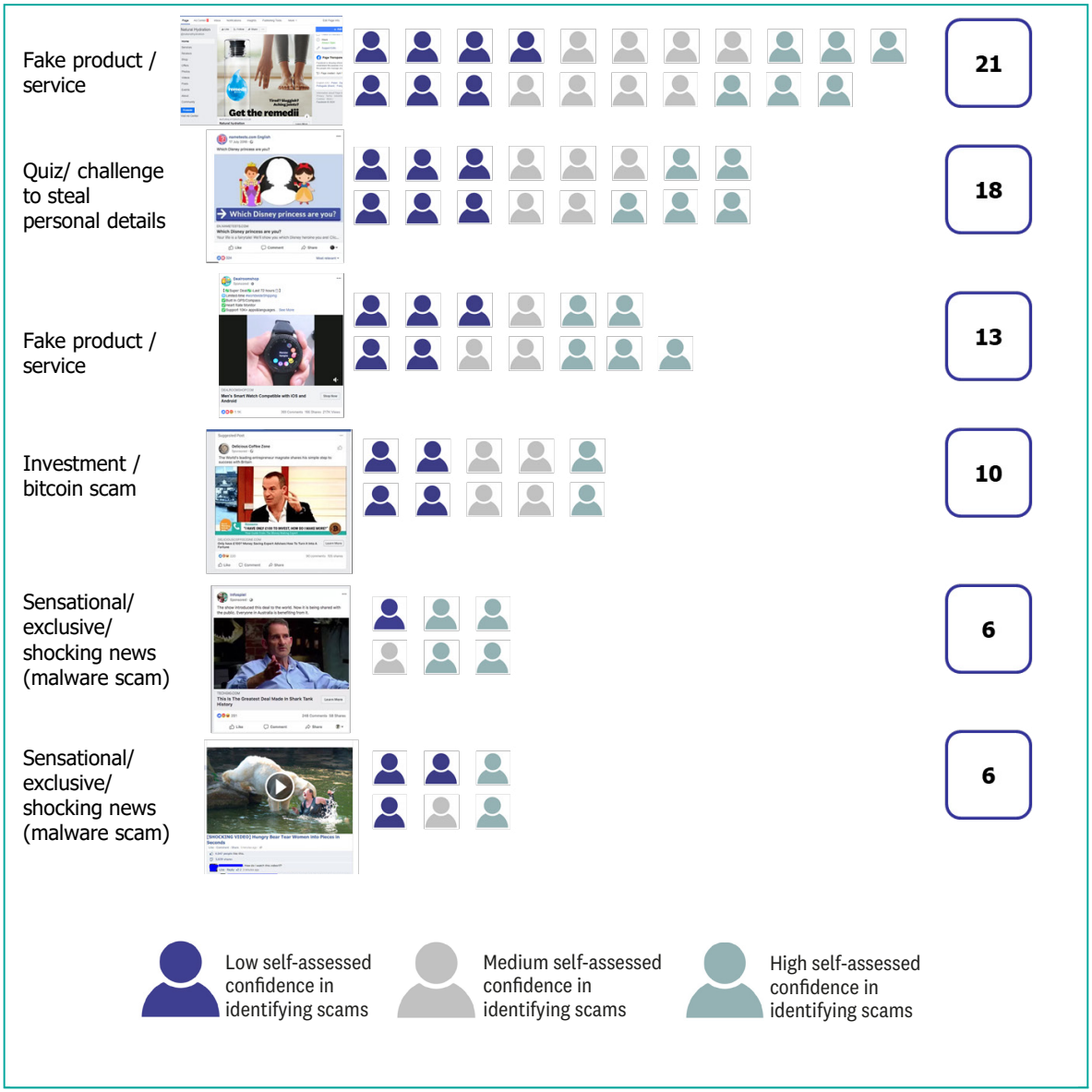
"I think I am confident that I would soon pick up if something was dodgy. I have been a very regular user of the internet for many years and have used a wide variety of websites and applications so I think I am quite aware of the risks."

Figure 5.2: Participants' confidence in spotting scams compared with their ability to identify scam content



The types of scams that were most commonly mistakenly identified as legitimate are those which are more sophisticated (for instance, well designed, free from spelling errors) or seemingly innocuous (for instance, a Disney quiz). Worryingly though, some users are still caught out by scams which may well be considered overt or common. For instance, 10 (of 48) of our online community participants did not recognise the ad featuring Martin Lewis as a scam. Figure 5.3 shows the scams that participants most commonly saw as legitimate.

Figure 5.3: Top-six most commonly misidentified scams by participants



This indicates that participants lack self-awareness when it comes to their ability to identify, and therefore avoid, scams. The implication of this is that they may have higher susceptibility to being scammed because they are overconfident.[26]

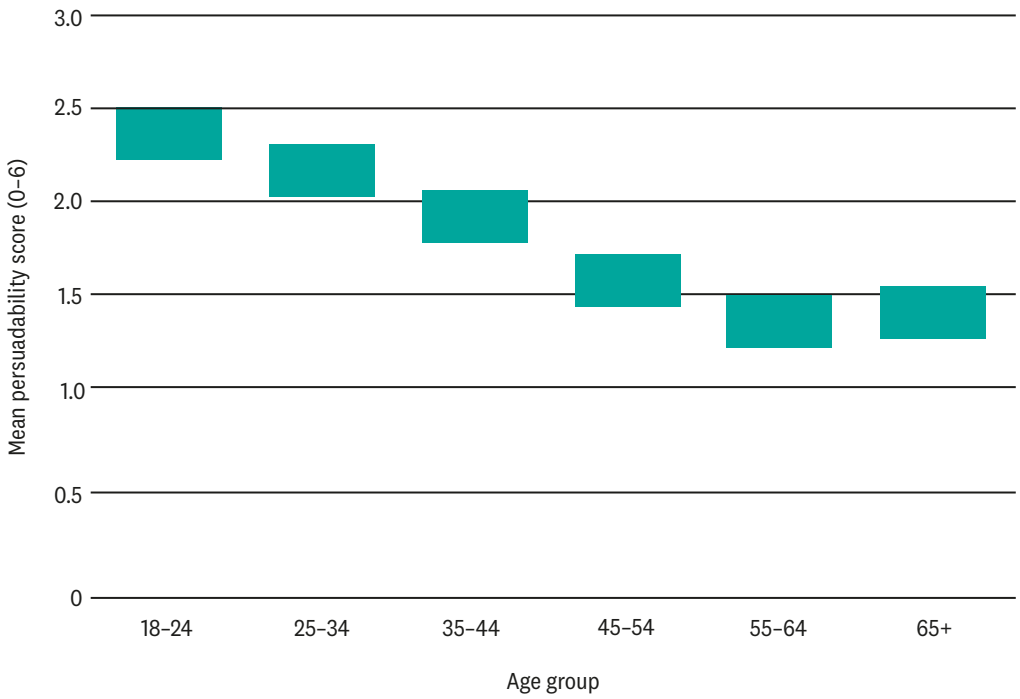
5.3 Susceptibility to be scammed across demographic groups

The preceding sub-sections have explained how our qualitative study found that Facebook users can lack awareness of scams, yet be overconfident in their ability to identify them. To explore whether some groups of users may be more susceptible to being scammed we incorporated the

work of Modic (2012) into the online survey. This involved identifying which types of Facebook users are most likely to have characteristics that make them more persuadable, and then exploring whether these users are more or less likely to engage in riskier behaviours on Facebook.

We found that although older survey respondents were more concerned about the risk of scams younger survey respondents may be more susceptible to actually falling victim to scams. Our survey provides evidence that self-rated susceptibility to persuasion (mean scores on agreement with statements "I am easily persuaded to do things by my friends", "My friends do not easily influence me" (scale reversed) and "I often follow the crowd, even when that is not in my best interest") declines significantly with increasing age (see Figure 5.4).

Figure 5.4: Mean self-rated persuadability scores for survey respondents, by age



Note: The bars represent 95% confidence intervals around the mean score for each age group.
Based on all respondents answering (236 18–24 year olds, 329 25–34, 311 35–44, 347 45–54, 335 55–64 and 508 65 years or older).

In terms of behaviour on the platform, we also found that younger respondents are more likely to engage in activities that would leave them more exposed to certain types of scams. Younger respondents to our survey were:

- More likely to shop through Facebook (50% of 18–24 year olds and 59% of 25–34 and 53% of 35–44 year olds, compared with 29% and 25% of respondents aged 55–64 years old and 65+ respectively) roughly by a ratio of 2:1.
- More likely to complete quizzes (60% of 18–24 year olds and 68% of 25–34 and 60% of 35–44 year olds, compared with 50% and 46% of respondents aged 55–64 years old and 65+ respectively).
- More likely to engage with other content (89% of 18–24 year olds, 92% of 25–34, and 86% of 35–44 year olds, compared with 76% and 67% of respondents aged 55–64 years old and 65+ respectively).

Taken together, these findings suggest that younger people (under the age of 44) are more likely to fall victim to a scam than their more concerned older counterparts. While some older people may have more to lose having accumulated wealth over their lifetimes, younger people may lose smaller amounts more frequently.

5.4 Summary

Our qualitative research has demonstrated that Facebook users commonly both lack awareness of types of scams and overestimate their ability to identify, and hence protect themselves from, scams. These failings were seen across our online community. The survey suggested that younger rather than older people are more exposed to scams through their social media behaviour and are more at risk by virtue of their persuadability.

6. Knowledge and use of Facebook's systems and processes to reduce the risk of scams

Key insights

- Participants expected Facebook to have systems and processes in place to prevent scams appearing on the platform and to identify and remove scams that slipped through the net, but specific knowledge of what these systems are and how effectively they worked was extremely limited.
- It was felt that Facebook's systems and processes were not as effective as people had believed they would be and that more could be done to strengthen what's already in place.
- There was limited awareness of Facebook's scam reporting tool, with just 30% of respondents saying that they were aware of the tool.
- Users also lacked motivation to use the tool, in part because they do not feel well-placed to identify scams and are concerned about repercussions from using the tool. Only about 10% of the total sample had used it.

The previous chapters have shown that Facebook users may be susceptible to scams because they feel safe in the social environment and don't consider the possibility of being scammed, while they also overestimate their ability to identify and avoid scams.

In this chapter we explore to what extent users know and understand the systems and processes Facebook has in place to help users to stay safe from scams. This matters because if users overestimate how well protected they are by Facebook then this might contribute to their lack of consideration of scams when on the platform. We also examine to what extent users are engaging with the support that Facebook has available to them. Clearly, little engagement with these tools could be increasing the risk of being scammed.

We explored three stages of the scams prevention process: stopping scams from appearing, identifying content as a scam, and the removal of scam content. Separately we looked at the types of support – education, tools, etc. – consumers are provided with to help them stay safe and avoid scams and their uptake.

In explaining to participants what Facebook does to reduce scams, we told them we would show them what we "understand are Facebook's systems and processes based on what is available in the public domain. Some of what Facebook does, it deliberately keeps private – this is because if scammers know how Facebook identifies fake, fraudulent or scam content they may change what they do (making it harder for Facebook to find them)."

6.1 Expectations of and reactions to Facebook's systems and processes to stopping scams

Reinforcing the earlier finding that scams are not a top of mind concern for many social media users, a number of participants had little idea about what Facebook does to prevent scam content on the site. Participants typically expected Facebook would have measures in place to prevent scams appearing on their site, but were largely uncertain over what preventative measures are actually used.

Participants thought different types of content would be treated differently. Most assumed that advertising content is "vetted" or reviewed, but while participants assumed Facebook had standards and requirements for individuals to open an account and that this was a way of ensuring users are who they say they are, there was acknowledgement that organic content posted by individual users would be more challenging to vet. A few thought Facebook actively monitored what was being posted, but more commonly they thought that Facebook waited for content to be reported and then removed duplicate or suspicious accounts.

> *"What is more difficult is scams unknowingly posted by friends. Usually when they've been hacked. Room for improvement there."*

Beyond this, a few participants expected that Facebook would collaborate with external agencies or employ third parties to identify potential criminals and stop them preemptively. For instance, one participant believed Facebook monitored scam websites to identify if scams were coming from a particular IP address, while another thought Facebook would collaborate with anti-fraud agencies.

In terms of identifying and taking down scam content, participants expected that Facebook would use advanced technology such as AI that would analyse users' comments on content, scan review posts for certain keywords or phrases associated with scams, look for odd online behaviour and fake accounts - and then remove anything deemed suspicious.

When participants were shown the systems that Facebook has in place to stop scams appearing and to identify and remove scam content (see Figures 6.1 and 6.2), their responses were mixed. Some were reassured that they existed at all, but others questioned whether this is an effective suite of measures, especially in the light of learning that criminals operating on social media are more sophisticated and cunning than they first thought.

> *"Q[uestion] - if the process is so rigorous at review level then how can 'fake' ad's get through?"*

Figure 6.1: How Facebook attempts to stop scams appearing in the first place.

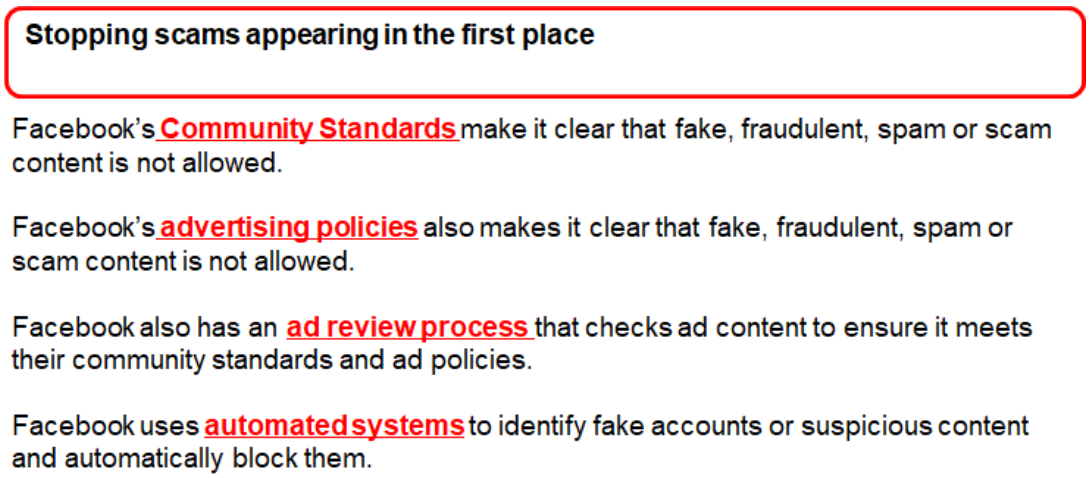


Figure 6.2: How Facebook identifies and removes scam content that does appear on Facebook.

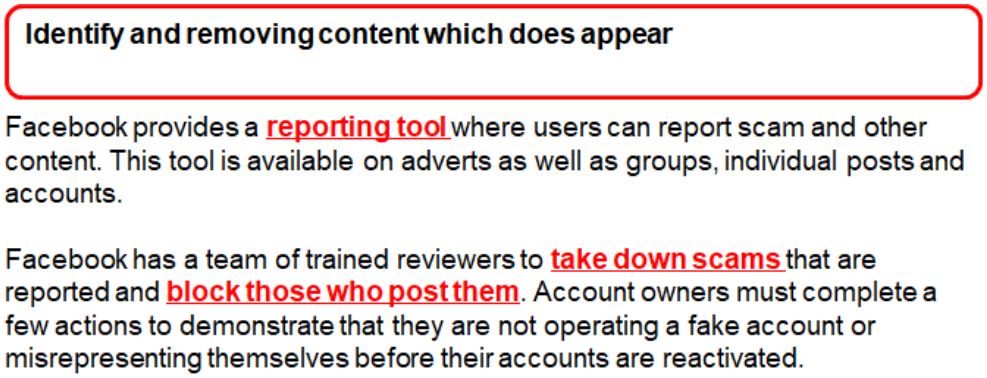


Figure 6.3 summarises participants' expectations of and reactions to Facebook's systems and processes to address scams. It also summarises the expectations gap and the implications of these. In general, these suggest that there is a misalignment between the high expectations that some users have about Facebook's systems and processes to prevent, identify and remove scam-enabling content and the effectiveness of the processes that actually exist. While the headline descriptions of what Facebook does is generally endorsed as appropriate, the prevalence of suspicious and scam content on the sites leaves some feeling that it lacks rigour. There was a strong sense among research participants that Facebook is 'reactive' rather than 'proactive' when it comes to stopping scams appearing.

Figure 6.3: Summary table of social media users' expectations of Facebook's systems and processes to address scams.

	Expectations	Reactions to reality	Gaps	So what?
Preventing scams appearing in the first place	Participants generally expected to see some systems and processes in place to stop scams appearing believing it was good business sense to do so.	They expressed reservations over how effective these systems are in stopping/ preventing scams, as criminals have been able to get round the systems.	There is a need for these systems to work better to reduce things slipping through the net.	There is a concern about the effectiveness of systems with worries that they are reactive rather than proactive.
Identification and removal of scams	There was a general expectation that Facebook monitors content and reviews content to identify and remove scams using AI and some user reporting.	Awareness of Facebook's reporting tool was low and there was doubt it was being widely used, and there was no way of knowing if it was effective due to the lack of feedback mechanisms.	This lack of a feedback mechanism within the tool raised a suspicion that it was tick box exercise or window dressing.	The lack of feedback from the platform tool elicits low confidence in its effectiveness. The impact of reporting is unknown and this is not motivating.
Helping users' to identify and avoid scams	There was an overall lack of awareness of the full suite of processes Facebook has in place to protect users from scams, although some have used or enabled some privacy or security features, e.g. changing password when prompted and two-factor authentication.	After being shown the types of help Facebook offers, it is clear that awareness of these is relatively low – although most liked what they saw.	Participants felt there should be increased promotion of support tools, better warning of scam content and appropriate advice/ guidance for users. They claimed they would act on this guidance.	Users would like to increase their awareness of scams and the support Facebook provides but it is questionable whether this will lead to more use of Facebook's existing privacy and security tools or whether defaulting users to the safest option would be more appropriate.

6.2 User behaviours to keep themselves and others safe

Participants had adopted various strategies in order to keep themselves safe from scams on social media and considered their day-to-day behaviour in the online environment as key to avoiding scams. In most cases, participants looked to family and friends, search engines and their wider experiences on the internet (either at work or in their personal lives) to inform how to keep themselves safe.

Most adopted 'protective behaviours' to limit their risk of being scammed (only having a small circle of friends, not accepting requests from strangers) and being cautious or only engaging with the types of content they considered safe. This included scrolling past content they considered suspicious rather than engaging with it in any way (even to report it). However, some had used tools provided by Facebook to protect themselves or others, most notably privacy settings and Facebook's scam reporting tool, which was launched following Facebook's legal settlement with Martin Lewis.

6.2.1 Privacy settings and Facebook advice and guidance

One way in which users might be able to reduce their risk of falling victim to scams is to use the privacy settings that Facebook offers. However, uptake and use of functionality provided by Facebook for users to tailor their security and privacy settings specifically as a way of providing protection from scams was somewhat limited.

Facebook also publishes articles on how to spot and avoid scams. These include advice such as not to click on suspicious links, even if they appear to come from a friend, to watch out for malicious software, and not to accept friend requests from people you don't know. However, awareness of Facebook's scam advice and guidance appears to be low as only a handful of participants said they had received advice from or sought information from Facebook directly.

Once participants were introduced to the types of resources Facebook provides to users, most welcomed them but felt they could be more effectively promoted. Participants commonly felt it was important for individual users to act responsibly and that being provided with information and tools for doing this would support greater user safety.

> *"A determined scammer or spammer will always do anything to get around anything Facebook tries to do to block them. I think equal responsibility lies with the Facebook user to use the privacy tools available and use their common sense. I think there are more pros than cons to the platform and users should try to educate themselves on what not to do."*

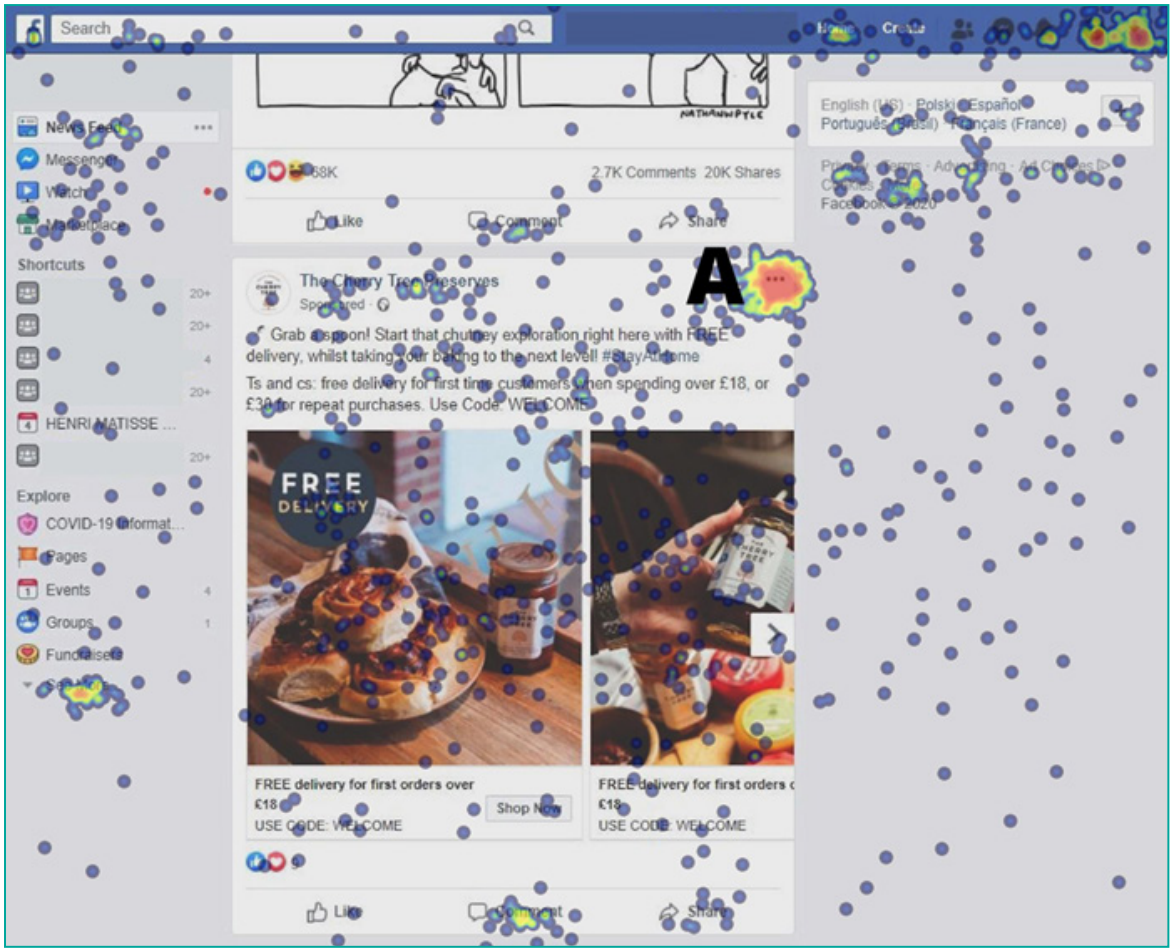
6.2.2 Facebook scams reporting tool

Participants in the online community tended to assume that Facebook would have a tool for reporting suspicious content, but awareness of Facebook's actual scam ad reporting tool was relatively low. Few had used the tool themselves while others identified barriers to its use (e.g. not being certain something was a scam, lack of interest, etc.) making it less effective in reality than it would appear on paper. To investigate this further, we used our online survey of Facebook. We found that awareness of the tool was low with just 30% of respondents saying that they were aware of the tool. Only a third of these (10% of the total sample) said that they had used the tool themselves.

A barrier to use of the tool appears to be that its location is not immediately apparent or intuitive. We asked respondents to our survey where they would click if they wanted to report an advert as a potential scam/fraud using the reporting tool. Although respondents did commonly identify the correct place to report a scam (figure A in the image below showing a "hotspot" where the scams

reporting tool can be found), there were hotspots in multiple other places on the homepage and clicking on these other places would potentially navigate users away from the content they were trying to report. Since ads and sponsored content are not typically static in users' feeds this would mean they would not get a second attempt to get it right.

Figure 6.4: Heatmap of where participants would click in order to find the Scams Reporting Tool



There are likely also behavioural barriers to reporting scams using the reporting tool. Facebook users most common response to potentially suspicious content was to keep scrolling rather than report the content to Facebook (29% said they would keep scrolling in responses to an advert featuring Martin Lewis promoting bitcoin investments because they found it suspicious and 29% said they would do the same in response to a scam Disney princess quiz). To understand why this might be the case we asked respondents "why they might not immediately report a suspected scam" and analysed their responses using the behavioural COM-B model.[27]

We found that most common barriers related to a lack of motivation, although a lack of opportunity and capability did also play a role. For some, it simply did not cross their mind that they should report a scam or were not interested in doing so – some respondents simply did not see it as their role, either because scams do not affect them directly, or they see it as the responsibility of "others", such as Facebook or actual and potential victims.

In other cases, the lack of motivation to report stemmed from uncertainty about the efficacy of the process – assuming it would be a hassle and/or not a good use of limited time. The scale of the issue (the number of scams people felt were out there) made some feel there were too many

scams to report, and did not want to risk engaging with suspicious posts in any way. Others were concerned about the consequences of reporting a scam, being identified or getting involved in a subsequent confrontation. Some had poor past experiences reporting content and lacked confidence that reports would be acted upon.

This resonates with reported frustrations from participants in the online community in relation to the absence of feedback they had received from Facebook on the outcome of their reporting. For some this lack of feedback bred a degree of scepticism about the tool as there was no way of telling whether it was worthwhile reporting content. This lack of transparency undermined trust and confidence in the efficacy of tools.

> *"Facebook has had a report button for some time now and I don't believe it works… They should have a [section on their site where it says] "concerned about [a] site then please send us your concerns and we will get back to you", that way you will get a response as to what happens instead of radio silence"*

Finally, some people's lack of motivation stemmed from difficulties in identifying scam content – people didn't want to misreport suspect content due to the impact on someone's business/ reputation and did not appear motivated enough to investigate beyond their initial, in-the-moment impression of the content.

6.3 Summary

Knowledge among users of what Facebook does to protect people from becoming a victim of scams is low, although users assume that Facebook does have systems and processes in place to stop scam content appearing and to identify and take it down. When given knowledge of Facebook's actual systems and processes, users are sceptical about their efficacy and questioned whether they are sufficient.

There are also questions over the adequacy of the ways in which support, advice and guidance are promoted to users by Facebook given their current reliance on friends and family, search engines and more general experiences of using the internet for how to stay safe online. The appeal of Facebook's privacy and scams reporting tools were high, although awareness and uptake was low. While promotion of these tools cannot be solely relied upon for improving users safety given current low levels of uptake, their targeted promotion alongside a greater use of defaults to ensure users are as safe as possible without needing to take proactive measures may support users' safety.

7. Consumer attitudes on how to make social media users safe from scams

Key insights

- Users feel that Facebook must take a leading role in keeping its platform safe from scams given its technology and know-how, and that it must do what it can to strengthen protections of people's data.
- While recognising Facebook users have an individual responsibility to stay alert and that other organisations (regulators, banks, the police, etc.) could provide better support for consumers, participants looked to Facebook to enhance protections and make it harder for criminals to open accounts and for scam content to be posted.

In the preceding chapter we identified that Facebook users have concerns about the efficacy of existing systems to prevent scam content from appearing on the platform and to identify and take down scam content. In this chapter we investigate what users would like to happen to improve the current situation.

7.1 The role of Facebook

Participants saw Facebook as having the leading role and responsibility in stopping users being scammed on its site. These views were based on a mixture of beliefs about what participants thought feasible and morally just given Facebook's position of power.

First, participants believed that large social media platforms, such as Facebook, are best placed to do this because only they have access to the data and technology to spot and remove scams. Many assumed they could use the same technology they use to serve content to users (e.g. AI, behavioural insights) to crack down on criminals, identify suspicious behaviour and remove content. Ultimately, Facebook users had high expectations for what Facebook would do behind the scenes to keep them safe.

Second, participants believed Facebook ultimately set the rules of the game for what could happen on its platform. They understood Facebook set standards/rules over what could appear on its site and, given it controlled the site's infrastructure, could decide what functionality was enabled, the tools available to users (e.g. scam reporting tools) and the settings users were able to access/tailor on their accounts. Although individual users should abide by these standards and use available tools, participants felt Facebook had a responsibility to set and enforce appropriate standards, hold users to account and encourage users to make use of functions that would keep them safe. A few suggested Facebook should default people into the safest option and/or target resources at those most at risk.

Participants particulary felt that preventative systems to vet people and content needed to be better to effectively protect users and that these should activate at the earliest possible opportunity, i.e. before publication. In particular, participants felt the ad review process could be improved. However, participants did recognise that there are some limits to what Facebook should do to protect users. For example, participants were somewhat divided over how much

discretion Facebook should have to decide what content is removed, and while there was some support for Facebook to penalise those they had identified as trying to place scams on their site (e.g. passing their details onto the police and other agencies), others were concerned this would be an overextension of Facebook's power.

7.2 The role of other organisations

Participants commonly recognised that Facebook operates in a broader social, legal and ethical context and that while Facebook was viewed as having the greatest responsibility, participants did not feel this was an exclusive one. Participants identified a broad supporting cast of organisations to help address scams and criminals on social media, including:

- **Regulators**: Participants recognised their online experiences are shaped by wider rules on data protection. Awareness that laws exist to protect people's personal data (GDPR) was relatively common, if only at a superficial level, as was the fact these requirements are ultimately set by governments. Further, some questioned whether Facebook would have the incentive to act in users' best interests given a large proportion of its revenue comes from serving ads. Participants felt the government had a responsibility to make sure social media users are appropriately protected in law.
- **The police**: Participants recognised that scams are crimes, and as such felt the police and other related organisations have a role in prevention and reduction.
- **Banks and payment systems providers**: Participants expected to be able to access support from banks or their payment systems provider (e.g. debit/credit card providers, PayPal) if they were scammed and that these bodies would have systems in place to spot suspicious transactions.

7.3 The role of individuals

Finally, participants felt they as individuals also had some responsibility to keep themselves safe from scams on social media. Participants believed Facebook users should not be overly naive when they interact with individuals and content on social media and that they should use their common sense: if an offer seems too good to be true, it probably is.

That said, participants believed individual Facebook users could only protect themselves so far (a sentiment affirmed by our findings in the preceding chapters). They were particularly concerned that more vulnerable social media users may not be able to do so. This view was reinforced as the community progressed and participants learnt more about the range of scams and their sophistication and subtlety, with participants feeling more should be done to increase social media users' awareness of scams and support them in staying safe. Ultimately, participants emphasised it was not reasonable to place too great an onus for scams identification, avoidance and reporting on individual Facebook users.

> *"I think Facebook have more of a responsibility to deal with this rather than the users, as it should be a safe space for users to go and express themselves and see safe content that is relevant to them, knowing that those links and sites can be trusted."*

7.4 Summary

Participants saw Facebook as central to keeping Facebook users safe from scams and criminals and as having a responsibility to help keep its users and their data safe. Although participants recognised other stakeholders had some responsibility to prevent scams and help those who are scammed, Facebook's position was seen as unique. The platform was believed to have enormous untapped capabilities to monitor what content is posted on Facebook, set appropriate community standards and have other appropriate systems and processes in place.

There was a strong belief that Facebook should act with users' best interests in mind, given that individual users are not best placed to identify and avoid scams even when they believe they have the skills and are behaving in a 'common sense' way. However, in spite of believing it was Facebook's duty to protect the interests of its users, questions remained over whether Facebook should do this unchecked. As such, there was support for appropriate regulation and guidance for social media platforms to ensure users interests were adequately protected.

8. Conclusions and recommendations

There is growing concern about the number of scams that are perpetrated using social media and the substantial harm that this causes to victims. In this report we have presented the findings of research that has explored the attitudes and behaviours of social media users so that we can understand the best way to protect them from becoming victims of scams. Our findings highlight that, while users have some responsibility to protect themselves, their ability to do so may sometimes be limited by a lack of awareness, overconfidence in their ability to spot scams and in what they believe the social media platform does to keep them safe, and because the perceived threat of scams might be reduced by seeing the platform as a social space.

Which? believes that social media platforms are best placed to tackle scams and in this chapter we set out our recommendations to reduce the risk of social media users falling victim to scams. Since the recommendations follow from our research, these are mostly made to Facebook, but we think they could apply more broadly to other social media platforms. While most platforms can show that they have taken steps towards blocking bad actors and taking down suspicious content or introducing reporting tools, these have been piecemeal and we do not think these changes have been sufficiently effective. We also include calls to the Government as we believe it will be necessary to compel platforms to take appropriate measures.

8.1 Improving existing initiatives

Facebook has already implemented some measures to tackle scams on its site. Alongside efforts to take down fraudulent content when it is identified, most notably, last year Facebook developed and introduced its scam ad reporting tool and gave £3m to Citizens Advice to set up a new anti-scams initiative, including support for scam victims and general awareness raising of the risk of online scams. By definition, these measures have a strong focus on content reporting and awareness, but there are many limitations to how effective these types of initiatives can be, which we have demonstrated in this research.

Reporting tool

An effective reporting system can assist Facebook with the identification of scam content that has not been picked up through its automated systems. However, scam content by its nature is intended to deceive or mislead and can be very convincing, so any over-reliance on user reporting will lead to an ineffective system of protecting users. Our findings that only three in ten Facebook users are aware of the tool and only one in ten have used it clearly indicate the limited effectiveness of the current reporting system.

The research has identified a number of barriers users face when reporting suspicious content with the tool. Some of these barriers could potentially be overcome, for example users not knowing how to access the reporting tool and a feeling of uncertainty about the reporting process and whether reports would be acted upon. We recommend that **Facebook takes actions to raise awareness of the reporting tool and,** to build confidence in the efficacy of the tool, we recommend **that Facebook considers how it can report back on what happened next to users of the tool.**

However, we also found other, more fundamental barriers. These include a lack of motivation among users due to a sense that it was not their role to report these things and difficulty identifying scam content, as consumers neither want to put themselves in harms way by investigating further or incorrectly report legitimate content as a scam. These barriers to reporting mean there will always be limitations to how effective a user-led reporting tool can be.

Raising awareness of scams

We accept that it will not be possible for Facebook to eliminate all scam content and social media users need to be supported to protect themselves when they encounter scam content. Interventions, through advice and warnings, to educate social media users about the variety and sophistication of scams will be important to do this and, since our research has shown that scams are typically not top of mind, it will be particularly important to increase awareness about the harm from scams. While organisations like Citizens Advice and Which? can play a role in this, social media platforms also have a responsibility. Facebook currently does have scam advice and guidance, but we found that awareness of this was low. Therefore, we recommend that **Facebook should raise awareness of its existing advice and guidance and do more to raise understanding of the harm from scams,** for example by increasing awareness that scammers steal personal data as well as money.

Raising awareness of the variety and sophistication of scams should challenge peoples' perceptions about the risk from scams and help them to avoid being scammed. However, this research has also shown that education interventions need to be made carefully if they are to be effective at reducing harm. The limited relationship between confidence and scam-spotting ability indicated by this research suggests that if heightened awareness leads to overconfidence then it may not be helpful. Facebook could experiment with warning banners or targeted messaging and whether they should be provided at all times or at particular moments where users are more at risk, such as when clicking on links that take them off the site. It would be important to test these options, as there may be limits to their effectiveness at raising awareness if Facebook users become blind to warning messages due to overexposure.

We do not want to raise awareness so much that consumers become overconfident in spotting scams, but we want them to think of social media as a place where scams are present and where they should be on their guard. Ultimately, increasing consumer awareness of the risk of scams on social media should be included in the range of measures to tackle this problem, but it cannot be a measure in isolation.

8.2 Facebook must have effective systems and processes

This research has clearly demonstrated why it is unreasonable to put the onus for identifying and avoiding scams on consumers, so it is essential that Facebook has effective systems and processes in place to tackle illegal and fraudulent content and reduce consumers' exposure to it. As discussed above, the measures introduced to date to tackle scams are not sufficient, as demonstrated by the many examples of fraudulent content that still slip through and the harm they can cause.

Monitoring, blocking and removal

Which? would like to see Facebook introduce both proactive and reactive measures to deal with illegal content as part of these effective systems and processes. As much as possible, Facebook should be working to prevent the presence of illegal and harmful content on its site through effective automated monitoring systems, clear site conduct policies, and blocking bad actors from accessing and re-accessing their sites. Where harmful content slips through despite these

proactive measures, Facebook must remove the content as quickly as possible, ideally within a defined timeframe.

Our research has shown that many consumers already have expectations that Facebook has effective systems and processes in place for the prevention and removal of harmful content. However, research participants became more sceptical of the effectiveness of these as they learned more about the existing systems and the range of scam content that still slips through. **Facebook must work to improve the effectiveness of existing systems for identification, removal and prevention of harmful content**, but it can and should go further.

Targeted alerts and warnings

Facebook, with the amount of information it holds about its users and what they engage with, is in a unique position to be able to help notify its users if they have engaged with harmful or fraudulent content. We recommend that **when fraudulent content is identified on the site, Facebook should use the information it already holds to alert the users who have engaged with the content** (for example, those who have clicked on an ad that is later found to be a scam or have shared content that links to phishing domains or malware). We are aware that Facebook introduced warning messages for those who had interacted with harmful and misleading COVID-19 content. This is a positive step from Facebook to keep people informed and limit misinformation about the coronavirus crisis, and it also demonstrates that Facebook has the capability to target warning messages to those who most need them. Such alerts should be introduced for fraudulent and scam content. These alerts should state when the content was removed and why, and include information or signposting to where users can seek help if they need it, such as where they could seek advice about getting money back after a scam.

Advertiser verification

In addition to the above, Facebook should have systems and processes in place to prevent fraudulent ads from being listed on its platform. Facebook has Advertising Policies setting out what is and is not allowed and operates a review process against these, but it is clear that many fraudulent ads still make it through these checks. During the research, participants made a range of suggestions for how Facebook users could be better protected from scams, with participants commonly suggesting that Facebook should introduce more stringent vetting processes for ads in order to ensure scam ads do not reach consumers.

Anyone who buys advertising is a customer of Facebook, not just a user, and **there should be a requirement for Facebook to verify the identity of its customers**. This would prevent many scammers being able to operate anonymously via social media platforms. We acknowledge that the steps required to verify all advertisers may be onerous for Facebook, but we believe this is a process that could be rolled out incrementally, as long as, in the interim, **Facebook is clear which ads have and have not been verified**. This should be displayed clearly on each ad so consumers can judge for themselves the risks involved with engaging with that ad.

8.3 What Government and regulators must do

Social media platforms are best placed to tackle scams, but our research has shown that people do not trust Facebook to decide what is harmful, scam-enabling material and how to respond to it. Further, given the limited measures introduced by platforms to date have been brought in voluntarily, we believe it is unlikely that platforms will take sufficient steps without bringing in a strong regulatory framework that requires it. Unless online platforms are required to tackle this problem, the incidence of scams will continue to grow and cause financial and emotional harm for social media users.

For this reason, and to make sure Facebook and others introduce the measures we recommend in section 8.2, the responsibilities of platforms must be brought more in line with the expectations of consumers for social media sites to keep their users safe. **Social media platforms should be given a legal responsibility for preventing scam content from appearing on their sites**, as well as more responsibility for taking quick action to remove harmful content when it is reported. **Legislation should set out the requirement for the proactive and reactive measures** discussed above and require platforms to demonstrate how they are implementing measures to protect their users.

In addition to a requirement for effective systems and processes (including both proactive and reactive measures), **platforms should also be made legally responsible for the design of their systems to prevent illegal activities, including scams and fraud**. This could include efforts to be transparent about the potential risks users may face on social media and that not all content has been moderated; for example, building in clear labelling of verified and unverified ads into their systems.

We know that Facebook and other social media platforms are not fighting scams in isolation. Research participants acknowledged that other bodies – such as law enforcement, banks and regulators – have a part to play, but that Facebook has a leading role regarding the scam or scam-enabling content that appears on the platform given the amount of information it holds about its users and activity on its platform. Therefore, **a legal requirement for transparency about illegal activity on their sites and to report to relevant regulators and law enforcement bodies should also be applied to platforms**. This should require platforms to have processes in place for reporting illegal activity to appropriate bodies, while the transparency requirements should call for reporting on the number of complaints, response times and resolutions, the amount of content removed, and the number of bad actor accounts disabled. Finally, the regulatory framework must be monitored by a regulator that can set out expectations for platforms and that has sufficient powers to enforce them.

Endnotes

1 UK Finance (2019), *Fraud The Facts 2019*.

2 Action Fraud (2020), *Fraud Crime Trends 2019–20*: https://data.actionfraud.police.uk/cms/wp-content/uploads/2020/07/Fraud-crime-trends.pdf

3 Ibid.

4 Cross C, Richards K & Smith R (2016), *The reporting experiences and support needs of victims of online fraud*. In: Trends & issues in crime and criminal justice no. 518: https://www.aic.gov.au/publications/tandi/tandi518

5 Button, M, Lewis, C, & Tapley, J (2014), *Not a victimless crime: The impact of fraud on individual victims and their families*, Security Journal, 27(1), 36–54.

6 OFT (2006), *Research report on impact of mass marketed scams*: https://webarchive.nationalarchives.gov.uk/20090903184457/http://www.oft.gov.uk/shared_oft/reports/consumer_protection/oft883.pdf

7 Modic, D & Anderson, R (2015), *It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud*, Ieee Security & Privacy, 13(5), 99–103: https://www.cl.cam.ac.uk/~rja14/Papers/modicanderson-over15.pdf

8 As at 4: Cross C, Richards K & Smith R (2016).

9 Ibid.

10 Cialdini, R (2007), *Influence: The psychology of persuasion*.

11 Kahneman, D & Tversky, A (1979) *Prospect theory: An analysis of decision under risk*. In: Econometrica, 47.2, pp. 263–291.

12 Tversky, A & Kahneman, D (1992) *Advances in prospect theory: Cumulative representation of uncertainty*. In: Journal of Risk and Uncertainty, 5.4, pp. 297–323.

13 Lea, S, Fischer, P & Evans, K (2009), *The psychology of scams: Provoking and committing errors of judgement*: Available at: https://ore.exeter.ac.uk/repository/handle/10871/20958

14 Modic, D (2012), *Willing to be scammed: How self-control impacts Internet scam compliance*, University of Exeter. Available at: https://ore.exeter.ac.uk/repository/bitstream/handle/10871/8044/ModicD.pdf?sequence=2

15 Modic, D & Lea, S (2013), *Scam compliance and the psychology of persuasion*, University of Exeter: https://r.deception.org.uk/sites/research.deception.org.uk/files/research/Modic%2C%20D.%20and%20Lea%2C%20S.%20%282013%29%20Scam%20Compliance.pdf

16 As at 13: Lea, S, Fischer, P & Evans, K (2009).

17 Which? (2016), *Why intelligent people fall for fraud*. In: Which? Magazine, September 2016.

18 Ross, M, Grossmann, I & Schryer, E (2014), *Contrary to psychological and popular opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud*. In: Perspectives on Psychological Science 9.4, pp.427–442.

19 As at 15: Modic, D & Lea, S (2013).

20 NFIB (2020), " NFIB Fraud and Cyber Crime Dashboard": https://colpolice.maps.arcgis.com/apps/opsdashboard/index.html#/60499304565045b0bce05d2ca7e1e56c;

21 As at 2: Action Fraud (2020).

22 Ofcom (2020), *Adults' Media Use & Attitudes report 2020*: https://www.ofcom.org.uk/__data/assets/pdf_file/0031/196375/adults-media-use-and-attitudes-2020-report.pdf. Note, in 2018 Which? conducted a general public survey part of the aim of which was to understand the demographics and behaviours of Facebook users.

23 Day 7 fell on a weekend had no scheduled activities to allow participants to 'catch-up' if they had fallen behind with daily activities

24 As at 14: Modic, D (2012).

25 We set minimum quotas at recruitment on participants' general confidence in their abilities to identify scams online to ensure that a spread of self-assessed confidence was included in the research. In the

context of the online community we explicitly asked about participants' confidence in spotting potential scams on Facebook

26 Individuals' self-assessments changed through the course of the online community as participants learnt more about scams: for many, the more they learnt about scams, the greater their confidence in their ability to spot scams became. However, any increase in self-assessed confidence in the context of the research should be seen as having shaky foundations given the inaccuracies of their initial self-assessment.

27 Michie, S, Atkins, L, and West, R (2020), *The Behaviour Change Wheel A Guide To Designing Interventions*, Available at http://www.behaviourchangewheel.com/about-wheel

Which?, 2 Marylebone Road,
London NW1 4DF
Phone +44 (0)20 7770 7000
Fax +44 (0)20 7770 7600