‘The internet acts as a level playing field. All it takes is one slip-up’: Online fraud and the sense of pervasive threat

Jessica Jacobson, Bina Bhardwa, Alexandra Murray

July 2024

Institute for Crime & Justice Policy Research (ICPR),
Birkbeck, University of London

Contents

Key Messages 1

Introduction 2

Matter-of-fact perceptions of unavoidable risk 3

Cautiously optimistic perceptions of containable risk 5

Anxiety and vigilance 8

Implications for tackling online fraud 9

ANNEX: The focus groups 11

Acknowledgements

This piece was written using the data generated from focus groups with members of the public conducted for the *Tackling Online Fraud* research project, funded by the Dawes Trust.

We would like to thank our project partners, Crest Advisory and the Police Foundation, especially Manon Roberts and Dr Michael Skidmore for reviewing and providing feedback on this piece. Thanks are also due to the focus group participants for their open and thoughtful contributions to the project.

Key Messages

- Much of the public and policy debate about the cost of fraud does not take into account the extent to which fraud *attempts*, regardless of whether they result in victimisation, impact on individuals and society as a whole.
- In a series of focus groups involving members of the public, participants described exposure to the risk of fraud as an intrinsic part of lives that are lived at least partly online.
- The focus group participants variously spoke about the pervasive threat of online fraud as:
    - unavoidable but not a cause of great concern;
    - largely containable, thanks to their own knowledge and skills;
    - a source of real anxiety and something they needed to be constantly vigilant against.
- There was a general perception that members of the public should take responsibility for protecting themselves – and each other – against the rapidly evolving threat of fraud, and little trust in the efficacy of reporting fraud attempts.
- The focus group findings make clear the importance of strengthening responses to fraud attempts, as part of efforts to tackling online fraud, including through:
    - improved understanding of how members of the public experience these attempts and the factors that deter reporting;
    - clear, concise and targeted public information that empowers individuals to protect themselves;
    - developing and promoting quick and easy mechanisms for reporting;
    - simple messaging that allays anxiety by making the problem of online fraud seem less overwhelming.

Introduction

Online fraud imposes heavy costs – both financial and psychological – on victims[1] and on society as a whole. The statistics are striking:

- Fraud accounts for around 40% of all crime in England and Wales;
- An estimated 3.2 million fraud offences are committed each year;
- The estimated total cost of fraud to England and Wales is £6.8.[2]

The internet and communication technologies have radically changed the nature of fraud – increasing its frequency, scale and sophistication. Reflecting the increase in online activity across society and particularly since the Covid-19 pandemic, a growing proportion of fraud is now being carried out wholly or partly online.[3] For the purposes of this paper, we are using the term 'online fraud' to refer to acts of deception or misrepresentation for personal gain which involve some use of the internet and digital technologies.

Much of the public and policy debate about the cost of fraud, however, does not take into account the extent to which fraud *attempts*, regardless of whether they result in victimisation, impact on individuals and society as a whole. Almost every member of society who has some engagement with the digital world – whether through work, online shopping or banking, social media or entertainment platforms, or in other ways – is likely to regularly encounter phishing[4] and other online activity aimed at fraudulently accessing data, money, property or services. In this paper we discuss some of the consequences of the pervasive threat of online fraud – drawing on the findings of focus groups[5] with the general public which were conducted as part of the *Tackling Online Fraud* project.[6]

While the focus groups explored participants' views and experiences in relation to many different aspects of online fraud, some of the most interesting findings pertained to understandings of and responses to fraud attempts. It became clear that the focus group participants tended to regard the risk of fraud as an intrinsic part of lives that are lived at least

[1] See the Crest Advisory and ICPR project report on victimisation, Behind the screen: Perceptions and experiences of online fraud, 16 May 2024.

[2] Home Office, 'Major crime to fight fraud launched', 12 February 2024.

[3] Office for National Statistics, Nature of fraud and computer misuse in England and Wales: year ending 2022 reports that the proportion of frauds recorded as 'cyber-related' rose from 53% to 61% over the two years since the year ending March 2020.

[4] Phishing is defined by Action Fraud, the UK's national reporting centre for fraud and cybercrime, as follows: 'Cyber criminals use fake messages as bait to lure you into clicking on the links within their scam email or text message, or to give away sensitive information (such as bank details)', https://www.actionfraud.police.uk/a-z-of-fraud/phishing.

[5] See Annex for more information on the focus groups.

[6] This project, funded by the Dawes Trust, is being conducted by Crest Advisory; the Institute for Crime and Justice Policy Research (ICPR) at Birkbeck, University of London; and the Police Foundation.

partly online, and that they were affected by this sense of pervasive threat in differing ways. Participants' perceptions of the nature and repercussions of the risk of online fraud can be loosely categorised as follows, on the understanding that these are overlapping rather than discrete categories:

1. Matter-of-fact perceptions of exposure to the risk as unavoidable, and something to which no one is immune;

2. Cautiously optimistic perceptions of the risk as containable, provided that one is appropriately careful and equipped with the knowledge and skills to recognise and take action to mitigate it;

3. Anxiety about the risk, associated with a perceived need to be in a state of constant vigilance.

Below we discuss, in turn, each of these three broad characterisations of the pervasive risk of online fraud. We then conclude the paper by briefly considering the implications for tackling online fraud.

Matter-of-fact perceptions of unavoidable risk

Some focus group participants spoke of the risk of online fraud as 'background noise', or a constant aspect of life of which they were aware, but which they were not unduly concerned about. One participant pointed out that participation in the focus group itself depended on his and others' preparedness to respond to messages from the research recruitment agency that might have been seen as suspicious: 'None of us would be sat here if we weren't filling in, giving shadowy people our information.'

> 'I get so many of them [phishing emails] that it just becomes background noise. … Most of the time mine go into spam, so I don't have to deal with it. I don't even open as they are already identified as spam. Because to me, I feel like ever since I've had emails since I was young, I've got these random messages. It's nothing new. Like it's just kind of part of life. Yeah, but they're always there'.

It was sometimes stressed that no one is immune to the risk of fraud – no matter who they are or how knowledgeable they might consider themselves to be. Accordingly, there was said to be a problem of 'complacency', especially among those who are young and have grown up with the internet. It was also pointed out that many online interactions and other activities are carried out in a largely unthinking or semi-automated way (such as ticking boxes to accept

cookies or data-sharing without reading the detail). This prioritisation of speed and convenience during routine or everyday online interactions was said to add to the risk of victimisation.

> 'I think everyone's at risk. I don't know anybody that's not been a victim. At some point.'
>
> 'Say on a day to day, I don't have too many concerns. ... [But] at the back of my mind, knowing it could always happen.'
>
> 'I'm coming back to people my age, where I'm tech savvy, love my computer, whatever, whatever. But maybe I'm too complacent: "Yeah, well, I know about these things." And so, I skipped the checks … You know, when we accept cookies on sites and stuff like that you do just sort of whizz past things like that.'
>
> 'It's indiscriminate: I think everybody is at risk without a shadow of a doubt… But sometimes I think what can happen is because it's talked about so much … that people become quite complacent about it. Like, "Yeah, yeah, I know. Yeah. Yeah. I'm careful. It's fine." But then maybe not so careful.'

A frequently recurring theme in such comments was the ease with which anyone can, on occasion, become a victim of online fraud. This might be when an offer looks so appealing that it overrides one's usual caution – 'Are we not all tempted by something that could be better than what we've got?' – or at a moment of tiredness, stress or other distraction. What this means, as one participant expressed it, is that 'The internet acts as a level playing field. All it takes is one slip-up.' Narratives about 'slipping up' or falling prey to temptation accord with tendencies to victim-blame and self-blame for victimisation in relation to online fraud (as further discussed below).[7]

> 'It could be a moment of panic of like your bank calling you and saying, "OK, we've blocked access to your account, you need to do X and Y"… So, I do feel that at moments times, I could slip.'
>
> 'I could always be caught out… There's always times where you're a little bit grumpy or a little bit tired. And, you know, that's when you click on this sort of stuff.'
>
> 'When you're on social media a lot and these things come up and you might just be, I don't know, tired or you know, a moment of weakness and you think, oh, I'll get that sounds really good.'
>
> 'You feel a day's gonna come when you're not gonna spot it.'
>
> 'So, you're very aware, you're alert to the kind of standard phishing … [But if there's] something that comes to you from a slightly different angle, you might not be so fast to pick it up.'

[7] See also the project report on victimisation, Behind the screen, for an examination of many facets of victims' experiences, including self-blame.

Reinforcing perceptions that exposure to risk of fraud was unavoidable, for those who spend time online, was a general belief that there was little to be gained from reporting fraud attempts to the authorities. A lack of knowledge about how and where to report appeared to be a factor that deterred some from taking action; it is notable, for example, that the majority of focus group participants had not heard of Action Fraud – the national reporting centre for fraud. However, a more significant deterrent to reporting was the sense that the volume of fraud attempts was so great that reporting would be too time-consuming and unlikely to give rise to effective responses from the authorities.

> ‘[If you reported everything], you wouldn't have a life!’
>
> ‘I think it's so widespread. I don't know how it can be clamped down on really, because the internet's like, got a mind of its own hasn't it? You know, it's sort of run away with itself.’
>
> ‘I think it's happening such a lot on such a massive scale that you feel like you're just a drop in the ocean.’
>
> ‘No point [reporting] plus the time and effort to do it… So, I know it's a scam coming in. It's happening to everybody anyway. Just ignore.’
>
> ‘I have sometimes forwarded them as phishing emails. But I rarely do it because you never get any feedback to see - has anything happened as a consequence of it? And it's so common you could be doing it several times a day.’

Cautiously optimistic perceptions of containable risk

While being aware of the increasingly pervasive threat of online fraud, many focus group participants nevertheless felt confident of their ability (at least, relative to others) to protect themselves or mitigate the risk of becoming a victim. This cautious optimism about online fraud reflected their belief that they were sufficiently careful and aware when engaging in online activities; had relevant technical knowledge; and were able to detect the difference between genuine and fake offers or contacts.

The focus group discussions became sites for sharing the various methods deployed by participants to mitigate online fraud risks. Most participants spoke of having at least some knowledge or skills that helped them to protect themselves from online fraud. For example, they discussed common tell-tale signs of suspected fraud, such as spelling mistakes in emails and contacts from ‘dodgy’ or strange-looking email addresses; and they spoke about how they exercised care and discretion when considering whether to make online purchases. Some also talked about the use of specific security software, such as firewalls, as protective measures.

However, there was a recognition that the threat landscape is constantly evolving, and that the relevant skill-set and technical know-how therefore requires constant updating.

> 'For me personally, it's not much of an issue because I find it quite easy to [ascertain] what's real and what's fake, but I can understand that for other people who might not be as used to that that it can be quite difficult.'
>
> 'It can be something to be wary of. But I have like firewalls and stuff like that, so it's not too much on my mind that much.'

In some cases, the participants who felt safer and more able to manage online risks effectively felt that this was due to their age and having 'grown up on the internet'. Younger people were said to have a familiarity with the internet and online life that made them better placed than older people to 'spot scams'.

> 'I also think that the younger you are like the less likely you are to fall for online scams… So, I think people kind of grew up like that, people my age, grew up knowing that these types of things happen to them more wary anyway. '
>
> 'We grew up around computers: you know, all of us. So, we're aware.'
>
> 'I've now just been accustomed to using computers and the internet all the time. So, I always am careful when I log onto the internet when I try to insert details or choose whether to save them or not.'
>
> 'It can be something to be wary of. But I have like firewalls and stuff like that, so it's not too much on my mind that much.'

Many participants stressed the importance of caution, awareness of the potential risks arising from being online, and the associated need to exercise control over their own behaviour in order to protect themselves. This, again, suggests a tendency towards victim-blaming, with victimisation understood as something that happens when individuals 'fall for' scams because they are insufficiently careful or aware, rather than the outcome of concerted and deliberate action by fraudsters. Culpability, in other words, is thought to lie with the careless victim as well as with the offender. Perceptions of the need for self-protection are also rooted in perceptions of the state and its agencies, such as the police, as lacking the resources, expertise and powers to tackle the pervasive threat of online fraud.[8] We observed, above, that participants tended to see little point in reporting fraud attempts to the authorities.

> 'We get a sixth sense to develop. We need a second skin almost.'

[8] For wider discussion of the inherent limitations of the state's mechanisms for crime control and prevention see, for example: D. Garland (1996) 'The limits of the sovereign state strategies of crime control in contemporary society', *British Journal of Criminology*, 36 (4), 445–471; Button, M. and Whittacker, J. (2021) 'Exploring the voluntary response to cyber-fraud: from vigilantism to responsibilisation', *International Journal of Law, Crime and Justice*, 66, article 100482.

‘I think it's got to start with yourself, it's hard when something looks too good to be true. … I think you've got to take a little bit of responsibility.’

‘Because it is your own fault as well. Like, if there isn't as much help out there, I guess we have to, like, take the responsibility to learn ourselves. Be aware of it.’

‘I think there's a lot more awareness needs to be done around how we protect ourselves first and foremost, I don't think people change passwords regularly, you know, I think some people don't realise the precautions that could be taken.’

'I think you all have to be responsible, whether it's [car theft]…or an internet fraud – you do unfortunately have to think: well, what could I have done better? And if it is something as simple as lock the door or lock your car, move the car keys away, don't save your bank details on a website, don't save passwords on a website.’

The onus placed on self-protection and caution was also an intergenerational concern for the focus group participants. They spoke about the importance of experiential knowledge and many evidently felt that they had a duty to pass on information to friends, family and those perceived to be at greatest risk of victimisation. This exchange of information was considered particularly important because many people do not seem to take the risks of fraud seriously until they become victims – or nearly become victims – themselves.

‘I like to think I'm pretty savvy. But I'm concerned for my father. He's not really that intimate with it. You know, he does try. Me and my sisters are always warning him, or advising him, saying “if you get anything contact us first.” So, I think I'm pretty savvy.’

‘My parents [worked] in a bank for years and even they can get scammed sometimes because they just aren't aware of things. Like my dad works in the criminal investigations department and he's just like, not tech savvy at all. And even [he shows me] something like that, “Oh, isn't this great?” I'm like "don't press on that thing.” But he's one of those people who's meant to know about it, but he doesn’t.’

'And tell your friends or your family [about it], like if you see this scam like try not to fall for it.’

‘I think generally if you've been caught out by something, you take a closer look next time round. But I think for me it's only after the event has happened that, you know, then I'm more careful and advise my friends about it.’

Anxiety and vigilance

While many participants felt reasonably confident of their ability to contain the pervasive risk of online fraud, some tended to express more anxiety about risk – especially in the face of what was understood to be increasingly sophisticated criminal activity, such as that involving use of AI-generated 'deep fakes'.

> 'Even deepfake videos looks so real. Yeah, it's actually kind ... that kind of worries me as well. Because yeah, AI is getting out of control. You can make explicit images. You can do anything other people's faces. That worries me.'
>
> 'I think because I deal with it on a daily basis [at work], I feel worried for myself. And I've become extra wary with anything online etc., anything like that. So, I personally do think about it and worry quite a lot to be honest.'
>
> 'It's so sophisticated, and I do think as we move to a society where your doctors appointments, your bills - I mean there's such a reluctance to have anything in person now… But also people are just getting more sophisticated with it aren't they?'
>
> 'I think it's frightening because it seems so much easier to do that, to pull the wool over people's eyes. … Because we spend so much time online and you just get tons of emails and things and, I don't know, can all just get swept along together.'

The anxiety and fear felt by some participants about the growing sophistication of scams and online fraud attempts were compounded by awareness of the speed of technological change and innovation. The fast pace of change was said to undermine whatever efforts individuals make to protect themselves.

> 'You can self-educate as much as you want, but they change so much, and there's so many different types out there… So, you might already [be] educated, but you just haven't been fully protected.'
>
> 'We always have to be on it, because they're always changing.'

The perceived need for constant vigilance against the ever-changing and multiplying threats was a cause of fatigue as well as anxiety. It also seemed to generate, for some, a deepening mistrust in the digital world and its capacity to offer a sense of safety.

> 'You can't actually relax, ever … you have to double-check everything; you've got to always be savvy.'
>
> 'So I'm very careful and I am very worried. Like, is my money safe? So every morning, as soon as I get up, I look at all my accounts every day without fail. This is, like, it is not necessary, but I'm doing it.'

'I'm just gonna say it gets tiring, like, it drains your energy to avoid everything.'

'I go and check my bank account balance every day and also my other savings account and credit card accounts. I check regularly because I am quite neurotic about the prospect of fraud – you hear so much of it. … But it's time consuming and very annoying that you have to do it because nowadays there's so many things that you just can't do other than online.'

Implications for tackling online fraud

Drawing on empirical findings from focus groups with the general public, this paper highlights the pervasiveness of the online fraud threat and explores how it is variously experienced and responded to. While all of the focus group participants were aware that they were exposed to the risk of online fraud, their attitudes towards that risk varied widely. Some indicated that they were not unduly concerned about what they essentially regarded as 'background noise', or were inclined to speak confidently about their ability to navigate and mitigate risks of online fraud. Other participants experienced evident anxiety about the threat of fraud and were in a constant – and often wearying – state of vigilance.

What do these findings mean for efforts to tackle online fraud?

Paying attention to fraud attempts

Tackling online fraud reactively in response to reports of victimisation to the police and others should be accompanied by greater proactive attention to reports of online fraud *attempts.* Better understanding of how these attempts are variously experienced and responded to by members of the public, and particularly the factors that deter reporting, would enhance the effectiveness of prevention and enforcement measures and, in due course, help to protect individuals and society from victimisation.

Empowering individuals to protect themselves

Many focus group participants recognised that responsibility for tackling online fraud rests with 'everybody'. This includes members of the public themselves, as well as the police and other statutory authorities, and private and third sector organisations.

Given the ubiquity and increasing sophistication of online fraud, the possibility of 'slip-up' and becoming a victim to online fraud is widely seen as an unavoidable aspect of spending time online. Empowering individuals to better protect themselves is thus essential. Clear, concise and targeted public information – from trusted sources – about risks of fraud and how to tackle them can help replace feelings of powerlessness with a sense of agency and effective online vigilance. At the same time, it is important that public messaging does not reinforce victim-blaming narratives, but rather validates victims' experiences and makes clear that it is the offenders, not the victims, who are culpable and must be held to account by the state.

Encouraging reporting

Public information campaigns about online fraud should include a specific focus on where and how to report phishing, other fraud attempts, and incidents of victimisation – ensuring also that mechanisms for reporting are quick and easy to use. As noted above, most of the focus group participants had not heard of Action Fraud. This should coincide with public reassurance that the relevant authorities – statutory and non-statutory alike – take effective action in response to reports.

Allaying anxiety

For the focus group participants, anxiety about online fraud often reflected limited knowledge about how to navigate and mitigate the risks and not knowing what is next on the horizon. This anxiety grows in the absence of official or trusted information. In such a context, and borrowing from Cross and Kelly,[9] public information and awareness campaigns are perhaps most effective if they focus on a small part of the equation: namely, the importance of protecting personal details and money. A narrow and simple focus makes the problem seem less overwhelming and the task of protecting oneself less daunting.

> *…current fraud prevention approaches are overly complex and irrelevant from an offender's perspective. It is asserted that they are characterised by 'white noise', in that they fail to adequately articulate the critical point of any victimisation experience, being the sending of money or personal details. All prevention messages culminate in success or failure at the point where a person is confronted with the decision to send or not send… future prevention approaches need to be focused on the simplistic message of protecting money and protecting personal information. While detailed knowledge and information of different fraud types and how they are perpetrated are important, it should not be the basis for a prevention approach (*Cross and Kelly, 2016: 816).

As online fraud seeps into more and more parts of our everyday lives, simple messaging and a clear focus should empower individuals to understand the risks and to respond to them more effectively.

[9] Cross, C. and Kelly, M. (2016) 'The problem of "white noise": examining current prevention approaches to online fraud', *Journal of Financial Crime*, 23 (4), 806-818.

ANNEX: The focus groups

Twelve focus groups were conducted with a total of 96 participants, who were recruited by a market research company. Eight of the groups were conducted in person (in London and Manchester), and four online. To allow for exploration of diverse perspectives and experiences, selection of participants was based on the following criteria:

- Three groups with participants in each of the following categories
    - aged over 65
    - full-time students
    - those with (self-defined) disabilities
    - aged 25 to 65.
- Have a smartphone and use the internet daily
- Roughly equal numbers of men and women
- Ethnicity and socioeconomic characteristics broadly reflective of the population from which the group is drawn.

Focus group participants were asked to give their views on the meaning of 'online fraud'; the ways in which they had been personally affected by online fraud attempts and victimisation; their own and others' vulnerability to online fraud; the differences between online fraud and other forms of crime victimisation; and the government fraud strategy.

All the focus group discussions were audio-recorded and transcribed, and the transcriptions were subjected to thematic analysis.