

Scambaiters

Police struggle to catch online fraudsters, often operating from overseas, but now a new breed of amateurs are taking matters into their own hands

[Rosie Okumura](#), 35, frequently messes with the minds of the scammers. For the past two years, the LA-based voice actor has run a reverse call centre, deliberately ringing the people most of us hang up on – scammers who pose as tax agencies or tech-support companies or inform you that you’ve recently been in a car accident you somehow don’t recall. When Okumura gets a scammer on the line, she will pretend to be an old lady, or a six-year-old girl, or do an uncanny impression of Apple’s virtual assistant Siri. “I waste their time,” she explains, “and now so they’re not stealing from someone’s grandma.”

Okumura is a “scambaiter” – a type of vigilante who disrupts, exposes or even scams the world’s scammers. Okumura has more than 1.5 million followers across both video platforms, where she likes to keep things “funny and light”.

In April, the then junior UK health minister [Lord Bethell](#) tweeted about a “massive sudden increase” in spam calls, while a month earlier the consumer group Which? found that phone and text fraud was up 83% during the pandemic. In May, Ofcom warned that scammers are able to “spoof” legitimate telephone numbers. In this environment, scambaiters seem like superheroes – but is the story that simple? What motivates people like Okumura? How helpful is their vigilantism?

Okumura became a scambaiter after her mum was scammed out of \$500. In her 60s and living alone, her mother saw a strange pop-up on her computer one day in 2019. It was emblazoned with the Windows logo and said she had a virus; there was also a number to call to get the virus removed. “And so she called and they told her, ‘You’ve got this virus, why don’t we connect to your computer and have a look.’” Okumura’s mother granted the scammer remote access to her computer, meaning they could see all of her files. She paid them \$500 to “remove the virus” and they also stole personal details, including her social security number.

Thankfully, the bank was able to stop the money leaving her mother’s account, but Okumura wanted more than just a refund. She asked her mum to give her the number she’d called and called it herself, spending an hour and 45 minutes wasting the scammer’s time. “My computer’s giving me the worst vibes,” she began in Kim Kardashian’s voice. “Are you in front of your computer right now?” asked the scammer. “Yeah, well it’s in front of me, is that... that’s like the same thing?” Okumura put the video on YouTube and since then has made over 200 more videos, through which she earns regular advertising revenue..

“A lot of it is entertainment – it’s funny; it’s fun to do; it makes people happy,” she says when asked why she scambaits. “But I also get a few emails a day saying, ‘Oh, thank you so much, if it weren’t for that video, I would’ve lost \$1,500.’” Okumura isn’t naive – she knows she can’t stop people scamming, but she hopes to stop people falling for scams. “I think just educating people and preventing it from happening in the first place is easier than trying to get all the scammers put in jail.”

She has a point – in October 2020, the UK’s national fraud hotline, run by City of London Police-affiliated [Action Fraud](#), was labelled “not fit for purpose” after a report by Birmingham City University. An earlier undercover investigation by the *Times* found that as few as one in 50 fraud reports leads to a suspect being caught, with Action Fraud frequently abandoning cases. Throughout the pandemic, there has been a proliferation of text-based scams asking people to pay delivery fees for nonexistent parcels – one victim lost £80,000 after filling in their details to pay for the “delivery”. (To report a spam text, forward it to 7726.)

Asked whether vigilante scambaiters help or hinder the fight against fraud, an Action Fraud spokesperson skirted the issue. “It is important people who are approached by fraudsters use the correct reporting channels to assist police and other law enforcement agencies with gathering vital intelligence,” they said via email. “Word of mouth can be very helpful in terms of protecting people from fraud, so we would always encourage you to tell your friends and family about any scams you know to be circulating.”

Indeed, some scambaiters do report scammers to the police as part of their operation. [Jim Browning](#) is the alias of a Northern Irish YouTuber with nearly 3.5 million subscribers who has been posting scambaiting videos for the past seven years. Browning regularly gets access to scammers’ computers and has even managed to hack into the CCTV footage of call centres in order to identify individuals. He then passes this information to the “relevant authorities” including the police, money-processing firms and internet service providers.

“I wouldn’t call myself a vigilante, but I do enough to say, ‘This is who is running the scam,’ and I pass it on to the right authorities.” He adds that there have only been two instances where he’s seen a scammer get arrested. Earlier this year, he worked with BBC’s *Panorama* to investigate an Indian call centre – as a result, the centre was raided by local police and the owner was taken into custody.

Browning says becoming a YouTuber was “accidental”. He originally started uploading his footage so he could send links to the authorities as evidence, but then viewers came flooding in. “Unfortunately, YouTube tends to attract a younger audience and the people I’d really love to see looking at videos would be older folks,” he says. As only 10% of Browning’s audience are over 60, he collaborates with the American Association of Retired People to raise awareness of [scams](#) in its official magazine. “I deliberately work with them so I can get the message a little bit further afield.”

Still, that doesn’t mean Browning isn’t an entertainer. In his most popular upload, with 40m views, he calmly calls scammers by their real names. “You’ve gone very quiet for some strange reason,” Browning says in the middle of a call, “Are you going to report this to Archit?”

But while YouTube’s biggest and most boisterous stars earn millions, Browning regularly finds his videos demonetised by the platform – YouTube’s guidelines are broad, with one clause reading “content that may upset, disgust or shock viewers may not be suitable for advertising”. As such, Browning still also has a full-time job.

YouTube isn’t alone in expressing reservations about scambaiting. Jack Whittaker is a PhD candidate in criminology at the University of Surrey who recently wrote a paper on scambaiting. “I’m someone who quite firmly believes that we should live in a system where

there's a rule of law," Whittaker says. For scambaiting to have credibility, he believes baiters must move past unethical and illegal actions, such as hacking into a scammer's computer and deleting all their files (one YouTube video entitled ["Scammer Rages When I Delete His Files!"](#) has more than 14m views). "I think scambaiters have all the right skills to do some real good in the world. However, they're directionless," Whittaker says. "I think there has to be some soul-searching in terms of how we can better utilise volunteers within the policing system as a whole."

At least one former scambaiter agrees with Whittaker. Edward is an American software engineer who engaged in an infamous bait on the world's largest scambaiting forum in the early 2000s. Together with some online friends, Edward managed to convince a scammer named Omar that he had been offered a lucrative job. Omar paid for a 600-mile flight to Lagos only to end up stranded.

"He was calling us because he had no money. He had no idea how to get back home. He was crying," Edward explains. "And I mean, I don't know if I believe him or not, but that was the one where I was like, 'Ah, maybe I'm taking things a little too far.'" Edward stopped scambaiting after that – he'd taken it up when stationed in a remote location while in the military. He describes spending four or five hours a day scambaiting: it was a "part-time job" that gave him "a sense of community and friendship".

While the public continue to feel powerless in the face of increasingly sophisticated scams (this summer, Browning himself fell for an email scam which resulted in his YouTube channel being temporarily deleted), But scambaiting likely isn't going anywhere. [Cassandra Raposo](#), 23, from Ontario began scambaiting during the first lockdown in 2020. Since then, one of her TikTok videos has been viewed 1.5m times. She has told scammers her name is Nancy Drew, given them the address of a police station when asked for her personal details, and repeatedly played dumb to frustrate them.

"I believe the police and tech companies need to do more to prevent and stop these scams, but I understand it's difficult," says Raposo, who argues that the authorities and scambaiters should work together. She hopes her videos will encourage young people to talk to their grandparents about the tactics scammers employ and, like Browning, has received grateful emails from potential victims who've avoided scams thanks to her content. "My videos are making a small but important difference out there," she says. "As long as they call me, I'll keep answering."

For Okumura, education and prevention remain key, but she's also had a hand in helping a scammer change heart. "I've become friends with a student in school. He stopped scamming and explained why he got into it. The country he lives in doesn't have a lot of jobs, that's the norm out there." The scammer told Okumura he was under the impression that, "Americans are all rich and stupid and selfish," and that stealing from them ultimately didn't impact their lives. (Browning is more sceptical – while remotely accessing scammers' computers, he's seen many of them browsing for the latest iPhone online.)

"At the end of the day, some people are just desperate," Okumura says. "Some of them really are jerks and don't care... and that's why I keep things funny and light. The worst thing I've done is waste their time." © 2021 Guardian News & Media Limited or its affiliated companies. All rights reserved. (modern) 20211011