2.5 billion dollars lost over a decade as Nigerian princes lose their sheen but scams are on the rise

Cassandra Cross, *Queensland University of Technology*

Last year, Australians reported more than A$634 million lost to fraud, a significant jump from $489.7 million the year before.

The Australian Competition and Consumer Commission (ACCC) has released its latest annual Targeting Scams report.

But despite increased awareness, scam alerts and targeted education campaigns, more Australians are being targeted than ever before.

With all the technological tools we have, why does fraud continue to be so pervasive? And how can the damage be reduced?

Latest key findings

According to the ACCC's report, "business email compromise" fraud rose to dominance in 2019.

At $132 million, it became the highest category of financial loss reported – the first time this has happened. This usually involves using phishing and hacking to infiltrate company systems and email accounts.

Offenders can intercept payment invoices, or create their own, and funnel victims' funds into their own accounts. Businesses and individuals make their payments as usual, but unknowingly pay the offender.

Investment and romance schemes also continue to defraud victims. Reports of investment fraud totalled $126 million, up from $80 million in 2018. And romance fraud losses totalled $83 million, up from $60.5 million in 2018.

Overall, men reported higher financial losses ($77.5 million) than women ($63.6 million).

Years of statistics

Reflecting on a decade of the ACCC's Targeting Scams reports, we can see how fraud has changed with the times.

Since the first report in 2009 (which recorded $69.9 million in losses) Australians have collectively reported more than $2.5 billion in losses.

The number of reports has increased significantly. While this likely reflects a higher percentage of the population being targeted, it also represents more authorities receiving complaints and contributing statistics.

For instance, 2019 marked the first year the big four Australian banks (Westpac, NAB, Commonwealth Bank and ANZ) contributed their data.

The ‘prince of Nigeria’ needs your help

Today’s offenders have very different approaches to those of ten years ago. There were once many more stories of Nigerian princes (although these still exist).

These days, victims are most often contacted by telephone, although email, text message and social media communications are also common.

Payment methods have advanced, too, with bitcoin and cryptocurrencies becoming popular ways for offenders to receive money.

Why is fraud still so successful?

While technology has long helped scammers, it has also helped improve cybersecurity options such as antivirus software, and email filters to block spam. So why do we still have fraud?

Essentially, fraud takes a human approach. Criminals seek to capitalise on victims’ weaknesses in a calculated manner. For example, this year Australians looking to buy pets during lockdown lost almost $300,000 to puppy scams.

Offenders have also shifted their focus to counteract fraud prevention messages to the public from police and other agencies. One prime example is the Little Black Book of Scams released by the ACCC in 2008.

It provides comprehensive details of many common fraud schemes and has influenced fraud-prevention messaging across both the United Kingdom and Canada.

To counter prevention messaging, offenders now recruit Australians to launder their funds. Known as “money mules”, they are often victims themselves, asked to receive and transfer money on behalf of offenders.

From a victim’s perspective, there are fewer red flags when asked to send money to a Big Four bank account in Melbourne, compared to sending money to Lagos.

Similarly, since there has been a strong push against sending money to people you don’t know, offenders have embraced the use of romance fraud (which targeted more women than men in 2019).

Offenders develop relationships and build trust to eventually cheat victims. And as last year’s report notes, they are now initiating relationships through channels other than dating apps, such as Instagram and even the online game Words with Friends.

With a focus on building relationships with victims, fraud requests are no longer as outrageous as they once were (although this Nigerian astronaut scam was an exception).

Manipulation and monopolising on emotions

As we gain a better understanding of how offenders operate, we’re starting to learn how effectively victims can be persuaded.

Fraud relies on the use of social engineering techniques such as authority and urgency to gain compliance. Offenders often take on the identity of someone with power and status to persuade victims to send money. They also stress the urgency of the request, to stop victims from thinking too much.

Psychological abuse techniques are also used to isolate and monopolise on victims. In this way, offenders try to remove victims from their support networks and place an air of secrecy around their interactions.

And this limits a victims ability to seek support when needed.

There has been a greater recognition of the problem across government and industry. Despite this, there's still often a sense of shame and embarrassment at being deceived, and victims have difficulty reporting.

Defences for the future

The latest Targeting Scams report shows us offenders are still looking to gain a financial advantage, and will do whatever it takes. While you can't guarantee safety, there are some simple steps that can help reduce the likelihood of fraud:

- recognise your own vulnerability to fraud. Everyone is a potential target.
- talk about fraud-related experiences with family and friends in a non-judgemental way. Offenders want victims to stay silent.
- in an uncertain situation, don't feel pressured to xfrespond, as offenders rely on people making quick decisions. Hang up the phone, delete the email, or simply step back.

Now, more than ever, we must recognise the prevalence of fraud and the ways it impacts individuals and organisations across society. If we can learn from the past decade, maybe we can improve our defences for the next decade.

Cassandra Cross, Senior Research Fellow, Faculty of Law, Cybersecurity Cooperative Research Centre, *Queensland University of Technology*