CYBERCRIME, SCAMS AND IDENTITY THEFT

Motion

HON KATE DOUST (South Metropolitan) [11.23 am] — without notice: I move —

> That the Legislative Council acknowledges the complexity in dealing with cybercrime, scams and identity theft and —
>
> (a) that as scams become more sophisticated, more Western Australians are falling victim to them, resulting in larger losses;
>
> (b) the importance of fostering awareness and resilience in the fight against cybercrimes, scams and identity theft; and
>
> (c) that combating cybercrime, scams and identity theft requires cross-party support at all levels of government.

I hope we have taken the heat out after that last debate. I deliberately moved a motion that I thought we could have an adult conversation around, because this impacts all of us. As members know, I have had a long interest in this area. We were talking about cybersecurity issues when we were in opposition at length and ad nauseam. As we have come out of COVID, during which time we became more digitally aware and active because we had to—which some saw as a silver lining—one of the greater negatives out of that is that criminals have also become more digitally aware and active in how they function and operate. Cybercrime is perhaps one of the most successful forms of crime that we now have to be aware of. It does not pay attention to borders and it does not respect who the individual or the corporation is that it is attacking. It is all about the dollar. This is an issue that we need to come back to time and again, because as each day changes, so does their method of operation and their target.

A number of years ago I was in London with Hon Martin Aldridge for a cybercrime forum through the Commonwealth Parliamentary Association. We were very fortunate because we were taken to a venue I have been to twice now. The Parliament in London has its own cybersecurity room, if you like. It is off site and it is one of the most secure places I have been to. We watched in real time the attacks that happen 24/7, and as they changed from country to country, and from their time to local time. It is quite eye opening to realise the extent, volume and depth of this type of crime and the thought that goes into it. I know that it can be a challenge for both the corporate sector and government to get their head around something that is constantly changing in the manner in which those criminals operate.

In recent times we have seen via the media, and some of us in this room have probably been victim to, the very significant hacks that have occurred through Medibank, Optus and some larger companies, such as Latitude, whereby 14 million people were allegedly impacted. I think for Medibank it was over nine million and for Optus at least 100 000. I was hacked as part of the Medibank hack, and all I got was a polite letter from Medibank saying, "You've been hacked; this is what you need to think about." I want to talk about that a bit more later. Having looked at the Western Australian example from our own minister, we see from our local response to cybercrime last year that over 1 200 people were directly impacted by cybercrime, and almost $16 million was lost to individuals as a result of a whole range of scams.

There is no fixed form of scam. Cybercriminals are extremely creative in how they target every element of an individual's life. As a result of coming out of COVID and being so much more online, we are so much more vulnerable. Almost every day we see an article in the media about a victim of cybercrime. It might have been just a minor hit or it may have been a total clean-out of every dollar they had in an account. There was a story in the ABC this week that certainly resonated. A couple had gone away on holidays and their phone had been ported. I think it tracked back to the Medibank hack, and the criminals had access to all their details. Their phone had been ported and the cybercriminals were able to tap into every single account that that person had on their phone, be it banking, superannuation, retail, private medical data—whatever they had to take the whole identity. These poor people thought that by shutting down their bank accounts and everything that they were secure, but found that no, it did not stop it; they were totally cleaned out.

I have another example. One of my staff has given me permission to share what happened with her father-in-law. This is a real issue that we need to think about, again coming out of COVID and with the shift from paper mail to online mail. For a lot of our constituents of a certain age, if they are not used to dealing with online mail, they do not always understand when somebody legitimate is contacting them. I know this with my father. If he gets a text message, it may very well be from his heart consultant, but because he does not know, he deletes it because he thinks it is a scam. Then he gets a phone call asking, "Why have you cancelled your appointment?" People are very nervous. Sometimes they get phone calls. We all know about the Telstra and Microsoft scams in which people were getting abused. They deliberately target certain demographics.

We had a scammer phone my office a few years ago and for some reason decided to spill their guts, if you like, about who they target, what time they target, what budget they are on every day, how much money they had to achieve—all the details. We logged all that and provided it to Consumer Protection. It was quite illuminating about how structured and scientific their processes were to get money out of people, and I think that is a real concern. I just wanted to share with members a story of this person who is a bit close to home. She says —

> Dad received several emails and phone calls from a group purporting to be a foreign investment firm based overseas. Terminology used involved "investments, crypto currency, stock exchange.'

For some people, when they hear the word "cryptocurrency", the hairs on the back of their neck would go up straightaway. But a senior who may not be fully conversant with the language may not understand what that means. The email goes on —

> There were numerous emails/calls and Dad bought into it all. Over $20,000 was taken from Dad on the guise of being invested into the stock exchange. Dad did not authorise the full amount, it seems that they managed to gain access to Dad's account and helped themselves to most of the funds. When Dad tried to follow up, he could not get any responses and was subjected to verbal abuse at first. Then the calls and emails would go unanswered. The Bank was not at all helpful at first, but after much encouragement, agreed to refund part of the funds that had been accessed via Dad's credit card.

I think that is probably a good example of what happens to a significant number of people, particularly in the senior cohort of our community. If someone is contacted repeatedly and pressure is put on them, and if it is sold as a really good investment or they build a relationship, which I am sure they do, they make that initial bite. Sometimes it is that test of the first dollar coming out of their account, and once they have succeeded with that, it is open slather. There are some significant issues. I think they have upped the ante post COVID and we have seen not just at a state level an increase of people who have been conned and have lost significant amounts of money. If we look more globally, I understand that across Australia people have lost more than $3 billion to a variety of scams.

I have only six minutes. It goes really fast when we are talking about something such as this. I acknowledge that the state government has been running some good education programs over an extended period, and I acknowledge the contribution of a variety of organisations across the state that participate in those programs. In Western Australia about 20 different community-based education programs have also been rolled out recently. I think those things are really good and really important and I know there will be more of it. I sometimes worry that perhaps we are not getting to as many people as we need to and many parts of our community do not necessarily understand the need to be better educated. Coming out of COVID they have gained a greater understanding of the need to be private about their information, but they do not always know how to go about doing that. They do not know how to go about putting in place the mechanisms to protect themselves.

We also have to deal with issues around language barriers, and cultural issues around losing money or being conned. I think for a particular part of our community of a certain age there is an issue around not being computer literate. I am sure the minister will have some responses on that, but I think that is a significant problem area. We have all got or, hopefully, a lot of us have still got parents. Some of us are moving into that more senior cohort—we have to own it—and we need to be more careful. I was hacked a few years ago. I went to pay for a couple of items on one day and, unfortunately, it was the day before I was due to go away. I had made one payment with a credit card over the phone to the retailer and the other one face to face. A couple of hours later I got a message from my bank saying that it was shutting down my credit card because I had just bought X products in the eastern states. I said I would never buy products from those particular places, so we knew it was a scam. It took a couple of months for the bank to work through the system and acknowledge that it had been fraud and to repay it.

That brings us to the next question: what needs to be done? I think that each state and federal government has been doing some very interesting things to deal with this issue, but, as I said earlier, this whole problem is constantly changing and I do not know whether governments are always able to keep up with the speed of change. I know that we have a new federal cybersecurity commissioner. I think that is a great thing to have, but he has already come out and acknowledged that issues need to be dealt with. That is about getting the banks and the corporate sector on board and better educating people so they understand what they need to do to protect themselves. Significant work needs to be done right across the sector at all levels to educate, promote and put in place mechanisms to protect people. The idea that somebody can lose their life savings, their superannuation or in some cases their house—we have seen that happen here in Western Australia in the past—is just shocking.

These are highly corporatised and structured businesses run out of a variety of other places that are not only focused on taking our money and our identity, but are also into cyberbullying, trolling, child porn—all the nasties we can think of. I think a serious piece of work needs to be done by governments through legislation. I look to the British model. I know Hon Wilson Tucker will correct me. I think it is the General Data Protection Regulation laws. They have been updated in recent times because of the Brexit changes and they have circled the wagons, if you like, to protect themselves. There are some good models out there that we can look to. I know that the federal government

is trying to look at models. I do not know whether that will result in uniform legislation for the states, but it needs to be done in collaboration with all sectors of enterprise, with all tiers of government and in view of bringing the community on board. At the heart of it, it needs consumer protection so that consumers have the final say on how their data is looked after and utilised. That comes back to the issue around privacy legislation, which I know has been under review federally. That is also something the British government has focused on with its consumer protection under data regulations. The consumer in the UK and the European Union always has the right to decide how their data will be used.

There is a huge piece of work to be done on this issue. I really wanted to bring this up today because I know this is something people are interested in. It impacts on all of us and all our constituents. It is something that is constantly changing. As a society, we need to keep ourselves up to speed with this change. We need to make sure that appropriate penalties are in place for these criminals. The difficulty, of course, is because they are not necessarily operating within our state or our Australian boundaries—they are usually offshore—it is about those international relationships linking in. Things such as the Budapest protocols set a very good template for legislation and relationships. We are just trying to do whatever we can to reduce the negative impacts of cybercrime.

Before I finish, I just want to promote that the Commonwealth Women Parliamentarians association will be meeting today. We have received money from the Commonwealth Parliamentary Association to run training programs for women MPs to learn how to deal with cybercrime, cyber-trolling and bullying. I encourage any women MPs to come along to the training session that we will run later this year. Women MPs are also having to deal with this issue on a separate level in a range of Parliaments around the world. It is quite a hot topic. I wanted to put in that plug.

I hope members take on board these initial comments. This is a really serious issue and it is one that we need to come back to and refresh ourselves on from time to time.

HON DAN CADDY (North Metropolitan) [11.38 am]: I start by thanking my friend and colleague Hon Kate Doust for bringing this important motion to the house. Scams and the effects of scams in Western Australia have been widely reported in the media. I had a quick look. I wanted to get an idea of how often they are reported, and it is almost daily. Only a few days ago, we saw in *The West Australian* an article that outlined the number of phone scams that have been blocked by service providers. The number of scam calls that have been blocked is reported to be in the billions. More than 256 million scam calls were blocked in the three months to July this year alone. These scams target individuals. A lot of scams target businesses as well. An article in *The West Australian* of 30 May by Anthony Anderson outlined that three real estate and settlement agents had lost more than $100 000 between them after scammers had called them. These are professional people who understand their businesses. The role of a settlement agent is highly specialised. As reported in the article, in each case the scammers knew, when speaking to the settlement agents, the payments that had gone through to the dollar. This goes to the level of sophistication of scammers. If someone is presented with an exact figure in the thousands, it is entirely understandable for them to think that they are speaking with someone who is legitimate.

The government has obviously been across this issue and has taken an active role in trying to inform the public, and I will come back to that a little later if I get time. An article by Josh Zimmerman published on 31 January this year quoted the Leader of the House, Hon Sue Ellery, in her capacity as Minister for Commerce. Hon Sue Ellery outlined that criminal rackets were becoming more and more sophisticated, which was obviously borne out in my previous example. This article contains something that is important to repeat about the sophistication of scammers and how they create a sense of urgency. Josh Zimmerman quoted the minister as saying —

> "One of the most important messages that we want to give people today is to actually take the time, practice the pause, stop to think about whether what you're being asked to do is legitimate," …

I want to come back to that because I want to talk about seniors as well. I feel that our seniors are one of the cohorts that we really need to educate and protect.

I first want to go off on a slightly different tack. This issue obviously affects Western Australia and Australia, but I want to give a quick overview of some worldwide statistics because this is a problem across the globe. *The global state of scams report*, published by Group-IB in 2022, contains a couple of interesting quotes. Obviously, as the report notes, scammers are becoming more successful. One of the quotes that I want to provide is about Australia. The report states —

> … 96% of Australians have been exposed to a scam in the last 5 years …

Ninety-six per cent! That is almost the entire population. Another interesting figure quoted in the report is that in the United Kingdom, 50 per cent of telephonic survey respondents had reported being caught up in a scam in a one-month period. Hon Kate Doust talked about cryptocurrency. The report notes that the Turkish government was forced to suspend trading in cryptocurrencies, freezing more than $2 billion worth of assets because of the

problems it was experiencing. There was also a single case in Singapore in which $US6.4 million was lost. It is a massive problem all over the world, not just in Australia.

I want to pick up the third limb of Hon Kate Doust's motion, which states —

> that combating cybercrime, scams and identity theft requires cross-party support at all levels of government.

At an international level, it requires all states to come together. We need only a couple of outliers to make a negative difference. Unfortunately, although there is a lot of global cooperation, it is not absolute. I say "unfortunately" because there are a couple of outliers. One issue that I want to point out is when countries export their domain extensions. Taiwan and Poland are two examples of that, but the one that I especially want to point out is Russia. Nearly two and a half million Russian domain names are external to Russia. This problem needs to be addressed, not just at a state and federal government level, but also globally.

I want to go back to seniors because I do not have long. Unlike our younger generations who have grown up with technology and do not have to adapt to it, our seniors are particularly vulnerable to scammers. Seniors are adapting to the technology, and threats, scams and cybercrime are an extension of that. Our younger cohorts deal with those things because technology is second nature to them, but, as Hon Kate Doust said, some of our seniors may not understand the language or concepts that are put to them by scammers. That goes back to scammers using such terms to create a sense of urgency. The key to this is education. I know that Hon Dr Steve Thomas does not like this, but I will congratulate the government for its programs to educate seniors and people across the state. It is not just the government as a beast that is doing this. I want to give a shout-out to some local members in the north metropolitan region who have run forums on cybercrime, sometimes specifically for seniors and sometimes more generally. They are educating people about cybercrime and the scams that are out there at all levels. My great mate and now minister, the member for Balcatta, ran one just last Friday. I know that the member for Landsdale, Margaret Quirk, regularly runs this sort of forum. My friend the member for Joondalup, Emily Hamilton, has run several forums. They are some of her best-attended forums, with large numbers of people coming along. I have seen the same thing happen in Burns Beach as well.

Hon Martin Pritchard: And in Hillarys.

Hon DAN CADDY: I was just getting to Caitlin Collins, who is one of the hardest-working members of the lower house. She has run forums as well and has reported a massive number of attendees. I know that the member for Churchlands has done them. I know full well that the member for Nedlands has run more than one—I think she did one with Hon Sue Ellery in her capacity as minister—because I heard all about it from my mother who attended. She loves reporting back to me on exactly what happens at community forums. She goes to every community forum that she can. It is kind of cute and kind of not.

Hon Kate Doust: Is that the only chance she can get to see you?

Hon DAN CADDY: That may well be the case, Hon Kate Doust. I know that I have missed some members in the north metro region. I know that John Carey has done them as well. Apologies to any of my colleagues whom I have missed. I just wanted to make that point because education, and especially education for our seniors, is everybody's responsibility. I am sure that members opposite have done this as well. It is everyone's responsibility. Seniors are a cohort that we really need to look after.

HON TJORN SIBMA (North Metropolitan) [11.48 am]: Bearing in mind that this is private members' business, I will make my remarks very brief. I think this is a truly excellent motion. There are opportunities for this chamber to concentrate on vectors of threat—issues that are effectively metastasising at a great rate throughout the community and compel us to some action. Hon Kate Doust and Hon Dan Caddy highlighted the point that everybody is affected by this. I have been affected by cybercrime, too, in a way that I think will probably resonate with individual members in this chamber. It is a crime that gets you when you are sleeping. It is a confronting and really pragmatic problem to wake up one day to find that your credit card has been cancelled, particularly if it is a joint account with your wife, because there have been some really weird transactions made in Istanbul, Paris or wherever, which bear no relation to any of your own transaction conduct.

From personal experience, I must say that dealing with my bank was woeful. The banks themselves have a lot to do to improve their security and to improve their responsiveness to customers who are affected by this, without undertaking any activity, without being at fault even to a small degree. I am also a customer of Medibank Private so I have been caught up in that scam as well.

Hon Kate Doust: I hope you didn't get the trifecta.

Hon TJORN SIBMA: Not yet, and I say "not yet" because there is a degree of thinking: what next? If your personal identifying data is released and effectively exchanged by a connection of legitimate and illegitimate intermediaries—your data is onsold—you do not know when the next scam is coming. I filled out a survey a couple of years ago in Western Australia. As a protection, I used an alias. About six months after I completed that survey, I received a number of calls for other surveys or unsolicited offers using the alias. The alias I used was "Stefan"—I just made

it up. Communications to Stefan offered me all kinds of cryptocurrency deals and a range of other exotic financial instruments every other week. Who is that person? It is a fictitious character but it illustrates the point —

Hon Sue Ellery: It's your evil twin brother.

Hon TJORN SIBMA: By reflection, that must mean I am not evil. I will accept that glowing character endorsement!

Limb (c) of this motion is critical because this is something that we, as representatives of our communities, have a joint responsibility to help people solve. It is a reasonably valid observation that some members of our community are more vulnerable or susceptible than others to this kind of criminality. Our conversation has focused on seniors for understandable reasons because of technological developments and a degree of computer or mobile phone illiteracy. They are also, to a degree, condemned by their own politeness. Being a politician, I treat everybody equally suspiciously. I do not want to respond immediately to anything, but there is a cultural disposition among many of our seniors just to entertain, to be polite, and that is a disposition I think is preyed upon.

However, there are other vectors of risk and I do not think young people are entirely immune from the predations of these criminal enterprises either. I have young children. At some stage they will get into online gaming. That will open up a portal of risk to them and my home. It has also struck me that young men between the ages of 20 and 25 years are increasingly susceptible to a kind of romantic scamming, which is probably the politest way of putting it. They volunteer intimate images of themselves and have the images used as extortion against them. That underscores another dimension to this; when people are caught in a scam, they feel embarrassed. The Leader of the House put out a media statement earlier this year attempting to quantify the dollar value of scams. I think it was around $15 million. I suspect a lot of it would be underreported.

Hon Sue Ellery: It's huge. Only about 13 per cent are reported.

Hon TJORN SIBMA: Being aware of that, it should start turning the wheels of cogitation and policy making about how we destigmatise being a victim of this or provide people with, to a degree, anonymous reporting. A lot of people are bedevilled by their own circumstances but I think a consistent view that has been expressed to me by individuals who come to the office and say this has happened to them is that they do not want this to happen to somebody else. They do not want this to happen to somebody else's mother or brother, or small business. That is another dimension, which is probably not intentionally overlooked but overlooked in the conversation. Small to medium business enterprises, which must have an online presence to be commercially viable, are also at great risk of having their business enterprises derailed by successful scams. I am not sure whether we have established the mechanisms at a state or federal level, or at the banking level, to address that.

That is all I want to say at the moment. I absolutely commend this motion. I am particularly seized by the third limb. If I were to venture a suggestion, this is the kind of issue that justifies the creation of a select committee of some kind of this Parliament to look into our framework in Western Australia and its interrelation with commonwealth laws and perhaps international laws. We might be able to do something good for our own people.

HON SUE ELLERY (South Metropolitan — Leader of the House) [11.56 am]: I want to thank Hon Kate Doust for bringing this motion to the house because this is a very important matter and one that bedevils us all as we try to keep up. We are not even trying to get in front because they just keep moving so fast. Hon Tjorn Sibma made the point that this happens while you are asleep. That is a good point because at 11 past three this morning, I received a text message. I sleep with the phone right next to the bed. I have an elderly father and another elderly family member. It is not unusual for me to get calls at all times of the day or night to take somebody to hospital. This was the message: "AUS.taxx+.mygov: Read new unread refunds message. Click here." Then there was a link. The most appropriate response was to delete it but I knew I would be talking on this motion today so I thought, at 11 past three this morning, "I'm going to take a screenshot of this" then I deleted it.

Scams are everywhere and getting us everywhere. I was caught up in the Latitude Financial Services scam. I did not even know what Latitude was but it provided a service to another organisation that I used probably about 10 years ago. As a consequence of that, my identity was caught up in that scam. It is happening every day, increasingly. The top scam is phishing and the most highly reported one is the "Hi Mum" scam. People get a message from someone claiming to be their child, saying they are in trouble and have lost their phone or it is broken, and they need help. It is specifically designed to appeal to the inner need to respond and to protect. It catches people pretty much every day. The second-highest form of scam is classified ads on social media like Facebook marketplace; it is people selling things. We did an event last Thursday or Friday about how to avoid dodgy car deals. A woman there told the story that she purchased a car online for $4 500. There was a photo; she did not go and see the car. She purchased it on the basis of a photo. She transferred the money. The next thing she got was a text message telling her that the car was in Darwin and there was a $2 000 transfer cost, which she needed to pay now. That is what triggered her so she rang WA ScamNet. They said to her it was most likely a scam and they tried to help her. She did not get the $4 500 back. She has had to purchase another car, having said goodbye to that money.

Other scams include fake online shopping websites and romance scams or sextortion, which appeal to people's vulnerability. I find this hard to believe, but I know of a woman—she lives next door to my friend and I have seen

her occasionally at events over the years—who genuinely believes that she has been married to a man in Nigeria for 10 years. She sends him money. She is a professional. She thinks she is married to that guy. Her family have made enormous interventions; they have cut her off financially because they could not get through to her that the marriage is not real. Romance scams appeal to people's most inner vulnerabilities and absolutely destroy lives, which is why this government takes them seriously. One of most important things that we do is work with the federal government, which I will talk about in a minute.

WA ScamNet, which is run by the Consumer Protection division of the Department of Mines, Industry Regulation and Safety, works with Crimestoppers, the Western Australia Police Force, the Australian Competition and Consumer Commission and the Australian Securities and Investments Commission to support victims of scams. The top tips, which have been mentioned, are to always be suspicious. If people catch themselves wondering whether they should be suspicious, the answer is yes, they should. As one member said, they should practise the pause. They should stop. The hardest thing to get across, particularly to older people, is that they do not need to immediately respond. There is nothing so urgent that they cannot take the time to ring somebody or check the information. People should stop and think and run the situation they are being asked to respond to by somebody else before responding. Another thing to note is that Consumer Protection recently teamed up with IDCARE, a not-for-profit organisation that provides identity and cyber support services to help the thousands of people whose identities have been compromised. One of the things it talks about—other members have mentioned this—is encouraging people to speak up and get over the embarrassment of feeling like a fool because they have been caught up in such a situation. That is an important part of the message that we want to get across to people.

Just a couple of months ago—I think it was in May—Stephen Jones, the Assistant Treasurer and Minister for Financial Services in the Albanese government, was in Perth as part of the budget rollout. He talked about the federal government's $86.5 million package to combat scams and online fraud, which was headlined by the establishment of the National Anti-Scam Centre. The importance of that is that the federal government controls the levers around banking regulations, telecommunications and a range of other levers that the state government cannot control. Having both state and federal governments on the same page to address some of these issues is really important. I was delighted to join Stephen Jones as part of that announcement.

I know that other members want to speak. The state government takes this issue seriously. We are actively engaged in educating people about how to protect themselves. I encourage members to take advantage of the information that is available through Consumer Protection to help their constituents and, again, commend Hon Kate Doust for moving this motion.

HON KLARA ANDRIC (South Metropolitan) [12.03 pm]: I, too, thank Hon Kate Doust for moving this very important motion in the house today. Like the Leader of the House, I received a text message—but it was this morning, not in the middle of the night—because, for the first time, last night I accessed Coles shopping online because I had no food to feed my children. I need a delivery today otherwise I will be in trouble! When I got home from Parliament last night, I used Coles online shopping for the first time. This morning at 10.00 am, I received a text from the same number I received a text message for the two-factor authentication from Coles last night. It read, "This is your pin. If this is not you, please call us on 1 300." It was not me so as soon as I get out of here, I will call Coles to say that it was not me and ask that it does not forward any of my details. Hopefully, the two-factor authentication code will assist in making sure that whoever is trying to use my credit card will not be able to do so. I thank Kate for bringing this motion to the house because it is a real issue in our community and it is making people nervous. Similar to Hon Dan Caddy, I, too, believe that education is key in ensuring that as many people as possible avoid being scammed.

In 2022, Hon Simone McGurk, the member for Fremantle, and I hosted two cybersecurity sessions, one in Fremantle on 14 September and the other in Spearwood on 12 October at one of my favourite clubs in my electorate, the Dalmatinac Sport and Community Club. Approximately 120 people attended those cybersecurity forum sessions. They were a huge success. Many of the community members who attended were happy to ask basic questions such as "Should I keep Facebook or am I being compromised?" The purpose of those forums was to educate people in the electorate on cybersecurity and scam awareness and give them tools to better identify a scam and protect themselves and their online information from scams such as the ones I often receive from what is claimed to be Australia Post and the toll people. Thankfully, I know that we do not have road tolls in WA, so I know that those texts are scams. The avenues that these people—I do not like to use the word "vultures" but they are vultures because they prey on the most vulnerable—go to to commit these sorts of crimes is absolutely outstanding.

Hon Darren West: Sleazy.

Hon KLARA ANDRIC: Hon Darren West can say that, but I will not. I will leave that to the honourable member.

Dr David Cook, a lecturer at the School of Science at Edith Cowan University, presented at the two forum sessions. Dr Cook is a member of the ECU Security Research Institute, a member of the Australian Centre for Cyber Security Excellence and a Fellow of the Australian Computer Society. He told the 120-or-so attendees the basic things that

they can do to protect their themselves and their passcodes and who they should and should not share their information with. The other presenter at both those sessions was Senior Sergeant Debbie Barrett from Murdoch Police Station. Debbie was there in her capacity as a police officer who often deals with people's complaints about potential scams and having been scammed. As Kate said, and as it is stated in her motion, a multi-tiered effort is required to educate people about what they should and should not do and the things to look out for. It takes a multi-tiered effort to combat cybercrime.

I am not sure I will have too much time to talk about this, but one of my favourite episodes on Australian television is an episode of *Gogglebox. I* do not know whether members know about this show; it is a program about people who watch TV. It is bizarre. Only the other night I was watching *Gogglebox*. The episode was on deep fakes. This was the first time I had ever heard the term "deep fake". Essentially, a deep fake is a fake video. It is classed as a manipulated medium consisting of advanced artificial intelligence techniques to create fake content. I am talking about deep fakes on this motion today because I want to use it as an example of just how far these people have come in the intelligence and techniques they are using to create videos. There was a video of Barack Obama making commentary about the previous President of the United States. Although I knew that that video was fake, I did not necessarily disagree with the comments in that fake video of Barack Obama about former president Donald Trump! With all of this, I am trying to say that the technologies have improved to the point at which we do not know what the future holds. These people are very skilled, and that raises a lot of concerns. The moral of the story is that these people are becoming very sophisticated.

The Leader of the House and some other members have already gone over government programs such as WA ScamNet. I believe Hon Sue Ellery mentioned the 2022 annual report. It showed a financial loss to scams of almost $16 million. That is an incredible amount. It also recorded that a seven per cent increase to consumer loss had occurred compared with 2021. There were 2 417 reports received by ScamNet in 2022. As mentioned by previous members, a lot of this comes from romance scams. The highest financial loss in WA from a romance scam was one person losing $800 000—I stand to be corrected, but I believe that is what I read. The data showed that online shopping is one of the biggest scamming mechanisms. Yes, it predominantly affects older people, but a staff member of mine, Joe, just recently accidentally entered his details when he received the AusPost scam about a delivery being redirected and lost $500 on his credit card. I do not normally shout out to banks, but I do give a shout-out to Bankwest for saying it would refund him the loss because it was the result of a scam. My mum left for Europe following the "hey mum, hey dad" text scam. She said to me, "If anything happens when dad and I are overseas and I need money, we lose money or God forbid"—in her words, as she says!—"and I need to send you a text, we need to have a secret code word." It is not as if we do not FaceTime nearly every second day, anyway! I asked her what she meant and she told me that there were these tech scams with parents and kids and she wanted to make sure that we were not caught up in that. I have subsequently forgotten the code word—do not tell Mum! Nevertheless, people are genuinely worried about all of this, and rightfully so. I have to wrap this up, but I have copies of a book put out by the by the Australian Competition and Consumer Commission called *The Little Black Book of Scams*. It is a fantastic book. I have 10 copies if anybody would like one in their electorate office or to have a look through it. I note those members. It is a fantastic book and a great guide for constituents on how to avoid being scammed.

HON SHELLEY PAYNE (Agricultural) [12.13 pm]: I, too, would like to thank Hon Kate Doust for moving this motion today. It is a very important motion. She talked to bit about education and the work the government is doing. Hon Klara Andric talked about some of the forums she has held, and that is really great. I commend Minister Sue Ellery on a lot of the work she has been doing online with the Cyber Security Awareness Toolkit. She was formerly Minister for Education and Training and I note all the work that North Metropolitan TAFE is doing on its cybersecurity training centre, which is the first centre in WA to offer certificate courses in cybersecurity. As part of our partnership with the federal government there are free courses and people can do an introduction to cybersecurity skill set. A lot of good work has been done on training. The North Metropolitan TAFE website talks about the absolute shortage of people working in cybersecurity. This is a great initiative by North Metropolitan TAFE, and some of the other TAFEs are coming on board.

Hon Tjorn Sibma briefly talked about small businesses, and I want to talk a bit about the impact of scams on small businesses and mention some of the work the Small Business Development Corporation is doing, through Hon Jackie Jarvis as Minister for Small Business, on helping small businesses understand some of the risks. In my area in particular, the Agricultural Region, there are a lot of small family farming businesses, and I want to talk about how some of these scams have been affecting them.

A couple of years ago, we heard a lot about fake websites selling agricultural machinery, and I think last year there were losses of over $1 million. I commend the work of the WA ScamNet site. Members can go to that site to see all the fake agricultural machinery sales sites. There have also been quite a lot of scams with the sale of livestock and things like that. Of concern of late has been some of the scams hacking into the online systems of small businesses. I have one constituent around the Newdegate area who runs his own farming operation. He also leases a couple of neighbouring farms owned by a Chinese company. He makes his lease payments twice a year. He made his

$66 000 payment in January last year and he received his next invoice that he needed to pay by the end of August, and noticed it had different bank details. He tried to ring up the company to ascertain whether there had been different bank details and ascertained that the details had changed. He made the payment and it turned out the payment never went through. It had actually gone to a scam location. It was quite fortunate that there is a 10-day delay for overseas electronic payments, and, about 12 days later, he managed to get his money back from Westpac. He told me that quite a lot of other farmers in the Lake Grace area had been affected, probably half a dozen of them, by the same scam. One farmer even lost $450 000 on a house payment.

Another farming family just north of Esperance was similarly impacted recently through one of its grain contracts worth one-quarter of a million dollars. Someone had hacked into their system and made a fake invoice with changed bank details. Because there is a lot of trust in these supplier relationships, the change of bank details was taken on face value and the money was sent through. The money did not go through. That is because some of these scammers change their bank accounts very quickly to avoid detection so that when a second request goes through to change bank details again and use another account, it makes the proponent think that they had better ring to check. When the proponent rang the farming family, they found out that it was a scam and that their whole system had been hacked.

This has also happened to some of our machinery suppliers in Esperance. An invoice went out for a header for $450 000—these headers are pretty expensive. The invoice was intercepted and the payment details changed. The person who was buying the machine obviously got an invoice with the wrong details. It is now really common for a lot of Esperance suppliers not to put any bank details on their invoices so they can avoid a lot of the stuff that has been happening.

I also want to bring up another thing because we have not talked much today about identity theft. I want to talk about a staff member in my office. Earlier this year she had a case of identity theft that caused her extreme stress. I will tell the story about what happened to her. She got a text from MyGov saying her email address and contact details had changed and advised her to phone a 1800 number if she had not made the changes. She went online to her MyGov account and found out that her ATO was linked, but she could not access it. When she rang up she found that someone had hacked into her system. They had hacked into the ATO, submitted a tax return and changed previous years' tax returns. They had changed bank details and had tax refunds sent to an overseas bank account. She had to go through the stress of trying to work this out. Incidentally, she had a lot of help from IDCARE, which Hon Sue Ellery talked about earlier, that we are partnering with, and they were very helpful. Rob Blackmore helped her out a lot. She recorded it through the WA police website, which was very helpful in telling her to go to the Scamwatch federal website where she got advice about how to secure her details—because her superannuation is attached to the ATO—how to secure her bank accounts, her phone accounts et cetera.

She had to set up a new MyGov account. She can never, for the foreseeable future, file tax returns or have a link with ATO through her MyGov account. She has to call the fraud unit at ATO every time she wants to access the ATO online, then it will give her 24 hours' access before she has to phone again. She has a child who goes to child care and this had a huge impact with Centrelink because there was a hold on the ATO and an incorrect tax return filing, and then Centrelink was on her back wanting her to repay the amount she had received for the year for her childcare rebate. It took a lot of effort for her to go through and work that out. Fortunately, she worked it all out, but it has been extremely stressful. I wanted to tell that story. I will tell one more scam story. Hon Kate Doust talked about how they will sometimes just take a dollar and from there they will go on to get other details —

Hon Kate Doust: Then they'll take the rest of your money.

Hon SHELLEY PAYNE: I do not know whether members have had a package delivered and received a text with an instruction to pay $1.50 to get the package redirected or delivered on a different day. It is funny, I was with my dad the other day and he was telling me that he was expecting a package. He told me, "Oh, my package isn't coming today. I've had to go online and select a different day, so it is coming on Sunday." Everything was fine, he paid his $1.50, then the package arrived on his doorstep that afternoon. I said, "Dad, didn't you just change that?" I looked at the email he got, which looked legitimate until I clicked on the email address and it was a different email address. When I clicked through it looked like a legitimate website, but when I clicked on the bottom, nothing worked. He had to cancel his credit card because he realised they now had his credit card details. When you are old and have payments coming out of a credit card every month, it is a real pain in the arse to set up all the automatic payments again for all the different companies. I commend the government for the work it has done in helping to bring this to the forefront and educate people on how they can be aware of scams, and I thank Hon Kate Doust for bringing this important motion today.

Motion lapsed, pursuant to standing orders.