**Teachers Mutual Bank**

**Podcast 2 – Scams**

**Announcer:** This is a Queensland Department of Education podcast.

Proudly sponsored by Teacher’s Mutual Bank. The bank founded by teachers for teachers.

**Virginia Bowdidge:** This podcast is for education and entertainment purposes. Any advice offered is general financial advice only, and it doesn’t take into account your objectives, financial situation or needs. Because of this, you should consider if the advice is appropriate before acting. If you do choose to buy a financial product, read the product disclosure statement and obtain appropriate financial advice, tailored to your needs.

Scams and fraud are on the rise in Australia. They are getting increasingly sophisticated and can be very hard to detect. Despite warnings, frequent media coverage, and the work of various agencies and businesses, Australians are losing more money than ever – currently in the vicinity of $2 billion a year - to scams.

I’m Virginia from the Department of Education and joining me is Michele Oliver from the fraud department of Teachers Mutual Bank. Michelle is here to help us understand what to look out for when it comes to scams is.

Welcome Michele.

**Michele Oliver:** Thanks for having me, Virginia. This is such an important issue for people to be aware of – I’m really thankful for the opportunity to get the message out.

**Virginia Bowdidge:** So, Michele, I touched on the enormity of this this issue, but could you explain how has it become such a big issue? Surely, something can be done about it?

**Michele Oliver:** I think it’s really important to start by understanding that these scams are often run by organised crime.

This isn’t just small-scale individuals stealing someone’s credit card or selling something that doesn’t exist. Even though that does happen.

These are large criminal professional enterprises who are getting increasingly sophisticated at how they go about it. And the people that work within these criminal organisations are professionals, who are highly skilled at stealing money through fraud, deception and manipulation.

They are highly opportunistic – and with all the stress and change of the recent years with COVID and natural disasters, financial pressures combined with an increasing reliance on the internet. It’s creating a perfect environment for these criminals to prosper.

Unfortunately, it’s a growth industry and definitely not the kind of industry we want at all, let alone growing.

**Virginia Bowdidge:** That does sound quite frightening. How have they become so successful and how do we protect ourselves?

**Michele Oliver:** Manipulation of people’s emotion is really where a lot of scammers shine. Whether it’s appealing to a person’s desire to make money, or to not be lonely and have companionship or to misrepresent themselves as an authority or even someone you love who is in trouble, scammers have multiple ways of getting people on the hook. And once on the hook, they know how to manipulate and get people off balance, so they aren’t thinking clearly enough to recognise the risks.

They have a lot of tricks, like creating a sense of urgency – if you don’t do this today you’ll miss out or something dire will happen. Or they could be trawling social media looking for clues around if you’re busy or travelling or even children’s names. They can pick up on the smallest bits of information and use it against you to their advantage.

I can’t reinforce enough the importance of not giving into demands or requests immediately.

Take a moment.

Walk away, put down the phone. Call a trusted friend or family member. Even check some websites including Scamwatch or Cyber.gov.au.

Stepping away and taking time to think and gather information is a great way, to avoid getting sucked into a scam. Which is why scammers will try manipulate you to ensure you don’t do that. They want you making quick, rushed, emotionally charged decisions and it works for them not for you.

**Virginia Bowdidge:** Thanks Michele I’ll list those websites in the transcript. Can you give us some examples of current popular scams?

**Michele Oliver:** Of course. But how about we give your listeners a chance to work out how scam savvy they already are, while we do so?

**Virginia Bowdidge:** That sounds interesting.

**Michele Oliver:** So, you decide to sell some of the things your kids have outgrown on Facebook marketplace. You get a good offer from someone and they will pay via credit card, but they pay even more than you agree. They contact you and explain they made a mistake and ask you to refund the excess by an online banking transfer to their account.

So Virginia, do you think you should send them the money?

**Virginia Bowdidge:** I don’t think so, it sounds a bit dodgy to me.

**Michele Oliver:** Great pick up. Overpayment scams are very common. At the heart of them, the original payment is usually cancelled so you don’t receive that money in the end and you’ve also lost the money you sent them. And you’ve lost the items you were selling if have already sent them.

So make sure you never refund money to a different account or through a wire transfer. And don’t be afraid to tell people, you’ll need to wait a couple of days until the funds have cleared, before you’ll send them anything or take any action.

Now, how about you get a call from someone professing to me your IT department and they need to take over access to your computer to install some new security software and scan to make sure you have any viruses? Do you give them access?

Signs to watch out for in this scam” Somebody makes an offer to buy something you have for sale and pays you more than the agreed price with a cheque or credit card. You receive an email from the scammer claiming that they have made payment but the amount is being held until you have forwarded on the extra amount. You are asked to refund or forward on the overpaid amount to a specific bank account or through a wire transfer.

**Virginia Bowdidge:** Is it someone I know from work?

**Michele Oliver:** No, he says he’s just joined. And he works remotely so he hasn’t been able to meet you yet.

**Virginia Bowdidge:** Is it someone I know from work?

**Michele Oliver:** No, he says he’s just joined. And he works remotely, so he hasn’t been able to meet you yet.

**Virginia Bowdidge:** Well, I have had to give IT remote access before, but I’m not sure about this case scenario.

**Michele Oliver:** I can see you’ve got good instincts. You should definitely not give remote access then and there. It’s very likely a scammer, who’s trying to gain access to your bank accounts and other important information that you have. Once they have access these, they can access any site where you’ve saved your passwords in your browser.

If there’s a chance it is a colleague, it’s okay to hang up and go and check the internal directory or send a message to your Help Desk. They’ll be glad you’re playing it safe.

**Virginia Bowdidge:** Some scams seem like they can expose use to greater losses than others. What are some of the other more serious scams where should be on the lookout for, particularly around our banking and finances?

**Michele Oliver:** That’s a great point, Virginia. Not all scams have the same potential impact. Some might steal from you, others would potentially take your entire savings. Others can steal your identity and that can have devastating impacts for you. That said, it’s important to remember that for some people, losing $100 is as devastating to them as losing 10 times more money to someone else. So, it’s important we stay vigilant and report even the smallest scale and don’t just write it off to experience.

That aside, banking scams are increasingly common and you do not want your banking information to get into the hands of the wrong people. There are a couple of things to be on the lookout for. Phishing, that’s with a P-H and spoofing. Phishing is where you get a spoofed email or message pretending to be from your bank or someone like Australia Post or the ATO. That encourages you to provide sensitive data that will be used to access your account or steal your identity.

The messages are linked to spoofed websites that could even look like your bank’s website, but you have a slightly different address. So, then a click on a link in an email or message, that is asking you for sensitive information.

If your bank is asking you to do something, type your bank’s online banking address into your browser and access your app directly, not through the link. And there are a few other things you can look for. Hover over a link to see what the underlying address is. Look for slight discrepancies in the address. Spelling errors and grammar errors can be another giveaway, as is addressing you by your proper name. But some scammers are so sophisticated now, they’ve stopped making the obvious errors. So, if in doubt, don’t respond to the email, find an alternative way to contact them by using a verified and reputable contact method, not from the email. And ask a company representative about the email.

**Virginia Bowdidge:** Thanks for the tips to protect yourself and your money. But what about people who are looking to make money? How do they keep themselves safe from some of the investment scams we hear about?

**Michele Oliver:** So, investment scams are another area of incredible growth and sophistication. There are so many variations too: government bonds, crypto currency, real estate. No investment type is immune. The scammers are very organised, even down to the fact they have set up fake websites and email addresses to catch people out. Investing money always comes with risk. But these days you need to be extra careful that you are actually investing and not just giving your money over to a criminal. Email addresses from investment companies or any firm that serious, will come from a registered domain address, but even these can be spoofed. I recently helped a member who sent me an email supposedly from an investment company in Sydney. I investigated and found out that the person no longer worked for the company and had left six months ago, but the email had looked to be from him as his old workplace address. Another member carried out all transactions online and when asked if he could meet with the person face to face, the deal went sour and communication was abruptly halted. So, all that glimmers is not gold. Remember, if it sounds too good to be true, it probably is. But it doesn’t have to be an exaggerated claim to make it fraud. Do your homework. Don’t just take the phone numbers these people give you as gospel. Try to find them another way and contact them via that avenue. Meet them in person if you can, but even then they may still be scammers. Go to a reputable company who deals with investments. Don’t just delve into the world without prior knowledge. Get a second opinion from a professional in the field, who can help you check they have the right licences and verify them with any parent company they claim. Go to the ASIC website, the ACCC as well. They have a lot of information on their website. Check ASIC offers list database. ASICs connects professional registers, Moneysmart companies you should not deal with, International Organisations of Securities Commission, the IOSCO, Investor Alerts and also Moneysmart’s face regulators and exchanges.

**Virginia Bowdidge:** Can we just check them online? Can you just go to the website and check them, or do you have to register or is it different for each one?

**Michele Oliver:** No. You can just, you can just go to the websites and check them.

**Virginia Bowdidge:** Okay, great. That makes it a bit easier. So, in general, what is some good tips to remember?

**Michele Oliver:** Well first off, check everything. If something sounds too good to be true, it probably is. Police, the ATO won’t ask you to buy and sent giftcards. Create a secret codeword with your families. If they ever need to ask you for help, you can ask for the magic word. If they can’t give it to you or try to argue why you shouldn’t, then you know that it’s not them. Second, your data and online identity, is a precious commodity. Treat it carefully and with great respect. Protect the privacy of your personal information. Cause there are scammers out there, trawling for personal data they can steal and use for financial gain. If someone is pressuring you to make a quick decision or if someone is manipulating you through pleads for immediate help, especially if that help is financial, don’t do anything until you’ve had a chance to talk it through. Take a moment, walk away, put down the phone, call a trusted friend or family member. Check websites including some of the great government sites. Stepping away and taking time to think and gather information is a great way to avoid getting sucked into a scam. And if the worst does happen, and if you do fall for something and your financial details have been compromised, call your bank immediately. You may also want to stop your credit card.

**Virginia Bowdidge:** You mentioned creating a secret code for family members, is that for those WhatsApp scams that I’ve heard about in the media?

**Michele Oliver:** Yes. TheWhatsApp or the hi mum scam that some people refer to and that is where your so-called daughter or son will contact you via WhatsApp on a different number and say they have lost their phone, or some people have even said that they’ve phone’s gone down the toilet. And they need to send money or pay a bill quickly. So, the only way that you can really verify they’re you son or daughter, is perhaps with a secret codeword.

**Virginia Bowdidge:** What about using your credit card for payment, rather than direct debit if you’re not sure?

**Michele Oliver:** So, with the good thing about credit card or your Visa debit card, is a much better way of payment. Specifically because those particular companies have chargeback rules that we can use, if a payment goes astray or you don’t get the goods or services that you want. If you give someone your BSB and account number, it’s much harder to get that money back.

**Virginia Bowdidge:** It sounds like we have to be constantly vigilant about scams.

**Michele Oliver:** We do.

**Virginia Bowdidge:** Well, thank you for your time, Michele. It’s really interesting to hear all about those scams. It’s quite terrifying actually. I’m always quite-

**Michele Oliver:** Yeah.

**Virginia Bowdidge:** Paranoid about it. But thank you for your time and thanks for telling us all about them.

**Michele Oliver:** No worries. Thank you, Virginia. Thanks very much.

**Virginia Bowdidge:** We hope you enjoyed today’s podcast.

We need to remind listeners that this podcast is for education and entertainment purposes. Any advice offered is general financial advice only and doesn’t take into account your objectives, financial situation or needs.

Because of this, you should consider if the advice is appropriate before acting. If you do choose to buy a financial product, read the product disclosure statement and obtain appropriate financial advice tailored to your needs.

**Announcer** You have been listening to a Queensland Department of Education podcast.

The Department of Education acknowledges the Traditional Owners of the lands from across Queensland. We pay our respects to the Elders, past and present, for they hold the memories, the traditions, the culture, and hopes of Aboriginal and Torres Strait Islander peoples.