PENNY HOLBURN COACHING

It's about You and Results

Outsmarting the Scammers

26 March 2026

Last year, 2025, I had two clients who had family members who were defrauded by scammers and subsequently committed suicide because of the losses sustained from the scams. The one was also receiving treatment for cancer and so it was a particularly difficult time for her. Then of course there are thousands of other people who are also caught up in scams, some of which damage their lives more than just financially. Unfortunately, the world we live in requires that one of the life skills we need to develop is to be able to spot the unsavoury characters that prey on innocent people. And once we have detected them, to be able to get away from their clutches.

Now you may think that it is easy to not get caught in a scam. If you are careful and not naïve, many people think you can't get scammed. That is not the case. Scammers today make huge amounts of money and are very sophisticated in whom they target and how they target their victims. They tend to select people who they think are very trusting and giving and see the good in people. So, women, and people in the helping professions are often targets. The elderly and young adults, and even teenagers are also targets. They don't just target you, they study you. They study your habits, your interests, your personality, your friends, your location, and more. They learn exactly how and what will hook you. They tailor their persuasive language to your psychological profile. They prepare for any questions you may ask to verify their authenticity and usually have someone or some place on hand to be able to produce whatever it is that you want in order for them to prove they are legitimate. If you ask to speak to someone to verify they are who they say they are, they will provide someone. If you ask for accounts or financial statements or bank transactions as proof they are telling the truth, they will provide them. If this is starting to sound scary, it should. Scammers have a lot of resources to back them up. They are forever finding new ways to con people. They know what people look for and will ask. They know how to build up a relationship. They have practiced an answer to every question you are likely to ask them.

Below are some points to bear in mind. In this article I cannot cover everything and of course new ways to scam people appear weekly, but note all the points below and if you are concerned you might be scammed then read and research even more. Often financial institutions and the media publish information and messages around the types of fraud scams going around and how to avoid getting sucked in to them.

1. Be careful of the personal information you communicate. If you are seen as someone who is generous and kind, you are more likely to be a target. If people think you are extremely

wealthy you could also be a target. You don't have to change who you are as a person, just don't tell everyone everything about you.

2. Never, ever share your passwords or pins with anyone. No one, not even your bank needs to know these. And don't carry them on your person where it is easy to get hold of them. When you do use a pin or password, place your other hand as a cover over the hand typing in the information.
3. If someone wants a copy of your identity card, driver's licence, or passport check them out several times before they get it. Identity theft is common. And it is not fun to fix.
4. Do not click on any email, SMS, or WhatsApp links unless you are expecting a link and you are 100% sure who the link is from. And if you are not sure rather wait 24 hours than click on anything. If you can phone or text someone to confirm they sent the link then do so. There are endless scams trying to get your banking details. If you are getting a refund phone and check that you are getting a refund in another way. If an attachment ends with .exe, don't open it.
5. There are a lot of scams linked to recruitment. Check the source of any messages or links. Google the company or person and see if either exist. Phone and check the existence of the company and the person. Don't ever give money. Recruitment agencies do not take money to get you a job. When you are placed the hiring company pays a fee.
6. Make your passwords strong passwords. Minimum 8 characters (preferably more) and a mix of capital and small letters, numbers and symbols. Most legitimate companies will not allow a weak password. A client once asked me if I thought a job offer was legitimate or not. The text suggested creating an account with the password 123456. I said to her, if anyone suggests that as a password, delete them. It cannot be legit. There were other aspects also suggesting a scam, such as the country of origin of the message.
7. Don't ever give anyone money unless you know and have met the person and you really, really want to give them money. Also, don't expect to get the money back. If it is a charity, then they must prove they are a charity.
8. If someone sends an email or text saying you have money due to you or a payment has been made and you are not expecting one from that source, check it out.
9. Use two-factor or multi-factor authentication.
10. A recent scam I heard about occurs in the supermarket. A stranger approaches you and asks you to buy them groceries. People do this. Then they come back into the supermarket and say they are returning the groceries and want the money. Some of the stores in SA are wise to this and I have seen people escorted from the shops because they tried this once too often. If you want to give food, then give it to the legitimate organisations that feed people and direct anyone who approaches you to such an organisation.
11. Be cautious of websites. It is easy to make one up. Like Facebook, though, they usually do not have a lot of information on them. So be suspicious of websites or profile pages that are thin on information and postings.
12. Inheritance scams have been around forever. They still do occur. If you have a dead relative who left you money then check it out another way.
13. Couriers and delivery services seem to have, in their employ, people who are part of scams. I think almost every day I have an email or text telling me I need to pay x amount before my goods can be delivered. Never once has this been legitimate.
14. Set up transaction alerts for your bank accounts. Most banks already do this. That way you immediately get a message when a transaction has taken place.
15. Be very sceptical of offers and investments. If it seems too good to be true it probably is too good to be true. Be especially careful if someone wants immediate payment. By making you

feel pressured it is easier to manipulate you. Understand what a Ponzi scheme is and how to identify one.

16. Use anti-virus software on your computers and phones.

One of my clients last year, who had a sister who committed suicide because of being scammed, told me she carried on playing with the scammers. I immediately expressed my concern, but she told me the police were involved and this was a sting operation. The police did get them and charge them, so those people were taken out of the loop. However, I know of a few people who, on their own, like to play games with someone who is trying to scam them. People have even said to me, they want to win this. I think this is a dangerous way to think. If someone is trying to scam you, then have nothing to do with them. You want to stay as far away from such people as possible. Check the legitimacy of everyone you deal with. If you are in doubt, then stay away. Just don't get involved. For most people daily life is hard enough, without having someone embroil you in a scam.