Mastering Money Podcast

Season 9 – Dark side of money

With our commitment to promote the accessibility of webinars that we offer, we endeavour to provide transcripts that accurately reflect the information conveyed. However, please note that there may be instances where we are unable to accurately capture what was said. If you have any questions or concerns about the transcripts provided, please contact us at financialliteracy@cpacanada.ca.

S9 E03: Love, Lies, and Illusions – Unveiling Romance Scams and Money Mule Tactics

MUSIC PLAYING

00:00:00.49

DORETTA THOMPSON

00:00:11.66

Hi. You're listening to Mastering Money, where we explore the many aspects of good financial decision-making. I'm Doretta Thompson, financial literacy leader for Chartered Professional Accountants of Canada. We provide no-cost programs and free online resources that help Canadians own their finances and learn the language of money.

This season, we're looking at the dark side of money. We'll be diving into hot button topics, like how romance scams target vulnerable people, how we can protect ourselves and deal with the aftermath of robbery with the sharp increase in street crimes, to the fraudulent property sales that jeopardize our homes.

Today's episode is all about romance scams that prey on vulnerable people seeking love and connection online, how they manipulate their emotions and trust for financial gain. We'll talk about the tactics used by scammers, discuss the devastating impact on victims' emotions and finances, and provide expert advice on staying safe and avoiding these traps.

My guest today is Jeff Horncastle, the acting client and communications outreach officer at the Canadian Anti-Fraud Centre. Jeff, welcome to Mastering Money.

JEFF HORNCASTLE

00:01:26.82

Happy to be here.

DORETTA THOMPSON

00:01:28.49

So before we dive into this very sad and difficult topic, I think, tell us a little bit about yourself and the kind of work that you do at the Canadian Anti-Fraud Centre, and maybe a bit about the Canadian Anti-Fraud Centre as well.

JEFF HORNCASTLE

00:01:42.56

Yeah. So as mentioned, I'm the current client and communications outreach officer. I've been working in the fraud prevention and intake unit for roughly six years. I've worked in our call center, spoke with victims on a on a daily basis. I've been working in my current position for over two years now, where I coordinate fraud prevention initiatives with the CFC, including outreach through either presentations through the media, social media, and our website among many other initiatives.

About the CFC. The Canadian Anti-Fraud Centre is a national police service that gathers intelligence and fraud across Canada and assists police of jurisdiction or police, local police. With enforcement and prevention efforts, we help citizens and businesses report fraud, learn about different types of fraud, recognize the warning signs of fraud, protect themselves. And we also provide information on law enforcement and governments in Canada and around the world.

DORETTA THOMPSON

00:02:43.11

Sounds like a very serious mandate and one, sadly, for which there's increasing need.

JEFF HORNCASTLE

00:02:48.54

Absolutely.

DORETTA THOMPSON

00:02:49.83

So before we begin, can you tell us exactly what a romance fraud is. What is it we think of from the perspective of Anti-Fraud when you think about a romance fraud?

JEFF HORNCASTLE

00:03:01.92

Yeah. So a romance fraud typically starts off on a dating website or social media or even online games. We see that that's where the communication typically starts. After communication gets going, victims are asked to switch to a different method of communication, either an encrypted method of communication So it's more difficult to define the information or whatever the case may be.

So for example, if the communication started on dating website, they may ask to go to email, or WhatsApp, or things like that. It's common for suspects to use pictures found on social media of real people. For example, business people, members of the military. They'll really craft their profiles to make everything more believable to the victim.

They may even go to the extent of looking at the victim's profile and making their profile match what they think that person might like, which might include pet photos, and hobbies, stuff like that. Scammers, they'll do anything. For the most part, it's organized crime that's behind these types of scams.

That's basically how it works from the beginning at what they do, and they claim that they're overseas and they need money for whatever reason they come up with. Either their bank accounts are frozen. They claim that they have unexpected business expenses. They need travel fees to return home. So that's really what to watch out for. I think we'll get into a little bit more of the prevention a little later, but that's typically how the romance scam starts.

DORETTA THOMPSON

00:04:31.86

And so a romance scam is one where they're actually creating a kind of romantic relationship with the targeted individual so that they're dating or the person that's been targeted feels like they're in a genuine relationship with a real person.

JEFF HORNCASTLE

00:04:49.50

Exactly, and that's what's different about romance scams and other scams because it might take — they might communicate for months before asking, going in and asking to borrow money from the victim. They want to make sure that emotional connection is there before they can really go in and potentially steal a lot of money from the victim.

DORETTA THOMPSON

00:05:06.90

How prevalent is this?

JEFF HORNCASTLE

00:05:09.51

Unfortunately, romance scams have been very prevalent for many years based on dollar loss reported to the Canadian Anti-Fraud Centre. Romance scams have been in the top two or three scams since 2021. In 2022, over $59 million was lost to romance scams. And in the first six months of 2023, nearly 27 million was lost.

Now comparing this to 2020, where for the full year $27 million was lost. We saw that amount double when we're comparing 2020 to 2022, mostly because habits have changed after the pandemic, where people were generally spending more time online, looking for companionship online more than they have in the past, and among a few other factors there, but that's the main one.

DORETTA THOMPSON

00:05:56.01

And who is it that these scammers target? Is there sort of a particular or typical profile?

JEFF HORNCASTLE

00:06:02.67

From what we're seeing, anyone can be a target. Like I mentioned, with the habits changing and the general public spending more time online, communicating through social media, doing online shopping — so this is very common across the board for all scams, where it's not a certain demographic that's targeted more than the other. We're seeing that everyone can be a target. Yeah, it affects all demographics, fortunately.

DORETTA THOMPSON

00:06:29.46

Well, and it's scary that the numbers seem to be going up by the reported amounts. And do you think that what we see reported, what you folks see reported, is probably just a fraction of what's happening? Do you think there is a sense of shame attached to it that people don't report it?

JEFF HORNCASTLE

00:06:45.87

100%. Yeah, we estimate that only 5% to 10% of Canadians actually report to the Canadian Anti-Fraud Centre. The numbers we're giving is unfortunately just a drop in the bucket. It's a small sample of what's actually out there and what's happening.

DORETTA THOMPSON

00:07:01.47

So let's dig a little bit deeper into how these scams work. You were saying that these scammers seem to have their fingers everywhere where they can try to connect to an individual.

JEFF HORNCASTLE

00:07:15.06

Yeah. So like I mentioned, they'll use social media, online game platforms, dating websites. Any platform they think they can prey on victims, they'll use. And after that communication is started, that's where they begin manipulating the victim emotionally. And unfortunately, with all scams, they prey on vulnerabilities. So they're able to gauge what vulnerability the victim might have by communicating and they really manipulate them, unfortunately.

DORETTA THOMPSON

00:07:42.82

And what does that manipulation start to look like?

JEFF HORNCASTLE

00:07:46.06

So the manipulation is, once they know they have that connection, that's where they come up and start requesting money. They do this for a living, unfortunately. It's organized crime, and that's where they come up with the reasons, personal or family emergency.

They might claim that they have no access to their existing funds because they're working abroad, their bank accounts are frozen, unexpected business expenses, legal expenses, or professional fees. They might claim that they're investing in a new business. I mean, they always promise that they're going to pay the victim back. They claim that their bank account, for example, is frozen temporarily and they assure the victim that they're going to pay them back, but of course, it doesn't happen.

DORETTA THOMPSON

00:08:26.50

Yeah, they never do. They never do. We hear about money mules and romance scams. Can you tell us how a victim might become a money mule?

JEFF HORNCASTLE

00:08:35.29

Yeah. So first of all, I'll explain a little bit of what a money mule is. A money mule is an individual who is recruited by fraudsters to serve as a middle person to transfer proceeds of crime frauds. The mule may or may not be aware that they are a pawn in a larger network.

When a mule moves money, it becomes difficult to identify the fraudsters from the victims because in a lot of cases, it goes through a lot of hands before the funds go through a lot of channels or hands before getting to the victim. The money is often transferred using bank wire transfers, email money transfers, money service businesses, and virtual currencies. Typically, mules get paid for their services, receiving a small percentage of the money transferred.

So how does this work with the romance scam? In a lot of cases, going back to the example that I gave, where the suspect might claim that their bank account is frozen, they don't have access to funds, they ask the victim to accept transfers for them and to transfer the funds to an alternate account, for example. So that's typically how it works with the romance scam, of course, the victim not knowing that the funds are coming from. Other victims is transferring the funds to the criminals.

DORETTA THOMPSON

00:09:42.79

So when you go after someone like that, you start at the end of the thread and work backwards. Is that how it works?

JEFF HORNCASTLE

00:09:50.26

So wouldn't be able to comment on the investigative part too much, but typically, from what we're seeing, yeah, there are numerous channels and numerous steps before the funds actually get to the criminals.

DORETTA THOMPSON

00:10:01.27

I'm just curious. Can you give us, share with us some of the examples of stories that you've heard?

JEFF HORNCASTLE

00:10:08.11

That's a difficult one. What I explain there is the typical story that we hear. That being said, there are more difficult ones to hear than others. Because being a victim to fraud affects everyone differently, it's a difficult kind of question to answer, right?

Losing a couple of thousands might be more detrimental to a person than it might be to another victim. Being a victim to a scam can also have long-term effects on the victim, which are obviously hard to gauge for the Canadian Anti-Fraud Centre because we take the report, and sometimes that's where it ends, unless there's follow up from our senior support unit.

But with that being said, we have received reports of victims taking their own lives from being a victim to a scam, unfortunately. But going back to the beginning, generally, the romance scam, that's how it starts. They come up with a sad story, family emergency, and they need money. Unfortunately, in a lot of cases, victims lose all their life savings.

DORETTA THOMPSON

00:11:08.41

It's so sad. Romance scams, I guess, have always been with us. I mean, people have been taken in, but social media just adds this whole dimension of being able to do multiple scams simultaneously for some of these people.

JEFF HORNCASTLE

00:11:23.83

Exactly. Now with the emergence of artificial intelligence, now there's potential for criminals to use this to their advantage like they have with any other technology. The victim might think that they're communicating with the real person, but they might actually in fact be communicating with a an AI bot that has the ability to make it look or to seem very realistic.

DORETTA THOMPSON

00:11:47.28

Oh, that's terrifying.

JEFF HORNCASTLE

00:11:49.65

It is, and that's why it's so important to focus on, what do I have to watch for so I am not a victim? And of course, there's nothing wrong with going online and trying to meet somebody. A lot of people are lonely, they're looking for companionship online, but it's so important to know what to, watch for and what the red flags are because the longer you communicate the more at risk you're putting yourself. So the quicker you're able to see those red flags, the quicker you'll save yourself from being a victim.

DORETTA THOMPSON

00:12:22.29

So tell me about some of these red flags. What should people be watching for?

JEFF HORNCASTLE

00:12:26.73

You want to watch for profiles that seem too perfect. In a lot of cases, these fraudsters they'll take pictures from a celebrity in a different country that we're not familiar with, someone you haven't met in person, professes their love for you very quickly.

Any attempts to meet in person. So if the victim wants to meet in person and the dates get canceled all the time, that's a huge red flag. A person who discourages you from talking about them to their friends and family. So very common where the criminals will say, hey, don't discuss the relationship with your daughter or any of your friends or any of your family, that's a very big red flag as well.

Poorly written messages or messages addressed to the wrong name. This is important because a lot of fraudsters are communicating with multiple victims at once. So they might have a hiccup and call you a different name. So it's just another thing to watch out for, another very big red flag.

How to protect yourself? Don't give out your personal information, your name, your address date of birth. Of course, you're putting yourself at risk for identity fraud. If you don't accept friend requests on social media from people you don't know, then you're protecting yourself from — you're not putting yourself at risk.

Be careful who you share images with. Suspects will often use explicit pictures to extort victims into sending more money, so that's where it kind of turns into sextortion, which is a whole other category at the Canadian Anti-Fraud Centre. Never send money to someone you haven't met.

So under any circumstance, if you haven't met the person and they're asking you for money, if you go by the rule of not sending money to someone you haven't met, then — and not just for romance scams, it's for all scams. So if you haven't met them in person, don't send them money.

DORETTA THOMPSON

00:14:09.55

I'm curious. You did say that you're seeing victims from across all demographics. Are women more likely to be targeted than men?

JEFF HORNCASTLE

00:14:17.23

It's actually quite even for men and women. So men are looking for to date online or companionship just as much as women are based on the reports that we're getting at the Canadian Anti-Fraud Centre.

DORETTA THOMPSON

00:14:29.35

So one of the things you were talking about was the photographs, using photographs from celebrities from other cultures, et cetera. Is there a way that you would suggest people check those photos? Because I think Google actually has a tool that lets you do that.

JEFF HORNCASTLE

00:14:46.57

Yes. Yes, 100%. So it's actually a tool that we suggest to — for example, if there's a family member calling in on behalf of, let's say, their mother who is a victim of a romance scam and the daughter is trying to convince the mother that they're in a romance scam and they're not believing anything that they say.

That's really challenging because you don't want to affect the relationship you have with the family member either. So it's — there's a line you don't want to cross. But with that being said, there are tools like you mentioned to try to convince subtly.

So you can actually do a reverse image search with, let's say, the suspect's profile picture that they're using and by doing the reverse image search on Google or tineye.com — is another one that we suggest using. It'll actually pull up all the names that have been used with that photo. So if you're able to pull this up and in the example that I gave where you're trying to convince a family member, it's a good tool to show them that there's a good chance it's a scam.

DORETTA THOMPSON

00:15:44.08

And for our listeners, we'll be including the links to any of these tools that Jeff mentioned in the notes to the podcast app. That actually leads to another question in terms of — we've talked about ways you can protect yourself. Do you often hear from people who are concerned about family members and what the red flags are that family members should be worried about if they think that somebody's close to them has been targeted?

JEFF HORNCASTLE

00:16:12.16

It's challenging because there's only so much a family member can do. They can try to do the reverse image search, but I mean, there's red flags. The family member might be hiding some of their chats, or their phone calls, or something to watch out for, acting differently, being secretive about what they're doing online, all red flags, but it's a really challenging situation.

If you're able to gather some of the payment information and some of the communications, you can reach out to local police or the Canadian Anti-Fraud Centre, where we can potentially give advice to try to help.

DORETTA THOMPSON

00:16:46.16

One thing that we've seen lately is some examples of romance scam victims being lured into things like cryptocurrency, fraudulent activities, et cetera. Can you explain a little bit how those work?

JEFF HORNCASTLE

00:17:04.47

Yeah. So it starts off the same way. Great question, by the way because there has been a huge increase in romance and investment scam, very closely linked together. So they typically start off the same way. Communication starts off on social media, or a dating app, or website, and after the suspect knows they have that emotional connection.

Sometimes they'll wait months or three, four, or five months, and then they'll present this investment opportunity that they claim that they made a lot of money on and they ask the victim to invest as well. And what they do is, they create these very legitimate looking platforms, websites online, where you know the victim if they agree to invest a little bit of their money, $200,000 or $300,000, they can actually withdraw a bit of that money to convince them that it's an actual legitimate cryptocurrency investment platform.

So what happens is, the victim then decides to invest a little bit more with time, more and more. And of course, when it comes time to withdraw what they've put in, they're not able to. This can last sometimes over a year, where victims have lost, in some cases, all their life savings.

DORETTA THOMPSON

00:18:19.93

It's really sad and scary. And when you think about AI and the potential for AI to create these very real appearing platforms, et cetera, I guess there's a real risk that this is really going to just continue to grow very, very rapidly.

JEFF HORNCASTLE

00:18:39.73

Unfortunately, yes. I mean, with AI, it's just the beginning. And that's not to scare people, but it's important to know what technology is out there and how it's being used. That being said, even with the AI, what to watch for and how to protect yourself doesn't really change a lot much. You always want to do your research as much as you can. We're looking at investment scams.

Remember that if you send a cryptocurrency payment, chances are, you're not going to get that back, very hard to trace. So just it's important to know what to watch for and how to protect yourself. So even if — another form of AI that we've been seeing or observing is deepfake videos.

So in a lot of cases with these fraudulent crypto investment platforms, they'll deepfake, which means a fake video. Fraudsters will take a picture and a voice clip of a celebrity. We have seen news anchors promoting fraudulent websites, merchandise, or investment. So just know that those videos are out there, there are fake videos out there. It's probably going to be used as an extra tool to try to steal your money.

DORETTA THOMPSON

00:19:47.90

Is there a way that people can check to see if those videos are fake?

JEFF HORNCASTLE

00:19:53.45

Right now not that we're aware of. That being said, there are things to watch for if the video seems a little choppy. There are a little irregularities with these videos, but unfortunately, in some cases, they're not. It's very hard to detect with the naked eye.

So just the fact of knowing that these fake videos are out there — it's like, if you see a celebrity promoting something online that you're not sure about, then believe that it's fake until you can prove otherwise type thing, where you want to research to prove that, is a fake or is it real?

DORETTA THOMPSON

00:20:26.69

What about sites like Snopes? Is that a good place to fact check things?

JEFF HORNCASTLE

00:20:31.64

It is. It's not just one tool that you want to focus on. You want to combine a bunch of different tools depending on — if you're looking to purchase merchandise, then you want to look at reviews, keeping in mind that reviews can be fake as well.

You mentioned Snopes. Whatever tool you have at your disposal, try to use it as much as you can. And of course, we always advise reaching out to a friend or family member for their opinion and make it a group decision instead of a quick decision because we see that the victimization for an individual can happen very quickly in most cases.

DORETTA THOMPSON

00:21:06.44

I think that's a really good litmus test of, if you're prepared to discuss this with somebody you know, and that if you feel compelled to keep it secret, you've got to ask yourself why.

JEFF HORNCASTLE

00:21:18.44

Exactly.

DORETTA THOMPSON

00:21:19.61

Yeah, good litmus test. So if you feel that you have or if you've been the victim of a fraud like this, where do you report it?

JEFF HORNCASTLE

00:21:29.26

Well if you have been a victim, very important to you to report to your local police and to the Canadian Anti-Fraud Centre. There are two ways to report to the CAFC. You can do it by calling our toll free line, 1-888-495-8501, or you can use our online fraud reporting system at antifraudcentre.ca to report online as well.

Now depending on if you have lost money or if you're a victim of identity theft, there are different steps to follow, which are listed on our website. But if you send funds through your bank account, then you want to reach out to your financial institution and report it to them as well.

DORETTA THOMPSON

00:22:02.99

Why is it important? I think it's really, really important that we stress just how important it is to report these scams despite the shame that may be involved, et cetera.

JEFF HORNCASTLE

00:22:14.42

Yeah. So I think that there's a few different reasons why — going back to the fact that we estimate that only 5% to 10% of victims report to the Canadian Anti-Fraud Centre, one of the factors is being ashamed, you don't want to discuss what happened. There might be a thought that law enforcement won't do anything. They can't do anything because this is more than likely coming from overseas, right, or not knowing what the Canadian Anti-Fraud Centre does. A victim might think that, well, you know what, the Canadian Anti-Fraud Centre doesn't investigate, so there's no point in reporting.

Now it's important to understand what the mandate is at the Canadian Anti-Fraud Centre. We collect the information. We're the central repository for mass marketing fraud, and we share the information with international law enforcement agencies and law enforcement agencies across the country as well.

So I always give the example of — let's say a romance scam is being investigated by a law enforcement agency abroad and there's a victim in, let's say, Halifax and another victim in Vancouver. The information can easily be linked together in that central repository, which is a Canadian Anti-Fraud Centre.

On top of us being able to share prevention messaging based on the information we're collecting, so if we're seeing something new, then we typically get an alert out to make sure the Canadians are aware that either new technology is being used, like AI, like we discussed. Or if there's some kind of a new twist to a scam that we're seeing, we use this information to try to protect Canadians.

DORETTA THOMPSON

00:23:47.07

So really, one of the most important reasons to share this is that you can actually help other people learn from your experience.

JEFF HORNCASTLE

00:23:55.62

Exactly.

DORETTA THOMPSON

00:23:56.49

Jeff, thanks so much for this.

You've been listening to mastery money from Chartered Professional Accountants of Canada. You can click to all the resources mentioned in this episode in the description for this podcast in your podcast app. Please rate and review us. And if you'd like to get in touch, our email is **financialliteracy@cpacanada.ca**.

Please note, the views expressed by our guests are theirs alone and not necessarily the views of CPA Canada. This is a recorded podcast. The information presented is current as of the date of recording. New and changing government legislation and programs may have come into effect since the recording date. Please seek additional professional advice or information before acting on any podcast information. Be well, be safe, and remember, if it's too good to be true, it probably is.

MUSIC PLAYING

00:24:47.20