Understanding Cybersecurity: Education, Prevention, and Response Strategies

Announcer: Welcome to the Empowered Investor Podcast. Have you ever felt overwhelmed by the sheer volume of choices and voices telling you how to plan or invest for your future? With a straightforward approach, host Keith Matthews of Tulett, Matthews & Associates cuts through the noise to help you create a winning action plan for you and your family. The decision-making framework discussed in this show can transform you and your investment experiences and will increase your odds of becoming financially secure. Learn more and subscribe today at TMA-invest.

Marcelo: Welcome to the Empowered Investor Podcast. I'm joined today by Lawrence Greenberg, and we're going to talk about a very important subject with a very special guest. But first of all, Lawrence, congratulations on getting your CFA. Big props to you, my man.

Lawrence: Yeah, thanks very much. It's a big relief after a couple of years of hard work, and it's nice to see it pay off. I'm sure it'll benefit clients in the long run. So all good.

Marcelo: So tell me, what was your biggest takeaway from three years of pain and suffering?

Lawrence: Obviously, the hard skills are great and the soft skills, but really, it's a lot of resilience. You really have to stick to it. It's a lot of self-study and a lot of examinations. I think on the other end of it, I'm a lot sharper and a harder worker. So I think it paid off in the long run.

Marcelo: It amazes me to see the team we have now, how everybody's going for the gold standards, studying, trying to become better. I think that raises the bar for everybody, and at the end of the day, clients benefit. But today, we're going to talk about a very important subject. As you know, everybody has their lives online right now, whether you're doing banking, talking to a relative, talking to your friends, or doing Zoom through work, our lives are online. We can't avoid it. And cyber fraud, scams, phishing—you call it, but there are many names for it—are at an all-time high. People are losing their identity and social security numbers. When they fall for the scams, it's not only their information but also it costs them money, right? So for that, we have a very special guest. So talk to me about our guest today.

Lawrence: So our guest today is James Fournier. He's been with the firm for a long time. He went to Concordia and has been in the industry for over 20 years. So he's seen the industry and the sector evolve over time, seeing what trends are happening, his pulse on what's going on. He's been extremely active in the firm, working with team members to ensure we're sharp, have a keen eye, and are aware of bad actors and phishing and all that stuff. He has an emphasis on cybersecurity, which is extremely relevant and is really the focus of this episode. So a wealth of knowledge, and I think listeners will really benefit from what he has to say.

Marcelo: So James has been instrumental in training everybody here on what to be aware of, what to do, and what not to do. We are actually going to talk about that in the episode—the do's and the don'ts, what type of software to use, and two-factor authentication. So it's a great episode for everybody. It's a great resource, a little bit different from investing, but I think listeners will greatly enjoy. Absolutely. All right. Thank you for listening. Enjoy. So James, thank you for being here with us today.

James: It's a pleasure to be here.

Marcelo: I am super pumped because we have a lot in common. You, like myself, are an old soul. We both like whiskey. We're both young guys trapped in a 60-year-old person's body.

James: Sounds about right.

Marcelo: Actually, I don't know if I should introduce you as a collector of watches turned into IT professional or the other way around. Like which one comes first?

James: Oh, that's a good question. I guess I was a watch collector long before I enjoyed computers or liked looking after them anyways.

Marcelo: You're very passionate about it. So I do appreciate that. I still don't wear a watch, but I think eventually, after talking to you so much, I'll end up wearing a watch. So look, today we're going to talk about something super important. Cybersecurity, how all these types of scams are going on in the industry. I think it's a super important subject. I always say the biggest risk we face is not somebody walking in with a shotgun here and saying, "Give me everything you have and all the information you have."

James: Although that would be a big risk.

Marcelo: It would, but it is actually cybersecurity. Everything is done online now. So before we get going, just let me read some stats that I pulled out, and we're going to unpack this. Don't worry. So it's going to be a lot now, but we're going to unpack this as we go in the episode. According to the RCMP in 2022, the Canadian Anti-Fraud Center received fraud and cybercrime reports totaling a staggering $530 million in victim losses, nearly a 40 percent increase from the unprecedented $380 million losses in 2021. Unfortunately, the increase in financial loss isn't tied to an increase in reporting. The Canadian Anti-Fraud Center estimates that only five to ten percent of people report fraud. So another report from TransUnion says that financial services digital fraud attempts have increased by 218 percent in the last two years. So you look around, and it's happening in travel and leisure. It's happening in telecommunications. It's happening across the industry. And as we move to more digital technology, I'm going to ask you, what are the types of scams and frauds that we're seeing? You're going to unpack that for us. And I saw another statistic that really scared me. It said that, according to a survey from TD this year's fraud prevention month, 62 percent of Canadians believe they are targets more than ever due to the changing economic conditions and rising living costs. However, nearly half, so 47 percent, haven't taken any steps to educate themselves on fraud prevention or protection in the past year. Nearly eight in ten,

so 78 percent of Canadians admit they lack the confidence in their capacity to spot possible frauds or scams.

James: There's some really important stuff in that last sentence of yours there. We can get into that later, but there are some key elements there.

Marcelo: Okay. So before we jump in, tell me a little bit about yourself. How did you get into the IT world? How did you end up running the business that you run?

James: About... I've been at this for over 20 years now. It all started when I was working for a company, nothing to do with IT. The IT guy, who was very overworked in those days, finally went on vacation. He gave the boss no option. He was going. He hadn't had a vacation in years. He was done. So my position in that company was such that it fell on me to keep the computers running. And I didn't know too much about them. I used one, but I didn't know too much about them. But I quickly learned that I really enjoyed them. So from there, I just went. I signed up for school. I went back to school, decided to change my career, and studied computers. While I was in school, there was this important moment where my teacher would change all of our passwords when we went for lunch. And he'd do this to teach an important lesson. He'd do this to teach that if you're in charge of a network and you have all the keys to the kingdom, if you don't lock your terminal, which is the access to that kingdom, then someone can come and use that to your disadvantage.

Marcelo: So that's like giving Dracula the keys to the blood bank.

James: Yeah, it's leaving the bank vault open and then being surprised when someone steals something. So this, I found, was a very important lesson. And subsequently, a few days later, he made the same mistake, and I did it back to him. I locked him out of his computer, which sent him into an understandable tizzy. He was very mad at me. He stormed out of the classroom after tearing all the cables out of the back of my computer. And the whole class was looking at me like, "Good job." I felt horrible. I went to him, long story short, apologized, and we were all good from that point forward. But I explained to him that I thought it was a two-way street. I thought we were back and forth, and that was not the case. So anyways, that was my exposure to security and how you can manipulate it and how you can use it to your advantage, or it can be used against you and I loved it. So I continued school, and there was not really a focus on security unless you chose one personally, which is what I did. I've always focused on that and there you go. Out of school, I was hired as a part-time employee, and that turned into a partnership with my first business. And then as things grew and I was less enchanted with the retail side of things, I struck off as a consultant and kept going, and that's how I started. And I've been doing that ever since.

Marcelo: And I tell you, the work you've done for us, our cybersecurity hygiene and IT hygiene has significantly increased. I speak personally. I think we have a very tight ship here. Everybody's ready, but the first vector of risk is the advisory, it's us, but then the client is also a huge risk, right?

James: Yes. What we've experienced here is the proper management response to these threats, and that's something I don't see across all my clients. Most people are concerned more with cost than security, and here there's a very clear difference and kind of a full investment, full concern with security, and that has enabled me to have the tools and resources to deploy the kind of network that I want to see. So often there's a difference between management and IT. IT knows what we need. We know what to do. We know how to do it. We know what it costs. But management rarely wants to pay for it. That's really what it boils down to here. We don't have that problem here. What I need is what I get. And thus, you, as a user of this network, are experiencing how a well-funded and well-designed network can be. And that's management. That's not because I've done anything special for you. It's just because I've been allowed to do what I feel you guys need. And the results speak for themselves.

Marcelo: And I think we're also translating this knowledge that we have into clients and we're helping clients understand this, but I don't want to get into a tangent here. Let's just unpack cybersecurity. How would one define cybersecurity?

James: I would define it as the defense of any asset that is exposed to the internet. What does that mean? It can mean your data. It can mean your information. It can mean medical records in a hospital sense. It can mean financial records in an investment firm. It can mean your money in a banking sense. It can mean your privacy in a more personal home user kind of experience. All those things are assets. All of them are exposed online like almost everything is. We can go further to say things like infrastructure or hydro, but that's out of the scope of this. But it's really any asset, anything that's of value personally or financially, and its defense, hence cybersecurity.

Marcelo: Talk to me about some of those assets.

James: Okay, so very straightforward would be your money. So if you get scammed out of 500 bucks or 1,000 bucks, or in the case of ransomware, which we'll get into more at some point, tens of thousands of dollars potentially, then it's just money out of pocket that you didn't need to spend that was either stolen from you or you had to pay to regain access to your information. It can also be things like identity theft, which leads to credit cards being opened, loans being taken in your name, all sorts of other things. And then there are some personal elements where they can use identity theft to try and trick your friends. So all your friends think, in the end, that you're doing it to them. Now, it's not hard to prove otherwise, so it's not a lasting issue, but it does lead to an embarrassing situation where all your friends are being scammed for 500 bucks, and it's all coming from your name. So those are the kinds of things. I also worry about institutions like this. I worry about privacy data, like social insurance numbers, and in healthcare, medical records, stuff like that. It's all at risk. And what can that lead to? It doesn't really matter. It's your information. And it shouldn't be available to bad guys who steal it. That's the end of it. So those are really the stuff: personal information and your money. What's more important than that to everyone out there?

Marcelo: If they do take your social security number and all this information that you're talking about, it's like this private real estate. They can build a new identity and just pretend to be yourself, right?

James: They can do a shocking amount of things.

Marcelo: Wow. It's crazy. We're going to get into exactly how this happens, but tell me, what are the most common pitfalls when it comes to cybersecurity? What are the pitfalls that people fall into that make them get into trouble?

James: The first thing I would say is that largely, most people don't have enough training or understanding to protect themselves. So by that, I've always told my clients, if I can train people, if I can give people the knowledge that they need, it will provide 99 percent of the defense required. And why is that? Often in scenarios where people have gotten scammed, there was a trick. We call it phishing, spelled P-H-I-S-H-I-N-G. And the idea of phishing is you throw out a bit of bait on a hook. You throw it out in terms of the internet to hundreds of millions of people. And if only a small percentage bite, then you have them. So it really is a matter of identifying what is bait and what is real. And that's a little bit of training. It doesn't require a lot of knowledge. We're not talking about everyone should go to computer engineering school. We know the rules of the road when we drive. We know that a dark alley in a big city late at night is dangerous. But on the internet, we seem to feel like anything goes. We don't read warnings. We click next way too fast, and we're curious about that invoice that we got in our email or something that we got in our email that's made us curious, and we just don't recognize the sender. We don't know what it's about, but we're curious, and it says something that's designed to drive us to click it, and we click it, and then there's consequences.

Marcelo: Yeah, no, I totally get it. I was trying to think about an analogy in terms of perception, right? They say you have way more likelihood of dying in a car accident than you have in a plane, yet people are way more scared to be in a plane because it moves and you have no control. Whereas in a car, you're holding onto the wheel, and the vectors of risks are so much higher, but you feel like you're in control. And sometimes on the internet, it's like this idea that, again, like somebody walking in with a shotgun or mugging you on the street is completely unpredictable, and there's some risk. But when it comes to cybersecurity, you feel like you're in control because you have passwords, you're dealing with this network thing that you call the internet, and you have this element that you think is safe, but there are so many vectors of risk that we're not aware of. It's just crazy. Think about the pandemic, right? The pandemic moved everyone to a more virtual world. And right now, there's not an aspect of our lives that isn't online.

James: It's the wild west. Everything's online. Regulations are few and far between. Security is really left up to the user. Companies, the major telcos, will provide you with a potentially a feeling of security or some products that will help you there. But without fully understanding the way those products are being used or how to use them even, or are they even being used? Just because they're provided doesn't mean they're being deployed. It means that your security is really still a big question mark.

Marcelo: Okay. So in the context of our business and our clients, just walk me through one of the most common examples of scams, what people should look out for, and how these guys are trying to trick people. Give me some tangible examples that people can say, "Okay, I've experienced that."

James: Oh, the big one that I'm seeing an awful lot of is, to go back to that phishing, phishing will involve usually an email. It does happen. It does exist with phone calls as well, but we'll limit this to cybersecurity. So you'll get an email, and the email will look like it's from a friend, or it will look like it's from your bank, or it will look like it's from a service provider, Videotron, Bell, doesn't matter, anyone out there. And the idea really is that you look at this, and you say, "This is an email from Bank XYZ. And I'm a client of Bank XYZ, so it must have been properly directed to me." And in reality, the way it works is the bad guy or bad person sends out a hundred million emails. And in those hundred million emails, some people will be clients of that bank. So those people will naturally identify and think it's real. There'll often be a link in that email saying, for example, "We've detected fraud on your account. Click here to secure your account." And these are emails that we've seen before in legitimate formats. They're not unfamiliar to us. And so you click that link, and it will take you to a site that will look like that bank's actual website. And I think what people fail to always realize is that anyone can make a website that looks nearly identical, especially in faraway countries where trademarks aren't necessarily respected or able to be enforced. If these banks even know, because a lot of these operations are here one day, gone the next, they collect as much as they can, and then they move on. So they make a website that looks just like the real thing. And then they give you a login. And that login will be, "Type in your account number and your PIN," and you type that in. And the really smart ones will even connect that back to the real website so that when you click through, you end up in your actual internet banking, and you feel perfectly secure like nothing's happened. But this man in the middle, this connection in between, has then logged, stored your card number or your account number and your password, which they can then use to go back in. Now, banks are protected, and you have some recourse there, but it is always advisable to keep that stuff protected rather than having to deal with the consequences after the fact. So that is far and away the biggest. We see simplified versions of that attacking services like Facebook, social media, which are then used to gather more people. And that's where you can get messages from people that look like they're you, or you get messages from people that you think you know, I should say. You have a natural trust for those people, so you tend to accept what's in those emails. That's another type of phishing. We also see where someone will clone an account. So, Marcelo, someone will get your picture off of Tulett Matthews' website, and they'll take your picture. They've got your name, and they'll create a Facebook account with your picture, your name. Maybe they'll throw in a number two or an extra L or something that makes it very hard for people to recognize that this isn't the real Marcelo. And then they'll go around, and they'll start asking you things. They'll ask you for details. They'll ask you for, "Hey, can you send me that account number for..." and we've seen that here where people have made requests pretending to be one of the owners asking employees to please send them this information or that information. And thankfully, everyone here knows what to look for and is able to catch that right away. And it never even gets to my level because you guys detect it immediately, and it's shut down. But this is the thing that I feel is like the number one threat. It's the thing I see catching most of my clients

if they're going to get caught with something. It can lead not just to theft, but in some cases, it can lead to different types of malware. Malware is any sort of software that's malicious, hence malware.

Marcelo: I was just going to ask because sometimes they don't necessarily take the information, right? Like they don't take your social insurance number or anything like that, but you click on a link, and it'll install a type of virus in your computer, right? So that's what you're referring to.

James: Yeah, that's what I'm referring to. And there's one particularly insidious type referred to as ransomware. And this is a type of software that will effectively encrypt your entire computer. So encryption is a means of scrambling the contents of a computer with a mathematical algorithm that can then only be unlocked with a key. Encryption is used to protect your online banking. It's used to protect your Wi-Fi connection. It's used all over the place. You might not even know it's there, but it's really a powerful way of beaming information in open spaces that people can intercept but can't read because it's scrambled.

Marcelo: Okay, so it will be really hard to open up something that's encrypted.

James: Next to impossible. Some of this stuff, you're looking at government assets and years of work to break in. So it's really tough stuff to break. What they'll do is they'll use this type of encryption, scramble all your data, and then when you open up your computer, you get a message saying, "We've got your data. We've scrambled it all, and if you want it back, send us this much money in Bitcoin." Bitcoin is used because it's not traceable. That's why they do it that way. And then you have this choice: Do I lose all of my data, or do I pay the ransom? Now, interestingly, these guys are smart. So if you pay the ransom, you will get your data. A lot of people are concerned that you pay, and then they'll just ask you for more money. And no, they're actually really good at it. If you pay, you get your stuff back. And the reason for that is they want it to be known. They want guys like me to tell you that if you pay, you'll get it back. That way, you're likely to pay. And at the end of the day, what they want is that money.

Marcelo: So they do have some ethics.

James: They have some business structure. They have some guidelines, but I'd say ethics aren't the right word.

Marcelo: Okay, what about the other one that we talked about often here in the office where they'll send a message saying, "We caught you doing some things on the computer. We have you on camera, blah blah blah." That's a common one, right?

James: Yeah, that's a common one. It's a bit of a nasty one, too. They'll effectively send you an email saying, "We've caught you doing some unsavory things on your webcam. We have recorded the footage. We've also recorded the website that you were watching at the time," and it'll usually be something that is very distasteful—child pornography, something that would really be damaging. And of course, none of it's true, but that's what they say.

Marcelo: By the way, I know it's uncomfortable to talk about these things, but the reality is that they're happening all the time.

James: It's true. And if we bury our head in the sand, it's not going to help anybody. Yeah, they send this email, they scare the heck out of you because you start thinking, "Did I? Could it have been a mistaken website? Could it have been something like... is there any way?" Because if that information were to come out, you'd be ruined. Even though it's not true, just the suggestion of it could ruin you. So you start to panic a little bit, and they, of course, again request money via Bitcoin to make it go away, but it's once again a phishing technique. This email is blasted out to hundreds of millions of people. Even if they have your name, that's not enough. There are huge databases out there of emails correlated with names. So the truth is that if they really had such a video, if you really wanted to extort someone that way, you'd show them the video. It's digital. It's the internet. You can show them and still keep a copy. It's not like a VHS tape that if you give away the original, you lose it. If they really had such an asset against you or such a tool against you, they would show it to you and say, "Pay up." I have never seen that in the thousands of times clients have brought this type of issue to me in a sheer panic. And we've looked at it from head to toe. At the end of the day, no one has ever been able to produce any evidence that such a video exists. We've never engaged, we've never paid, and there's never been a consequence. So it's purely a trick. It's meant to scare you. It's scareware. We have a term for that too, and it's made to freak you out and make you jump the gun and do something that is... I shouldn't say stupid, but to make you do something in a moment of panic rather than in a well-thought-out cause and effect. And of course, no one is being caught this way. The technology to break into webcams, although not impossible—there's a famous case of it here in Quebec, Saint-Alphonse, actually—there was someone who was caught for that, it is actually quite rare. And breaking into webcams on a computer versus a camera that's a security camera is two different things. It's very unlikely to begin with.

Marcelo: Okay. What about the type of scam—trying to cover everything here, I'm sure I'm missing some—but I've heard, "Oh, I got a request for an inheritance, and they're asking me to make a deposit so I can unlock it." Do you hear that a lot?

James: Yeah. What is that? The Nigerian 7-1-1 scam or something like that? The idea there, and I can remember, I am old enough to remember when these scams were done via post, via mail, where you'd get this letter in paper form in your mailbox. The idea is very simple. So-and-so has died. They've left an inheritance of X number of dollars. Usually, it's a considerable or attractive amount. And we've gone through the records, and you're the next of kin because this person didn't have any direct family, and you're the 18th cousin, 15 times removed, but you're the last one in the list. Do you want the money? And if so, you need to pay some lawyer's fees or some account setup fees or some transfer fees. They come up with some label for it. So you pay them the money, and often there'll be requests for more money after that, and you've paid out. And in the end, there's no payout. It's a very old scam that is clearly still working because 30 years after I saw that paper copy, we're still seeing that scam.

Marcelo: I've also heard of people who are looking for apartments—and this could happen to seniors who are downsizing their house and looking for apartments—where they'll say, "Hey, come see the apartment, but I'm requesting a thousand-dollar deposit," or a nominal amount like that. And they'll pay up, and then the person just disappears. But I think increasingly since the pandemic, they've become way more creative. And that's what's scary because, like you said, I get emails all the time from, say, Don or Keith, "Transfer this type of money." I even got them from clients' names, but I want to get into two things. Actually, tell me, let's say the person gets caught in one of these things. So you've got ransomware on your computer. You've been scammed. What's the next step? Because you saw reporting is a big problem, right? It's not only that people are falling for it more, but also people are reporting less and less because they feel ashamed. Obviously, we're dealing with smart people. It can happen to everybody, right? So you get caught or you have ransomware on your computer. What do you do? What are the next steps that a person should take?

James: Let me step back here for a second. And that is that Benjamin Franklin once said, "An ounce of prevention is worth a pound of cure." So that really is the trick. The trick is to have systems or procedures in place before you get caught, either as preventative or as recourse. So that's the best way to solve this. And it really is the only reasonable solution. So ransomware, for example. To mitigate ransomware, we need to go back in time, get a copy of our data before the encryption happened. That's a backup system known as versioning, so it stores multiple versions of your data, and they are cost-effective, common, available. And this would allow you to say, "Okay, I got caught on Tuesday. Let's go back to the copy of data I had on Monday." And maybe I lose some work that I did on Tuesday. However, I get everything back, and I don't have to pay a ransom. And that's just a matter of investment in some hardware and some software and maybe some training or some consulting to get that set up. But once it's done, you're protected.

Marcelo: Thank you for that answer. But that's more for us. But I'm thinking more of our client who may have an iPad or a laptop, and they have ransomware. You fell for a scam and you paid. That's it. It's done. We can't go back and get the money. I get that. But let's say they fall for ransomware. They have a nasty virus on their computer. What can they do? Is there something they can do?

James: That answer sounds like it was for you, but I did intend it for your home users. So that type of technology, that kind of stuff is very much available to individual home users at a reasonable cost and acceptable cost for a home user. It's not big enterprise stuff. It's not the kind of stuff you have to have a large firm to be able to afford. It does scale, so there are versions of this for home, and that's really what people need. You have insurance for your home. You buy it before an accident for when there is an accident. Consider a proper backup an insurance for your data before something goes wrong. So that's number one. Now, what if we don't have that? So I think that was the crux of your question. What if we don't have that? In that case, we'll need to decide whether we're paying the ransom or not. If you decide you're not paying, then we want to erase the computer. At the very least, we can treat it for the virus. We can try and scan for the virus. Now, a proper IT technician will know when we need to scan and when we need to erase the computer and start over. But we basically want to recover the computer in a way that we know that there isn't a virus still

lurking or hiding in there. If it comes to the stuff where there's identity theft, when it comes to stuff where something is now out of our control and we need to rein it back in, that's a bit of a trickier situation. And you mentioned it at the top there. Right off the bat, you should contact the Canadian Anti-Fraud Center. You need to let them know that this has happened. You've lost control of something, even if you're not sure what you've lost control of. You just know that something's happened. You spoke to someone on the phone. Now you've got a bad feeling. Something's wrong. You want to contact the Canadian Anti-Fraud Center. You want to contact the police, your local police station. Go down there, file a report. You may want to contact a consultant, an expert, a computer expert. It's reasonable. We're not talking about thousands of dollars. We're talking about hundreds of dollars. And you may want to have an expert kind of go through this with you because they'll know what to look for. They'll know what's happened. They'll be able to understand what's happened. That can be a really useful thing. But if you feel confident, you should go through and change any passwords that you feel might have been affected. Now, if it's a really important thing like your email or your bank password and you're not sure, in a lot of these situations, we're not really sure what the reach is, just go change them anyways. We don't like changing passwords. We have too many passwords to remember. Do it anyways. If there's concern or questions, if you're unsure, just change them. That locks everything out.

Marcelo: If your social insurance number is being compromised, you should contact the credit monitoring system.

James: Yeah, Equifax and TransUnion. You should inform both of them. You should just do a courtesy call to your bank. Let them know as well. So although that's not official, they do put a record on your file that this has happened. I don't know how their internal systems work, but they do keep an eye out, or at least their systems now have a bit of a paranoid mode, if you will, where it looks for things that are outside of the norm. It's useful to do that as well. You can also go and enable—we'll probably get into this more—two-factor authentication or multi-factor authentication.

Marcelo: So before we jump into that, I want to ask you a broad question. What are the things—give me a game plan. So to me, when you say prevention is the best option, that is clear as water to me. You have to keep an eye. You have to be paranoid. You have to be the person that questions everything when it comes to all the links you're getting. But what are the good-to-go steps that you should absolutely be doing when you're dealing with anything in a virtual environment? Two-factor authentication, password manager, give me your go-to things that somebody should be doing.

James: Okay, so the whole list there would be every account that can have it should have two-factor authentication.

Marcelo: Okay, and define that for me, please.

James: Two-factor authentication, also known as multi-factor authentication, is essentially where you either have an app on your phone or the service will send you a text message to your phone with a code. Thus, multi-factor. So you have your password—that's one factor.

You have this code, which is the other factor. And what that prevents, or what it forces, is anyone who's trying to gain access to a service or an account or whatever requires you to have, or requires them to have, your phone—something which you tend to keep quite close to you. They need your password, and they need your phone. Pretty hard to get both of those. There are ways around it. There's SIM cloning. There's stuff we won't go into here, but it really makes it very difficult for a bad guy to have both and thus makes it virtually impossible for someone to gain access to your account even if they have your password. Multi-factor is really strong.

Marcelo: And now a lot of apps and banking apps, they offer that, right?

James: They offer it; a lot of them even force it. I know I'm with RBC, and they forced me to do it through their own app. So they send this message saying, "Is this you? Do you allow it?" Your app is connected to their banking system, and if you allow it, then you've got your phone that's confirmed it, and the computer that you're trying to log in has confirmed it via password. Very effective.

Marcelo: Yeah, I see that a lot now, but some apps will still ask you, "Do you want to do two-factor authentication?" I think that's a bad move because the default should be everybody should do it.

James: It's becoming more and more standard, and I think easing people into some security like this has some value too. I've seen an awful lot of clients get locked out of accounts. On trade, I think you're right. I think two-factor should just be forced, and everyone will get up to speed, they'll learn it, and they'll use it.

Marcelo: I think people get annoyed.

James: People get annoyed, and some companies are concerned with making their clients angry. So they take a softer, optional approach. But by and large, we're heading towards a system where it's going to be everywhere and it's going to be mandatory. And I think it's key.

Marcelo: Password manager.

James: Password manager. So I can remember as a student fresh out of school, I had an internship, a stage. And while we were there, a new IT czar came into power, and he had this broad view of security and wanted everything locked down. So he made very complex passwords mandatory, enforced by the system. So you had no choice but to choose them, and they rotated with great frequency. So every, I think, two months, you had to choose another one. Very quickly, people stopped being able to remember their passwords. I was working at the help desk there, and we would get huge volumes of calls from people who just couldn't remember their password. And as time went on, what people would do, because they needed a way to manage—keep in mind this was all before password managers—they would write down their password on a post-it note and stick it under the keyboard. Now, it became such a running joke that when we would get a service call, the

way we were supposed to handle it is we'd contact the client, the individual employee, and we'd make an arrangement to meet them at their desk where they would give us the password because we weren't supposed to send it over email, and then we could fix their computer. You need the password to fix the computer. We stopped doing that because it was so reliable that the password was under the keyboard that we could just go in. We'd just go sit down at the desk, go do what we need to do, and get on with work. So how do we deal with that? One of the recommendations is we need complex passwords. We need to rotate them frequently. This is real. This IT czar I was referring to, he was right. However, there's a human element here that often in security, not just cybersecurity but often, is ignored. And we need to work within the limitations of what people are able to do. Otherwise, they'll find shortcuts. Favorite example is if you find a park, and the park has a beautiful path, but there's a diagonal across that park that commuters might want to take. If they don't build a walkway down on that diagonal, people will walk it anyways and will trample the grass, and you'll get a dirt path where there shouldn't be one. So what you need to do is recognize that, put the path where people are going to walk. So back to IT, we need a process for people to get what they need done in a convenient way so that they use it, hence password manager. So what a password manager is, a bit of software. They are built into Microsoft Edge, they're built into Firefox, they're built into Chrome—so the major browsers built into Safari. They're also built into Windows, Android, iOS, OSX, all the major operating systems for mobile and PCs. And what they let you do is remember one master password or use a fingerprint or maybe a face ID to unlock this database of many complex passwords.

Marcelo: I guess it goes without saying that your master password shouldn't be doggy123, right?

James: You want something that's a little bit more complex. You want something that's maybe biometric. You want something that is not going to be guessed. But now you only have to remember one password. And you take that, it unlocks this list of passwords, and you can go do what you need to do. You can rotate those passwords. Critically, you can use different passwords for every service. That's something we haven't talked about. Something that often happens is when a service is breached. So let's say you subscribe to a major website. That website gets hacked, and the list of all the users and all their passwords and all their information gets stolen. That ends up on the dark web where people can buy it. It's a product that's for sale. People buy this list, and they take it, and what they'll do is they'll say, "Okay, Marcelo uses password doggy123. Let's go try it on all the other major services. Chances are he's human, and he has reused that password all over the place because he can't be bothered to remember—not bothered, that's the wrong word—he can't manage the volume of passwords that would be required, so he's reused it probably all over the place for his Hotmail, for his Gmail, for his Netflix, for this, that, and the other thing."

Marcelo: I was having a conversation with a friend not long ago, and she was saying, "Yeah, I got hacked recently, and it's been a headache and all that." And I asked, "Do you use different passwords?" And she's all proud, "Yes, I do." And then I said, "Are all those different passwords iterations of the same password?" And she said, "Yes." It's like, bingo.

James: Bingo. Yeah. So you end up with one breach, and the next thing you know, you're fully exposed, and you're trying to remember. But if you had different passwords for each, they might have your email address. They'll go to Netflix, and you might have a Netflix account. But if the password is different, or let's bring it back to two-factor, if you have two-factor, they're not getting past that point. Password managers solve this, and they just make it convenient to have complex passwords—like really random stuff, long complex passwords, many of them different for all services—and you don't have to remember them. A lot of these ones will synchronize with your phone so that you set up a password on your PC, and then you don't have to try and do it again on your phone. It just works.

Marcelo: We use Dashlane here, and it's been a game changer because I have it on my iPad, I have it on my iPhone, I have it on my computer. All my passwords are managed through there. And it'll tell me which ones are compromised. It'll tell me which ones I should change. It'll tell me which ones are weak. And then when I'm changing a password, it'll automatically just fill the blank and change it on the system. So it's been a game changer. And just for the listeners, we are putting a document together for our clients that is like a one-sheet paper with all the stuff that we're talking about here on how you can protect yourself on the internet. So that's going to be coming.

James: It's gone through editing, and it's in kind of final checks. It's imminent.

Marcelo: Two-factor authentication, password manager. What about any antivirus? Should people install anything on their computer like that?

James: Yeah, so antivirus is certain basic protection. It's like having a lock on your front door. It may not be the be-all and end-all of security, but it does take care of some low-hanging fruit. And why wouldn't you want to do that? In many cases, I'll get a call from a client saying, "I think I was infected." And when I go look at the antivirus logs, the truth is they weren't. The antivirus had done its job, stopped the infection in its place. They saw the notification, they saw the word "virus," they got scared, they called me. I love it when they do that because I'd rather go in and check myself, be sure, be confident, than have any sort of floating questions as to whether this virus actually was able to penetrate the system.

Marcelo: Is there one you recommend?

James: For Windows computers, there is one that's built in, Windows Defender, and it is excellent.

Marcelo: So do your updates, right?

James: Yeah, do your updates. So that goes without saying—your OS updates, your antivirus updates, your software updates. Anytime there's a vulnerability, companies will release an update to close that backdoor. But you want a good antivirus. There are many on the market. I like Windows Defender because it's fast, it's free, and it's shown to be one of the more effective ones out there. So why would I go spend money on something else when this one does such a good job? But there are other reasons you might want different antiviruses.

They have different features, and there are many good brands out there. There are also many bad brands. I don't want to go through a list of those right now, but you can ask any sort of consultant or PC technician, and they should be able to tell you what's good and what's not. I'd say the only thing to look out for is often we can be financially rewarded for selling software. A lot of these companies will actually give us a kickback, and that's why you'll find most new computers come with McAfee or Norton installed. They're paying the PC manufacturers to put these free trials in. The trials expire, and then they ask you for money, and you pay the company, and that's their business model.

Marcelo: Would it be fair to say I would think the majority of our clients have Windows computers and maybe a Mac? So if you do your software updates on them regularly, is it fair to say that they'll be fairly protected when it comes to antivirus?

James: If we're talking about updates for the OS, for the operating system, for Windows, no, you're not adequately protected. It needs to be done anyways because what it does is it closes all the historical backdoors. So if we don't do it, we leave our exposure to all time, okay? Instead of just whatever's current, whatever's hot, and that's a much smaller group than all time. So that's that. Now, if we're talking about antivirus updates—so those are definition updates. What those are is a list of detected viruses, what they look like. Think of it as a list of mugshots that the police might use to identify a bad guy. It's literally a bunch of pictures of bad software. And so with those definition updates, they can recognize the latest viruses that come out, which each time they look a little bit different. Are you adequately protected with that? I would say no, you're still not adequately protected. It is a great baseline security. It is a crucial baseline security, but it is still baseline. Again, it's that lock on your front door. It's not a high-security deadbolt. It's just a basic lock on your front door, but you still need it. Don't be mistaken. You still need it. How do you do better than that? The rest of it really comes down to training. You need to understand if you're taking the risk because if you're requiring an antivirus to stop something you did or a backup to undo something you did, it makes sense that if you don't do it to begin with, you're going to not need any of these resources we've talked about. And that really comes down to understanding training. There are books on this. There are people that can train you on this. There are services you can go online and read to your heart's content. You can become a security expert with free information online. It's all out there. But we need the time to seek it out. I recognize that's not always possible, but I think with the future the way it is, with the way things are now and what the future holds, it is incumbent on everybody who uses this stuff to seek out that information, to understand better what they're clicking, what they're using, how certain things protect them, and how things are risks to them. Because at the end of the day, it's them who's at risk. It's their stuff that is threatened. They need to know. They need to understand.

Marcelo: Thank you for that, James. I do appreciate you taking the time, and we'll put together that resource for clients. And if anybody who's a listener is interested, please reach out to us. Where can people reach you if they need your services, if they want to check out what you offer for businesses or clients?

James: You can go to my website, www.jfits.ca, and my contact information is there.

Marcelo: Perfect. Thank you so much, and thank you for listening.

James: Thank you, Marcelo.

Announcer: You've been listening to the Empowered Investor Podcast hosted by Keith Matthews. Please visit TMAinvest.com to subscribe to this podcast, learn more about how his firm helps Canadian investors, or to request a complimentary copy of The Empowered Investor. Investments and investing strategies should be evaluated based on your own objectives. Listeners of this podcast should use their best judgment and consult a financial expert prior to making any investment decisions based on the information found in this podcast.