The real-life consequences of having your identity stolen

PLEASE NOTE: This transcription was created using an AI transcription tool and may not be a 100% accurate representation of the recorded audio.

**James Rowe:** Having your identity used without your permission is far from ideal, and the consequences could last a lot longer than you'd expect. Welcome to this podcast from which, hello and welcome to this episode of Witch Money. It's James here sitting in for Lucia Ariano again. This week, but thankfully it's not just me.

**James Rowe:** Here in the witch studio, uh, from Witch are Fraud and Scams expert. Fair Lipson. Hello, how are you?

**Faye Lipson:** Hello. I'm good. Thank you.

**James Rowe:** Nice to have you back with us. And, uh, for the first time on the Witch Money Podcast, Steve Goddard from Financial Crime Prevention Firm Feature Space. Steve, welcome.

**Steve Goddard:** Thank you very much.

**Steve Goddard:** Good to be here.

**James Rowe:** Likewise. Um, I'm gonna start with you Fare because you've written a great piece called The Changing Phase of ID Fraud for the latest. Issue of which Money Magazine. Do you wanna just give us an idea into how fraud has been changing or specifically ID fraud has been changing over, I guess, the last few years or so.

**Faye Lipson:** Sure. So, um, a couple of years back I did a piece on, um. The kind of ne, the new kind of never ending nature of ID fraud, in which we, we have this traditional idea that Id fraud, it happens to you, might happen intensively over the course of a few months, that lots of accounts get opened in your name, and then the fraudster moves on from your identity and it's over.

**Faye Lipson:** But what we found was that there were lots of people where they were being targeted repeatedly over the course of months or even years. We had one case, which was going on for four years. Wow. Which was awful for the victim. So that's, um, a really significant change that's happened in recent years. And then, um, even more recently than that, we are seeing frauds getting quite creative with the kinds of targets.

**Faye Lipson:** So the kind of traditional, um, accounts that people are trying to open, our bank accounts, credit cards, loans, things like that. Things where the target. Is obvious, you know, they're perhaps trying to, you know, get access to a credit facility. But we are now seeing quite unusual targets like, um, mobile phone contracts or savings accounts, and we are also seeing a lot of account takeover where people's, um, existing mobile phone contract or their Amazon account get taken over.

**Faye Lipson:** So, um, there's some, lots of things happening and the frauds are kind of being very agile and changing their tactics very quickly in this space.

**James Rowe:** And the number of. Cases is on the up as well. It's not that just that they're trying new techniques, it's the number of actual cases on the up as well.

**Faye Lipson:** Absolutely. So I think there were nearly a quarter of a million cases reported to, to the fraud, um, prevention database CFAs in 2024. So that's huge. That's more than half of all of the cases that get reported to them, and it was up by 5% on the previous year. So it's, it's really. Dominated the, the overall fraud picture for some time, and that shows no sign of changing, unfortunately.

**James Rowe:** And just backtracking for a, a moment, you mentioned, uh, traditionally Frauders might try and get a credit card in somebody else's name. Or get a, a loan taken out in somebody else's name. I guess what they're trying to do there is just get their hands on some money that isn't theirs and they don't necessarily have to pay it back.

**James Rowe:** That's the straightforward nature of that, right?

**Faye Lipson:** Yeah. That's very much the case. Um, and yes, one of the most common products, in fact, I believe the most common product for this type of fraud is bank accounts. It's often the case that overdrafts are targeted, but it can also be the case that the accounts are kind of desired for money Muleing at.

**Faye Lipson:** So it, it will provide a useful conduit for fraudsters to channel, um, money that they've stolen from people through to launder it basically.

**James Rowe:** So those are the most common reasons. And remind us what you mean by money mulling.

**Faye Lipson:** Sure. So this is when, um, somebody is. Essentially recruited to, um, offer their bank account to fraudsters and they'll receive money in, which is often money that's been paid in by a scam victim, um, thinking that they're receiving some sort of service.

**Faye Lipson:** Um, and they'll pay that money in and they'll pay it to the details of the money Mule. The money Mule will ask no questions and we'll forward it onto the actual fraudster so that, uh, uh. This kind of breaks the link between the victim and the perpetrator. Sometimes the money mill knows what they're up to.

**Faye Lipson:** They know that they're involved in fraud, but very often they've just kind of been a bit gullible or naive, I suppose. And they've just accepted money for the use of their bank account and haven't really asked the right questions.

**James Rowe:** And Steve, based on what Faye's been telling us there, do you think fraudsters are.

**James Rowe:** Are they getting more sophisticated or do you think just they're generally diversifying a bit more?

**Steve Goddard:** Um, generally diversifying, so. So fraudsters will do what works. If it works, if it's simple, then they will, they will continue doing that. If there is a good return of investment for them, then why change if it works?

**Steve Goddard:** And again, it could work in different regions as well, in different countries. And, and that what we're seeing now and what we've always seen really is, is fraud. Fraud migrates. So as soon as some country, region, bank, whoever puts up controls, maybe the education is improved, then they'll go, they'll move somewhere else where there isn't that knowledge, that experience.

**Steve Goddard:** So you've got the, you've got the. You know, from an ID theft, PERS perspective, you know, you've got the historical, it's, you know, going through your bins, looking for your bank statements mm-hmm. With your name, address, and details on there. So that still happens, but as TE technology improves and it's got more sophisticated, it's a lot more, you're able to scale that you're able to, to scrape information off, off the internet.

**Steve Goddard:** Um, you load able to share information. The, the frauders are able to share information a lot more easily. And being able to, like I said, be able to scale that whole process a lot more than just, you know, somebody nipping into your bins, finding a bank statement and setting up an account in your name. And it's, uh, like, like Faye said, it's, it's the effectively, you know, they want money at the end of it.

**Steve Goddard:** So it's, you know, setting up a credit card or, or a, or, um, a phone, a phone contract very simply. But it's also building up good credit. So these could be, these could be dormant for a number of years, or they could be, they look like genuine activity for a nu for, you know, period of months and years. And then that's when something happens.

**Steve Goddard:** So they look like a really good customer. They pay their bills on time, they credit gets extended to them so they can get more and more money. So they're playing the long game as well as the short. So it's a very sophisticated, complex kind of, you know, fraud doesn't look like one thing. It looks like a lot of different things.

**Steve Goddard:** So you're also always kind of keeping an eye on the very simple techniques, things that have been there around, around there for, for decades. You know, I've worked in fraud for, for, for 20 years now. Some things haven't changed. Some things have. So your, your, your day-to-day job is, is it just gets broader and broader every day.

**Steve Goddard:** The more technology exists, the more, um, uh, techniques kind of get, get, get perfected over time. You're constantly kind of facing this kind of ongoing battle.

**James Rowe:** As you say, you have worked in this industry for a long time as an expert, I should say, not, not as a fraud yourself. Thank you for clarification. Yes.

**James Rowe:** Um, but you, uh, you were a victim, which sounds like a, a, a brutal term, but, but you, you were right.

**Steve Goddard:** Yes. I, it's, it's not, it, it shouldn't be a brutal term. I am, I am in a position where I am confident and happy to, not happy to say, but I am, I'm willing to go out and say that I have been a victim of identity fraud.

**Steve Goddard:** Um, part of the, you know, there is a huge amount of stigma around being the victim of fraud and terminology and, and, and wording that we use around it. Um, so I feel that in my position, I, I, you know, I have the experience and I able to say, actually. Fraud does happen. Fraud happens to, can, can happen to anyone.

**Steve Goddard:** Me as a quote expert, um, you know, it can still happen to, to, to somebody like me, no matter, you know, what things I put in place. You know, the, my, um, how careful I am with my, with my details. You know, I shred my, any documentation, I make sure you need to take labels off your Amazon packages with your name and address on it.

**Steve Goddard:** All of the things like that. You can do everything in a world, but actually you are, everyone is susceptible to being, to being a victim, um, at some point in their life, unfortunately.

**James Rowe:** So take us back to the moment it happened. What happened and when did it happen and how did you find out?

**Steve Goddard:** So there's, there's, there's been a couple of different things.

**Steve Goddard:** There's, there's been a few things that have happened to me. So initially I got a letter from. Um, from Company's house congratulating me on becoming a director of a company in Wales. Right. Uh, which was a massive surprise to me. Um, and that followed a couple of letters from a couple of banks to say. Um, the first one said that a bank account, my bank account had been closed due to the suspicious activity that had been seen on that, on that account.

**Steve Goddard:** Um, what followed was another letter congratulating me on the opening of a, of a new savings account. So savings accounts are slightly different because you're not applying for credit, so it won't show in your credit score

**James Rowe:** and presumably you, you know, you check your credit score regularly, hence why you didn't spot this come up.

**James Rowe:** Yes.

**Steve Goddard:** Yeah, I mean, I mean, I, I've been working in the industry. This is the advice we give other people. So, you know, you're racking your brain saying, this is what I tell other people to do all the time. What do I need to do myself? And, and yes. You know, I I, I keep an eye on my credit report, making sure everything looks fine, but 'cause it was a savings account 'cause you're not applying for credit.

**Steve Goddard:** You, it doesn't show up. Sometimes it shows up as a soft check, but it doesn't flag to say, you know, you, you've applied for credit, you know, blah, blah, blah. This is your name and address. Um, which kind of goes into, to, to, to faith pointing around the, the mule accounts. You know, these, these accounts are being set up for the purposes of Muleing.

**Steve Goddard:** Um, but transferring money, being that gonna point in between. The, the, the, the, the scammer and them, um, taking their money away. There's been a couple of incidents subsequently as well. So a van insurance was taken out in my name. I don't have a van, so that was an, the immediate kind of red flag. Um, but that one's a great example.

**Steve Goddard:** 'cause you know, I had the, um, I had the registration number of the, of the van in, in, in question, so I could pass that on to, to action fraud and the police to take forward with. Um, and again, recently, uh, I had another, um, a flag to say a. A check was, was taken, was, was done to open a, a credit card in my name.

**Steve Goddard:** I phoned, phoned the institution and they confirmed that no account was set up and it didn't progress. 'cause after the first couple, I, I actually put my name, I requested to have my name on the, um, on the CFAs list. So anything that does flag up like that will, will, will flag to them to say, you know, this person has been a victim of fraud.

**Steve Goddard:** Take extra care going forward. Um. So, so yeah, that was, that was my experience and, you know, happy to, happy to share that and, and tell people, and advise people of what I did and just kinda get the word out so people aren't, aren't, you know, afraid to, to come forward and, and kind of report this as well.

**James Rowe:** Yeah, it's really important, isn't it, that people, especially in your circumstances, are happy to go on the record and say, look, it can, if it can happen to me. Then it can happen to you. And very, um, you speak to a, a lot of people all the time who are also in Steve's position where they're victims as well.

**Faye Lipson:** Absolutely. Uh, as, as Steve said, there's, there's really no blame attached. It really can happen to anyone. It doesn't mean that you've been the weak point very often, that your da your data may have been in a, a data breach with a company that's, you know. Not your responsibility at all, or they've got other ways of scraping it off off the web.

**Faye Lipson:** Or if you are on company's house anyway because you are a company director or company officer, then you are very much more exposed. So yes, it's really common and we see victims from all walks of life, including people who are, you know, very careful, very, um, knowledgeable about this issue.

**James Rowe:** And Steve, just to go back to you quickly, you mentioned you'd asked for your name to be put on, uh, a list.

**James Rowe:** Remind us what that was, and can other people do that as well?

**Steve Goddard:** Yes. So that's the, that's the CFAs list. Uh, C-I-F-A-S. Um, so you can go online and you can, you can request to have your details on there. The institutions that I actually spoke to, they, they, they did the same thing. So they, you can ask to be on that list.

**Steve Goddard:** You know, you speak to the, you know, the institutions in question, um, or you can, you can kind of request to do that yourself. So that's, that's, that's a, that's a good, that's a good step. You know, face it at the very beginning, you know, there's, this could go on for, for years, for months, you know, who, who knows.

**Steve Goddard:** So it's good to kind of have that reassurance to know that there is something in place to, to protect you. You know, you still still check your, your, your, um, your credit score, you know, sign up for all the buries that you can. Um, sometimes you get it free with your bank account, so just kind of, you know, build it into your kind of your, your, your, your regular routine to kind of check those things and

**James Rowe:** keep on top of it.

**James Rowe:** Going back to the examples of, of you being a victim, why, why were you a victim so many times? Is it a case of once fraudster has your details, they're gonna try and exploit as much as they can

**Steve Goddard:** because it worked. They, again, different groups were using it, you know, the company's house group. It, it was a, it was, uh, my name and, and my address.

**Steve Goddard:** That was, that was all that was needed to set up the bank accounts. It was my name and my address. Uh, the email address and the, the phone number and the date of birth were all different. But that didn't, that didn't mean anything. They had a name and they had an address and that name, my name is registered at this address on the electoral role.

**Steve Goddard:** So that was a, that's an in for them, you know, they can stick in a different email address and, and phone number. 'cause you know, they, they, they, they kind of want the communication to go there. But it worked. They had success. They tried it and, and it, and it worked there. There was an accountant which they could use.

**Steve Goddard:** If they tried it and it didn't work, then they move on to the next one.

**Faye Lipson:** So I think this is a really good point. So there's this traditional idea, I suppose, in identity fraud, pre prevention, that, um, frauders kind of, um, use your identity over a short space of time. And then, um, the banks kind of wise up to it and then they move on.

**Faye Lipson:** And then you're not a victim of identity fraud anymore and you don't need to be so vigilant anymore. And, um. That's, in my experience, that's sadly no longer the case, if it ever was. Um, we see actually that people's identities don't lose value to Frauders over the time. They, they gain value because they've been proven, they've been proven to work, as Steve says.

**Faye Lipson:** And so they just gain in value and every time one avenue is closed off, like. You know, for example, um, you go on the SFAs Register and, um, all of the industries that tend to check that, such as the financial industries, uh, that might be closed off to you, but then they're going to try perhaps something a bit different.

**Faye Lipson:** You know, they'll try perhaps a savings account or something that doesn't perform quite the high level of checks that a bank account with a credit facility might do. They're gonna branch off into different industries. You might see gambling accounts set up in your name, you know, online gaming accounts.

**Faye Lipson:** Things like that. And so what we see is that it can go on for a very long time. And, um, SI fFast protective registration lasts for two years, which you would hope would be enough, but I have seen cases go on for longer than that. And in some cases people might need to sign up again if they're still experiencing fraud.

**James Rowe:** It's pretty scary. Isn't.

**Faye Lipson:** Yeah,

**James Rowe:** it is though, isn't it? I mean, just, just the, you know, the list of things you mentioned there. It almost seems like an endless list of, uh, of targets for, for each and every one

**Steve Goddard:** of us and the digitization of the world. It, it means that, you know, you. Uh, when was the last time you got paper bank statements?

**Steve Goddard:** Oh, yeah. It might even be a decade. It doesn't, it doesn't happen anymore. Yeah. You get emails, you get, you get SMSs and I mean, luckily I got these two letters, but that was, that was rare. One. The, the first one, I didn't get a letter to say the account was opened, only that it was closed. Luckily, the, um, the, the second one, it was a letter to say it opened.

**Steve Goddard:** Yeah, but you know, they, they could have, and I've, I've had this with, with other kind of genuine, uh, I was adding, I was, uh, getting a, um, a sim card for my daughter and I was logging in through, through, through my account and at one point they asked if I wanted the confirmation to go to a different email address.

**James Rowe:** Mm-hmm.

**Steve Goddard:** And that was a great example of where if I was a, if I was a fraudster, then I could go in and add a different email address to that and then that goes somewhere else. And I is the original account. Isn't aware that that's happened.

**Faye Lipson:** Yeah. And, and fraudsters, they, they have forums, don't they, where they share tips about which providers Absolutely.

**Faye Lipson:** Yeahs, do things like this and they, they share those vulnerabilities with each other. Yeah. So that the, the, the process gets refined over time. Um, and it's, yeah, it's pretty scary stuff. They're looking for

**Steve Goddard:** weak spots, aren't these? Absolutely. So this is where I get to use my favorite analogy. This is, I love a film analogy.

**Steve Goddard:** So I, I, when I talk about this, I, I, I, I liken it again, it shows my age to, uh, to Jurassic Park, to the very first one, not any of the subsequent films. Um, but the, the raptors are testing the cages, uh, the, the fences to see if they're electrified or not. Mm. If they are. They'll move on to the next one. Frauds and scammers are exactly the same thing.

**Steve Goddard:** They get to a point, and if they get stopped, they'll go, they'll go somewhere else, they'll try something else. If they get stopped there, they'll go somewhere else. There's money to be made. There's a good return of investment for them here. So it is in their best interest to, to find a way through. And they, and they will.

**Steve Goddard:** And like, like Faye said, they will share that level of information, their, their collaboration unfortunately puts, puts our in the, in the, you know, in the genuine world. To shame sometimes. It's a good analogy,

**James Rowe:** by the way. Thank you very much. And we'll remember it further on from today. Um, can we talk about telecom fraud?

**James Rowe:** Because again, in your piece fair, uh, in big, bold letters, it said telecoms fraud is on the rise.

**Faye Lipson:** Yeah, that's right. So, um, this is really lucrative for fraudsters, isn't it? Because if they can use some innocent person's identity and take out, um, a mobile phone contract, they can often get, for example, the latest sty iPhone shipped out, and that could be worth, you know, more than a thousand pounds in many cases, and they'll intercept that.

**Faye Lipson:** Um, and then the, the poor person whose, uh, whose name has been used on the account kind of ends up in the firing line. Like, you, you know, we've sent this out, it's been received. Are you telling us that you didn't do that? And, and that's exactly what's happened. We've, we've got, uh, a case study, a really, you know, stressful experience for a lady that found that, um, the mobile phone company that had sent out a phone in her name did kind of, didn't really believe her.

**Faye Lipson:** When, um, she said she hadn't received it. This is the case of

**James Rowe:** Elaine, isn't it? That's right. I, I was reading this a, a little bit earlier on, and she felt as if Virgin, uh, virgin media were almost trying to catch her out because she, she felt as if they didn't believe. What she, what, what she was telling them.

**Faye Lipson:** Yes, she said, she said that, um, during one of the many phone calls she had to try and sort this out. She said that one of the, uh, Virgin Mobile employees actually said to her, look, I believe you, but my colleagues in the fraud team don't, which is a horrible position to be in. And what transpired in her case is that.

**Faye Lipson:** Um, somehow fraudsters had obtained a picture of her door and possibly edited it to make it look like her parcel had been left there, um, and uploaded that so that it looked for all the World. Two Virgin Mobile likes that the correct address had received this phone. But, um, the only reason she feels that, that, that she could prove her innocent.

**Faye Lipson:** Um, was that actually she had repainted that door in the last year, and so it looks like the fraudsters may have taken the picture of the door from Google Maps, like a slightly outdated image of the door. And she told us that she felt that was how she was able to prove her innocence due to the she fluke of having repainted the door.

**Faye Lipson:** But, um, Virgin Media disputed that they said that, you know, if, if the door had still been the same color, they would've continued to investigate and they would've got to the bottom of it eventually. Nonetheless, that's a really stressful experience for someone. And, and that's, you know, this type of fraud is really on the rise.

**Faye Lipson:** So

**Steve Goddard:** it's a really good example. 'cause again, back to, so I, when I first started in fraud 20 years ago, I used to investigate direct debit fraud for, for, for a bank. And, and that's exactly what we saw. We saw phone contracts being being opened in people's names. A phone would be shipped out, then, you know, they would, they would sell the phone because it's, it holds a lot of value.

**Steve Goddard:** And then just be left with a direct debit payment. And then there would be the investigation you'd, you claim as, you know, I didn't open this account. And then, you know, they would have to go through the refunding of their direct debit payments. Yeah. So it's a great example of. Things, things haven't necessarily changed.

**Steve Goddard:** The, the attack has maintained the same, but the scale of it has, has increased.

**Faye Lipson:** Absolutely. Yeah. So it's, it's not quite doubled, but almost so the, these kinds of telecoms impersonations have increased by 73% in a year. So that's huge. Absolutely huge. And then an adjacent, uh, form of fraud that we are seeing is where, um, it's an account takeover type of fraud where people, it will typically start where people will receive, um, a phone call off, a fake phone call, offering them an upgrade from somebody posing as their network.

**Faye Lipson:** And, um, the person will give them all, all the details, um, of their account. And then that fraudster will take those details and actually, you know, compromise the victim's account. Or register a new account for themselves. So that's quite common as well. But yes, these, these, um, telecom telecoms contracts and products are really, are really in favor with identity fraudsters right now.

**James Rowe:** And with that example you just gave there, it shows a very direct link between the fraudster and the victim. You know, that's a phone call between the victim and the fraudster. Absolutely. But for other cases. I, I guess for a lot of victims, they just don't know how they became a victim. Like for Elaine, for example.

**Faye Lipson:** Exactly. I guess

**James Rowe:** she has no idea how or why she was targeted.

**Faye Lipson:** It, it, it can be exactly that. It can be, it can be a kind of jigsaw of different things. So it could be a few details lifted from social media. It could be a few details lifted from a data breach for the same person or, you know, scraped from other sources and just pieced together to make a more complete, um, picture of that person's identity.

**James Rowe:** Uh, and just to say, um, just to make sure we give Virgin Media's point of view as well, uh, they said that they work hard to tackle fraud and will always work closely with individuals who report such activity to investigate what happened. Uh, and where required ensure correct action is taken off the back of that.

**James Rowe:** Steve, do you think that companies almost need to do more to protect their own customers?

**Steve Goddard:** This is, this is a difficult one because I think the, the, the perception from an outside view is yes, they need to do more, but there often, often isn't the visibility of the huge amount of work that that does take place.

**Steve Goddard:** These institutions do, do. You know, fraud is, fraud is a big part of any kind of business. You know, they spend a lot of money. There is a lot of overhead from the individuals doing the investigation, the software that they use, the solutions there is, there is a lot there. And we, we, we talk about all of the, or the negatives, all of the, um, unfort unfortunate victims, you know, myself, one of them as well.

**Steve Goddard:** And I'm, I can, can say that from, from, from, you know, from, from my point of view. But there's also a huge amount of, of people who, who didn't become victims because of all the work that these organizations do in, in the background, we hear about all the bad stuff that happens, and that's terrible. We always wanna reduce that.

**Steve Goddard:** But there is also a huge amount of work done to, to protect a lot of people, to stop them becoming victims too.

**James Rowe:** Because the either of you, I imagine both of you speak to a lot of people who tell you, I think I was almost about to be scammed and then I spotted something. Or they might tell you a story about how they were scammed and, you know, getting in touch with the, with the company involved was an nice, easy process and things got resolved pretty quickly.

**James Rowe:** Is that fair to say as well?

**Faye Lipson:** Yeah. Absolutely. Yeah. I, I think it's also fair to say that kind of different industries are at different points along this journey, so you might, I think it's fairly uncontroversial to say that banks are kind of much further along in this, in this journey, uh, than, than some other industries are.

**Faye Lipson:** And actually bank the banking industry, UK Finance, has expressed its frustration with other industries that. Perhaps not as far along as they are. So, um, yes, it really kind of depends which, um, industry you're talking about in some ways as well.

**Steve Goddard:** Yeah. And there isn't, there isn't a, a, there isn't a silver bullet.

**Steve Goddard:** There is, it isn't one group's responsibility. It's not my responsibility. It's not the banks, it's not, it's not the telecom's companies. It's, it's everybody's responsibility to, to to, to do what they can, you know, law enforcement as well. Everybody, everybody is, is kind of struggling with, with, with budgets and finances and availability and resources.

**Steve Goddard:** Because like we've said, you know, fraud is, fraud has increased massively, and sometimes you don't have the same, the same resources that that you used to have. It's, it's, it's, it's tough and you are spinning all these plates and you are, you know, you're trying to keep, keep your head above water and make sure you are, you're protecting everybody.

**Steve Goddard:** But it's, it's difficult.

**James Rowe:** And for AI is just complicated in this matter, even more, isn't it?

**Faye Lipson:** Yeah, absolutely. I think it just, um, it enables the fraudster to. Send out the kinds of phishing, really highly convincing and accurate looking phishing attacks that, that gather so much of this, this, um, stolen data that can then be funneled into this type of identity crime.

**Faye Lipson:** So yeah, it, it enables them to kind of create hugely compelling looking emails that look like they're from government agencies or, um. Bailiffs, you know, debt collectors or whatever that actually cite the correct legislation and use industry jargon and terminology. Even though the fraudster doesn't know it themselves, they can just ask AI to put it in.

**Faye Lipson:** And that's why it's, it's just easier than ever for fraudsters to kind of make these, make these big fishing expeditions for this kind of data. Um, and that's why they're, they're, they're gonna carry on. 'cause the, the barriers to entry are, are lower than ever before.

**James Rowe:** And fake IDs as well. Uh, just, just how easy is it for a fraud to, to sit and generate a, a fake ID of, of me or you, for example.

**Faye Lipson:** Yeah, so that's an interesting one. So, um, from speaking to experts on this, what, what I've learned is that if you were to just ask, for example, um, an AI. Image generator or chat GPT or something to, to create a fake ID for you. It, it looks rubbish. It's really unconvincing. Um, uh, but what frauds does actually do is they layer on different technologies.

**Faye Lipson:** So they'll have coding, they'll have templates, they'll have ai, and they'll, they can create really convincing, um, kind. Digital images of like driving driver's licenses, for example. This way, especially if they have managed to steal, um, or trick you into giving a, a digital image of your, your genuine, um, driving license.

**Faye Lipson:** So what they can do is they've got that, say, say they've tricked you into thinking that you're speaking to the DVLA or something and they've managed to obtain that from you. What they can do is then kind of bring all their tricks into play, um, image editing, coding and, and layered templates and ai. To, to swap your photo for their photo, but then keep all of your details so then they can kind of use that as, um, a form of entry to online bank accounts and things like that.

**Faye Lipson:** So it's really scary and, and that's, it's one of the reasons why it's so important. A, I suppose, just to keep hold of your. Physical wallet sounds like really old school advice, but it's really important. And also just to, if, if you ever kind of receive, um, a request via email or if you are on a, a website that seems to be asking you to submit an image of your, um, identity documents, just think really carefully.

**Faye Lipson:** Like, how do I know that this is genuinely who I. Who I think I'm interacting with and just stop and verify it. 'cause there are many, many fake websites out there. Impersonating government agencies, banks, and all, all kinds of institutions really.

**James Rowe:** And Steve, how quickly do you think this is gonna continue to evolve, especially with AI now, it just develops so quickly in itself.

**James Rowe:** But putting that on top of, uh, ID fraud. Just, where are we gonna go with this over the next few months or few years?

**Steve Goddard:** It's, it's, it's just gonna continue to scale. As I say, it's, it's, it works. And when it, when it, if it, if it works, then, then, then why change? When we used new technology, we have to, we had to abide by, by, by laws and regulations and compliance.

**Steve Goddard:** They don't, they can jump ahead to how can we exploit this, how can we use it, like face said, to make, to make fake IDs to, you know, when there's a data breach to kind of, to, to troll through and pass all that data into usable format that I can, I can use and exploit, exploit individuals and, uh, and, and do what I want to do with it to, you know, to, to, to make money and, and have that power and control.

**James Rowe:** So let's do some advice then, uh, to try and get ahead of the, the fraudsters. Uh, what have we got? I've got a few notes here to begin with. Check your credit score. I guess that's a, a, a good one to see if anything's already happened.

**Steve Goddard:** Yeah, and there's, there's a number of bureaus, so you might have, again, like I said, you might have one with your bank account, but be with one and different, different organizations.

**Steve Goddard:** This is where it gets frustrating. Different organizations use different credit bureaus. To do those checks. So just because it doesn't flag on on your one doesn't mean it's not gonna flag on someone else's one. So having a, a kind of broad sweep of as many of those bureaus as possible should say

**James Rowe:** Equifax, Experian, and TransUnion are the three we should be checking.

**James Rowe:** Yes. Hundred percent. I wasn't sure if we can use the names, but thank you very much. Absolutely. So

**Faye Lipson:** we've got a witch guide on how to do it, and in most cases, I think in all of. Cases now all three of them, you there are kind of free versions available. Um, and some of them will even email you once a month to remind you to check and sometimes they will even email you to let you know something's changed.

**Faye Lipson:** So yeah, that it's well worth doing. And I think we can share that in the show notes, can't we? Yeah,

**James Rowe:** for sure. We'll pop some useful links in there. Um, say what else, what else should be people be doing in the, in the meantime?

**Faye Lipson:** So, um, I know, I know it is, it gets boring almost saying this, but like. You must set, uh, a strong, unique, complex password for every single account, and I know it's a pain.

**Faye Lipson:** Um, what's been a game changer for me is using a password manager. Um, not, not just to store the passwords, but it actually suggests passwords as well. It's just, just. Takes seconds. It will, it will suggest a completely random string of letters, numbers, symbols, et cetera. And then it'll save it for you. And that's, that's wonderfully easy if you don't want to use that or you're nervous about doing so, you can use the three random words, uh, kind of pass phrase method where you, you literally just pick three completely random words that are related to each other, and then you kind of insert some numbers and symbols in as well, perhaps kind of.

**Faye Lipson:** Um, replacing some of the letters with them or putting them in between the words, for example, and

**Steve Goddard:** even, even, even Google does password management and things like that. Exactly. And also looks for, um, where your details might have been compromised as well.

**Faye Lipson:** Absolutely. Yeah. So there's, there's loads of free tools available and it, while you're strengthening all your passwords and making sure they're all unique, turn on two fa, wherever it's.

**Faye Lipson:** Available. This is two factor authentication. Yeah. So this means that, um, that you are gonna need to provide an extra piece of information that confirms who you are. So, um, it might be that you have an authenticator app on your phone or that you receive, um, uh, a short, um, one-time passcode to your phone via SMS.

**Faye Lipson:** Um, that that's always. Always turn that on. If that, if that's an option, even if it's not on by default, but it's an option, please turn it on 'cause it's always worth doing.

**James Rowe:** And also check your post as well in case a letter comes and says You've opened a bank account. And you're like, I have not opened a bank account.

**Steve Goddard:** If you are, yeah, check your post. And if you are, if you're expecting a letter from, from an organization and you don't receive it as well, that's another thing. It may have been redirected. So these, you know, things that you need to be aware. Check your, check your statements on your, you know, on your phone, your device, if you still get the paper statements still, we still go through that as, as, as often as you can to look for that kind of activity.

**Steve Goddard:** You know, checking, checking letters, you know, you know, maybe the label's been peeled off or, or things like that of suspicious packages. You know, they're just making sure they're validating the address is, is, is, is genuine. All of those kinds of little things. Any kind of little trusty gut, I would say. A hundred percent.

**James Rowe:** Well, we've learnt loads and plenty to take away as well from today. Uh, fa thanks very much for joining us. Thank you. And Steve, thank you. Thank you very much. Thanks for listening to this podcast from which the UK's consumer champion. You can find plenty more advice about what we discuss today in the show notes.

**James Rowe:** There you'll also find a link to become a witch member for 50% off the usual price. An offer exclusively available to you are podcast listeners joining, which will not only give you access to all of our product reviews, our app, one to one, personalized buying advice, and every issue of which magazine across the air, but you'll also be helping us to make life simpler, fairer, and safer.

**James Rowe:** For everyone. Don't forget to hit subscribe wherever you're listening. That way you'll be notified whenever we release a new episode of which Money, which Shorts or another podcast that we make for you. And if you wanna get in touch with us, then follow us on social media, where at which uk or you can drop us an email to podcasts@which.co uk.

**James Rowe:** See you next time.