FSCS Podcast – Episode 46: How to spot a scam in 7 steps

Martyn Beauchamp 00:01

Welcome to Protect your money with FSCS, the podcast from the Financial Services Compensation Scheme. I'm Martyn Beauchamp, CEO at FSCS, and in this series, the fantastic FSCS team will help you understand how we can help protect your money so you can feel confident that your money is safe. I hope you enjoy the podcast.

Amy Alford 00:26

Hello and welcome to the podcast. I'm Amy Alford, a Content Editor here at FSCS, and today I'm going to be talking about fraud and scams and how you can tell whether a message claiming to be from FSCS is genuine.

Here to help me with this is my content team colleague, Blessing Zoe-Shamah. Welcome to the podcast, Blessing. Could you tell us what you do here at FSCS?

Blessing Zoe-Shamah 00:48

Hi, I'm Blessing and I'm also Content Editor at FSCS. Thanks for having me on the podcast, Amy.

Amy Alford 00:54

Brilliant and thanks for joining me. Now today's episode is specifically going to look at scams that use our name or logo to make a message seem legitimate, usually with the aim of tricking you into parting with money or personal details.

We've noticed there are quite a few telltale signs or red flags that you can look out for, so we've made a list of the seven most common ones. We're going to take you through these one by one and we'll share examples of some of the fraudulent messages we've seen recently along the way.

Before we do that though, I think we should give a quick overview of FSCS and what we do in case we have any new listeners joining us.

Blessing Zoe-Shamah 01:28

Yep, sounds good. So FSCS, which is short for the Financial Services Compensation Scheme, exists to protect customers of authorised financial services firms if they fail, or have stopped trading. If the financial firm you've been using goes out of business and can't pay your money back itself, we may be able to step in to pay compensation, assuming you meet our eligibility criteria. We protect lots of financial products, but not all of them, so do visit our website for more information.

As we're talking about scams today, we should also note that in most situations, FSCS unfortunately can't compensate people for money that has been lost due to scams or fraud. The exception to this is if you've received bad advice from an authorised financial advisor to invest in something that turns out to be a scam. We'd need to assess each individual claim to check our eligibility criteria has been met, but we may potentially be able to pay compensation in this situation.

Amy Alford 02:19

We're committed to doing everything we can to fight fraud and scams though and the tips we're going to share in this episode will hopefully help you spot and avoid messages that have come from a scammer.

If you ever receive an email, letter, phone call, or any other sort of message from someone claiming to be from FSCS and have any doubts about whether it's genuine, please get in touch with us through our website at www.fscs.org.uk or by calling 0800 678 1100. Please don't give out any personal information or make any payments. We'd always much rather you play it safe and check with us, so don't be afraid to contact us if you're at all unsure.

So Blessing, where shall we start? What's the most obvious sign that a message might be a scam?

Blessing Zoe-Shamah 03:04

The biggest telltale sign that a message isn't genuinely from FSCS is if you're asked for money. Our service is completely free of charge when you come to us direct and we'll never ask you to make any sort of payment. Not before you start, not during the claims process and not afterwards. We'll also never ask you for credit or debit card details or security codes.

Amy Alford 03:23

And while it's often obvious that you're being asked for money or personal details, this could also be more subtle. You have an example, don't you?

Blessing Zoe-Shamah 03:31

Yes, that's right. We've recently seen a fraudulent letter that promises the return of some invested money if a trade reference number can be provided. If the customer doesn't have this number - which they won't, because it's not a real thing - they're encouraged to call the scammer and pay for a temporary licence.

So the request for money and payment details is disguised, but still very much there. And it's important to be aware that this type of fraud, which is often called phishing, can come in many different forms.

Amy Alford 03:56

Yes, so in that example, the customer received a letter in the post and was then encouraged to call a phone number. But we've seen other cases in which scammers have tried to trick people into giving away details by filling in a form or by clicking on a link that takes them to a fake website.

They could also get in touch by calling you out of the blue, sending an email or contacting you in another way, such as through social media. And that leads us on to the second sign that can tell you a message isn't really from FSCS, that it's come through an unusual channel. Blessing, can you tell us a bit more?

Blessing Zoe-Shamah 04:27

I can. We've noticed that scammers will sometimes use WhatsApp, Facebook, Instagram, X and other social media accounts to contact people.

FSCS doesn't use WhatsApp, and while we do have a page on some social media sites, we don't send messages to people out of the blue from these channels. We'll only get in touch with customers by email, letter or phone call. There's also a web chat on our website that you can use to contact us.

So if you get a message claiming to be from FSCS in any other way, that's a sign that it isn't genuine and that you should ignore it.

Amy Alford 04:57

You can report the message to us by using the contact details on our website too. We'll review it for you and let you know if it's likely to be fraudulent. We may also share an example of it on our website and on social media to warn others.

As we're not an enforcement agency, we can't take any steps against the suspected scammers, but we'd encourage you to report scams to Action Fraud who may be able to. You can do this by visiting their website at www.actionfraud.police.uk

Okay, what should we cover next?

Blessing Zoe-Shamah 05:29

The next thing I'd look out for is if the phone number you're asked to call isn't the one on our website. Before calling any number, you can do a quick online search to check that it belongs to the organisation you expect it to. FSCS's number is 0800 678 1100 and international customers can also use +44 207 741 4100. Both are listed on our website.

I think we should note here that telephone numbers can also be spoofed. So it's possible for a scammer to use a fake caller ID to make it look as though they're calling you from FSCS. We've been seeing a rise in this sort of scam, unfortunately.

Amy Alford 06:06

And what can people do if they get a phone call and aren't sure whether it's really from FSCS?

Blessing Zoe-Shamah 06:12

Well, if you have any doubts, hang up and get in touch with us via the details listed on the Contact us page of our website instead. Don't worry about appearing rude. We'd much rather that you're cautious and stay alert for scams, so hang up and call us back if you're at all unsure.

Amy Alford 06:26

Thanks, Blessing. Now the next point we want to cover is similar. So, another telltale sign that a message hasn't really come from FSCS, and is likely to be a scam, is if it's been sent from an email address that doesn't end with @fscs.org.uk

Blessing Zoe-Shamah 06:41

Yes, we've seen fraudsters use addresses ending with @fscsrecovery.org or @fscs.com for example.

Scams are becoming ever more sophisticated too and it's possible for scammers to make it look like they have an official FSCS email address. So you should still be careful, even if the address does seem to end with @fscs.org.uk

Amy Alford 07:00

And as with a phone call, if you're ever unsure whether an email or any other type of message is really from FSCS, you can get in touch with us to double check by using the contact details on our website.

I think we're up to our fifth point now, Blessing. What's the next red flag to look out for?

Blessing Zoe-Shamah 07:16

Next up is if the message is about a firm that isn't authorised by a UK regulator. That's the Financial Conduct Authority (FCA) or Prudential Regulation Authority (PRA).

FSCS can only pay compensation when certain requirements set out by the regulators are met, and one of these is that the firm must have been authorised at the time you did business with it.

You can check the Financial Services Register on the FCA's website at register.fca.org.uk to see if the firm mentioned is authorised. If it isn't, that's a sign that the message isn't really from FSCS and is probably a scam.

Amy Alford 07:48

I think we should mention that scammers could, of course, try to use the names of authorised companies to get you to part with money or personal details too. But as Blessing says, if the firm isn't regulated then it's very likely that the message you've received isn't genuine, because it wouldn't be something we'd be contacting you about.

Blessing Zoe-Shamah 08:05

Exactly. Most cryptoassets, for example, aren't FSCS protected because they're not regulated. This includes virtual currencies like Bitcoin or Litecoin. So when a customer got in touch to show us an email they'd received claiming to be from FSCS, we could quickly confirm that it was fraudulent.

It included a section that said, "we have identified a Bitcoin wallet registered in your name holding an available balance of approximately $154,000 US dollars". Fortunately, the customer didn't fall for the scam, and we've been able to share the example on our social media pages to make others aware of what to look out for.

Amy Alford 08:39

And that leads us neatly on to another way to spot that a message is a scam, which is if you're offered or promised FSCS compensation in a foreign currency, or if you're contacted about a firm in another country. We are the UK's financial services compensation scheme. We're based in the UK and protect UK-authorised firms.

We pay compensation in pound sterling, not in any other currency. So in the example Blessing's just mentioned, another red flag about the email was that it mentioned US dollars.

Blessing Zoe-Shamah 09:07

That's right. It also included American spellings throughout the email, which are actually part of the final telltale sign we have on our list.

So spelling mistakes, typos, or using American spellings instead of British ones, are all clues that a message might not really be from us.

Amy Alford 09:22

Yes, things like using a Z instead of an S in a word like organisation, for example.

Blessing Zoe-Shamah 09:27

Exactly.

Amy Alford 09:28

Well, that final point has brought us to the end of what we wanted to cover today. I really hope you found this episode useful and that the seven tips we've shared will help you spot and avoid messages claiming to be from FSCS, that have really come from a scammer.

Just as a quick recap, the seven telltale signs or red flags we mentioned today were:

1) If you're asked for money or payment details.
2) If the message has come from an unusual source, like WhatsApp.
3) If the phone number listed isn't the one on our website.
4) If the email address used doesn't end with @fscs.org.uk
5) If the message is about a firm that isn't regulated, such as those providing cryptoassets.
6) If you're offered compensation in a currency other than pound sterling, or if you're contacted about a firm in a different country.
7) If the message includes American spellings or spelling errors.

If you'd like more information or to see examples of messages that have been reported to us recently, visit the dedicated page on our website at www.fscs.org.uk/scams

And Blessing, can you tell us what people can do if they think they've been a victim of fraud?

Blessing Zoe-Shamah 10:40

So as a reminder, if you're ever in doubt that a message or call is from FSCS, end the call and phone us back or send us a message by using the details on the Contact us page of our website. Don't give out personal details or make any payments.

If you have given out payment details and realise that it might have been a scam, speak to your bank, building society or credit union as they can protect and reimburse victims of certain types of fraud.

You can also report scams to Action Fraud by visiting their website, which is www.actionfraud.police.uk

Amy Alford 11:11

Thanks Blessing and thanks so much for joining me today. Now, as this is your first time on the podcast, I'm going to ask you the final question we ask all our guests.

So we're all about keeping your money safe at FSCS, but what was the toy that would have got you breaking open your piggy bank as a child?

Blessing Zoe-Shamah 11:27

Oh, that's a good question. I probably would have loved - I'm not sure what they're called - but one of those digital robot dogs that you could get. I remember pouring over the Argos catalogue when I was really young and I'd ask for one every year for Christmas. So yeah, it probably would have been that.

Amy Alford 11:40

I remember those and I really remember looking through the Argos catalogue as well. That’s a great answer.

Now, the final thing for me to say is thank you to everyone who's listened to this episode. If you'd like to hear more from FSCS, you can find all of our episodes on our website or wherever you usually listen to your podcasts. If you follow us, you'll never miss a new episode.