**How to spot a scam and avoid it**

We've got really amazing panel for you today and I'm fairly confident. There are not many questions that they can't answer. So, I'll just wait another couple of minutes. Cause I can see the number of participants is still going up. As soon as that levels off, we'll get going.

Okay.

What was this waiting for everyone to arrive? I just introduced myself. Um, my name is Sarah and I am the marketing manager for free services at ability net. This is great to be welcoming you all today. Um, our role in free services is to, um, support older and disabled people through tech. Um, which is why we're hosting this webinar today.

Um, and also, as I said, I'm very mindful that, um, people who may previously not have been, um, engaging with, uh, commercial sites or buying online might be doing so more at this time when we're less able to get to the high street. So we just really want to make sure we can give out a few safety tips and make sure that, um, Everybody has a good, safe Christmas, um, thing.

That's never been more important at this strange time that we're living through.

So the numbers are stabilizing now. So, um, I will, um, Kickoff the webinar. Um, and we'll move on. So as I said, we've got some great panelists today from get safe online, take five, um, age UK, which, and friends gate scams. Um, and there'll be an opportunity to meet them all very soon. So just a little bit of housekeeping.

This is what we'll be doing today. Um, a welcome from me. Um, I've just briefly introduce ability net and some of the services that we can offer. We'll meet our amazing, um, team of panelists. Um, we'll have a discussion as some of the, um, Key areas around scams, what to locate for, um, um, our panelists there, we'll be sharing some tips with you all.

Um, and then, you know, there's an opportunity for FAQ. Um, and, um, there's lots of links and things that are embedded in the slides, um, for people to view at their leisure afterwards, you'll receive an email and a link to the website. So don't worry if we're skipping through some of the information, because you'll get a link to view some of that afterwards.

And a recording. So you can see some captions coming up to the bottom of the screen here. Um, they're not perfect, but, um, they're okay. Hopefully for people to be able to follow along, um, they've been provided by, um, the tool within PowerPoint. As they say, after the webinar and slides a transcript and a recording would all be made available on our website.

And you'll receive a link after that. Um, please do pop any questions you have in the Q and a window. And Chris is poised and keeping an eye on, uh, we've disabled, the chat window, just because it's easier for us to keep an eye on one thing. And there are also some accessibility issues in that the chat window reads out everything in there.

If somebody is using a screen reader, Um, and please do give us any feedback after the webinar. We're always keen to make improvements for the next one. So just moving on to, um, a brief introduction to us, um, our mission is a digital world accessible to all. And as I said, we have a role in supporting people at home at work.

And in education, we have a network of over 300, um, trusted and friendly. I should point out, um, DBS check volunteers. Um, normally they would be providing support at home, but we very quickly adapt to the service so that you can, um, access aspire or free helpline. Um, and they'll be able to provide telephone support.

Um, and we've also been doing a great job in terms of like providing remote support as well. That are free online tools. We have a database called my computer my way, um, which shows you how to adapt, um, your device to make it more accessible. It could be simple things like, um, how to use Siri and you can search on operating system, or you can look at things that will help you if you have low or no vision, for example.

Um, and we also have a range of free fact sheets. Um, So in terms of making a difference, we know that that, that support is really helping people. Um, and it's not just about being better, able to use technology. 80% of people are able to do that thanks to support. But again, particularly at this time, what we're finding is that, um, we're helping people to 69%, for instance, feel less isolated and 76%.

Feel more independent. And this webinar is part of that. As I say, helping people to be able to shop and do things online with confidence, um, and where that the fear of being caught. So I will just launch our first poll because I'm keen to hear, um, from the people that we've got in the room. So. Hopefully you should see it pop up on your screen.

So the question that we're asking you is have you ever been a victim of an online scam? So it's a simple yes or no. So I'll just allow a few seconds, 30, 40 seconds for everyone to be able to put something there.

And I'm here. The panelists will come on to talk later about, you know, it's so easy. I've been tripped up myself in the past. So I think it's, you know, the question is, is nonjudgmental. I'm sure all of our experts of Harvard, their cursor and thought works mainly got caught out there. So.

Great. So I think we're stabilizing now, so I'll just end the poll and share it. So if I share the results, we can see that, um, 31% of people. Have said yes. And 69% have said, no, I'm sorry. I don't know how that resonates with our experts, but I'm sure they'll be able to give us their views. Yeah.

So meet our expert panel, um, and we will meet them very soon. So I'm really jealous. I too, today to be joined by Tony from get safe online, who has a really long history working in this area. And then his biog is on the website and lots of information about all our panelists there. We've got Joe joining us from age UK.

Katie from wish. Um, and really delighted to halfway is joining us today. Sarah, from tape five who's I know has got lots of really brilliant, um, easy tips to follow. Um, and Adam, I'm not sure we have time for, um, all of your 12 scams of Christmas, but I know you've got lots of really easy accessible tips for people, um, who to make sure that they don't get caught out.

And I'm joined by, um, Chris and Alex, um, From ability net and Alex is, um, our front support on the help lines of you call it. You're very likely to speak to him. And he's a friendly too. So moving on. So Tony, if we kick off with you, um, I was saying earlier that, um, I think this thing called social engineering is, um, key in terms of.

Understanding how scammers catches out. So it's just wondering if you could say something about what is that and how an understanding of social engineering can help protect us from scammers and how has that changed over time? Yeah, certainly. I think it frightens a lot of people when they hear the word social engineering, they think it's, it's quite technical.

Actually. It's just somebody trying to get you to do something you wouldn't normally do. Um, now this is normally a criminal trying to get information, financial information, maybe passwords, make me get to new, to buy something online and, um, and being online now, I think it's fantastic. Let me just say from the very beginning, I'm passionate about the internet, but I'm even more passionate about people being insecure.

And, and every day we see millions of successful interactions and transactions every, every single day, but there's horror stories. And unfortunately, um, this. Hosting panel is going to be here to talk about the bad news stories. Let's remember how good it is, especially in lockdown. So, um, social engineering is there.

It's been with us for an awful long time. Um, I was a assuming police officer, uh, working with, uh, online, serious and organized crime and social engineering was working then. So it's just understanding what that is and not falling fall from it. It's about seeing adverts on, um, maybe social media, uh, platforms and you full flow of re maybe somebody phoning you up seems to be a big problem at the moment.

Somebody's phoning up saying that they're they're they're from, uh, a particular organization might be a government organization. Even the police. Um, what you gotta do is put the phone down politely and, uh, check with that organization separately. So social engineering is there. Um, it's trying to scam us is trying to get you to do things that you normally wouldn't do.

And I think your point, um, Tony, about, you know, how technology is so amazing is, is a really valid one. And in a way, this session engineering point is no different from somebody who used to maybe knock on your door and say, Oh, you've got a couple of dodgy roof tiles up there. They're just using the tools that are available to them.

And so we mustn't get hung up on technology, being a bad thing. It's the people that are abusing it, who are the problem? No. I think people are scared of technology. And, uh, you know, I still, I talk to lots of grandparents and lots of parents and they say, Oh, my children are, uh, uh, much clever on it, on the internet than I am.

Well, we need to be clever on the technology, but they're not telling clever about life. And you as a, as a person that maybe you've lived a lot longer than most children. Um, no, when there's something and there's an old scene, which really, really comes home when it comes to this. If something sounds too good to be true.

It probably is. So bear that in mind, when it comes to social engineering, don't automatically do it. I mean, you're going to have Sarah from take five. Who's going to say, take five, you know, have a little gap in between listening to something. Nothing is that urgent that you get on the internet. You can't take us, take a step back.

Maybe give it to, and then think about what you do and the ability, first of all, to speak to other people. Um, maybe friends, relatives to find out what they think about the particular issue that's come through all the internet itself. The internet is a fantastic place to find out information. So when someone comes through and says, and gives you something or suggests something, um, do some research on it, you know, never ceases to amaze me when people say, Oh, I've won the lottery.

And, uh, and I say to them, did you do the lottery? Well, it's quite difficult to win a lottery when you haven't done it. So there's things like that too, if you sounds too good to be true, it probably is great advice. And I'm sure we'll hear that a lot during this session. So thank you very much. Um, so this is something we're going to come back to as well, but I'll just launch our second poll because I think, um, As I say, it's very easy to be caught out.

Um, and, and the important thing as you say, is to act quickly. So, um, I just want to invite people to join in with this panel as well. So if I launch it, the question we're asking here is would you know where to report an online scam? Um, and we can come back and discuss this later, but I think maybe it's, it's not always as, as obvious as it might be.

So again, I just allow a little bit of time here. Um,

interesting results actually. I'll share them in a minute, but, um, yeah, just a few people still voting on this one.

See 84% of people voted. So just allow a little bit longer for people to join in if they wish to.

Okay, so I'm gonna, um, end the poll and share the results. Okay. So the numbers are quite different on this one, which I think is interesting actually saying that, um, only 45% of people would know where to go. And I know Katie's going to give us some tips later about, um, you're right. Some way you can go, if you feel like you have been, um, called out along the way, um, And it looks like it's an area that people do need some support with.

And as I say, at the end of the PowerPoint, which you can come back to later, uh, links to support from ourselves and from, from all the people who've kindly joined the panel as well. So there's lots of help there. Great. So moving on. So, um, this is for everyone present will speak at once. I'm sure. Um, we'll all be able to chip in with this one, but be good to just, um, build on what Tony's been talking about.

You know, their social engineering runs through the heart of all these scams, but what are some of the things that people can watch out for? There's some technical terms here, fittings and spoofing, remote access. Who'd like to maybe, um, Maybe Adam, if we come to you, not all 12 of your scams of Christmas, but if you could maybe start with them a couple of common scams and things that warning signs for people.

So, uh, we've recently run a, uh, cool docking project for our friends getting scans. Uh, as part of that, we received information on the numbers that are being, uh, being blocked by these true coal units. Some 9,000 in the UK, uh, and remote access scams is, is, is quite a big one at the moment. So that would be someone phoning a consumer saying I'm from Microsoft or, I mean, Microsoft is generally the, the, the used one.

And they'll say there's a problem with your computer. Uh, and what they'll do is they'll, they'll, they'll convince you to allow that person on the other end of the phone, someone you don't know, never heard of never spoken to before to access your computer. And whilst they're in your computer, they'll try and steal, gain important financial impersonal information.

Uh, and again, I think it comes back to what Sarah is going to say about take five. And it's about. Uh, taking five minutes and own and kind of thinking about what you're being asked. Do you know that person on the other end of the phone, can you trust them? If. Okay. I suppose you just need to kind of think about what you're being asked, sort of ask for.

Yeah. And Katie, I know you were talking earlier and this is one that I have hold my hand up to being caught out by, but it's these adverts that pop up on Facebook and all kinds of places that are offering us really amazing things for not much money at all. You said you've seen it. A rise in those types of scams.

Maybe you'd like to tell us a little bit about that. Yeah, sure. Sarah, thank you. So, um, we've seen quite, quite a rise in people being caught out by ads that are used by scammers. So, you know, it's important to remember that just because you see an ad for either on Facebook or another social media platform, or even on Google that you think carefully about it.

So. Just because it's on there doesn't necessarily mean that it's always a hundred percent bonafide, 80. Scammers can impersonate, um, real legitimate businesses and postdocs. In fact, it's actually quite easy for them to do so. Um, we're doing some work with social media companies. I'm with Google to try and convince them of the need to verify their appetizers better so that consumers don't get caught out.

But, um, for example, uh, which we've written quite extensively about this recently, we've seen scammers impersonate. Some banks, um, specifically the Revolut, um, bank and, um, host ads off, you know, identifying that the customer services number. So now that we'll say revenue customer services, so you, you go into Google type in revenue, customer services, the ad pops up and you think then that you're calling the number.

Of that bank. And in fact, it, isn't the number of that buying community get through to some scammers and that's then a big problem because those scammers have already got your trust because you call the number, et cetera, and they can convince you to move money around. So it is important that just because you see ads that you don't necessarily always believe them.

And especially when you're searching for important information that you. Perhaps double-check with the original source. So you have things from your bank that, you know, are real, um, either emails or paper, bank statements, use the phone numbers on those rather than necessarily relying on what you find online.

That's great. And Jen, I wonder if we could come to you because the email ones, um, quite clever in terms of, um, targeting particular demographics, I've seen quite a, if you offering, um, life insurance and things like that. And I wonder if age UK you've got any specific advice, um, For the people that you're working with or for carers of people that you talking to around those sorts of email scams, um, and, and how to handle a relative who rings up and is in a panic advantage.

Um, yeah, sure. Hello everybody. Um, I mean, there's, there's, there's lots of, uh, scams out there. Um, I mean, you mentioned a few, then there's also of pension and investment fraud, scums. Um, a lot of romance fraud is happening at the moment where people, um, might be approached generally on email, um, and can start to try and develop a relationship with somebody.

And then. That Germany leads to someone making a request for some sort of financial payment. Um, it might be false later to help their friend or their family or themselves to do something. Um, I'm playing on the vulnerabilities of people sometimes. Um, sometimes people might be isolated or lonely and then try and.

Build a relationship with somebody, um, and over time, um, uh, scamming them out of money that can obviously result in obviously the, the financial hit, which is awful, but then also the. The emotional and the mentor, um, difficulties that people might face after that. And what we've found through, um, some of the work that we've done is that sometimes people can not report that because they may feel that they, um, be duped or a bit of shame.

If that would, obviously that's not right. I mean, people should feel confident in reporting things. Um, we would always say wherever possible, um, as others have said, Just take some time to check through what's actually happening. Um, I mean, I get emails all the time from, from, uh, from scams, from scammers and they look really, really genuine.

And unless you start to look into it a little bit, um, sometimes if, if you get an email, you can click on the actual email address itself and it might look realistic, but when you click on it, you'll see that it's actually false when the details come up, but also just read. Well, it's actually in the EMR because often the language in there, it won't be, um, proper English.

Um, and if it was coming from a reputable organization, you'd expect them to be able to write grammatically. Correct. So just take some time to think through what's actually happening. Um, I mean, in terms of carers and, and know, um, what people can do to support that the people that they, uh, they may be caring for, or their friends or their family, There's lots of things, um, that people can do.

Um, in terms of cyber safety, keeping safe, online, trying to have separate passwords for email. Um, if it's a, if it's a gateway to your other accounts, um, so someone gets access to one of your passwords, unfortunately. Um, you didn't want them to be able to stop them, getting access to other things as well.

Try and keep your passwords as secure as possible. Um, I might've been quite difficult to, to, to, to work out. Um, some people can search online for information about you. And if it's your so name or your pet's name, um, that you use as your password, they might be able to guess that. But if it's something that's quite complicated, um, that, that it might be a bit more difficult, um, in terms of phone scams, um, There's the telephone preference service, which is free, allows you to opt out of any unsolicited live tele sales calls.

Um, does the information on how you can do that? Um, as Sarah said, we've got lots of links at the end of the, of the presentation. So that's definitely something that you can do. Um, And that just allows you to block off a certain amount of people that might be trying to contact you anyway. Um, and you can also talk to your home phone provider to see what privacy services is that they might offer.

And they might also offer, call blocking services as well. Again, that's just a stock, a lot of the calls that come through. Um, if you have a mobile, you can use the settings on your phone to block on once numbers. Again, we've got information on how you can do that. Um, within some of the links that we've provided, um, at the end, um, that's all on the AGK website.

Um, and there's also blocking products that you can buy. I think someone earlier I mentioned. Again, set, set your phone up to allow the cause to be stopped at source. Um, that's brilliant. Thank you. And I think we'll come back to talking about some of these tips, but I, I really liked your one, um, which is as a warning sign for me.

It's amazing how many of these cameras can't actually spell? Um, always a warning sign, I think, um, for me, so. Um, Sarah, I think I've put this later, but I think lots of people have mentioned, um, your tip. So I think we'll get you in here to talk about, take five in that very simple piece of advice. Tell us what, what that's all about and how it can help people.

Yeah. So take five, um, has, has really involved, uh, evolved from, um, from the people that joined this webinar. Um, the information that we give very much comes from, um, what we hear from people that have been sort of victims of scans, um, and they really want to know. Quite simply, uh, the things that they should do.

Um, we all sort of fall into this trap sometimes of saying, well, you know, don't do this. You shouldn't do that. Never do this. Never share that. Um, and what take $5 is too. Um, keep that very, very simple, uh, mantra for people to remember, which is, you know, and again, this is across a multitude of, of channels, so it could be.

On the telephone online, uh, via a text message. Uh, if you see something on social media, um, and it's a very clear way for you to navigate your way through. And our, our key advice is number one is to stop. So you get an email, a text message, whatever that might be, just stop. Take a monument, uh, take some time to think.

Um, I think there is this, um, I'm probably, you know, we are. By nature, human beings are trusting. You get a call that you think is from your bank, or if you get a call from somebody saying that they're a police officer, that there's been some fraud on your account, we immediately go into this sort of protect mode.

Uh, but also into this sort of hot state where, where quite frankly is exactly what it says on the team. We all get. You know, uh, flustered and, and think, Oh my God, what's happening. I need to do something now. All of my money is going to be gone. That stop. Um, advice is to literally just take that moment, um, speak to a friend or a family member, or I get calls all the time from people asking me and, and emails asking me whether or not they think something's a scam or not.

Um, and talk to people. Um, talk to your friends, talk to a family member, um, and see what they think. Um, but also you can always, uh, you know, ring your bank to check. If it's somebody saying that they're calling from your bank, please do ring them up and check. They would prefer that you do that and come through to somebody to, to check something out, rather than you become a victim of a scam.

The challenge part really comes into play where. You know, and it's, it's treating as fantastic as the internet is. And I whole heartedly agree with, with Tony from earlier where he said, you know, that the internet is this great tool that we all use on a regular basis. But it's viewing things with a sort of, uh, a healthy level of, of sort of skepticism, not everything on the internet or a website or, or, you know, is actually genuine.

So it's thinking about, you know, could it be fake? Um, but also have that confidence to know that, you know, it's okay to refuse, reject, or ignore, um, requests for your personal financial information. You can always say. Thank you very much, but no, thanks. Put the phone down and again, it's, it's taking that time to sort of challenge everything as well.

Um, not to just, you know, uh, go with what the person on the phone or via the email or the text message is telling you. Yes, we can see he's got his hand up. It's that deliberate turn. You've got something to add. No, no, no. I'd like to say to finish, there was something additional I'd like to say about the, what we're talking about.

That was all three Sarah, carry on. I think, you know, in the, so for the last message that we have, which, um, sort of feeds in, I think to, um, the poll from earlier. Is, you know, if you think you have fallen for rescan, the most important point is the protect point. And, um, if it's, if it's with relation to your financial information, please please use the number.

Um, as, as Katie said earlier, the number from a bank statement, the number of the back of your bank cards. I'm pleased ring through to the bank, let them know what has happened. They want to help you. They will be able to help you. Um, We have that information and obviously reporting it through, um, to action fraud, which basically means that by doing that, and by reporting, you're helping also to protect other people.

Um, you know, not only are you, will you be able to protect yourself, but you might be able to protect somebody else at the same time. That's brilliant. Thanks. Um, and Tony, did you have something that you wanted to just bring in there as well? I was looking at the, um, the actual slide and I imagine there's a lot of people looking at that slide thinking.

What is emails, because we haven't really explained what that is. And it's quite scary, really because you, some people, you get some tools that can duplicate or copy somebody's email. So my email is told me it gets safe online. Um, if, if you've got the tools, you can copy that and send that. Oh, so when you receive something, it might say it's from Tony.

It gets safe online. And it isn't. So that's what the spoofing part is. Most people hopefully will know what fishing is. Um, but for those, those who don't, it's somebody who's fishing for your information. It's a phishing email trying to get something. And it's something that's now in common parlor. We, we should all know it's a bit like burglary or theft or salt.

It is now everyone should know what phishing is. Remote access. I think Adam explained really well and social media that's everything that we do. So it was just for those people sit in there. And if you need to know more about jargon busters, we've got everything you can think of. And we get Safeline website, but just for people who were sitting there thinking what is vivid.

Right. And then one, we haven't covered Richard. I've just very briefly. Um, because I want to move on from, from here is the quizzes. We had a quick chat with the panel earlier, and I think it's that thing that, you know, something as innocent as what was number one in the year that you were born, as Jerry was saying about, you know, the common passwords that we tend to default to or security information often year of birth is one of those questions that we get asked by our banks and things.

So putting that, I'm trying to think what was mine in the seventies, but Oh, just pick tainted left from the eighties was number one in my year of birth, um, is actually telling somebody that year that I was born in. So again, as Sarah says, take five. Why, why are you asking me this question? Is it a fun quiz or is it something slightly more sinister?

So I think that's really helpful. And thanks for doing that. Um, Jonathan thing for me now, just to add to that, Sara, um, so been examples of where Facebook, et cetera, accounts have been hacked by scammers and con friends. It looks like her friends contacting you look into, again, draw out that information.

Um, so I think it just goes back to that point of just think through, okay. Is this realistically what someone should be asking me. Um, because once they start to gather that information, then it can be very difficult. Exactly. My good friend may know that information already, Joe, they might know that you sworn because you were at school together or, you know, it's the simple tips.

I think that the ones that can help us all I'm. Kind of just come in with email, email scams and phishing scams reporting. These scams is actually quite easy now and you can forward all these emails. If you suspect anything to be suspicious, you can forward all these emails to an emerge dress called.

Reports@phishing.gov.uk. And that goes through to the national cyber crime center and they can screen those emails for any malicious content and they can have that minister's content removed. It's um, it's really, really handy tool. Hmm, brilliant. And I think with them what Katie was talking about with the adverts, and there's quite a lot of clothing, ones that pop up on Facebook.

And if you put the name of them and the word scam and you Google is Tony was saying, in terms of checking it out, it will often take you to somewhere like witch. Like Trustpilot, that will actually tell you whether this is a company that you want to do business with or not. So, yeah. As Tony said earlier, use the internet for your research as well as, um, Yeah.

one of the things that we haven't talked about is a skunkworks from Amazon and people can get clipped by those because my, my wife actually has a prime membership and, uh, don't want to, upon membership to finish, they would normally. Email you to your email address and they would not normally call you up.

I know who I just wanted to say is, uh, I gave my wife some money to buy something off the internet. And I think the company was digital that they weren't to Hong Kong and sending the goods to us. In the end, we went and wrote to. Now, if you have a MasterCard or a region card, there are departments where you can do charge back, which basically means if you don't get a good job for a certain amount of time, they will refund.

They. Money and jokey, my wife kept all your information shining. They said, I'll go two weeks in a and the Brown on your shame day. If you keep all your today. Information, because it may be something that you'll bank . I think that's a really good segue into UK tea actually. Cause I think that's what I wanted to talk to you about as which actually, which is, um, not just there's.

I think we've talked a bit about the steps that people can take to avoid falling for these scams, but be great to hear from which about. Some more times like Alex has just shared in terms of when you've been caught out, what are your rights and what can, can you do if you fall for a banking, phishing scam, if you've bought something and it doesn't arrive, can you give us some tips around?

Yeah, she was Sarah. Thank you. Thank you, Alex, for that. So the question as well, I think, um, you know, whilst we don't want to recommend that consumers only shop at the big. Um, online stores like Amazon, um, it is wise to think about how much you trust an online retailer before you make a purchase. And certainly the big guys, certainly Amazon will refund you if you don't get what you've paid for.

Um, and any, you know, UK high street retailer would do the same. I mean, you know, I'm looking at trying to do all my. Christmas shopping early this year and online, and it's hard, but cause you were sort of rushing and you don't want to, um, feel so rushed that you might accidentally use services that aren't perhaps as trustworthy as others.

I think. You know, sometimes things are advertised at lower costs from retailers you may not have heard of, and it's perhaps better to pay a couple of pounds more to buy the same thing from someone that you know, and trust. So I think there's something around that. Um, but we also see a lot of financial stance.

So not just in the sort of product scams where you might not get the goods. Or you look as you get might not be what you thought, but we see a lot of, um, financial scams at the moment. Um, and, uh, some of those are in investment scams and in terms of investment scams, there are lots of different types, but fundamentally they're all really the same type of scam.

So it doesn't matter if you've seen ads for, you know, invest in crypto currency or. Invest in Forex foreign currency exchange or invest your pension in some new fangled, um, investment scheme, the premise of all of these scams, regardless of what the financial vehicle is, is that. Scammers are trying to target people who want to get a bit more from their money.

And it's a huge problem at this time, not just in the run up to Christmas, but against the backdrop of COVID because as the UK faces a difficult economic outlook, we're not sure. Um, you know, the value of our investments. If we have savings and investments, if we're lucky enough to have that, our investments have probably gone down in value because of COVID.

And so it's appealing to anyone to want to get some of that money back, or at least put their money in the best place possible for growth. That's, that's a natural instinct and I don't think there's anything wrong with that. Um, You know, it's not greedy. It's just about trying to do the right thing with your money.

And lots of us are in that position. So, um, going back to the, the too good to be true, um, thing, I'm a strong believer in that, you know, if something seems too good to be true, it normally is now in the financial scam and space. We used to say, well, if someone's offering you 10% return on investment, that's too good to be true.

But in this financial climate, you might say a 5% return on investment is too good to be true. The bar has come down, you know? So you might think, well, scammers are only offering crazy returns, but actually they're being clever. And they're offering that just a little bit more than you get. From an ice or something like that to attract you and make you think, well, it's not too, too good to be true.

Um, so there's, you need to be careful about, um, you know, falling for something that is, uh, more than the norm and certainly too good to be true, but you know, not, not crazy. So in that, in that financial space, I think, um, it's, it's just about. Nope, not falling for things and not, um, I suppose, uh, understanding how scammers target people I think is key as well.

So often you might get contacted out of the blue and again, you have to think why, why am I being contacted and offered this great deal? Um, yeah. And just on that, um, because I want to start, I consider there's a lot of Q and a actually, so I might, um, Pause in a second and bring some of our attendees in, but, um, just briefly in terms of what shapes the Christmas, I know which today has, um, had not scams, but it's talking about black Friday, which is a different take on that too.

Good to be true. And I know I checked my spam box and I had about 10 emails in there earlier from various retailers telling me black Friday has arrived. Do you have any tips for us around that? Um, yeah, so kind of to echo Sarah's point, um, it's not just around scams, but stop and think about whether or not you actually want these products.

Um, because, uh, you know, there's so much hype around black Friday and the rules that are at home at the moment and not able to get to the real shops. Um, which is a shame. So it seems like a good thing to do to get, to go online and have a little splurge if it, if it's good value. But, um, I think, I think with anything it's just a case of think about, do you do actually want these products, um, you know, in, in the run up to Christmas, um, need to sort of be watching what we're buying a little bit more, Kathleen.

Great. I'm mindful of time. Can I add a couple of tips in for people who are listening? Absolutely. Please stay. If you're going to buy on online. And we all are a couple of things that I would certainly suggest, first of all, use the internet to check the shop that you use him. Give them. Ask them a question about what you're buying.

If they don't come back to you with, when you want to buy something, they're certainly not going to come back to you when you've got a problem, use a credit card because you've got extra security. If you spend over a hundred pounds, but maybe take out a credit card has got a very small amount of money on it.

So you use a separate car that may only have a hundred, 200 pound on it. So if something does happen, then you know that you're going to be okay. All you potentially could lose is that small amount of Johnny, your predicate, some really simple things that you can do, but again, use the internet, um, to do your research before you buy it.

That's fantastic. Um, Chris, are you there because, um, I do want to make sure we've got enough time for some of the Q and a that are coming through. I think we can come back to, um, some of the more formal points if we have time at the end that, um, this feels like. Yeah, I can see lots of questions coming in.

And are there, is there a theme or is there one in particular that you'd like to pick out there? Yeah, I think that was the first question that came up and this is a really good one from Steven senior. How do you define a victim? I think that's a really good question. Cause you know, there's different ways to talk about that, Donald, perhaps that's a good one for yourself and there's, I'm sure you've come across people in that state.

So, um, at the national dragon standard scam thing, we identify victims through, um, through the, through getting hold of victim lists through or what the cause of criminal is called in suckers lists. Uh, I suppose we would identify a victim is someone who has actually lost money to a, to a scam. That's, that's how we would identify a victim.

A chronic victim would be someone who's lost over a thousand pounds to a spam for us. Um, so yeah, it's, it's someone who has, who has responded or has fallen for a scam for us. Great. And I wonder, um, actually, Joe, if you'd like to come in there, cause you mentioned this briefly earlier that, um, sort of stigma and there, and maybe say, and Joe to talk about, um, that's the thing that stops people coming forward.

I think not wanting to be labeled as a victim. What would you say to people who have got those kinds of emotional concerns, maybe start with you, Joe, and then bring Sarah in afterwards. Yeah, sure. Um, I mean, it's really unfortunate if people do feel like that, but there is absolutely no shame in it. It happens to absolutely everybody.

I think I know I've been talking to you. I know others have said that I have, um, The only way really to try and stop it happening to yourself. Again, I know this is to try and report it. I mean, but you might not even be reporting it to, um, uh, people actually vote straight away, but to speak to somebody else.

If you think that something's a little bit unusual or if you feel a little bit uncomfortable, um, we were talking about carers earlier on. If there's any carers on, on the, on the session, if you, if you feel a bit uncomfortable for the person you care for, speak to somebody else about it, if there's anything that you think might be unusual, um, it might be that there's more phone calls coming through or more posts coming through the door because a lot of the times scanners can try and overwhelm people with lots and lots of phone calls, lots, not supposed lots and lots of emails.

And it might be an increase because once they, once people start to reply, The se-commerce thing that they've sort of got you there, and then they'll continue to bombard you with things until you respond. So anything can use your, just try and report to, obviously others have said report to action fraud.

Um, which is obviously the, that, uh, the organization sets up to investigate fraud. Um, we've got information on that again at the end of the session, um, you know, resources, um, also speak to your banks if. Um, do you think that there's anything new? I think others have said this. If someone phones you up and it sounds unusual, you can always put the phone down and then actually phone your official bank for the, for the telephone numbers that you have.

Banks will never ask you for pin numbers and things like that. So against transport, the science restaurant in Columbia unusual is happening. Right. So, or did you have anything to add there? Yeah, I think, um, you know, uh, just to, to go back on the point that's already been made, please, please don't feel embarrassed about falling for a scam.

Um, it can happen to anybody. Um, I, even some of the savviest people that I know, um, have sort of fallen for some of these scams, um, You know, so, so please don't be embarrassed about it. You know, if there's one thing I can say, uh, to make people feel, feel better is to say these scammers are incredibly sophisticated.

Some of the scams they do, and they are very good at what they do. They are, they have done their research on you. They can see things, um, You know, on your, uh, potentially say for example, if you're somebody that shares on Facebook, things like checking in at certain places, checking in at certain times. You know, um, when you put on there that you've checked in, say, for example, at the gym, they now know which gym you go to.

Um, all that sort of information. It's just about taking a little bit of care as to how much information we actually share about ourselves. Um, and to take the point of sort of, um, uh, somebody else's, you know, just remember that. Once you've put something on the internet, it is there for the world to see.

Um, you may think, you know, obviously if you're putting things on your social channels, et cetera, um, that that's just with your friends and family, but it's. It's actually, once you put stuff on the internet, it's there for a long time and it's there for other people to see. And that could unintentionally, unintentionally be obviously the criminals that are looking to do their bit of research on you and finding out all your sort of information.

So, yeah. If you get that call out of the blue, if you get that, um, sort of, you know, that text message that maybe knows a little bit of information about you, that's potentially something that they've just researched and that they've found. Um, so just a little bit of a healthy. You know, care being taken about how much information we sort of share, um, across the board and, and, you know, we've all of these things, um, is, is having the protections in place because obviously they're all wrong.

So things which we all know about that happen, uh, in terms of data breaches, and as an example, Um, you know, they can also be used by the fraudsters and are regularly used. Um, companies going into administration are used as, as ploys to, you know, get you to, to talk about things and share information. Um, so it's just a healthy level of.

Be careful about what you share online and, and making sure that obviously you're actually speaking to the right person. Um, I guess, um, I just wanted to bring Tony in there. Cause I think the right that they are very sophisticated and they use all those things. But 10, you were talking earlier about the kind of like email spacing and the phishing scams.

I think the flip side of that in terms of. Maybe feeling like a victim is that none of this is personal. Those emails go out to literally millions of people. So it isn't personal. Um, so in terms of feeling targeted, I don't know if that resonates Tony, if there's anything else that you want to add there.

It isn't personal. And as you say, millions of emails go out and it could be an email in relation to NatWest bank or Barclays bank. Well, if you're a loyal customer, you're gonna to ignore it. But if they've hit the right person, but it became become versatile. If you, if you respond to it, you know, I miss some horror stories out there.

There was an old man that we spoke to up in North Wales and he got done for 25,000 pounds. You actually told me that he realized it was a scam after 20,000, but the guy spent so long on the phone to him. It made him feel better because he doesn't know what else to talk to. So I didn't care less about scamming someone who was elderly out of that sort of money.

That's when it becomes personal, but 90% of the time, it doesn't. And I noticed somebody mentioned spear fishing because you can be targeted for fishing, email and spear fishing is when you. Targeting the big guys, um, and looking at someone very subsist, specifically, as Sarah said, and you, you get all your information, you gather about things like their dates of birth and mother's maiden name, and you target fishing maybe of CEO's financial directors.

So that type of thing can happen as well. Great. And Chris I'm really mindful of time. Is there another question that you can bring in? I'm sorry, we're not having enough time to go through the formal presentation, but um, really want to hear from people on the call. Yeah, I think PayPal's coming out too.

Obviously a lot of people using PayPal Christmas, coming up, asking how safe PayPal is and what to watch out for them on a paper for things not looking sick. Katie, I wonder if that's one for you. Yeah, possibly. So, um, I'm afraid I'm not completely up to speed on the exact terms of additions from PayPal.

Um, if you see certain products, I mean, they have a dispute resolution service. So if you have a problem with them, you can raise it and they will pass that on to, um, the vendor. And then they have a period of time in which they have to respond to you. So that can be very helpful. I've used it recently actually for something.

And it seemed to thing. I thought it was a scam isn't, it's just very slow. So sometimes that can be helpful. Um, but it's perhaps not as, um, direct as, or not as comprehensive in terms of payback, perhaps as your, the rules around your bank might be. So just for anyone who wants to know about what happens, if you lose money from your bank account, um, as opposed to PayPal, if you do lose money from your bank, the first people you should tell a lot is your bank.

You must call them up immediately and let them know. And then also if you've made a money transfer from your online banking to somebody else, Cool that bank. So find out who that is and call them because if you suspect that that's the account of the scammer, they might be able to do something about it.

And probably do that before, even reporting to the police, because speed is of the essence when it comes to money transfers, but there is something in the UK called the reimbursement code. Which banks have voluntary on banks have voluntarily signed up to, which means that they're duty bound. Once they've signed up to the code to get to reimburse customers, who've lost money to scams.

Um, and there are some banks are, let's say better at doing it than others. Um, and there are criteria that you'd have to meet in order to get your money back, but certainly if you lose money from your bank account, your bank needs to be your first port of call. That's brilliant. Sorry, just in there about sort of pay Powell.

Um, and, and in terms of just generally for shopping online, Um, obviously we all use lots of these different channels and different places. And I know if there is one piece of advice that I would really give is. Please don't stick away from the secure payment channel that the store or wherever it is that you're pulling from is offering you and advising that you use.

So if the seller is trying to convince you to buy paid by bank transfer, um, as opposed to say, for example, going through PayPal, Um, or some other secure mechanism that should automatically F ring a bit of an alarm bell and raise a little red flag, because if you do do that and you pay by bank transfer, you don't have the sort of protections that you had had you paid.

Using the secure, um, track, the secure channel that was there. Um, if you, if another way of doing that is obviously, uh, is to potentially think about paying by card. Um, obviously there are protections in place for people. Uh, if you pay by card over a hundred pounds, but under 30,000 pounds, there is obviously, um, section 75 where you have projections.

So, you know, if you are buying something that's potentially over a higher value to you personally, something that you wouldn't buy sort of every day of the week, um, you know, a big purchase for sure. Uh, a TV or a car or something else, please, please stay within the platform of where you are purchasing and no matter how much that, um, seller tries to convince you to pay by bank transfer.

Um, because if you think of things, like if you think of a faster payment, it's sort of, um, it's pretty much as if you're handing over cash. Hmm, um, on that, when it becomes incredibly difficult. And that's where obviously the, the, um, uh, the code that Katie has mentioned comes into play. And obviously as a, as a consumer, there will be things that, you know, uh, will be checked against in terms of making sure that, you know, you you've done the right things.

Um, but if you don't step away from the platform that they offer, um, and if you're being pressured to do that, Just, it should ring a big alarm bell. That's a really good tip. Thank you. Um, so I'm just going to check through, I think we've probably covered all of the information here. I'm just gonna chat and we were on question, so we've got five minutes left.

So, um, I think what we'll do is I will go through, um, the questions that we've had coming in and I will Ram some of those out and farm them out and we'll publish something on our website afterwards. So it was just five minutes to go. I was wondering if I could ask all of the panelists and I'll go through you in order on my screen to give me your one top tip that you would offer to people.

So Katie, or at the top of my screen. So if we start with you just very briefly, I've got about five minutes left. Well, I think mine would have to be trust your gut and if something feels too good to be true. Nearly always is great. I hope we're not all going to say that. Tony, how about you? Well, you've said that already.

I think passwords passwords are really important. Um, three words put together, uh, is really a good password. We can't afford to have one password. We wouldn't have one key for every lock that we've gotten a life would be nice, but you lose that one key. You lose everything. So numerous. Passwords for different aspects and making sure it's complicated and like your toothbrush, you mentioned your toothbrush.

Don't share your password. Great. Thank you, Sarah. You're next some way screened. So mine is super simple and it's stop challenge protect. So stop, take some time to think. Speak to a family member challenge. Could it be fake it's okay. And you're within your rights to refuse, reject or ignore. And if you think you fall of something, protect, pick up the phone to your bank is in the number on the back of your card or a bank statement and give them a call.

That was fantastic. Thank you, Adam. Just one of your 12 tips for Christmas. You're on you. I think. Sorry. Uh, I would say, be wary of versus script subscription traps in terms of what you're buying online. Make sure you're not going to be signed up and have money taken out of your account. Um, month by month.

I just wanted to also say that, um, uh, in terms of horizon scale, horizon scanning, I suppose, uh, TV licenses is, is something that's going to be quite big over the next couple of months. Um, it's no longer free for over 75. So unless you're you receive pension credit. Uh, and it's important to say that they will not contact you via email.

They'll only contact you by post. If you're over 75 and you need to apply for a TV license, that's a great tip. Thanks and Joe, over to you. I'm ready. Two quick ones, if that's okay. One would be always, I keep time with, um, looking into things. If you're feeling pressured, always make sure that you can walk away.

If someone's making you feel uneasy about giving them her information. And then the second one will be always to try and report things. If you do feel you've been targeted or scammed, you don't have to have had money taken to make the report. Um, but it's always helpful to report things. If you think that someone is talking to you.

That's brilliant. Um, and I'm so sorry. We've run out of time. This is really flamed by, I think with, uh, um, panelists with the caliber that we've got here today. I could happily have chatted all day, but I'm sure you've all got better things. Um, I just wanted to finish with the positive, they were personal story before we go.

Um, and that I ordered something from, um, one of the big retailers the other day, but from an independent seller on there. That wasn't right. And the power of tech. It was so amazing. I applied for a refund online. I took it to my local store, which is like a ups delivery. The mom put it in a bag for me. He scammed it.

He emailed me with the return, the receipt while I was standing in the shop. And, um, within a day I had the money back in my account. So I think I just echo what Tony said at the start, which is, you know, When it works. It's amazing. So please don't be put off, use some of the tips there. Um, our amazing panelists have said those simple ones, take five, have a cup of tea, ask a friend.

Um, and I'll have to finish it if it seems too good to be true, then it probably is. So thank you so much, everybody who's joined us today and thank you again to our panelists and to my colleagues. Who've been supporting in the background and we'll pick up as many of the Q and A's as we can afterwards.

Um, With the support there. Um, and just briefly to flick through, as I said, there's loads of contacts here, links to ourselves, all the organizations. Um, so lots to follow up on afterwards as well. So thanks ever so much guys. Um, it's been helpful and, um, please do stay safe.

Bye.