# How to avoid The 12 Scams of Christmas – Webinar Transcript

ANNIE: Hello everyone. Welcome to today’s webinar. From me on a very rainy day today. It's just gone one o'clock so I am just going to give everyone a chance to join, feel free to drop into the Q&A box and say high, we have disabled the chat feature but the Q&A option is still live. See the numbers going up. Just give it a few more moments for a few more people to join. Hello Marilyn from Woster, glad you can make it today. So we'll make a start now. So hello everyone and welcome to the webinar how to avoid the 12 scams at Christmas I am Annie Mannion and I will be running throughout session. We have live captions provided by MyClearText and you can turn on the captions using the CC option on the control panel and additional captions are available by Streamtext.net and we have slides available at slide share.net and on our website at AbilityNet. If you have any technical issues or

you need to leave early, don't worry, you will receive an email in a couple of days’ time with the recording, the transcript and the slides. And depending on how you joined the webinar, you will find a Q&A window. If you would like to ask the panel any questions do drop those in the Q&A area and anything we're unable to cover in today's session we'll answer. And add to the website. So just reminder for people that joined a little bit later we switched off the chat feature as it can cause problems for some using a screen reader but use the Q&A for any comments and we have a feedback survey you will be directed to at the end. So please do complete that in you are able. For those of you not familiar with AbilityNet we're now celebrating the 25th year and we support older and disabled people living with any disability or impairment to use technology to achieve their goals at home and work and in education and we do this by providing vision and training and free information like the fact sheets and this webinar. So today we're going to be discussing how to avoid the 12 scams of can Christmas and we have Hollie Bowker who is Cyber Prevent Officer from Greater Manchester Police and her expertise are engaging with people who are already committed cybercrimes and we have Lucy Walsh and she provides digital confident training to clients in the Cardiff area and we have Alex Barker who has worked with AbilityNet for nearly 20 years and he is a Disability Consultant at the charity. So hopefully by the end of today you will have collected some useful pointers to bear in mind when placed with potential digital scams. So I am just going to start with a poll to find out a bit more about everybody who is here before we start with the webinar content. So just going to launch the poll. So you should be able to see on screen have you ever been a victim of a digital scam. Yes, no, not sure or not applicable. You can respond in the Q&A panel. So just leave it a little bit longer for everybody to respond. Last few moments for everybody who wants to vote. Okay, going to end the poll and share the results. So, looking at the results, have you ever been the victim of a digital scam. 33% yes, 53% no, 14% not sure and then no results for not applicable. So it's useful to gauge the experiences of people who are joining us. I think today's speakers will be able to offer some really great advice, so now over to AbilityNet Alex and Lucy who will outline the most common scams.

ALEX: I want to say although there is a lot of news at the moment of scams and a lot of news about people taking advantage of people. The digital world is a wonderful place. I will give you an example, I have a disability and I met my wife who also has a rare disability. I was in Coventry. My wife was living in North Carolina in the states, we talked on Skype and Facetime and eventually, we got to meet in person. Got married in 2018 and we just celebrated together and I would say the internet brings a lot of people together and there is all sorts of things you can do on the internet. Unfortunately there is quite a number of scams and we just want to highlight the scams there are going around at the moment. So next slide please. So first things first. What is a scam? And sometimes it's quite hard to define what a scam is, so a scam is a trick, a ruse, a swindle a racket. And basically

someone wants to take money or information from you. And this Christmas we want today highlight some of the scams that you might experience, next slide please. Okay, so there is not many days to go before Christmas. Scammers are going to be really keen to try and convince you that you have received a parcel from X, Y and Z and to get the parcel you need to pay some money. So we have Evri and FedEx and Royal Mail. So they will send you a text or email saying you have got a parcel delivery and we want you to click on the link and you need to pay a delivery charge. To the best of my knowledge, no company will charge you, they will just take it back to the depo and try and deliver it again. So what are our top tips to check and see if the delivery is legitimate or not. So check the email and telephone from the sender. Or even go back to your original order and check the delivery from there. If you see any random links please don't click on them because they will take

you to a different website entirely. Can we have the next slide please. Okay, so sometimes, everyone knows people send cards in the post and sometimes you don't actually know where people live. But you have got their email addresses. So lots of people send E cards but what you have to do is if you receive an E card you have to check who the sender is. Do you recognise the name of the sender? Check who the card is send to. If someone sent me an E card I would expect it to go to Alex, you wouldn't expect it to go to my friend or a friend. Don't just assume that the card has a logo, anyone can copy a logo from any website. And certainly don't download any EXE files because an EXE files could cause problems on the computer. You can hover on the link to see where the details of where it came from. Next slide please. So, money is tight as Christmas and it's always really, really important to look out for finance scams. And there is many

different scams that you can be taken advantage of by. For example, there is the one that says, it looks like you are added a page to your account, if you haven't click on the link. Or you might get an email purporting to be from Netflix or anyone else asking you to update your payment details. Or you might get an email message from your bank saying they have been trying to contact you with regard to your account. So signs to look out for. So you might get an generic greeting and you might have information that your account is on hold. Or it might invite you to click on the link to update and verify and our top tip is use anti virus software and keep Apps up to date. So if an email looks suspicious don't click on it. So next slide please. So at the time you have a lot people calling around and you might be a victim of an impersonation scam. So people might proper port to be your son or daughter

and they say I am stuck in the airport and I need some money, can you help me and what you have to do, you have to call the original number that you saved for that person. If you get a message from your dad actually call the contact number in your phone. Does the wording sound the same. It might say for example to my favourite son, my dad would never say to my favourite son because he only has one son and it might be a good idea to ask a question that only your family member could answer. And it's really important that you do this because so many people have got scammed just thinking, it's one of my relations, I need to do something to help. We always say, look, what you have got to do is stop and think. Next slide please. Okay. The last slide I am going to talk about is text support scams. I wonder if I could ask you Annie to play the recording. So basically that was a call from someone who was be from a technical support team. What we would say is please

don't panic, hang up and if you want to check on the company, it has a website and get the customer service phone number and whatever you do don't allow remote access. And I don't know whether you noticed. They never said they were from Microsoft. They said, we're the windows technical support service. What I said before, don't panic and hang up. It will be a random call. You are just being targeted. Please don't panic and do anything rash. Now my colleague Lucy is going to talk about some more scams of Christmas.

LUCY: Thanks Alex. Okay, so following on from Alex I will outline a few other common scams one in the media the romance scams. Very often more often than not it would be females but not necessarily. Maybe targeted through social media potentially with photographs of people in very glamorous locations and possibly across the other side of the world. Where they create a fake profile, sorry, where they would create a fake profile and try and again their trust to make a relationship online. At some point it's likely that the scammer will then ask their target for some money and hope they receive it. At the ways in which they do that they could say they are isolated in a particular location and they can't get across to visit without that money or in some kind of danger and they rely on the trust of this individual to send money and that scammer would

receive the money and disappear. Some things we say to look out for. They will say they are far away and their profile will often seem to good to be true and they may very well isolate the individual asking them not to speak to anyone about it and it's their own little secret and perhaps they are talking about marriage, they may make promises to come and visit you but don't fulfil those promises and they will ask for money and they may ask for specific payment methods. Next slide please. Pet scams, so this one says here, meet your new best friend, pedigree Schnauzer puppies available now. They will very often have a reasonable cost for the pets, sometimes cheaper than you might getting elsewhere. Again it's a way of luring you in. They may very well ask for a deposit and that will need to be by bank transfer and they will tell you that will secure the puppy or whatever pet it might be.

Often they will likely put pressure on you and tell you there is just one of those kinds of dogs left and other people are interested in that particular pet. So if you need to secure the animal you will need to do it quickly and be wary of stock image, they are likely to be images of beautiful cute pets taken from other websites. And perhaps not the realistic ones you would see taken in somebody's home. And there is research, research and research, compare price breeders and review the sellers reviews and history and if you can use recommendations from trusted friend and families. And if thinking of buy pets its really important to see it in person. This particular one is energy scam. Energy fraud. This one shows a text from Gov.UK and luring people in saying they are eligible for discounted energy bills and possibly money back and suggesting you apply by selecting a link by a text message

and you can see on this particular one the telephone number at the top of the text just seems to be a random number. Or any where that you think might be legitimate and on these we just say stop and think, does it seem too good to be true and does the information look like from a real energy company. Come out of the text message and go to the energy provider and research. You could search in the search bar discounted energy costs and see if there is any offers there or energy bill support. Do you feel you are being pressured to transfer any money or give details that are unnecessary, are you being asked to pay in an unusual way. For example scammer may ask you to transfer money and use vouchers and or being asked to give away your personal information. Passwords and pins or verification codes which a legitimate organisation would not expect you to provide. And next one. Fake websites. So on here we would always say that we look at

the top there. You can see the HTTPS. And that helps you to side whether ss a secure website and there is the picture of the padlock we encourage people to look for but sometimes that's not enough. So our advise before you click on anything read the home page and check the web address and come off the site and revisit it again. Check whether it's a paid search engine advert and if you are looking to purchase anything it's much safer to use a credit card and keep your account secure using strong passwords and only complete mandatory details not giving any passwords away. Fake rewards and prizes, I am sure you would have all seen this kind of thing, very often in emails, text, social media, where you are again being lured in to click on a link that looks completely genuine and I am looking at the Aldi one in the centre of the page. It's wanting you to click on the link

and asking you to complete some personal details and luring you in telling you you will get some kind of reward. We have something from EE and Aldi and John Lewis black Friday and is it too good to be true? You can research even in Google and very often you will find if there are common scams they will be listed there. And can you find the same information in more than one place, can you go to a trusted source, so it's again perhaps not selecting that link, coming out of it and searching the Aldi site and seeing if they are offering everybody a £250 Coupon and fake endorsements here. I would urge everyone to be vigilant and always correct for addresses and verified social media accounts and very often they will use people and we have rich Branson and Martin Lewis endorsing particular scams and schemes and offers and trying to convince readers it's perfectly safe. And that might not necessarily be the case. We would need to read things

carefully to see if the advert has come from the sun. It says it's come from the sun. So just read things carefully and don't necessarily belief everything that you see. Come back out and research on that website. And the 12th one for us. Okay, car packing scams. I am sure we have all had to pay for parking and this is about when you are using your phone to use a QR code for example and what we understand is scammers are overlaying those QR stickers with fake ones that will take you through to different sites and encourage you to put payment details in that way. Make sure that you have downloaded any parking Apps through the official app store or use the telephone to make sure you are getting through to the official car parking payment site. Next slide. I think that's over to you Alex.

ALEX: So what can we do to stay safer. There are a number of things we can do. So if we can have the next slide please. So prevention is better than the cure. So first thing you can do is make sure that you have got your anti virus, it's all up to date. Passwords, make sure that you have got passwords and not just passwords like 1, 2, 3, will. Check a website,. Site is a really good place to get information about possession dodgy website. There is a website called have I been Pwned.com making sure no one else has the information because it's easy for criminals to sell information to other people. Always make sure you have padlocks on your browser if you are using your credit card on a browser which hadn't got a padlock. Personal information stays personal. Don't share your personal information around with people. Because they might not be as trustworthy as you think and they might use a website and computer to

defraud you with some of the information you have given them. And these are some of the steps you can prevent cyber crime and scams.

ANNIE: Thank you very much Alex and Lucy and great ideas and examples and hopefully gives you a good idea of the flavour and some of the common issues you might face. So now I would like to introduce Hollie Bowker from Greater Manchester Police and she's going provide some advice about staying safe online.

HOLLIE: My name is Hollie Bowker and I am a Cyber Prevent Officer from the Greater Manchester Police, so I will talk to you how cyber policing looks in the UK currently. So the first one is prepare. And basically that's a team of officers sitting in the office and they work along side organisations to plan responses to cyber incidents and try and do that one step ahead approach of the criminals. So the next one is protect. That's a little bit like what I am doing today and that's to reduce the vulnerability of people in the community. Next one please is cyber prevent. So that's my specific role. So I work with people who are on the Cusp of cyber crime and what I try and do opposed to giving them a criminal record at a young age I try to educate them into something positive and help to bridge of digital skills gap and the last one, that's our pursue officers and you may be used to seeing these on TV programmes and they are the ones

who do the morning raids and if someone has been an offender of a cyber crime it might be where they take the devices and things like that. And the next one please. Okay. So obviously Alex and Lucy touched on passwords and it's really important we just mention a lot of the incidents that come into my office could be prevented by having better passwords, so not trying to teach anybody how to suck eggs, it's really important to say do not disclose your passwords to anybody else. Especially younger children in the family and I do a lot of school talks where I talk about passwords year five and six upwards and they tell me your passwords. Having a look at passwords don't use anything personal. Don't use things like pets names and children's names and favourite band and football teams. If that information is out there people can guess it and weak passwords can be hacked in seconds, so this is why we say save

these passwords to browser managers and Apps, ensure all your accounts have different passwords, most people panic hearing this thinking how will we remember all. It's safe to use a password manager app on the phone or device or at the top of the browser, remember this password, use that function and if in don't write them in in the back of a would being. So better to have different passwords because if they guess one password and pop it into all your accounts they are locked out of everything. So I am going to tell you about how we make a strong password. So this is government guidance but we advise three random words, we all say long and strong passwords are the key. So we have 3 random words, pen, Apple and fish. The chances of that being guessed are very, very slim and what we also say is the magic number is 12. So the reason we say that is cyber criminals do brute force attack and that means they

systematically go through the characters of passwords, letters and numbers and to try and hack your passwords and crack the code. If your password is a mixture of letters, numbers, symbols and over 12 characters in length it can take years for somebody to crack that password. On to the next slide please. Okay, up dates. So lots of people will see up dates coming up on their phone, laptops and computers and any other devices and a lot of people think not that again. Because they have to put it down and they have to let it upload which takes time and it takes you time away from your device. But up dates include protection from viruses and software and that could maybe come on to your device through various Apps and things like that. So one of the symbols is a sticking plaster, what these up dates do is they stick a plaster over the top of the weakness and stops the criminals from getting through. On to the next slide. Two step verification. So if you are leaving your home, you might set your alarm and lock your front door and this is the same for the devices, it's just that extra layer to keep the cyber criminals out of your account and it's twice the protection. Even if a criminal was get into the was password without the two step verification they wouldn't be get into the need. So it often comes by text or code and you need to input the number on to the website to prove that's you. So Alex mentioned about the hi mum, hi dad scam, so they will say, my mum. I dropped my phone and I need to use somebody else's phone and I sent you the two step verification to get in but actually they are sending you a link for you to send them your two step code. So definitely don't ever send anybody your two step verification code and try and upload them to devices because it's that extra layer of security. So again Alex touched on this and it's called have I been Pwned.

But basically this website is really good because you put your email address into it and it will tell you in you had had any data breaches on your account. So that means your data may have been sold on. Your personal information may have been sold on when you downloaded a particular app. Most people who put their email address into the site may have a data breach. It will tell you where the data breach is so say for example it says an app that you use, say Facebook, you just need to go on to Facebook and change the password. The longer you have an email address the more likely you have had a breach. So try that out yourselves and see what it brings up and make sure you change the passwords where the information has been leaked. So on to the next slide. So we're going to talk a little bit phishing and phishing is about scam emails to trick victims and clicking on some sort of link to go to a website and as

Lucy and Alex alluded to, it will ask you to type in your details and a lot of the time this is something called spoofing, so they will replicate a website very well to try and get you to believe it's that legitimate website and you will input the details and you have share the personal data and they can use that against you, spear fishing, it's another type of phishing so where they target maybe a finance department they may pose as a director and email a financial department for funds to be released and whaling is they may pose admin or finance department and contact board members and managing directors asking them for informing and passwords for things, lots of people fall foul of these two in employment because they are very busy and they skim read things and maybe miss some of the signs I am going to tell you about. Vishing, so these are often HMRC scams where they pose as the government saying you owe us a specific amount

of money and if you don't send it we are going to send bailiffs to the address, there is always a matter of urgency and it's that take five and stepping back and bouncing the idea off someone, do you think it's right. If someone is shouting at you down the phone put the down down and go on to a search engine and type it in. A lot of the time things will come back and say they are not legitimate or tell you about ongoing scams. So if you are in doubt never ever click on the links or respond to what they are saying. You can forward emails on to report phishing. So I am going to put you to the test. So if you want to put it in the Q&A you are welcome to. But I am going to give you a few seconds to have a look at this page and think about how many letter Fs are on the page, so I am not going to give you loads of time but have a look and see what looks most to you.

So most people will see these ones here. Most people will think, there is the 7 that you can see there and if we just do one more click it will also incorporate the two at the top. The reason I show this is just to make you think about skim reading, so like I said earlier, lots of times we skim read things and it just looks like united utilities website. We need to start looking for the small details on pages. That we can identify the real from the fake. So that was just a little test for you guys but on to the next one please. So we're just going to look a little bit closer in phishing. Start with the Google document email. So we want to check the users details first and click on the URL. So the links and we want to explore the email address. So one more click. So it says here it's from Luke Johnson to me. So for the purpose of this I am mark Smith. And it's been sent at 11:57 at night and it's a department budget. And in this

document you can see it's a HTTP drive/Google.com. So have a think about what you might think about this. Does this look legitimate or fake and you can pop it in the Q&A or have a think about it. One thing I would mention I think Alex mentioned earlier there were looking at HTTP. There is no S. There is no padlock there. So if we just do one more click, so mousing over this link will show you that it actually goes to an insecure domain if you were to copy that into Google or search engine you would find it doesn't exist. If there is something you need to know it will be on the legitimate account and you will be able to change it there. More click. That's a phishing link. So these are some really useful resources, if you are ever a victim of fraud or think you have been you can get in touch with them. So there is action fraud here. That's the national fraud and cyber reporting centre. It's really good because it is national, it means that we

can support victims who are in one area whilst also the relevant police force can be hunting down the criminals in another area. That can go to the relevant police force and we can help people. It has a phone line that you can call and speak to a real person which sometimes is really beneficial. But if you are wanted to do something quickly you can do it online and someone can report on your behalf and it's really simple and easy to use. There is the national cyber security centre. That's the government website that provides all the most up to date advice on fraud and scam and cyber. It's really good because again there is a lot more detail on how to set your passwords and things like that and it will keep you up to date with the most recent scams and frauds and this is the cyber resilience centre about what is going on in the current climate and how we can protect ourselves against it. Think

Jessica and this is by a lady called Jessica and there is a paper booklet and an online version and it talks about all the different types of scams we mentioned today but in a bit more detail. Knowledge is power and so the more you know about something the better prepared you can be to protect yourself against it. And I mentioned about stepping back and taking five. This is one of the fraud campaigns out there and it's about just walking away from your device, giving your brain a chance to process what you have seen and whether actually, wait a minute, is that right? It's not in this advice to give but I do say be suspicious about things but unfortunately there is some not nice people trying to get your money or data. So just again that was a tour but a of a review, create a password and make it long and strong, have a look around a room and put it all together and save it in notes or on a password manager and it's easier to remember. So use those

password managers or another secure method to keep the password safe and turn on the two step verification and it's just that extra layer of security. Update your device and it just stops cyber criminals from getting access to the data you have on your device and it's that sticking plaster and last one is also turning on back ups. So save your personal information and things to another device, USB, the cloud. Save those things because if you are a victim and use the information it's a lot easier to recover the information. That's it from me. Do check the national cyber security centre website for the most up to date everything cyber.

ANNIE: Thank you so much holly for the available advice and you can access all the slides on the webinar page AbilityNet. So just before we move on to the Q&A from all of you. I just wanted to check in again with everyone to find out about your competence with tackling online scams having heard all the ideas from guest speakers today. So here's another poll for everyone to answer. Do you now feel better informed to identify potential scams? Answers are yes, no, not sure or not applicable and depending on how you joined the webinar you may find you can't see the poll but do respond in the Q&A panel if you like. Give everybody a chance to answer. Numbers creeping up. There is a clear contender which is a relief. Just give everybody last chance to participate and I will end the poll now. And the results are, resounding yes, you do feel better informs to identify potential scams, that's

93% of you. 1% is no. So hopefully when we send around some further information after today that might help. 3% not sure and 3% not applicable. So, thank you we'll share more tips with you in the email follow up that you will receive on Thursday, this week. So, now moving on to the Q&A. I am sure you have all got a lot of questions you would like to ask the panel. So if you have a question please fire away in the Q&A window. I don't we'll manage to cover everything right now. So we'll catch any unanswered questions on the website in the next couple of days and you will be sent a link to access them. So just going to have a look through now. There is a question from Sasha that came through on email. You can mark phishing as phishing but where does that go, might be a good question for holly.

HOLLIE: It goes to the national cyber security centre so they are the ones working in the background to take these people down. They do create things quite quickly but when you forward it there they will do the things in the backed to prevent that coming through to you again.

ANNIE: Thank you good advice and just comment, Paula said she just had a scam call as the session was going on, what are the chances? So just shows how rife the scams are. Do you have any tips wanting to inform new users of the internet about scams without sharing them off using the internet. This might be one for Alex and Lucy to cover.

ALEX: I think the answer is you have got to empower people to make the right decisions, not to get scammed. I certainly think if you tell them about what is good, you go to a website that has padlocks, if they haven't don't put your details in. Always think twice before responding to anything. Because it might be a scam email. Always talk to family members if you have got a suspicious email or text. By making sure you have got all the useful hints and tips at your disposal you can't go far wrong,.

LUCY: It can be scary for new users of the inter holly said there is a lot of nasty people out there trying to get your money and following the hints and tips around passwords and talking to other people before and just making sure, for me it's always about coming out of where ever those links are. Wherever they are don't click, come out of them, check out and go back in.

ANNIE: Thank you. So just moving on to know question this might be one for Hollie. Can you tell us about cards which have limited funds for buying online. Is that something you are able to share a bit more about?

HOLLIE: In terms of bank cards I am assuming?

ANNIE: I think so.

HOLLIE: I think there is benefits and risks to everything. And like I think Lucy said earlier, using credit cards and using things like Pay Pal is a way of monitoring your money more efficiently and a lot of times they are able to spot those incidents on your behalf. So you are more likely to get the money back and sometimes there is limits on cards with spending. I suppose that can be a benefit to your or sometimes an inconvenience and it really depend on what you are doing, if you research, you read up on it and you are comfortable with that and like I say you can always go on to the legitimate websites to make sure what the most up to date advice is.

ANNIE: Thank you. Just a brief recap on, it's a question from Robert. Since I am unsure can one find out if one's email address has been invaded. I know have I been Pwned might tell me if my email address has been used or does it also tell you if the email has been invaded.

HOLLIE: No it doesn't. O lot of information in the email, most people have it in their email. Energy providers and bank, it's likely you would know, they wouldn't keep hold of those very long, they would use them. Changing the passwords is really good because that information becomes obsolete. And like I say, if you have got that two step verification on, even if they have the password, without them having that code they can't get in any way.

ANNIE: Okay. Thank you. Got a few other questions here. Does using your Google wallet pose a security risk.

HOLLIE: there is risks to everything. It's a bit of how long is a piece of string, I am sure there has been incidents where somebody managed to get into that. I know sometime people pay contactless and a lot of time they are handing out cards to stop people scam those. I don't have any personal experience of that but there might be some information on the national cyber security website that outlines it.

ANNIE: Another piece of information that also might be on the national information security website. How do you check whether your security is up to date? Is that something you could find out there or is there another set of tips that you might be able to offer?

HOLLIE: I think by doing those regular up dates that's keeping in check with what the most recent update is for your device. So that will be staying that one step ahead of cyber criminals, so say for example they tried to get in using a particular app by way of update that will come to you as a sticking plaster. There are maybe further advice on the national cyber security website but looking for reputable anti virus are always good security methods as well.

ANNIE: Thank you. I think we have time for one more question. How do I verify if a phone number is a fraud. I know you can check on the official website but somebody said they made a purchase through a voucher from the company but the number keeps requesting the bank details. I don't know if that's a type of fraud.

HOLLIE: There is fraud where people are asked to buy gift vouchers. Be wary of somebody asking for bank details and that's a strong indicator that something is a bit untoward. So a lot of mobile phones do detect scam numbers, so if you think that's a scam you can forward that number on to 7726 to prevent other people becoming victims of that. If you feel that's not legitimate, I would saying potentially make a report to action fraud and they can look into it on your behalf but don't be giving anybody any banks details.

ANNIE: There is just one hopefully brief question that might be important for everybody to hear, is there anyway to validate a QR code before you scan it?

HOLLIE: Not in a I am aware of because it's very new. So they are referring to it at Qishing. I think speaking to where you are. So say for example you are in a shopping centre you would think someone with a stall in a shopping centre is legitimate but just double check and speak to information. Is maybe that someone pitched up a table and has a QR code and they are sticking them over parking. Check those things. And if in doubt use another form of payment. A lot of people use them for feedback and they are really handy and quick to do surveys on but there is loads of benefits to using QR codes, but check if there is somebody in an information point. If you are in McDonalds just ask, is this your QR code so you can enter.

ANNIE: Sorry we'll get to the questions after the webinar is completed. So thank you so much Alex and Lucy and Hollie and Judith with MyClearText and Kelly and Freya in the background. So as mentioned before AbilityNet offers free IT support at home and online and fact sheets and webinars so, you can follow the help line and calls cost no more than the national rate call to an 01 or 02 number and you can get free tech support and if you feel you have the tech skills and you would like to be a volunteer we would love to hear from you. And Lucy is joining us as part of our work with BT group and we're offering free digital skills training to people of 65 years and over. So you can find out more and register at AbilityNet.org.UK/ BT digital skills and you can choose a group or one-to-one session and you will receive some fact sheets and a jargon buster as part of that and the training provided is on a wide

range of topics including staying safer online and using social media and watching TV and accessing public services and banks and shopping online and loads more. So do get in touch and we also run online training sessions about digital accessibility and inclusion. You can find out more at/training and if you use the code AbilityNet webinar ten you can save ten percent on all of our courses and we have a free course how to build disability inclusive workplace followed by how to create accessible documents and presentations and very popular course and also accessible social media. So those are coming up next year and if you are joining us from an organisation, looking for staff training, we also have E learning that employers can complete anytime online. So that's/E learning on the website and you can sign up to the newsletter for latest advice about inclusion and don't forget about the next free webinars that you can access. So thanks again to everyone who joined us,

please do complete the feedback form you will be directed to and we'll be in touch with you soon so, bye everyone and have a great 2024. All the best.