**Sarah Botterill:** Welcome to our webinar, AbilityNet Live ‘Staying Safe Online’.

My name is Sarah, and I'm Free Services Marketing Manager for AbilityNet.

I'm really delighted today to be joined by Graham Cluley who is a security expert. And I'm going to introduce you properly to Graham in a second.

I'll just give you a brief overview of the webinar. We'll meet Graham properly in a second, and then we're going to talk a little bit about something called social engineering, and in the context of the world that we're living in today.

So that's just, I'm a little bit of background about the types of techniques that scammers use to catch you out.

Then we'll go into a bit more detail after that.

We'll be looking at how you can watch out and spot scams. We'll go into a bit more detail about some particular types of things that can catch you out.

So, phishing scams, email spoofing, social media, and then we'll come on to how you can safely take advantage of everything that the internet has to offer.

During this time of physical distance, we're all much more reliant on doing things online.

I've seen some of the banks giving out tips and advice and saying, you know, we're here for you. But, at the moment, the way that we would like you to do business with us is online.

It's perfectly safe as long as you follow a few simple rules.

Graham will be talking us through those [rules], the same with online shopping, and then we're going to look a little bit at misinformation. What the president likes to call fake news. So, we'll be looking at that a little bit later as well, and we'll be looking at software that can help to protect you and keep you safe.

So before we meet Graham; teasing him here, but before we do, I'll just go through a little bit of housekeeping and you can see that captions are appearing at the bottom of the screen and they will be there throughout the webinar. Once we finish, we'll be emailing you all and letting you know where you can find slides, a transcript, and a recording.

Please do use the Q and a window to ask questions. We've turned off the chat for accessibility reasons. So please do use the Q and A to ask questions there, and once we finished, there will be a feedback form to ask any follow-up questions post the webinar.

I'm delighted to be joined by Graham today. Graham and I have known each other for a long time, longer than I can remember. I think since the mid-nineties. Graham, I think it's that long. So perhaps you'd like to give us a brief overview of who you've worked for, and your experience of working in this field.

**Graham Cluley:** So I've been working in the field of, well, what we now call cybersecurity and probably wasn't called that way back then, um, for almost 30 years. Uh, the worst part of 30 years. So pretty much since I left the university, I've been working initially as a programmer, I used to write anti-virus software for a European antivirus company called Dr Solomon's. Some of you may remember that, and I then went to work for many years for a company called Sophos who are still operating.

For the last six years or so. I've been working for myself and basically I blog and write about computer security, how to keep yourself more private online.

I do a weekly podcast. I give talks and presentations all about the dangers which are out there, the tricks which the hackers are using in order to try and trick you out of your data or sensitive information or your finances, so that's, that's the kind of thing which I do and how long I've been doing it for.

**Sarah Botterill:** Great. I, as I say, we have both been around for a while. You must have witnessed a lots of changes, and I am, I just wondered if you could touch on some of the biggest changes that you've witnessed during that time?

**Graham Cluley:** One of the biggest changes is when I first joined the antivirus industry as it was then, the people who were writing computer viruses and Trojan horses were kids in the back bedrooms and they were doing it show off and they weren't doing it to make money.

It was really, cause they had nothing better in their life to do. Eventually they grew up and got girlfriends or whatever, you know, they flew out of the nest and they were no longer interested in doing that kind of thing because they matured.

Basically what we see now, of course, and what we've seen for some years is organized criminals using the internet to steal. And to hack and to make it an enormous amount of money. That's really probably the biggest change, which has happened over the last 30 years. So there are many, many more attacks out there.

There are many more attackers, and they've got more reason to want to hack you than ever before.

And that's a huge change. The slides… we're going through this pandemic right now. We have this issue of how do we keep in touch? And lots of us are moaning about, Oh, it's such a nuisance and all that. Just imagine if this had happened 20 years ago when we didn't have broadband, when many of us didn't have computers at home.

There'll be many more of us furloughed and unable to work at all as a consequence.

And we wouldn't have been able to so easily keep in touch with our friends and family. Because video conferencing simply wouldn't have existed. It wouldn't have worked. You wouldn't have had good enough bandwidth.

So the world has changed from that point of view.

But of course, all of this extra connectivity, which we have now is something which criminals able to take advantage of as well. So, there's all kinds of positives and all kinds of pluses, which the internet and increased connectivity has given us, but there are sadly also people out there trying to exploit it.

**Sarah Botterill:** And do you have any sense of, um, risk versus reward? Do the rewards outweigh the risk in your view?

**Graham:** I think if you're sensible, then definitely yes. If you follow simple advice on how to protect yourself online, then there are enormous benefits from being connected to the internet. The saddest thing I ever hear, or from people who can't keep in touch with their grandchildren anymore, who maybe they've emigrated or far away because they're too fearful to get on the internet because they've heard stories about hackers.

The truth is just following some fairly simple rules can dramatically increase your protection and strengthen your defenses and. Often with these financially motivated criminals, they're not going to invest a huge amount of time into hacking you if you're a little bit too difficult they will simply go and find someone easier to hack instead.

So as long as you manage to be a little bit more difficult to hack, than the next person that's probably been enough to protect you. It's a bit like, no. If there's a bear chasing you right, how fast do you have to run? We just have to run a little bit faster than someone else. You just need to run a little bit faster and that way you'll be safe.

Sarah Botterill: That's great. Thank you.

So I'll come on to our next slide now. We wanted to get everybody who's joined the webinar just to give us your take on how safe you feel. So I'm just going to launch our first poll, which hopefully, um, the majority of you can see on screen. S

o there are just some questions here about how concerned are you about online security?

So are you extremely worried? Very worried? Concerned, but confident that you can spot a scam, or not at all worried.

So we'll just allow a few more seconds and that everybody have their say.

In terms of the results it looks like 70% are saying that they are concerned, but confident that they can spot a scam, which is great. There are 26% of people who are very worried though, and we really genuinely hope that by the end of this webinar, you'll feel less worried. 2%, not at all worried. 2% extremely worried.

**Graham Cluley:** Well, those two people who are extremely worried, can I say thank you for joining the webinar because you must have been a little bit concerned. The first point, connecting to the internet to watch this. I think you're probably the bravest people of all, but hopefully at the end of this webinar you'll feel a little bit more confident about things.

**Sarah Botterill:** Can you just tell us a little bit about this term that I'm quite familiar with, but I think under this, for me, understanding social engineering is a great place to start in terms of understanding how these things work.

Can you tell us what that is and how scammers might be looking to take advantage, particularly during the pandemic?

**Graham Cluley:** So social engineering is basically a confidence trick. And what the bad guys will do is rather than trying to exploit a software bug on your computer or a flaw in your operating system, they instead target a bug, which is in your brain up here in your noodle. So they're, they're trying to find some human weakness in order to make their intended target make a bad decision.

And they can be absolute masters at this of the manipulation of the social manipulation making you think that one thing is happening when in fact it's that is something entirely different, which is occurring. So an example of this, for instance, right now we're. Obviously suffering this horrific pandemic, and lots of people are very concerned about their livelihoods, for instance, or keeping in touch with people.

An example of a scam, we saw one just last week, it's where emails have been sent out, claiming to be zoom. A video meeting notification and the video chat notification claiming to come from zoom claims to come from the human resources department at your company and saying that we need to have an urgent zoom meeting in 10 minutes to discuss your performance. And the implication is that basically you're going to have this call with HR because they're going to fire you. And if someone receives a message like that, particularly in the current climate. It's perfectly understandable that many people would think, crikey, what am I going to do? And they will click on that link without thinking. And when you clicked on that particular link in the scam, which is going around right now, it takes you to a webpage, pretends to be zoom, and it says you need to log in with your business email address and your business email password. And the intention is, of course, for the scammers to steal. You'll use name and password and then they will use that password to log into your business email. And then all manner of other hacks and mischief making can take place. And that's obviously not something that you want to do, but there is this risk because so many people are working remotely at the moment are worried about their jobs or simply they don't have their IT department within easy beck and call that they will believe an email like that and just click without thinking and enter their information.

I'm sure even as people enter their details and hit send... they might think, Oh, crumbs. I wonder if is this legitimate or not, but it's too late. So you've already entered that information. So that's the kind of trick which scammers will do.

And we've often seen them taken advantage of news stories.

Other times it might be something like, for instance, a delivery which has been delayed, or maybe a payment on your credit card. And you begin to see the red mist thinking, Oh, I've never bought anything. You know, I haven't spent $300 on an air flight.

And so you click on the attachment or click on the link and bam, they've got you.

**Sarah Botterill:** And I think that's a really good example. Both of those, there's even one in particular, because I know we're going to come onto this in a bit more detail, but is it that making you think you have to act quickly? One of the things that is that social engineering is something that really is quite triggering for you; and there's just a few of the things that we've listed here, which are the types of things that to watch out for at the moment. Lots of people are looking to get. Online delivery slots. So you might find that people start to ride that crest of a wave. As you say, there's a lot of insecurity around works and things like universal credit. You might get fake emails around that, or government support for self employed. So I think it's just being aware of the environment that you're in. Um, and, and just a, a what challenge, isn't it really around those kinds of things.

So it's think before you click. You know, it's just taken a little bit of time.

**Graham Cluley:** And a lot of us, of course, are under pressure. We might have kids around us and you know, there's all sorts of noise and havoc going on in the home. And so that can be a risk as well and a distraction from us. But just think before you click, um, as to whether this was the type of communication you would normally get and where the browser is actually going to take you.

**Sarah Botterill:** Okay, another phrase, it may or may not be familiar to people, is phishing, and I think, you know, an example of that type of phishing scam. Tell us what phishing is and talk us through the one that we've got on screen here. So for those who can't see the picture, it's, um, a screenshot of an email that I received, which is offering Best ISA rates with an 8% return to talk to talk us through this one and talk through phishing in general.

**Graham Cluley:** Yeah, so phishing is where the bad guys try and trick you into handing over some sensitive information. Quite normally it will be something like a password because they want to. Break into our accounts, and it's much easier to break into your account if they, if you've told them the password.

So what they will do is they will disguise their emails to pretend that they come from a legitimate organization. Maybe a company you do business with or your bank or may even pretend to come from your work.

In this particular case. Well, this is really a classic thing which you see a as part of social engineering is too good to be true. We've got ISA rates offering, was it 8% returns in this email, you know, that's fantastic. Wow. That's an incredible return rate.

And of course, lots of people are worried about their finances, and so they may think, that sounds like an excellent offer. I'll click where it suggests. And then of course, ultimately, you're going to get scammed and you're going to be entering personal information, but a closer look at the email, it makes it seem a little bit more suspicious.

So in this particular case, which you received, Sarah, the email pretends to come from an organization called ISA finder. It sounds like it might well exist. Maybe that is a service but the email has been sent from an address, which looks nothing like ISA finder.

So that's one indication already. This is likely to be a suspicious email.

Also, it tells you to click on a link in the email, and if you've received emails from your bank recently, you'll find that your banks don't actually like to embed links inside their emails because that is a trick which is so often used by scammers.

And instead, what your bank would normally tell you is just log onto your bank in the normal fashion in order to get the information.

And so if you are signed up for an ISA, find a service, for instance, you should go to the ISA or find a website and log in with your account in order to see if there's a message waiting for you there or see what they can offer. Another thing that you wish you can do…rather than clicking on this unsolicited email and clicking on links, which is dangerous, another thing you can do, of course, is that you can use the search engine.

So search for, for instance, ISA, find a scam in this case, and I think you did this, Sarah didn't you and found the second result. In Google, which you said was from the FCA saying, watch out for this particular email. Of course, if you don't find it in your search results, it doesn't necessarily mean it isn't a scam, but it's a useful, say, Oh, this is a known one, which you know, has maybe caught out other people.

**Sarah Botterill:** Thanks for talking us through that.

So another term that may or may not be familiar with, but this one is about, spoofing.

When I was little my Dad used to play a game called spoof with me, and that was a bit of a, of a con. He used to con me out of lots of money.

So tell me what an email spoof is?

We’ve got another email which says PayPal is looking out for you. So, yeah, all good news here.

Graham Cluley: Yeah, it's nice of PayPal, but in this particular case, what they've done is they've spoofed the email date details, the sender details. So if you look underneath that screenshot there. You will see that the sender says service@inteldotpaypaldotcom and paypal.com is the real PayPal website, and that's great, but actually that's the name part of the email address. T

he actual email address it was sent through is a great big load of old gobbledygook.

And so that is the email address. Now, PayPal wouldn't send their emails from that email address. So that's the first thing which you should spot. Looking at the email header, looking at the from address reveals that it's a nonsensical email address and it wouldn't be one that PayPal uses. We've also got another, again, a link embedded in the email telling you to log in now, which is something you should be suspicious of.

You can hover your mouse over those kinds of links. Instead, as I said before, go to the official website to log in. Another telltale sign of this one though is that the scammers made an elementary mistake because what they've done is they've included in the ‘to’ field, not just your email address, but about 40 or more other email addresses as well.

And PayPal, it's not going to send you in an email and CC dozens and scores of other people. That's not the kind of thing which they would do legitimately.

So that instantly should ring alarm bells. Another thing which I happen to know that PayPal does is they will often use your name inside the body of the email, or they may even quote your postcode, which has an additional level of reassurance that it is them.

So if they said. Dear Sarah, we've got some information for your, if they quoted your postcode thing can feel a little bit more confident because the scammer won't, we quite possibly won't know your real name and they very unlikely to know your postal code as well. So details like that, I can tell you whether it's likely to be a legitimate email or a phony.

And as you said before, like you actually have a PayPal account to go to the official website because the details will be there, always the advice or always go to the genuine website yourself.

Don't follow the links in the email, go to the actual website itself and log in. And if they have a genuine message for you, they're going to give it to you when you log into the real site as well.

**Sarah Botterill:** So perhaps you just like to sum up, so there's some of the sort of commonsense stuff that you've already been talking through on how to avoid these types of scams, or just perhaps a recap of some of these for people.

**Graham Cluley:** So the first thing is. Is the organization which has contact you, is it someone who you've had dealings with before? Are you a customer of theirs? Have you emailed them in the past? If you haven't, if they just come at you out of the blue, then you have to question why they emailed you. Now. It might be a scam. It may be a scammer. Thinking, Oh, chances are they've got an Apple account or something like that. We'll send it to all of them. You may have received a scam emails in the past from a bank, which you weren't actually banking with just a case of the scammer spewing it out.

It's hundreds of thousands of people in the hope that some of them might actually be customers of that organization. So, if you don't have a relationship with them don't trust the email at the very best. It's spam. At worst, it's a scam.

So have you asked the information? Same thing. Is he asking you to click on a link? And like we said, you know, some legitimate emails do ask you to do that, but I would recommend, again, generally go to the website, which you can visit instead.

That's going to be a better course of action in most cases. And of course, most email accounts these days, if you have a Gmail or Yahoo or Hotmail account or any of these things, I'll often have a spam filter, which can do a really good job at stopping most of these messages. Doesn't mean they're necessarily catch all of them. But they do catch the vast majority of them. So make sure that you've got that enabled.

And like we had mentioned earlier, use a search engine to see if it's a known scam. Because if you're being targeted by scammer, chances are thousands of other people have been scammed by someone similar in the past.

**Sarah Botterill:** That's brilliant. Thanks. And great advice there. So, um. As we've talked about, you know, we're all having to keep our distance physically, and lots of people are turning to social media at the moment for connecting with friends or, um, or just for entertainment or to, you know, to kind of connect with the outside world.

It's fantastic again, but as you, as we said, there's unfortunately some people will be taking advantage. So what are the sorts of things that we need to be watching out for when we're engaging with social media?

**Graham Cluley:** So one thing I'd be careful about on Facebook, and it's like, is these quizzes and online games, sometimes there's a bit of fun. For instance, you may be asked, find out, uh, what the number one hit record was on the day you were born. And so they'll ask you to enter your date of birth. Okay. Seems harmless. And then you share it for friends. Oh, you know, Dexy’s Midnight Runners or whatever it was, was number one when, I don't know why I said that, but when I was number one, I said I'd be so lucky that they were number one when I was born.

But anyway, so that is a way potentially for a scammer or an identity thief to find out your real date of birth. So don't participate in those other ones. Might say things like, well, what's your pet's name? Or what's your teacher's name? You know, that asks you information like that. And they're trying come up with some exciting answer. But thing is those questions you've just answered, they're often the security questions, which online accounts used to protect. Your account from hackers. You know, sometimes you create an account, it says, okay, you've created your password.

We can ask you some security questions in case you ever want to reset your password.

So tell us your, take your first, your favorite teacher's name. Tell us the name of your first pet. Well, if you've answered a Facebook quiz or run a game which asks you that information, you've given it to other people. So my advice is, I mean, it's a shame because some of these games can be quite fun. My advice, firstly is when you create an account. And it asks you these security questions. What was the name of your favorite pet or your first teacher? You might actually want to lie. You might want to tell it something which isn't true, and maybe write down those answers in a book so you don't ever forget them of course, or store them in a password manager. But you know, that can be a good piece of advice. But just being very careful about who you are sharing your personal information with, cause you don't know how it might be misused in the future.

**Sarah Botterill:** I know we've had a brief conversation about this the other day, Graham, but I was quite intrigued about why some quizzes want to capture my face. And you were talking to me about an example of this and this notion of fleeceware, what's that all about?

**Graham Cluley:** Yes. So just recently there've been some reports of Android and iPhone apps, which offer to find your celebrity look alike. And so the idea is that they scan your face, you take a selfie, you upload it to their service, or it will happens inside the app. And then they hopefully tell you who you look like. I actually did one of these and I was told I had a 73% likeness to Henry Kissinger, which I have to say, I did not find terribly flattering.

But anyway, that's, that's the thing which they decided to, uh, I should be compared to, the thing is why are they doing this? Well, a lot of this fleeceware, when we also see this with Zodiacs and astrology apps, they might say something like, Oh, you've got a doppelganger. Cause I uploaded my wife's face just out of interest. I thought, I wonder what is it we should come up with? And they said, you've got a doppelganger, but we're not going to reveal it.

Unless you take out a free trial of this app and read it in the small print, it said the free trial last three days, and after that you will be charged. I can't remember what it was, something like 30 pounds a week, three zero 30 pounds a week in order to access a fairly rudimentary sort of throw away app. And I'm sure lots of people will not have successfully canceled the app subscription within those three days. And this is something which we call fleeceware. Uh, where you know that they're tricking you to sign up for something. And if you're not very careful, you might find out that you're actually out of pocket for something where it really should be a completely free app and not something you would ever consider buying a subscription for.

**Sarah Botterill:** Okay. Brilliant. Thank you. I'll stop doing that. I don't know who I look like that. I'm going to stop doing it. Anyway, so moving on now. So, we've got our second poll, and so I'm just going to launch this and ask everybody to join in one second.

So, I don't know how brave people are feeling, but this is just to find out if anyone has fallen for an online scam. So a simple, yes or no. It would be interesting to just know whether, um, and it is, I guess, just to reiterate what we've been talking about, Graham.

They are extremely clever. Um, and there's no shame. You know, I was talking to you earlier and saying that, um, I'd got an app and it ended up being a subscription thing quite recently, and I didn't realize at all, um, very, very easy to fall for these things.

**Graham:** I'm like, we'll often use tricks to try and hide the fact that you're going to sign up for a subscription so like they might have texts, which tells you that, but it'd been light gray on a white background. So technically they told you, I mean, my eyesight's not the best, you know, particularly on a mobile phone.

I wouldn't necessarily be able to read that and realize quite what it was saying to me.

**Sarah Botterill:** Okay, let's see what this says… 24% of people are saying they have and 76% saying they haven't. So, many people haven't fallen for it, but you know, a reasonable proportion of people who have so I just share those.

I guess to come to the positives of what you can do online.

So as we were talking about earlier, and there's some really fantastic things that you can do, um, and internet banking is one of them. Perhaps you'd just like to talk us through how to bank safely. Um, and also just to reiterate again, some things to watch out for and things not to do when it comes to online banking.

**Graham Cluley:** So on this slide, we've got some great. Do's and don'ts. Let's go through some of the Dos. First of all. One is, uh, and obviously internet banking is so convenient and all the rest of it, but sometimes things go wrong or there may be a fraud alert and you might get a phone call from your bank.

And that's something which personally I have to say, I always appreciate, um, cause it's nice to know that they're looking at, at the transactions which are happening.

That kind of thing might be a little bit dodgy, but. When a bank does call, you be very careful about what information you give them back. If you have a bank which contacts you and say, hello, it's XYZ bank here, and uh, we're just calling you. Uh, but first of all, we need you to confirm your details. So can you tell us what your banking password is, please?

What, can you tell us what your account number is? And. Okay. Or giving information to someone like that who's just rung you up out of the blue. There is a danger that it could be a fraudster pretending to be your bank. So what I would actually suggest, and the person calling you will never complain about this.

If you say this to them, quite politely. Say, look, I feel uncomfortable doing that. We're having this conversation. I'm going to ring my bank instead. And we can have the conversation then and the only thing I would say there is if you do decide you're going to hang up and dial them back, use the official number listed on the bank's website or on the back of your bank card.

Don't use any phone number, which the person who's called you has just told you on the phone. Because sometimes what they've actually done is they've set up completely, uh, uh, fake, uh, switchboards where if you ring the number, which they give you, it answers as though it is your bank. And so it's quite a sophisticated scam, which can go on so.

So one of the sad things is you end up being more cynical and a little bit skeptical about the world and less trusting. But you have to do this be suspicious of unsolicited calls from your bank particularly, if they ask you for sensitive information.

Next do is this. You've got to have a unique password for your bank account, and some people say that you should regularly change your passwords. I don't actually agree with that. I think if you regularly change your passwords, there's a chance you might change it, something weaker, uh, or repetitive. So what I would suggest instead is keep your password and make sure you're not using it anywhere else on the internet.

And only change it if your bank tells you that you need to change your password. If there's been some kind of security incident. I don't think I've changed my banking password in many years, uh, because there hasn't been any need.

So they've got pretty good security in place. There's been no breaches. And if you do see any suspicious activity at any time on your financial statements, or if you receive dodgy looking emails, contact your bank.

Uh, let them know about the phishing attacks, which you're receiving. And if you do see strange transactions going on your account, contact them and say, Hey, I've got a feeling my credit card details may have been stolen, or whatever it is.

Uh, because of these odd transactions, which I certainly didn't make.

And they'll have dedicated teams. We're working to shut that down and protect you.

**Sarah Botterill:** That's great. I think, um, one there that we've talked about a lot already, which is the unsolicited links, and just to be very wary of those, um, as you said, in terms of of dos, I guess having a unique password, but don't share it with anyone.

And as you've said, um, if a call is unsolicited, you know, feel brave enough to say, actually, I'm not going to give you my details. I'm going to go and find a number and I'm going to call you back.

**Graham:** Yeah. They shouldn't even be asking you. No service should be ringing you up and asking you for your password. Quite frankly, it's just crazy that they would do that. Sometimes when you ring the bank, they might ask you to verify certain digits or seven characters, like, can you tell us the second and fifth character? Like suddenly would never ask for the whole password.

That's brilliant. Thank you very much. The same for shopping. You know, lots of us, um, uh, shopping online at the moment and what some tips to staying safe online when we're shopping for essential or for the odd luxury to keep us cheerful during these difficult times.

**Graham Cluley:** So the first thing is use a website you trust and have used before and have delivered the goods. Uh, you know, I think that'd be most people's first choice.

But of course, if, if you're tightening your belt and trying to save some money or you can't find the item which you want on your normal website, you may go looking elsewhere.

And so if a website is new to you, do your research, see if it has good reviews.

You could even search for it in a search engine and see if anyone else is complaining that they got scammed. After using the website so that, you know, do, do the footwork to find out that, um, obviously be very wary of any links inside emails, especially if you've haven't actually signed up to receive emails from them because it might be a scam.

And, uh, there's a common one, we sort of touched upon this earlier, but during the whole pandemic, a lot of people obviously are getting things delivered, uh, by courier. And. A very common fraud, which we see cause it uses a clever bit of social engineering is we've got a parcel. We wanted to deliver it to you. But there's a problem. And if you click on the link or if you click on the attachment, there's a danger that you might compromise your computer or compromise your details. So if you haven't ordered anything, if you're not expecting a delivery. Delete the email, right? Cause instantly, you know, this is nonsense, but also you should be asking yourself, well, what's the courier company actually know my email address? Quite often they wouldn't. Quite often they would, the courier company would simply know your postal address.

There'd be no way for FedEx or whoever to drop you an email. That's not the way in which they operate. another good piece of advice is when you're buying things online, maybe use your credit card because they offer you extra protection.

Uh, the credit company can rather than using a debit card. And another option which I choose to use sometimes on websites I've never done business with before, is I won't enter my credit card information. Instead, I'll use PayPal. A lot of online websites will accept payment via PayPal, and that gives you additional levels of protection as well, which is a, uh, a good thing to know about. But like we said before, you can also get PayPal spoof emails as well. Also, again, read the small print. If there's a problem with the thing which you're buying, make sure that there's a way to return it safely and easily in case you're disappointed with the real life experience compared to what it said on the website.

And once again, read the reviews on Amazon, for instance, you will see lots and lots of reviews of products. Sometimes those may not be completely true. There's a lot of, uh, you know, tricks people do to post fake reviews and sadly on these things. Um, but if you're buying on eBay, that's quite a good system as well. I find, you know, it's, it's a way of finding out whether people actually received the goods. I've got a good history of sellers have got a good history. Then you can feel more confident in purchasing products from them.

**Sarah Botterill:** That's great. Thanks ever so much for that.

There is software. I know, as you say, um, the scammers tend to play on, on us as, um, a weak link, but there are things that you can do to help protect yourself. Talk us through this little toolkit that you've put together here in terms of things that can help people.

**Graham Cluley:** Yeah. I wanted to suggest some products which are available for free, a few to try out and, and see how well they protect you.

Top of my list. I think something which many people don't have is a password manager. And this is something which securely stores all of your passwords, and that means that it's possible to have different passwords for every website, which you access it.

And that's my recommendation. You shouldn't be reusing passwords. I know most people do reuse their passwords, but my advice is you should have a unique, difficult to crack, impossible to remember password will the sites. Which you have to log into. I've got over 1000 different passwords. I couldn't tell you my email password or my Twitter password or any of those.

My password manager, knows it for me. So there's a couple of good solutions. Uh, LastPass is a good one BitWarden is a good one as well. Uh, I'd really recommend people look into password managers. Another thing ad blockers. Because there's a lot of dodgy advertising out there. Some of it designed to infect your computer, which obviously is unpleasant.

Nearly all of it slows down your computer and the other cases, it can be tracking your online activity. If you've ever wondered, one ad is popping up. But something on a website which you looked at weeks and weeks ago. It's because your movements around the web, but basically being tracked by advertisers.

I like don't like that.

So for my own privacy, I run an ad blocker and anti-tracking software and there's something you can plug into your browser. Uh, there's one here we were mentioning called Privacy Badger. Um, which sounds kind of cute. Uh, it does a very good job though, of stopping advertisers from tracking you and stopping those ads from appearing.

And finally; this is a real must have these days. I think most people realize they have to do this, run an antivirus program and keep it up to date.

The good news is the consumers that are free antivirus programs out there these days, perks from Bitdefender, Avast, Sophos, Malwarebytes. Those are four very well-known ones.

There are other ones out there as well. Um. I would tend to say go with one, which has an established name because unfortunately there are also scam antivirus products out there, but those ones I just mentioned, those are all legitimate. Go to the real websites for those companies and you'll be able to download a decent free antivirus from them.

**Sarah Botterill:** Great. Thank you Graham. That's a really good advice for people there. Um, so we have our final poll. Now, let me just launch this to everybody.

So this is just to find out, um, whether people do have their software and stored already.

So antivirus malware, are you using a password manager, or do you have, uh, none of the above? So just allow a little bit of time to see, um, see what people have got on their PCs, um, and what they're using.

It's a great safety net, but I think, as we've said, is no substitute for some of the other, other things that we've talked about….

**Graham Cluley:** yeah, yeah, technology plays its part, but I think it's very important what we can do as individuals, um, to protect ourselves. So ultimately it's us who click on the link or open the attachment or visit the dodgy website or into our credit card information. Uh, but security software can, can be a useful safety net to protect us as well for when we make mistakes.

**Sarah Botterill:** Fantastic. So let's see what everybody is saying. Um. So looks like there's a good spread there. 88% of people are running antivirus software. 52% have a malware program. Um, 26% using a password manager like you and, and just 6% using, uh, none of the above. Um, and people will have multiple options there.

So, um, you've mentioned this earlier. Um, and, um, I know that lots of us are using, as we all right now, have video conferencing.

Perhaps just a brief recap around, um, we've said scammers are trying to take advantage. Is it safe? You know, we're on zoom now. Is it safe and best practice around it?

**Graham Cluley:** I guess in terms of advice for people that, but there've been lots of headlines in recent weeks because of course zoom has come suddenly very suddenly become immensely popular cause so many more people needed to use it.

And there've been lots of new stories about security problems with zoom and. All kinds of, yeah, vulnerabilities with it. I think as long as you're keeping zoom up to date with the latest security patches, so you're installing updates as soon comes out, then it's a pretty good choice for most people. I think it's an effective way to communicate.

I think in the current situation in particular, we want face to face contact, but we can't be physically face to face zoom and some of the other video conferencing apps out there are very good. I wouldn't recommend it.

For highly sensitive communications. If I was, for instance, like government minister, I think zoom maybe isn't the right product to use, and there may be other ones which would be more appropriate for them. I'll let GCHQ advise the British government which one that should be, but okay. I think for most of us, the threat is really very small indeed.

And encouragingly, in the last few weeks, zoom has said all the right things has issued lots of updates of the concerns, which are found, and to be honest Yeah, there were bugs in zoom, but there are probably bugs in all the other video conferencing software out there as well, which equally need to be sorted out.

So zoom are making all the right noises right now. And I think most of us can be reassured about that. But there are things you can do to better protect your conversations on zoom.

And that includes password protecting your online meetings. So if you're having a video chat with someone, set a password for it, don't make it an easy pass or don't make it one, two, three, four, five. Don't make it password. Make it and only share that password with the people you want to join the meeting.

You may also want to set up a waiting room and allow other people to share their screen.

Maybe there's no need for other people to share the screen.

There's this problem at the moment with zoom bombing. Where people are breaking into other people's zoom conversations, and then they may be playing loud rock music or showing sexy videos on their screen, or unsexy videos on their stream and sharing that with everyone else who's obviously really unpleasant and antisocial.

So make sure that other people can’t, take over the screen, uh, if there's no need for them to do that. That's a good thing to do. So, and also, as we said before, right at the beginning, be careful about unsolicited emails, which might invite you to a zoom conversation. Make sure it's really going to zoom and not to somewhere else because that is going to be a common trick which the bad guys are going to use at the moment.

**Sarah Botterill:** And we're saying that, as you say, things like zoom bombing, some people might be alarmed. It's extremely rare, I think, isn't it, Graham?

**Graham Cluley:** Oh, yeah. I mean, if you think about how many hundreds of millions of zoom video chats are going on every day at the moment, and you might see one or two reports in the press… I saw one of the other day about some fitness gym or church, uh, zoom recording and those sort of things can easily be prevented by stopping people from sharing their screens and having tighter controlling in terms of passwords as to who can get in.

**Sarah Botterill:** Brilliant. Thank you. Um, so I'm not going to read all of these out, but there are, a few things on screen here, and these are some people who can help you out if you feel that you have fallen victim to a scam or have got any concerns, um, and please do also go back to that and the slide with Graham's face on it, and make sure you check out his podcast because it's excellent, as you, I'm sure you've had, he's got some great advice for people as well. So, um. Equally, we're here for you. Um, we are running a series of AbilityNet Live events you can call our helpline for free.

I've got to pass to my colleague Mark and see if we've had any questions coming through or any kind of trends that you've picked up on in the chat there.

**Mark Walker:** That's fantastic advice. So thank you. Um, I've got a couple of questions. Um, how safe is Apple pay? And I guess we might include other pay systems like that in your experience? Pretty safe.

**Graham Cluley:** Yeah. Apple, actually a company which has really tried to differentiate itself in terms of privacy and security.

Um, generally I would argue that the Apple ecosystem is more secure than Android. Um, although I'm sure the, uh, the Android equivalent to, uh, Apple pay is similarly well-constructed and engineered as well. But I think there's no greater issue with using Apple pay than using your regular credit card. I wouldn't be any more wary about using it than that.

Mark Walker: Right. Thank you. Um, someone says, I often get friend requests on Facebook from people I don't know, that looked like fake accounts. Do you know what this scam is?

**Graham Cluley:** So it might be that they are trying to, I mean, there's all types of scam, which they might be doing. They might be attempting a romance scam, for instance. They may just want to get a chat to you, but they may also be targeting someone who, you know, so once they friended you. The actual real person who they want to target. It could be someone in your friend group, so having friended you and maybe some other common associates, they may then target the genuine person and that person thinks, Oh, they must know they must be legitimate because Bob and Fiona know him already.

They're already Facebook friends with them. So be very careful. Never accept friend requests from people you don't recognize. I personally would be wary even of accepting friend requests from people. I do recognize because it's so easy to find out people who might've gone to school with, or people you might have worked with.

You can go on LinkedIn and find out that there's people could create fake accounts in their name if you want to be absolutely certain is the person you think it is. If you do happen to recognize the name, then you might want to bring them up, say, Oh, did you send me a Facebook friend request? And if they say, yeah, I did, then you can accept it.

And knowing it really was that person who did it rather than someone pretending to be then.

**Mark Walker:** Great. Thank you. As a couple of questions here around windows, and I guess the clearest one is, is windows defender enough? Is it sufficient to protect you? I.

**Graham Cluley:** Personally, I'm not a huge fan of it. I think you might be better off using some of the other antivirus solutions out there.

One of the problems with using windows defender is that it's the antivirus program, which is basically bundled with windows. And what that means is that if you're a hacker, you know the vast majority of people you're going to try and infect on their computers are likely to be running windows defender.

And so you will engineer your attack to get past windows defender. Because I think chances are they using windows defender. So if you're using something different, that's an additional level of protection. So, uh, personally I would use one of the products, which we mentioned earlier in the presentation over windows defender.

**Mark Walker:** And could you make any recommendations about particular packages?

**Graham Cluley:** Yeah, so we, we mentioned some free ones earlier and I think we mentioned avast, Sophos and Malwarebytes. Uh, those are all good solutions. You can try those out. You'll be able to download for free from their website and see how you get on with those personally. Although those, that, there are free options. I'm also, I have to make a bit of a fan of actually paying for my antivirus software because. If you do ever get infected and it's nasty and, and why wouldn't it be great to have someone you could phone up and say, I'm a customer of yours. I'm a paying customer of yours. Can you help me resolve this problem? And so, personally, I quite like the idea of spending 30 or 40 pounds a year to get an antivirus program with support included. Okay. No. If if money's tight, I totally understand that. And a free antivirus is better than no antivirus at all. Okay.

Thank you. Um, I don't know whether there's an obvious answer to this, but there's an issue that we see that I'm reading there…an issue we see is individuals with intellectual disabilities being vulnerable to scams. Training is clearly important for this group. Do you have any additional thoughts about how they could be protected?

**Graham Cluley:** I think all of us as a community can play our part as well. We may have loved ones or family members who have challenges in this area, may be more vulnerable to being scammed or believe in things. I'm on or not checking their facts properly. The challenge we have right now is we have even less visibility over what they are doing on that email than we did before the lockdown in the past. We could go around to the house once a week and say, Hey, what emails have you been getting? Let me have a look at it. Or are you doing that remotely? It's much more difficult to have that kind of conversation and just to keep your eye on certain people to make sure that they aren't, for instance, uh, sending money to a scammer, uh, who might have tricked them. It's a beastly thing, but these scammers really have no morals at all, and they don't care who they are exploiting. Well, what disguise is they might use because all they care about is fill in their pockets. So we've all got to be on the lookout for it. But don't just look out for yourself. Try and look out for your loved ones.

**Sarah Botterill:** I wonder if it's worth saying at this point as well that, um, so you mentioned earlier the scammers are not targeting you, cause that might be comfort to some people, particularly these vulnerable people who think, well why me and why is that inbox come to me specifically, but actually it's not, it's already gone to hundreds of thousands of other people.

**Graham:** It's an excellent point. A lot of people think they have been specifically targeted by criminals, and it's not true. The vast majority of occasions, they've sent their scam messages to hundreds of thousands of people, maybe with the hope that just near percentage full for the scam. Uh, to give you a quick example of that, there is something at the moment which has been coming for the last couple of years called a sex terrorism scam, where you receive an email and they may even quote an old password, which you've used, and they say, we've got your old password. We know that you went to an adult website and you looked at videos and we have secretly taken video of you. And unless you pay us so many Bitcoin. You. We are going to share this video we've taken of you with your friends and family, and obviously it'd be highly embarrassing. Those emails are complete and utter nonsense and you should just delete them. Like it didn't take any video of you. Um, your computer hasn't been hacked in any way and there's no chance of them embarrassing you with your friends and family.

The thing which tricks people. Is they might quote one of your old passwords, and the reason for that is the hackers have got hold of a database of a security breach, which maybe happened years ago, maybe at somewhere like LinkedIn, which happened years and years ago. It's out there in the public domain. And so if they quote that password to you, you think, Oh, crumbs, they must know all about me. No, they don't. I don't know anything about you and that possibly wouldn't even log them into LinkedIn any longer, but that can be enough to trick people into giving the scanners money. So please, please don't give the scammers money, even if they claim type all kinds of embarrassing information about you.

**Mark Walker:** I've got a couple of quick ones, and then, uh, I think I'm hopefully going to cover most of them. Um. Should we have a VPN? How about malicious browser extensions? And a third one was about ad blockers preventing you from getting onto a website because the ad blocker has prevented you from going to the website.

**Graham:** Okay. Let me try remember. So malicious browser extensions was the first one, so yeah. Yes, there is a danger. Uh, you can add all kinds of extensions to your browser. Some of them are very good. Occasionally a bad one will break into the Chrome web store. For instance, if you're using Google Chrome, Mmm. Yeah, that that is a danger. Google tries to police those kinds of things and remove them and get them kicked out when possible. But if you add too many browser extensions, you're obviously increasing the chances. One of them might be compromised. Uh, you asked about VPNs.

A VPN is something which you can use for two purposes. One is to hide your IP address. The other one is maybe you want to. Logging into a streaming service in another country. Maybe you're on holiday pay. None of us are on hold at the moment, but maybe you're abroad and you want to log into iPlayer, so you might want to try and use something like a VPN for that.

I think for security, a VPN is perhaps a little bit less important than it used to be because so many websites these days are using HTTPS without getting too nerdy. That means that your communications are already encrypted to them, but if you do choose a VPN. To, to sort of tunnel on the internet. Be careful who you purchase it from because you are sharing your information with the VPN company.

And some of those might be a little bit scammy, so it'd be, it'd be a little bit where that, and the final one, I can't remember what it was. Number three, do you remember it was about…

**Mark Walker:** if Adword blockers prevented us from getting onto the website? Yes. So some websites, because obviously they're making money out of the advertising. They will try and block you from accessing the website if you've got an ad blocker turned on.

And I think then you really have to make a choice. If you really want to access that website, what you can do inside the ad blockers, you can white list the website. Um, there are ways of getting round some of those, the systems which some websites have, but they're probably too nerdy to get into detail with, uh, on this particular webinar.

Um, but that's something in which you might want to consider is, is just white list in the site if you really have to get to it. Uh, I think a lot of websites right now are actually finding web advertising isn't working as well as it used to. Um, despite the increased web traffic, which is going on, it seems to be a market which is really struggling.

And maybe ad blockers have played their part in that, but I think websites need to start looking at different ways to monetize themselves than just through advertising.

**Sarah Botterill:** Okay, brilliant. Um, so just to say a massive thank you to everybody who's joined the webinar, but especially to Graham, it's been lovely to work with you again, Graham, and I think we've covered a lot of ground and there's some great advice there.

Um. Genuinely, um, at the moment, it's a a time when we want everybody to stay safe, stay well, and also to stay safe online. And I feel like you've given us a whole bunch of tips that will genuinely help people do that. So thank you ever so much. Um, we'll be sending out the recording the transcript, um, and putting up some additional links as well, um, in the next couple of days.

So please do watch out for those. So. Thanks ever so much everybody, and as I say, yes, please do stay safe. Stay safe online. Thank you.

**Graham:** Thank you. Cheers.