KAREN FOLEY: Welcome back to Student Hub Live. Well, I hope you're enjoying the fantastic array of guests that we've lined up for you today on the show. We're going to talk about keeping safe online, about digital security. And I'm going to introduce you to Jason Nicholls, who's an information security specialist at The Open University. He spends his days trying to keep hackers out of the OU network, away from our sensitive information.

And I met Jason in the days when Garmin was having a huge outage and ransomware CORE were holding all this data hostage. It was terribly exciting, but it made me think, actually, how important information security is. So we've got some great tips for you at home. Jason, can you start by telling us what information security is and why it's so important right now?

JASON NICHOLLS: Hi, Karen. Yeah, sure. So, information security is all about keeping the information that we think at the University is important, safe, secure and used responsibly. It's not just about keeping hackers out. We also need to make sure that we treat information with the proper care and respect that it deserves. And this is a legal responsibility the University has as part of the GDPR requirements. More than that, it's an important part of ensuring the University is a safe place to study and to work.

KAREN FOLEY: Brilliant. So we've met our Virtual Learning Environment. We know students are doing stuff online. Is there any risk? You're saying it's your responsibility - and I say yours - to keep the University safe from harm. Is there any sort of thing students should be aware of? Are there any risks for them in terms of studying online?

JASON NICHOLLS: Yeah, absolutely. So at any time using a computer there's always going to be risks. So hackers look for any opportunity to get into an account or any website because all accounts have some sort of value to them as part of, a sort of, information economy. And that basically means that your personal information has a value to it. The personal information of others has a value to it. And the study material at the University itself also has a value to it. We've seen many cases where people have signed up for a course at the University and they've been approached to copy the learning material, for instance.

But beyond that, computers themselves are worth money online. Your computer is a little place on the internet where they can start an attack. They can monitor information. They can watch what you're doing, try to get your payment details, try to understand more about you. And all of that information has a value nowadays. Even stuff like your email account and your social accounts - Facebook, Myspace, LinkedIn, Twitter, Instagram. They all have a value. They can be used to co-opt things, to advertise things, to promote fake news.

So what we really ask is the students follow the advice we give on our website, on the Help Centre, Safe and Secure Computing, and that provides some really great information on how to stay safe online. Really, if it looks wrong, doesn't feel right, seems too good to be true or too scary or very urgent - sorry. Out you go, Puss. Thank you.

KAREN FOLEY: [LAUGHING] Oh, my cat's sitting there being - actually, the dog's being trying to get up on the chair, but no avail. [LAUGHING]

JASON NICHOLLS: Oh, deary me. Yeah, and it's -

KAREN FOLEY: Yeah, I was watching -

JASON NICHOLLS: It's amazing, really.

KAREN FOLEY: I was watching *The Social Dilemma* on Netflix the other night, which I think highlights some of these things. And they said, if you aren't paying for the product, you are the product. Obviously, with The Open University, as you say, we have this responsibility to keep stuff safe. But nonetheless, like you say, with any online environment, people are very targeted and it's really increasing. What's some of the stuff you do to make sure your online - I guess, footprints are what we call it, isn't it? - is safe?

JASON NICHOLLS: Yeah. So at the University, we've got a large variety of security technologies that we use to try and keep things safe at our end. So we've got firewalls. We've got security appliances. We've got threat detection stuff to try and keep our end safe.

And we also conduct some monitoring to ensure that, the activity that you guys are doing seems safe and reasonable. So if you use our email system, we monitor for suspicious-looking emails that look like common spam. We look for quantity and quality, stuff like that.

But really, for your end, it's nice and simple. You don't have to worry too much. You just have to run an antivirus. You just have to keep a nice, strong set of passwords, a different one for every website. And you just need to be very suspicious of anything you receive by email, in the same way that you would be suspicious of a letter or anything like that.

KAREN FOLEY: No, absolutely. Well, the cat appears, and the students go wild at home, and Ruth's cat is zooming right now. I think she means running around, not in an online meeting. And we also have a question about the targeting of students to do with phishing - that's the P-H-I-S-H-I-N-G - and the cyber security warning over the last few months from the OU. So Kevin wants to know, what can we do to reduce the factors of this targeting?

JASON NICHOLLS: So, it's a two-part question, really. So there has been a massive uptick in phishing in this last year. I think, now that all the hackers also have to spend all their time at home, they're getting quite bored too, so they're running lots of interesting targeted campaigns. And of course, the University is a place that's absolutely stuffed full of useful and interesting information for a hacker, so they're going to try and get in as much as they can.

But they do a lot of research. For a targeted phishing attack, they can be very specific-seeming. They already know, for instance, you might be at university. They can Google your name, which is usually part of your email address, in many cases. Once they have your name, they can look for Address History. They could probably take a rough guess at your age from that information. There are websites online, which act as giant directory enquiries, and you can check out a lot of stuff.

I mean, I put a lot of effort into having a small internet footprint and making sure that it would be difficult to come up with a targeted phishing attack for me. But that said, I'm pretty sure that, if you all went to the internet right now and tried, having seen my face and know my name, you could probably turn up at my front door tomorrow. And that's a bit terrifying, but unfortunately, that is the world we live in nowadays.

So to protect against that, you just have to apply some simple, common sense rules. Pay attention to the emails you receive. Do they fit with what you know? Are you expecting a package? Why is HMRC e-mailing you here? That sort of thing. It just doesn't quite add up when you look at a phishing email.

It might be very targeted. They might know your name. They might know something about where you live or a course that you might be on or your partner's name or something like that. But that information is largely publicly available nowadays, so anyone can have it. So it might not necessarily prove that something's happening.

And these things always have a sort of call to action, so that you need to do something straightaway. You must click on this link. You really need to call this number. You've got to open this attachment. And that is suspicious. And if it seems like it might be something you need to deal with, then I would advise contacting the company directly by going to their website and using their contact page.

KAREN FOLEY: Brilliant. That's wonderful advice. Thank you. I hope that answers your question, Kelvin. Sorry I said Kevin. A bit of online dyslexia there from me. Now, the other thing that's going to get people going wild is talking about cookies. But we do not mean the type that we're going to eat. We're having a break, by the way, because I am hungry as well, in a few minutes time, so do save this for now. But Jason, I've been noticing so many more cookie requests and things, I think as a result of this GDPR things. What are those about and should I just keep accepting them?

JASON NICHOLLS: Right, absolutely. So as you say, there are loads of cookie warnings for websites now because of the GDPR. So GDPR stands for General Data Protection Regulations. It's basically a law from the European Union, which has been adopted in the UK, to try and protect personal information because, as we all know, it's absolutely everywhere. And we'll touch on that a little bit later as well.

Now, the aim of that is to make sure that personal data is only used in ways that you're comfortable with, which is really great. However, unfortunately, instead of companies taking this as an opportunity to be less invasive and track your personal data less obtrusively, many companies now just flood you with ninety or so GDPR requests when you join their website for the first time, and then they offer you a convenient little 'click here and accept all' button instead, which completely undermines the whole point of it.

And I would, from websites, certainly, that you use regularly, I would go through those and I would turn off all the targeted advertising that they recommend. I certainly do that. For some websites that are a bit more throw-away - just a link that a friend sent, maybe - you've just really got to weigh up the benefits of looking at the content against the idea that they might know, quite frankly, a scary amount of information about you once you've clicked on that site.

Now, not all cookies are bad. The original point of a cookie was to allow a computer on the internet to be able to identify you. So when you log into the University, you get a cookie from us that says, hello. Yes, I'm a student. This is my name. And then we can use that to provide you your learning experience. So our website wouldn't work at all. You'd have to click on exactly the course and say, yes, I'm this person, every single time you did everything, because otherwise the computer would have no way of remembering who you were. And now that's, really great.

Unfortunately, cookies have been kind of co-opted by targeted advertising, which is something we'll touch on a little bit later.

KAREN FOLEY: Perfect. No, that's absolutely wonderful. Now, I've noticed, because I often accept cookies, that I'm bombarded with a whole range of cycling ads and clothing ads and things, because normally when I'm not working, I'm looking at cycling clothing. So how does this targeted advertising work, and as you say, is it such a bad thing? Because I love seeing lots of cycling clothes. I'd much rather see that than anything else, for example. So how does that work and is there anything we should be mindful of?

JASON NICHOLLS: Absolutely. So targeted advertising is a really interesting area of the internet, and it's all part of the information economy, which is basically the buying and selling of information about people, to try and make advertising better. Now, the idea of making advertising better sounds very appealing. I would like to see adverts that are targeted and tailored to me. I wouldn't like to see adverts that are totally unrelated to me. They're very simple pariahs.

However, the internet tracking has gotten to a little bit of a, sort of, stalkery degree to it. So, when you go to a website that has tracking cookies on it, they live on your computer. And now one of the big internet companies knows a little bit more about you and a bit more about your habits, your feelings, your shopping habits, that sort of thing.

Amazon is an example. Every time you go to a website, you get a little Google cookie from many websites, Google Analytics. And then that website has a category in the larger ecosystem. So now, Google knows that you're into fishing, for example, or cycling. So now when you go to other websites, it ties those two things together. So now you're so interested in cycling and interested in clothing. So now Google knows that if it can sell something that converges both of those things together, then we can make a more targeted, more useful advert, which is really great.

However, they do that for everywhere you go. So now they know everything about you - your age, your gender, your rough location, connections you have with other people, that sort of thing. For instance, the Facebook app tracks your location, and it'll compare your location with the locations of other users. So then you can go and get 'advertised', people you've been near recently as people that you may know, or people that people that you've been near know, which is very unfortunate.

Now, there's a whole economy in the background where companies buy and sell that information. So Google will tell Tesco, for instance, oh, we've got this little bit of information about this person. And Tesco goes, okay, well, we know we have some of their card history records, which is a little bit creepy.

And then we can go into all sorts of stuff from beyond that where we ended up, a few years back, Tesco's accidentally ended up disclosing the fact that a member of a household was pregnant by sending the household pregnancy-related club card vouchers and coupons. Now, of course, the rest of the household didn't know that and I'm quite sure the person who was pregnant wanted to keep that a secret. But something as simply as innocuous as five percent off baby bottles or here's a voucher for some nappies, it can really have a very tangible effect in the real world, having all of these things linked together.

KAREN FOLEY: Absolutely. And I can imagine there's a much darker side to all of this also. Jason, we've got a couple of questions. We're nearly out of time, but let's quickly nip over to HJ and see what we can do to help people at home. I know there's been lots of chat about all sorts of cookies, and also Jaffa Cakes and cranberry cakes and much other stuff. HJ, what burning questions do we have for Jason?

HJ: Yeah, so, Devin's got a top one that I think we could address. So Devin's asked, so I have a few issues with this. My computer sometimes won't let me access an OU page because they say it's insecure. What does Devin do about this, or is it secure or is there something happening?

JASON NICHOLLS: Ah, yes. So this is a recent change within Google Chrome, which I personally am a very big fan of. So on the internet there's websites on http, which stands for hypertext transfer protocol, and https, hypertext transfer protocol secure. And those are the websites you see with the padlock.

Now Google, in its infinite wisdom, has decided that, if you don't have that little padlock, your website might not be secure, which is entirely true. But secure in the sense that people can see what you've browsed if they're on the same network as you. So if you were in a coffee shop, for instance, and you're not on a padlocked website, people can see that you've gone to that website.

Now, the University has a lot of websites. Some of the websites we have as secure and some of the websites we don't because they don't contain any information that is sensitive or personal or private in any way. For instance, our www main website is just information about the University and teaching material. So at the moment, it doesn't have the little padlock icon because anyone can go to that website and they'll see exactly the same sort of thing as you do.

However, when you go to our student home website or the VLE or the eTMA submissions website, they all have the padlock because that's information we want to stop people from seeing. We don't want people knowing what essays you've submitted. We don't want people being able to copy those things. We don't want them to have access to your personal information. So those are all locked up nice and tightly.

But the stuff that is public information, not that it doesn't matter, of course, but anyone can have a look at it. That's not secure at the moment. Now that's something we're looking at. It might just be worth us turning the padlock on for everything just so our users don't see that little non-secure thing because we do recognise it can be confusing.

KAREN FOLEY: Brilliant. Fiona says, it's all rather scary, George Orwell and being watched, and I think many of us are reminiscent of that. Naomi says, why are they called cookies? Is there a simple answer to that?

JASON NICHOLLS: Yes. So a lot of the early history of the internet is just basically puns. So all of the early computer operating systems had a wide variety of strange puns that people would write a little bit of a programme, and then add it on. For instance, when things used to just be text, there was a programme called 'more', and you could type more and see more of a file. And they made a better version of it called 'less', because less is more, which is a totally ludicrous pun. But that's just how the internet was back then.

And cookies - it's a sort of lost in translation American thing because it's about the story of Hansel and Gretel where there's a trail of breadcrumbs, or cookie crumbs, going back so that you can always find where you've been.

KAREN FOLEY: Brilliant. Would you like bread, I guess, is a lot less likely to be accepted, especially in the days of carb loading, et cetera. That's all we've got time for. Jason are you able to pop into the chat, because I know people have lots and lots of different questions. Is that something you can pop in and do now?

JASON NICHOLLS: Certainly. Yeah.

KAREN FOLEY: Lovely.

JASON NICHOLLS: I'll try and get into the chat in next five, six minutes then.

KAREN FOLEY: Brilliant. Perfect. Well, Jason's going to pop into the chat. Thank you so much, Jason. You've made that super interesting and so exciting. I wish we had more time, but we don't. We're going to have a short break now. Jason will be in the chat to answer any other questions. The chat's going to keep going.

We're going to show you a video about digital careers in a world of work, and then some other videos. We'll be back live at one, where we're going to roll on with our programme. I've got some wonderful tutors for you to meet. So you can find out about your relationship with your tutor, your student services. We'll be talking to the OU Students Association. We're looking at mental health and staying well in your studies.

Assessment - a key session there. Working hard and playing hard, those of you who wanted to look at time management. And then we're doing heaps more around Student Voice and the new Student Charter. So do stay tuned but do grab some lunch, and Jason will be in the chat to answer your questions. See you back live at one o'clock but do keep chatting. See you then.