**Young Scot Podcast for Cyber Scotland Week 2020**

Audio Transcript

18/02/2020

Narrator: This podcast is a collaboration between Young Scot and Jess Mcbeth from the UK Safer Internet Centre as part of Cyber Scotland Week 2020.

Narrator: Young Scot supports young people to share their own voices, views and opinions. The views expressed in this podcast are those of the young people who have taken part in the podcast, not necessarily the views of Young Scot.

[digital music]

Christopher: Hello and welcome to Cyber Scotland Week, we are in the Young Scot offices for a special cyber resilience themed podcast. So, I’m Christopher and I’m 18 and I’m from North Lanarkshire.

Kalina: I’m Kalina, and I’m 26 and I’m from Aberdeen.

Stanislaw: I’m Stanislaw, I’m 15 and I’m from Edinburgh.

Christopher: So, first, Kalina, what’s your interest in cyber?

Kalina: Well I volunteered to be a part of the Digi Know? steering group because cyber is such a diverse field. It’s developing so fast that I kind of wanted to be at the forefront of it and learn more about what’s happening and what careers, what opportunities you have in the field.

Stanislaw: I was just wanting to make sure that everyone was safe on the internet and I wanted to be a part of helping everyone.

Christopher: Well for me, I’m doing a degree in cyber security at university so I figured joining this project would be a good way to offer what I’ve learned and as well learn some more through the project.

Christopher: So, would you say you have learned anything from being part of the steering group?

Kalina: I have learned, as cheesy as it is, to change your passwords regularly and to be mindful of what you post online because everything leaves a trace and it’s really scary how people can track you down by your pictures.

Christopher: Stanislaw, have you learned anything being part of the group?

Stanislaw: Of course, I have learned that I need to know what I’m posting on the internet and that I don’t upload anything stupid that I don’t want anyone else to see.

Christopher: I think personally for me I learned about all of the meta data that can exist within a photo – we did a few sessions last year with an expert and they were showing us that photos have exact GPS coordinates in them and you can find out exactly where you were at exactly what time and people can just track your movements through various photos. As well, for instance, you can just search for the name of a ship and find out where it is, what it’s carrying… and just the extent of big data that exists is immense.

Christopher: So, we’ve learned what *you’ve* learned from Digi Know? and we’ve learned what made you join in the first place but what actually is Digi Know?

Kalina: So, the simplest way to explain this is that Digi Know? is a group of young people that want to help other young people discover their interest and love for all things cyber. So, things like cyber security, cyber resilience, and we wanna be able to give them practical skills that they can use in their everyday lives but also opportunities of what they can do as in a career in cyber and just all around keep them safe on the internet.

[digital music]

Chris: We now have Jess McBeth with us from the UK Safer Internet Centre. Would you like to tell us a bit more about what you do?

Jess: Oh hello, good morning! I’m an online safety consultant with the UK Safer Internet Centre so that means I work with children and parents and professionals… thinking about their online lives and supporting them to live a good life online and keep themselves safe at the same time. So, I’m based in Scotland, I represent the UK Safer Internet Centre here, and I promote Safer Internet Day here as well so, yeah, it’s a great job, I get to speak to loads of fabulous people such as yourselves.

Christopher: Thanks very much for coming along! So, if you don’t mind, I’d like to power straight on to the questions. Stanislaw, would you like to ask the first one?

Stanislaw: Do you ever look yourself up on the internet?

Jess: I do occasionally. I’m probably gonna do that again before this comes out [laughter] just to double check. Yes, I do, it is advice that I give, particularly to professionals. It’s something that adults don’t tend to think about so much, checking themselves online – is it something you guys do, do you look yourselves up?

Kalina: I have looked myself up.

Jess: Uh huh...

Kalina: Apparently there are a lot of women with the same name as me a lot more famous than I am.

[laughter]

Kalina: So, I have nothing to worry about!

Jess: That can sometimes be beneficial perhaps. What about the rest of you, have you looked yourselves up?

Christopher: I have but I couldn’t actually find myself, or other people with my name were just taking over the search results. And I think there was someone famous with a very similar name so it was trying to direct me that way and I’m like “Well that’s good, they can’t find me” [laughter]

Jess: Yeah, it’s pretty helpful. Sometimes it’s surprising, I looked myself up and this tweet came up on page two of the Google search results and it was me baking shortbread and for some reason it ranked quite highly so can be quite surprising.

Stanislaw: Yeah, I once looked myself up on the internet and I went on Google and Google images

Jess: Ooh, okay.

Stanislaw: And I found a picture of myself on a holiday and it was when I was eight.

Jess: So, you hadn’t posted that then, someone else had?

Stanislaw: No, I think it was on my dad’s Facebook.

Christopher: So, moving on - obviously social media is coming up more and more over the years and it’s still growing, there’s more and more users joining every day. So how easy would you say it is to be yourself in the new social media world?

Jess: So, I think for adults we’ve kind of had to make a conscious decision about how we represent ourselves online, and for a lot of us it falls into either we’ve got a professional presence online to promote that or it’s just personal. And obviously Facebook is the de facto place for adults to kind of share themselves. And in my experience, I think we’ve learned how to do these things well and how not to do them not so well over time, and we’ve got a better understanding now about data and what’s collected about you. But, of course, what I don’t have and what you do is that experience of growing up online, right? So, what it must be like to be a child and a young person and how you represent yourselves online? So, I guess the question is back to you, can you be yourselves online?

Kalina: Not necessarily - I was going to ask you, have you heard about personal branding?

Jess: Uh huh.

Kalina: So, for people who have grown up on the internet it’s all about their personal brand or curated Instagram feeds, what they post online, and who they associate with, so everything is kind of targeted toward a market. So, do you have any thoughts on how young people are actually taking advantage of the system? Some more vulnerable ones are actually thinking it’s real life when in reality it’s something we curate, like furnishing your flat, it’s the same way as furnishing your Instagram feed to present this unrealistic expectation.

Jess: Yeah absolutely, I mean I think it's only natural, particularly when you’re young and quite self-conscious. You're developing the relationships around you and how you want to represent yourself to the world around you and part of that is exploring your identity and who you are online – and we always want to be the best that we can be right? Who wants a horrible photograph of them online? Nobody does! But I do think there is specific pressure on young people – I think we struggle to be ourselves online, sometimes if you are yourself online that attracts negative comments, hate speech, and I think people try as much as they can to be who they are online but they find it difficult to do that. Does that resonate with you, do you feel like that, do you need to be a different person online than who you are like face to face?

Christopher: For me I’d say I'm a different person in each situation like there’s a slightly different side to me where if I’m in a corporate setting I can be quite business like and straight down, if I’m with my friends I mess around like have a bit of fun, when I’m online it’s like a mix of both. I mean I have my serious side and I have my jokey side so I really think it depends on which situation you're in whether or not if you can be yourself.

Kalina: So back to another topic which is: what are young people’s rights online? Because I know that if I request from Instagram something, I want taken down I have the right to do that, but is there something you would want to point out to our listeners?

Jess: Yeah, I would, I mean you're absolutely right - we can talk as much positive talk as we can about our online lives, but we have all at one time come across something online that we’re not happy about. So clearly if there's something about you online that you're’ not happy with the first step is to see if – I mean maybe you posted it, you can remove it – maybe somebody else posted it and you can ask them, and you can ask them very nicely and they might just take it down. So, the first step would be something along those lines. The main thing we think of, of course, is going to the provider. So, if it’s Instagram, going to them and saying; *“You’ve got this picture of me or whatever, this information, and I'm not happy about it and I want to get it taken down”* and they will have their reporting process to do that. Essentially if we want to get something removed from the internet, we’ve got two reasons to do that: so first of all, if something is illegal. So, it’s an inappropriate image of an under 18-year-old, then that’s an illegal image, you should be able to get it taken down. Certainly, on major platforms on the open web it’s illegal, so it should be straight forward. So, the illegal route is the obvious one. The other route is that it breaches the terms and conditions. So, you want to demonstrate to Instagram that for whatever reason this image or this information breaches their terms and conditions, and if you explain that to them then they should take it down. That’s where it becomes problematic because sometimes, they don’t. The other thing I would point out is a service we run at the UK Safer Internet Centre called Report Harmful Content. So you go to the website [reportharmfulcontent.com](https://reportharmfulcontent.com/) and we work with most of the major providers, we work directly with Facebook, Google, Instagram, Microsoft, etc and you say; *“I’ve been to Instagram and I can’t get this stuff removed”*

For about half of the cases we’ll explain to you why you can’t get it removed so it doesn’t, it’s not illegal, it doesn’t breach the terms and conditions, we’re very sorry. But for the other half we will actually take the case on for you and we’re expedite it, it’s straightforward because we’re a trusted flagger, so most, I can’t remember, but about 95% of those we will actually get removed. So that’s kind of the main bits that you can go through. There's, a few tips of things you can do to get information removed.

Chris: Obviously now you’ve got covered by the General Data Protection Regulation that was brought in by the EU and is now part of the UK law as well, so you can basically ask for anything that relates to you to be permanently deleted and that’s your right as the data subject.

Jess: Mhmm…

Chris: For instance you can go to a corporation say, Domino’s, you ordered from them and you get marketing emails - you can just contact them and be like “I want all of my information deleted from your systems” and they have to do it.

Jess: I mean there are some caveats to that just in terms of holding data – organisations can have a certain reason to hold data. So, for example if it’s a local authority they might have to have information about you in order to provide a service to you so they can rely on that. But certainly, things like receiving marketing information from an organisation you don’t absolutely want, yeah.

Jess: Okay so one of the things I wanted to ask you guys about was: what do adults, and by that I mean both adults at school or at college, but also parents – what do they need to know, what do they need to do differently what is not working and what needs to change?

Christopher: That not every person we speak to online is not a mad chainsaw man from America. For instance my brother in law met a friend online on Xbox Live and we were in the state he lived in and we met up, and folk were quite nervous about it and he was like “No it’s fine I know him” and it was fine, like he was just a great guy. And just know that though we might be talking to people that we’ve never met or are on the other side of the planet, like, we can still build a relationship. We can share things in common, for instance it could be that we both have the same favourite game and play with each other. So yeah just don’t worry about absolutely everyone, most people are pretty good. Like it’s only a very small selection that could be dangerous. And the young people these days are usually able to flag up that they are.

Jess: Do you think that young people are savvier than adults give them credit for? Do you know what I mean? That you’re able to manage this...

Everyone: Yeah.

Jess: Yeah, do you think?

Kalina: Definitely young people are a lot more savvy - they can spot someone fake from miles away. They can understand the lingo and know that “Oh, you're not who you’re supposed to be” So in that sense I think that parents and educators need to understand that young people know what they’re doing but sometimes… what can we do to help them when they get lost, say for example they send an inappropriate picture and then they regret it.

Jess: See if there’s an issue like that online, say if something went wrong, do you think… do young people go speak to a trusted adult?

[laughter]

Christopher: Uh, no.

Jess: Where do they go?

Stanislaw: I think most people just don’t report it. Most people just ignore it. I mean, it’s probably not a problem if, like if there’s a threat, if someone wants to talk to you that you don’t know or some sort of shady email you’re getting and you just ignore it, there’s no problem with that but reporting it will stop it from happening to other people.

Jess: Mhmm, yeah...

Stanislaw: But it's not gonna cause too many problems if you ignore it.

Jess: Yeah, but still that’s reporting it like reporting it online, or reporting it to the police if needed. I was wondering if we do, as young people, need to talk to parents or responsible adults that are around us. Is that something that people do or is that gonna get a load of grief?

Christopher: I’d say the block button works wonders.

[laughter]

Christopher: If I was maybe a wee bit suspicious about something, I’d probably be more likely to go to my friends who’ve also grown up on the internet. We’ve seen like all the ‘internet bad don’t do it’ [messaging] but we’ve also seen the good of the internet and we know that and we’ll be like ‘What do you guys think of this, I’m not too sure”, and perhaps like a pre-emptive block or talk to them and they’re like “No, that’s not good just block and report” to like that website. For instance, if you get like a shady Facebook message just block them and report it to Facebook. Problem solved on your end.

Jess: Does that mean then that actually all the tuition should be how to use the tools?

Christopher: Yeah.

Jess: So. we shouldn’t be focusing on ‘Talk to somebody that you trust’ is that what you’re thinking? Or does it depend on the age?

Christopher: I think it depends on the age, but definitely teach them to use the tools at their disposal as well. Talking to a trusted adult can't fix everything, like for instance if your parents aren’t particularly techy and you go talk to them, they’d probably be like; *“Well I dunno what to do?”*

[laughter]

Jess: You’ve probably just described like 90% of parents across Scotland!

Chris: They’d probably be like, I'm not too sure what to do but if we teach them how to use the tools and talk to a trusted adult, a lot would probably get solved a lot quicker.

Kalina: The tools are there to help us out after all and even though they might not be able to tell us what to do, they can offer us moral support and sometimes that’s enough to spur you into action you know? This bad thing happened but I have my support network, I have my people behind me and whatever comes next I’ll be able to face it. If it means I'll have to contact the developer of if it means I have to go to court in the worst-case scenario, I know I have people, they won’t be doing anything besides giving me moral support. So, in that sense I think we have to kind of bridge that gap?

Jess: Yeah you need it all.

Kalina: I recently had a very scary experience, well my friend had a scary experience, I kind of managed to dodge a bullet, cause I got this really weird message from her asking if I could send her, if I could verify a code for her or something and I kind of thought that was really strange cause she wouldn’t typically write to me out of the blue and the message kind of wasn’t grammatically correct as well. So luckily, I was on my laptop and I saw she was online on Facebook so I just messaged her, and she said “Oh please don't reply it’s a scam, someone got hold of my phone, I can’t retrieve my contacts... I called the police and they can’t really help me”. Luckily for her the story ends positively - she manages after a day to get hold of her account and everything is fine now. But during that one day they had access to all her contacts, they had access to me, and some people that didn’t know better might have responded and then it becomes like a chain reaction and they get hold of their phone and their contacts. And in that sense, it was a really scary experience. It makes you think “Oh what can I do to protect myself, what can I do to protect my phone, how do I spot this? Do you have any tips for our listeners?

Jess: First of all, I’d say you did the right thing by not responding right away and looking for a different way to get in touch with your friend to work out what this was and having those wits about you. Clearly when it comes to the cyber security side it is about having your wits about you. But there is no doubt, most people are gonna get hacked at some point, it’s just the way the world is going. In terms of security you know, we know the importance of passwords, setting really good long passwords, maybe using a password safe to manage all your passwords, not using the same password for different things and using multi factor authentication. So, we know all of those aspects are in place in terms of trying to prevent somebody from trying to get into your account, but I think really the whole of the cyber side is moving very fast. I would suggest it's really an area we really need to be alive to and really to me most of the problems we have online are not about making sure I’ve got a setting somewhere, it’s about using my brain and recognising what somebody's motivations might be and really kind of having the wits about us.   There’s no doubt it will happen so think about the data that you’ve got there, where you store your stuff, who is in your contacts…. prune your contacts you know, delete your old social media profiles. If you are not using a service, go back delete your profile on it and then uninstall - so there’s lots of things we can do to try to reduce the amount of data that is out there about us in the first place.

Stanislaw: So, Jess where do you think is a good place to go for more information if you’re struggling with something on the internet?

Jess: Okay, well, so, one of the places you can go to is the Safer Internet Day website which is [www.saferinternet.org.uk](http://www.saferinternet.org.uk). Safer Internet Day happens every year in February and it’s celebrated in 140+ countries all over the world so it’s a massive event, but as part of it we produce lots of educational materials and these are for people that work with young people but also for parents as well. There are videos on there as well that people might be interested in and lots of tips about managing yourself online. This year we are very much focussed on being you online, being authentic online, and we have the hashtag #freetobe - so free to be me, am I free to be me online? So, lots of resources on there so please do take a look at Safer Internet Day.

Kalina: Thank you so much for coming along Jess and for all the amazing tips, and for the great job you do with adults and young people and hopefully we get to hear back from you.

Jess: Thank you very much thank you for having me!

[digital music]

Narrator: Thanks for listening. For more information or for help and support on any of the topics covered in today's podcast please visit [young.scot/CyberScotlandWeek](https://young.scot/CyberScotlandWeek)