Welcome to the UP TechTalk Podcast. Coming to you from the new Academic Multimedia Studio on the University of Portland campus. Produced by: Academic Technology Services. With your hosts, Maria Erb and Sam Williams.

Sam: Thank you for joining us for our UP TechTalk. This is episode 2, and we have with us today Michelle Sunderland who is the Director of Technical Services for the University of Portland. Thank you Michelle for joining us today.

Michelle: Thank you for having me Sam.

Maria: Michelle we're really glad to have you today, especially since it's cyber security month, and we certainly like to celebrate whenever we can. But, you know we hear so much about data breaches and I think everybody is a little worried about their credit cards and especially with what's happened with Target and Home Depot. But in a university setting, is there any thing specific that we really should be concerned about?

Michelle: Some of the areas of threat that we're becoming aware of and are specific to higher ed, really focus on phishing attempts and, so one of our primary efforts with cyber security month, is going to be educating users on how to recognize phishing. Phishing is as simple as an email that comes through that is trying to fool you, and trying to get your personal information. And in higher ed, we're seeing a trend, an increased trend, in the techniques being used and, so it's something that we want to get the awareness out there for.

Maria: So, what kind of data is typically stolen in phishing?

Michelle: Yeah, so what can happen is they might pretend that they are the Help Desk looking for credentials for a user. And they might say, you need to reset your password, click this link. And, because the email looks so professional, they might match our logo, looks like it's coming from U of P, it's pretty easy to think that it's real. And a user can click the link, and provide their credentials. Then that might provide the attacker or attempted phishing person the ability to log-in and perhaps spam an outside community, and therefore impact our email services for example.

Maria: Are universities targeted for any particular reason? I mean, it's really usually a tech-savvy population here. Is there some reason we're at risk?

Michelle: Sure. So, probably the most sensitive, important data that we hold on our campus is student information, and it does include personally identifiable information like social security numbers, date of birth. And that can definitely lure malicious attackers. You know they're after that sensitive data. If they were to have a successful attempt, and breach that data, they could certainly, you know, provide that to others, sell it on the black market, and of course our biggest job at University of Portland is protecting that private sensitive data.

Sam: I was going say, some of those emails that come in, they do look pretty official, when they come into people's inboxes, especially for phishing attempts. Your department will never send out those types of emails typically, correct?

Michelle: Absolutely. We would never send an email asking you for your credentials, or putting any sort of timeline or pressure on you. And we would not include a link to click, we would give direction, what website to go to view. We might contact you by different means.

Sam: And if anybody has any questions, like you know, is this a phishing attempt or isn't a phishing attempt, they can always contact your office, is that correct?

Michelle: Yeah. So the best advice is, if it looks suspicious, if you're unsure at all, call the Help Desk. They're very good at recognizing phishing. They can then notify our email service administrators here. We can try to filter that phishing email out of our system and prevent others from being fooled.

Maria: How would a student know if their data has been compromised?

Michelle: Well, they may try to log-in and notice that they're logged out of their account, for example. And, we have had in recent history, a few successful attempts. They reached out to the Help Desk, they let them know. We very quickly put a stop to it by locking their account. We research, maybe, where the access came from. And we work with local agencies actually. We have a, RENIS Isaac that we're a member of which is the The Research and Education National Information Sharing Center, And we're able to work through them to try to track down, you know, where did this attempt come from, we pass it along. That might help other universities know, and they can certainly help us shut that down.

Sam: So I mean, it definitely sounds like you have, you know, a lot of thought being put into cyber security. And are there some simple tips for protecting user safety, identity, you know their online information that you could give to our audience?

Michelle: Yeah. What's great about this is that some of these tips are very simple and do not require a big investment of time at all. Some important advice is trying to limit what you do expose in terms of your personal information, for example on social media. The more that you're putting out there, the more at risk you are of somebody using that somehow to either fool you or somebody else. Some basic tips around mobile device security, is to certainly use a passcode on your mobile phone. A lot of people don't do it. And just by adding that extra layer, if your phone were to fall into the wrong hands, you know you have some means of keeping somebody out. We also encourage people with their laptops and their desktops to just keep their operating system up to date. Sounds very basic and simple, but some people fall behind, and most patches are for security reasons. So, when there's new patches released, be sure to apply those. And this is similar for browsers. Keep your

browsers up to date. Again, usually the updates to browsers are security related. And of course use anti-virus software.

Sam: And for the anti-virus, we do provide our population here at the university, with anti-virus software, is that correct?

Michelle: That's correct. So students and even faculty with personal mobile devices have access to our download center, and you can download the Symantec Anti-Virus that we provide to all campus community members. And, the additional tip there, in terms of passwords, would be the longer, the better. You know, there's a phrase called "keep it long and strong".

Maria: Often times though, and I know I'm guilty of this too, we just don't go for those longer passwords, they're just too hard to remember and if you right them down, somebody can read them. Is there something that you recommend that people to be doing?

Michelle: So there are some new best practices. We always try to, be aware of what those are and pass those on to people. Regarding length, the new standard, and this is going to sound overwhelming, is to have a 14-character password. For many people, they might not be able to come up with something that long. Myself personally, I try to use a standard, that when I have to go change my password, I have a word or phrase in front that I typically can generate and maybe swap out instead of letters some numbers that line up with those, that is something that will stick with my memory. It might be a meaningful piece of information in terms of family, although nothing sensitive. In addition, you could do multiple words that only you know, that aren't a sentence or a common phrase, and again swap out some of the letters for characters, and also generate, you know capital letters and special characters in there as you go to keep it more complex. This can certainly help with compromise prevention, but again that can be overwhelming, so come up with maybe a formula that works for you, that you can use across different apps what not. And what, another tip, that I really want to emphasize, because we're seeing an increased occurrence of incidents where something in social media for example, like Facebook, reports a breach where the usernames and password lists are available. If people use the same username and password across different social media apps or different web apps, then that breach can then run over into those other areas where they're using that same username and password. So I really encourage people, for example not to use their work log-in and password and carry that over into their social media log-in and password, just to keep those more secure.

Maria: Anything else that you're focusing on in particular right now?

Michelle: Well, we are excited about cyber security awareness month in general. Towards the end of October, we're going to be setting up some booths at some of the common areas on campus, hosting some surveys, questionnaires, quizzes, such that you can enter and potentially win some technology by proving your cyber tech-

savvyness. So we're looking forward to that. Otherwise, that's all I can think of for now, actually.

Sam: Well any time that you can have an event where somebody either gets free food or wins something, I think we should get some decent involvement. And again, if somebody has questions, what's the best way to contact technical services?

Michelle: Right. If you have any questions about security, any questions about email phishing, we encourage you to stop by the Help Desk located in Franz. If that's convenient for you, you can call, their extension is X7000. You can always email at help@up.edu. And you can also visit the new virtual service center. So that's available online, you can submit a question or issue or concern from that website.

Maria: I think we've covered a lot of ground.

Michelle: Yeah, just encourage people to take those simple steps to secure their devices and their data.

Sam: Very nice. Well thank you so much…

Maria: Thanks Michelle.

Michelle: Thank you for having me.

Sam: for being our guest on here. I'm sure we'll get you on here again at some point, because we do definitely want to remind people, over time, to protect themselves. I know, I've myself have been part of the Adobe attack and had a years worth of credit protection because of it. And so I think we've all been reminded of, so I really do thank you for your efforts at the University of Portland and to protecting our information.

Michelle: Thank you Sam. Thank you Maria.

Maria: Thanks Michelle.

Sam: Thank you for listening, and be sure to tune in next week for another episode of UP TechTalk.