Ep. 064: Cybersecurity

Podcast: https://ProDev.illinoisstate.edu/podcast/2020/ep064.shtml

We speak with Dan Taube, Illinois State University's Chief Information Security Officer, about how to keep ourselves and our students safe as we teach and learn online. As college instructors, we don't usually think about our teaching in terms of the exchange or storage of data. But it's an important consideration not just in terms of our personal online habits, but also in terms of ensuring students' privacy. Dan highlight's the best ways to prevent bad actors from getting a hold of the information they so desperately want. We discuss how to be mindful when interacting with email and websites, and we also explore the process the University when faculty or departments seek to incorporate new online tools into the curriculum. You'll also hear about the good cybersecurity habits instructors can model for their students.

Transcript

JIM: Hi there, I'm Jim and

DAN: I'm Dan.

JIM: Let's Talk Teaching.

[music playing]

JIM: Welcome to let's talk teaching a podcast from the Center for Teaching, Learning, and Technology here at Illinois State University. I'm Jim Gee and joining me today is Dan Taube. He is chief information security officer here at Illinois State, and we're here to talk about cyber security. Dan welcome.

DAN: Thank you.

JIM: So, what is cyber security? Maybe we should probably define our terms a little bit.

DAN: Certainly. So, cyber security primarily focuses on the protections and processes and people that get involved with using or collecting data of some sort. So, information and data is what it's about, but in our systems, in our computers, that's, that's cyber security's purpose.

JIM: Well, and of course, in the middle of, uh, we're recording this in October which is cyber security month, and we are in the middle of a of a global pandemic to boot. So, we're all working remotely. So, obviously, even though we were so engaged with all of this technology before, it seems like now more than ever, so, what are somethings that that instructors on campus should keep in mind when they're dealing with all of this?

DAN: The, the biggest, right now, there's, there's two that we would recommend to instructors. In particular, one is to consider that as they're working from home, they don't have some of the protections we heavily invest in on campus. And so, that's where all our advice on best practices, they should be really practiced at home more than even at the, the institution. There's a lot we do to protect on campus, and if

you're off campus you're more at risk. The second is be highly, highly critical of the messages you receive through email, by phone, by text. Mainly because what we notice is a very big increase in phishing, and social engineering attacks this year. They're utilizing the, the cultural shift and the environment we're in to be very effective in their attack.

JIM: So, when you're talking about phishing, that's a term that we hear sometimes but we may not understand exactly what it means. It has something to do with email. So, what is a phishing attack?

DAN: So, phishing is where, uh, I'll call them a threat actor, someone that, they may be doing for financial gain, maybe they're just doing it for fun. They reach out to you, they contact you in some, some method, and they're trying to get you to give up information about yourself. So, they're fishing, in effect. Um, and they're, that can be your username and password, or it might just be information about you that they'll use in a different way.

JIM: You know, we get I get so many email messages, and I know all of our instructors do, and all of us on campus do really. And it may be inevitable that we click on something, that we just out of muscle memory, you know what I mean.

DAN: Yep.

JIM: So, what happens if I do that. What should I do? So, if you accidentally click, you shouldn't feel bad because many, many people do. In the last year, just people that clicked it, and gave up their username and password, there's about a thousand. So, in 12 months a thousand people did just that, uh, so they're not alone by any means.

JIM: And, and that's on the campus of what 25,000-30,000 people. Okay. Yes, um, and in, uh, that's pretty consistent with most organizations. It's, it's about that kind of ratio that get compromised. Simple fact of, of digital life we have, um, the, the… If you should detect, and, and notice that, oh, yes, this looked like it was from someone I knew, or was a link to office 365 and it now looks suspicious to me. Immediately contacting us, and there's two ways to do that. If you need to call, you can contact the technology support center and, and their information is available at IT help.illinoisstate.edu. The other, is you can email the information security office at abuse@ilstu.edu. That email is constantly monitored. You can forward the email you got originally. Ask about the things you saw, get kind of confirmation. If, if you're not sure, and we'll handle the, the cases that way.

JIM: Well, I appreciate the fact that you explain it so calmly. Among other things, because this, this can be kind of scary a little bit, and I know I've worked with some faculty members and you've had contact with them too, who have had some issues using Zoom. We're all using this whole new thing for many of us this year. I think it's helpful for people to keep in mind. I think that's a great message that you have. That it does happen once in a while and that there are steps that we can take to kind, of kind of work through it.

DAN: Yep, it's, um, it's one that we need to all raise our own awareness and understanding of just how prevalent this is, because they're, they're exploiting our trust in either a name, or just the, the simple fact of the technology, we think that it's been protected by someone else. Um, they're using it and so I don't, I don't blame anyone that gets, falls for it. It happens every day.

JIM: As far as being an instructor goes, there are a lot of solicitations that come that are legitimate solicitations to, to try out or to use new teaching tools or new software platforms, and we have a list of them on our website at CTLT.illinoisstate.edu. of ones that we know are out there. That aren't officially supported by the university, but, but that we know they're being used. Do you have any words of advice for instructors who may be looking at incorporating some third-party, uh, platform or service or something in their teaching, and can you talk a little bit about the rigorous process that you folks, your office goes through, um, when we adopt something, officially, on campus.

DAN: Oh certainly, um, so the biggest consideration I'd recommend after, say, what they need to in terms of their instruction and the value of such a product or software, is the type of data that's going to be collected and used with that software. And respect that students have a desire for their privacy to be respected. And so, one of, one of the, the greater risks to the institution, less on an individual level, more of the, the university needs a concern itself with is how data, in a more-larger set, is transferred to third parties and used by third parties. There's plenty of cases in, in just the consumer world where the social media sites, uh, we're all familiar with, they, they might get compromised, or they share their data with another third party, and they get compromised. we don't want to play a part in that. So, you have to consider… Is the company someone I know already? Is, is it one of these major publishing companies that I know that they probably invest in security, and invest in protecting data, or is it a name I've never seen before? I look up their site, it doesn't really have contact information, or where they're from that's when you want to be careful and consider their, their promises. Not only for security, but maybe, they don't deliver what they're telling you they'll deliver. Beyond that, even if you're not looking to go the full, full path, you can reach out to us. And we'll provide guidance and advice, and we'll do that investigation. So, maybe you don't feel comfortable, you want that consultation, you can reach out to us and we'll do it. So, it doesn't require an actual purchase to be made for us to go through it. So, it's, it's something that we're facilitators or custodians over data. We need to consider that when we're looking at these, these other products. If it's something that's local to the computer, data's not being used, there's less need for that type of consideration. But, let's say, let's say it's one of these tools that, either, maybe, centrally we determined we want to buy it for campus and make it available to everyone because there's enough demand. Or, even a department says we want to buy it, or college says we want to buy it for everyone in our unit, that's where purchasing is getting involved, but we also get involved to assess what data is getting used. Uh, what the privacy policies might be, who, you know, what are the terms of data ownership? When we give data over do, we still own it, or now do they own it and we're doing contract reviews. We're doing conversations with the companies themselves on their, their practices and maybe certifications of compliance. We apply a lot of consideration because of the risks if we didn't do that. So, we reference that process as the data usage form or DUF. In short, it gets a lot of, a lot of negative press

because it can take some time. The sooner an instructor gets into that process the better. So that's where going back to your thinking about it, reaching out to us. Engage us. Sure.

JIM: Well I knew it was a pretty rigorous and extensive process. The other thing I'll add to that too is that, you know, if instructors find a particular bit of software out there, for example, that they think meets a need that they have in their teaching, they can also contact us over here at CTLT because there may very well be something that's already being used on campus that does something, if not identically, then similarly.

DAN: Yes.

JIM: And has already gone through this extensive process that you're talking about.

DAN: Exactly, because we so, we do not, we'll, we'll consider and maybe make a light reference, but we do not advise on the actual use of the tool and its value and whether or not there's other options.

JIM: Right.

DAN: So that's where they should certainly, engage CTLT and their own college resources if they have them.

JIM: You know, and again, we're talking about this in the context of protecting our students as well. So, that's one way that faculty members, when they start initiating the process of, uh, of looking for new technology to use, or new software to use, they can do that. But what would you like from, from your perspective? What would you like instructors to be telling students about cyber security? And what good behaviors would you like instructors to encourage in their students?

DAN: Number one, it goes back to the phishing attacks we see and what I would advise every user to do and if instructors can echo this with the students the better. Check the links in the emails. Check the sender address as well. Those two things usually evidence when it's not legitimate and it's a risk. In the links, you're usually looking, does it go to an ISU website, does it go to you know Microsoft's One drive type locations, um, is it going to google docs, maybe? When you see really suspicious websites, and it's saying, you know, login or secure your account you can kind of figure that out yourself and not click that link. And you can do that both just by hovering on a regular desktop computer the link. It will preview the, the URL, or on mobile devices you can touch and hold the link and it will give you a preview. Because you don't, there are a few cases where, clicking the link alone would compromise you. It will install malware, and, and be at risk so check that first. The other is, and this has spiked, um, in the last two months. There's impersonation of others going on, where the email will have a display name that matches our own names and this could be someone official, it could be another student, but if you look at the email address it'll usually be their name at gmail.com, or even their ULID gmail.com. Well you can know, at least, assess in that moment this didn't come from their ISU. So, maybe I should check with them, or reach out to them by phone or another contact method. That, that approach, that attack is getting used where it's a very simple message so it's hard for us to detect it because it

looks legitimate, and it starts off usually hey can I get your cell phone number so I can reach out to you, text, call, something else. In the long term of that scheme, if it plays out, is they're trying to get you buy gift cards or do apple pay to try and transfer money and do something along those lines. So, if you think every email that you kind of get, have a little suspicion, hover the link check the sender. That can protect most cases of what we're seeing.

JIM: So, one final question for you, Cybersecurity month very important, it's important to raise awareness, I think. If there's one message to get out of our conversation today, it's that these routine things that we do we need to be mindful as we're doing them. But beyond talking about kind of the season that we're in this fall semester for example or even over the summer as we were kind of transitioning to our new our new modalities of teaching or whatever you want to call them. What's one thing that you're happy about? What's one thing do you think we've done well on campus in terms of cyber security, information, technology, or just ISU in general?

DAN: I think some of the biggest two takeaways I've seen as a positive, because cyber security is always a challenge, it's, it's never convenient for users, it's never just simple and dry, what you have to put in place. So, so, it's always a challenge when you enter into it, and this year, despite all the impacts we had, we still introduced new controls, new protections, whether it was with college IT units, faculty, and instructors themselves, or within other IT groups. Centrally, for the administrative side, we did things that normally would take many years to implement and accomplish. So, what's positive about that, is people are communicating they're sharing and they're, they're participating. It's not like someone's just refusing and objecting to it. Um, that's something I had not seen before, and to have, in such a challenging year, is remarkable. The other thing is, we are now actually, treating cyber security as an institutional concern. Previously, it was much more about, do we get a state audit, do we get a new regulation that requires something, and we just did it by a check box approach. Now people that aren't in any capacity related cyber security are asking the right questions. Asking, you know, do I need to be concerned about this? do I need to consider that? That's new this year that I think it kind of shocked me and amazed me and, and some of it might come from the successful attacks like Zoom bombings and the phishing attacks. But it's something that's been positive in my opinion.

JIM: Dan thank you so much.

DAN: Certainly.

JIM: You can find out more about our podcast and about this very important topic of cybersecurity, go to our website CTLT.illinoisstate.edu, click on the podcast link, and you will be taken to this week's show page. We'll have links to some of the resources Dan has online, and some other material as well. For Dan Taube, for all my colleagues hereat the Center for Teaching, Learning, and Technology, until we talk again, happy teaching!