Jason Altmire (00:04):

Welcome to another edition of Career Education Report. I'm Jason Altmire. Today we are going to talk about a topic that is of great interest across the country in every business, every family thinks about it, every individual who carries a phone thinks about it, but it is really important in higher education. And I don't think we spend enough time thinking about cybersecurity. From the campus perspective, from the faculty, from the student perspective, it just touches every aspect of our life and the implications are enormous. And today we have an expert in cybersecurity, Dr. Ted Reynolds. He is the Director of the Terrorism Studies Program in the Office of Global Perspectives and International Initiatives at the University of Central Florida. And I can promise you, you're going to be interested in this episode, but you are also going to be scared after you hear what he has to say, because I've heard him talk about this and it just opens up so much uncertainty in your mind about how well protected are you as an individual, as a business, as a campus, as a student.

(01:14):

So Dr. Reynolds, thank you very much for being with us today.

Dr. Ted Reynolds (01:19):

Jason, thank you so much for inviting me. It's a pleasure to be here.

Jason Altmire (01:22):

I think a good place to start is why is cybersecurity an important issue? Why should people in higher education give it a second thought?

Dr. Ted Reynolds (01:32):

Well, it's important because it's all around us. Cyber is ubiquitous in our lives. You think about everything that we do, our cell phones, even watching television, our cable, everything we have around us is basically data. If you drive on the highway and you have an E-PASS on your car, that's data, it's recording that. All of that goes up into some database somewhere that can be accessed using cyber. So when we look at what is important, access to that information or denying access to that information, which is really our own personal concern, is very important to prevent people from using that data to either coerce us, to steal our money or to do things, I mean, we have foreign actors that use cyber to steal national security secrets and trade secrets and things like this. So cyber is all around us.

Jason Altmire (02:29):

We have cybersecurity programs in our sector that we represent at Career Education Colleges and Universities. It's a very high demand profession. It's also something that from the perspective of a student, it represents a very promising career path as well, right?

Dr. Ted Reynolds (02:47):

It absolutely does. And people don't realize that cyber is not just those individuals that do the coding, write the programs. Understanding the cyber world and the impact of cyber on multiple industries is important. If you work in a hospital and you understand the principles of cyber and why protecting that information is important, you're a valuable employee. So I tell my students, I don't care what major you're in, understanding the role of cyber in your enterprise is important. If you have a small business, protecting your interests, protecting your banking information, your client information is important. If you work in medicine with so much personal identifying information and medical information, protecting that information is important.

(03:38):

And so even in the cyber realm, when you have cybersecurity companies, having people that can communicate, understand, but not necessarily code, but people that can communicate between the coders and the boardroom. Because trust me, most people that are in the boardroom don't really understand cyber. So having that middle person to be able to communicate back and forth to help the board understand why it's important to invest in cybersecurity, to protect not just their interests, but the interest of their clients is essential.

Jason Altmire (04:12):

When you have your first day of class for your students, and you're talking about this issue, now, presumably some students probably major in the subject and know more about it than others, but at a big public university like UCF, I'd imagine a lot of them are just taking it for general interest or to fulfill some other requirement, and they're unaware of even the most basic aspects of their own cyber protection. And you've talked a little bit about in the past, I've heard you in other forums, just the simple act of taking a picture on your phone and how that can show, with precision, exactly where you are when you took that picture. You post it to social media, someone who's following you can see exactly where you are at that moment. How do you explain to students, to young people just starting out, why it is so important to pay attention to things like that?

Dr. Ted Reynolds (05:07):

I actually hold up my phone and say, "This device, this is not a phone. This is a tracking device that allows you to make phone calls." And so I do actually run them through the photograph lesson of, pick any photograph on your phone that you took and then swipe up. And when you do that, what you find is the metadata, GPS coordinates, Google Earth map of where you took that picture. So I say, if you're wondering why people are automatically showing up at these places where you're posting your picture on social media, it's because you're telling them where you are. And it's dangerous and young people today don't really understand how powerful their phones are. Your phone has more computing power than NASA had when they put a person on the moon, and that just blows them away. And so trying to get them to understand how data impacts their lives and how much data they're putting out there on a daily basis is really important. But then understanding how to practice what I call good cyber hygiene to protect themselves and their information from being stolen.

Jason Altmire (06:19):

And there's different levels of cybersecurity, and you deal with terrorism, and we'll hopefully at the end get into some of your research relating to social media and things like that. Start at the broadest level in higher education and kind of narrow it down to student implications for their personal devices and computers. But for researchers and academics, for faculty, what are some of the concerns that they should have related to their on-campus activities and cybersecurity?

Dr. Ted Reynolds (06:49):

Well, understanding professors, and really administrators as well have access to student information that is privileged. We have this thing called FERPA, I don't really remember what the acronym means, but it's basically, there's all this information that you are not allowed to communicate regarding the students. But if you're not careful and you click on a link that then allows a hacker to get into your system, they can actually download student information and it's privileged there, I'm talking names, addresses, social security numbers, class information. So it's really incumbent upon educators to understand the dos and don'ts of cyber. Like I say, you get an email, and everybody's had the phishing emails and scam emails, but you get a phishing email and somebody downloads a keystroke logger to your computer because you click that link and all of a sudden they're seeing everything that you type onto your computer, every program you access, every username and password.

Jason Altmire (07:50):

And sometimes that is for just malicious intent, ranging from financial implications, espionage, sometimes it's for theft of information. What are the more dangerous implications of that type of information, student data falling into the wrong hands?

Dr. Ted Reynolds (08:09):

Well, if you have a hacker that's working with, let's say a human trafficker, they can actually use that information to find out where people live, what their habits are. Most large universities have sensitive research that's going on. I know at the University of Central Florida, we do work for various government entities, and a lot of that research is, maybe not classified, but certainly controlled. So if hackers get in, then they have access to that information, that could either be sold on the market or it could be an adversarial government trying to steal that information. And that happens across the country. The FBI's talked about cases where large institutions that were doing government work were hacked, and those secrets were sent to one of our adversaries overseas. So it's really important that businesses, schools understand how to protect their information.

Jason Altmire (09:09):

It seems to be in the news a lot more along those lines also of the opportunity for the criminal, for the hacker, to ask for money in return, to lock down computer screens or data or access to a server or a system or with a threat of doing something with that, how prevalent is that really, both in academia and in corporate America, of that type of sort of a hostage situation?

Dr. Ted Reynolds (09:39):

It's prevalent and growing. It started out as individuals, persons, it's called ransomware. So what happens is, and you click on a link, it's corrupted, your computer gets shut down, and you see a message that we've got your computer, and if you send us $200, $300 with a Green Dot card, that's what they used to use, we'll open your computer back up. And then you were at their mercy, if you didn't know how to get rid of the ransomware, you could send them the money and they might or might not unlock your computer. That has evolved to criminal enterprises around the world demanding millions of dollars, in some cases, multi-million dollar ransoms to schools, to businesses, to municipalities. A few years ago, there were five cities in Florida that were hit with ransomware, some of them to the tune of $10, $15 million.

(10:37):

The commercial side of it really started, I don't know if it was the first case, the first one that I became aware of was a hospital in Hollywood, California that got hit, and they wanted Bitcoin to be paid before they would unlock the hospital's computer network. Now, for those of you that most of us have been in the hospital, you understand nothing happens in a hospital that doesn't go into the computer. So they were dead in the water. And so they wound up paying the ransom, which at the time was about $16,000 in Bitcoin, which turned out a few years later if they kept the Bitcoin, upwards of a quarter of a million dollars. But that's kind of how it started with the larger ransomware attacks. And they've just gotten bigger since.

(11:21):

Most companies don't want to talk about it, they don't want to advertise that, number one, they were vulnerable, and number two, they had to make these big payouts to get their data back. They're always at a risk of not getting their data back. And some ransomware attacks say, if you don't pay us by a certain time and date, we will start deleting your data. And if you'll allow me the time, what that speaks to then is the very, very important need for creating offline backups that allow you to be resilient in these situations so that you can say, no, thank you, and then you disconnect everything. You dump all of that, and then you start over again with the data that you just backed up the day before. And not online. And that's the whole thing. So your backups have to be what we call air-gapped so that they're not connected to the network and they can't be hacked.

Jason Altmire (12:14):

Yeah. We'll get into a little bit more about how people can protect themselves and institutions can protect themselves. How is it possible that the perpetrators, the cyber criminals that you're describing, are able to evade legal prosecution, that they don't get caught in doing this?

Dr. Ted Reynolds (12:34):

Some of them work in countries where we have no access to them. Years ago, there was a city in Romania that cyber crime was such a big part of their economy, it became known as Hackerville, and you can go online and Google it on YouTube, you'll see videos about Hackerville. We just recently negotiated extradition agreements with Romania. But then you have countries where a hackers operate, I will say with the tacit approval of the government, a lot of that is coming out of Russia, Iran, North Korea. They also are able to mask, for lack of a better term, mask their signal so they can spoof their location so people can't figure out where they are. And it does take the resources of the government to come in and try to solve these issues. The FBI has a cyber crimes division, but at the end of the day, there's not a big chance of the FBI going to Russia and arresting a hacker that just stole $10 million from the company. And they know that, so they can operate pretty much with impunity and hitting different targets.

Jason Altmire (13:45):

When you think about higher education, there's so many third party vendors that are out there to what we're talking about, processors, suppliers, various contractors, IT professionals, but every type of a vendor that an academic institution would be dealing with would seem to have these same threats, would be susceptible to the same type of issues. And it's often said that when you deal with third party vendors, that institutions of higher education cannot outsource accountability. So what are the implications of a hacker going after a vendor that's doing business with a campus or a school in some way, and what are the legal ramifications for the school?

Dr. Ted Reynolds (14:32):

It's a vector for schools or anyone really to be attacked. If you think back to the Iranian nuclear case of Stuxnet, the Iranian nuclear facility was not hacked directly. What happened was the Stuxnet virus was implanted into a subcontractor that was going to be going there to do maintenance and plug their laptop into the facility. That's how it got in. So I don't really have any understanding of the legal ramifications. That's not my area of expertise. But certainly you want to make sure your vendors are practicing good cyber hygiene and meet minimum cyber standards before you allow them to come in and work on your systems.

Jason Altmire (15:16):

Absolutely. And with regard to students, many schools provide computers for students. Sometimes they'll carry them into a coffee shop, they'll get on the wifi. Of course, they're always carrying their phones and personal devices, as we talked about. So from the student perspective, often dealing with young people, sometimes more naive perhaps than others. What are the threats that exist with regard to a campus environment for a young person with all of these devices that they're carrying around?

Dr. Ted Reynolds (15:51):

Well, especially when they go into coffee shops, places that offer free wifi. Now, campuses usually have their own wifi system. It has some sort of protection. But let's say you go to a coffee shop and you're on your laptop, you're open access, you're vulnerable to, if somebody has hacked into that system, anything you do on your computer, they can see. And so I ask my students, "How many of you pay your bills in Starbucks on your computer?" And hands go up. I said, "Well, you're potentially giving someone all of your banking information." And they asked me, they go, "Well, Dr. Reynolds, have you ever had your bank account hacked?" And I go, no, I don't do online banking at a coffee shop or on my phone. I don't even have an ATM card. So I don't use an ATM card to pay for things, so then nobody can get my bank account information that way. Just understanding what the threats are out there, and there are lots of them, makes you just a better consumer, and protecting your identity is essential in today's world.

Jason Altmire (16:58):

And what about we're in a Zoom environment with distance learning. You have that camera on your computer and there's concern about privacy issues related to that. Is that really a significant issue for people to worry about?

Dr. Ted Reynolds (17:13):

I've heard of cases where Zoom has been hacked. I've never really experienced that. I don't normally have my picture up when I'm online, either in Zoom or Teams or whatever, I have a picture that I put up there, but it's not live. But also, students especially need to understand that when they transmit pictures by social media, whatever, those things never go away. And companies today are asking for, and I've heard of cases where they're asking for username and passwords for social media accounts to make sure the individual that they're hiring doesn't have compromising information out there in the cyber world that could potentially be used against them to maybe divulge corporate secrets or embarrass them in some way. And particularly if you're going to work for the government in a classified environment, that's really important. So I tell them to please be careful with what you put up in that public space because it's public and it stays public. I don't care if you try to delete it. It's always there.

Jason Altmire (18:20):

That's a good transition into the current research that you're doing related to social media, and you're looking at computer mediated communications in relation to mass movements and terroristic threats and the ability of people with malicious intent to organize and use social media. And unfortunately in this day and age, campuses do have to worry about this type of thing. Can you talk a little bit about what your research has shown and what the concern might be in that regard?

Dr. Ted Reynolds (18:53):

Yeah. I look at how various groups, typically terrorist groups or violent extremist groups, use social media and other computer mediated communication to their advantage. And they have evolved. We can think of just in the last 20 years, Al-Qaeda used blogs and then ISIS came in. And they kind of up their game, social media, Twitter, you name it, they used it, encrypted communication apps, and what you find is through this social media analysis that there's a very, very small percentage of the people that might claim to be members or show as members, there's a very small percentage of people that are actually driving the dialogue. And understanding who those people are helps to work to counter that message. And understand that the problem is... Originally everybody thought, well, is social media problem's huge. Well, it's not as huge as we originally thought. There is a small cadre of influencers out there, and now we've come to be familiar with that term influencers.

(20:02):

But online influencers are driving the dialogue. And then what you have is a whole bunch of people that just either are not watching, but they did sign up. Or they're watching, but they're probably not ever going to do anything. Because it takes a huge leap from listening to actually being active in that type of environment to do something. And I've done quite a bit of work on that area to get people to understand that the problem, and I'll give you an example of the number of Muslims that left Europe to join ISIS was a fraction of a percent, given that there's 40 million Muslims across Europe. And it kind of helps find that whole situation where you go, okay, well, it's not everybody. It's a very, very small percentage, and that small percentage is the same across all groups. You've got a very, very small percentage of people that are willing to do something and everybody else is just standing by.

Jason Altmire (20:58):

Unfortunately, it only takes one to be successful to create a lot of problems.

Dr. Ted Reynolds (21:04):

And I make that point too. Look, it only takes one person to do a lot of damage. The challenge is, especially here in the United States, because we have our own extremist groups here in the United States, how do we find that one person, particularly in a country where we work to protect our citizens' civil liberties? And not just citizens, people in America? Because the government pretty much figures if you're here, then you have all the rights and privileges afforded you by the Constitution. Whether you're a US citizen or not, you're still entitled to those rights and privileges.

Jason Altmire (21:40):

As we close, Dr. Reynolds, how can an individual protect themselves to the fullest extent? How can a campus, a large organization protect themselves from some of the financial and data threats that exist? What are their best courses of action?

Dr. Ted Reynolds (21:57):

First, just be aware. The threats out there. Most people don't even understand that there's threats out there. Familiarize yourself with what they are. Understand that you shouldn't click on every link that's emailed to you. And unfortunately, the most vulnerable is our elderly population. They get inundated with emails for cheap drugs... All the things that are important to them, they'll get an email with a link, and if they click on it, they're likely to get hacked. So be aware of those things, practice good cyber hygiene, change your passwords, have good passwords. Make sure if you have a wireless router, it's password protected so people can't see what you're doing. Anymore when I'm working online, I'm using a virtual private network, a VPN. I do other things when I'm doing research, so people can't figure out where I am. But familiarize yourself with the threats and make yourself as small a target as you can. And that's the biggest thing. And even, I used to tell people physically, the bad guys are looking for easy targets. Don't make yourself an easy target.

Jason Altmire (23:04):

This has been incredibly interesting. Our guest has been Dr. Ted Reynolds, the Director of Terrorism Studies Program at the Office of Global Perspectives and International Initiatives at the University of Central Florida. Dr. Reynolds, thank you for being with us today.

Dr. Ted Reynolds (23:19):

Jason, thank you very much. It's been a pleasure.

Jason Altmire (23:27):

Thanks for joining me for this episode of the Career Education Report. Subscribe and rate us on Apple Podcasts, Google Play, Spotify, or wherever you listen to podcasts. For more information, visit our website Career.org and follow us on Twitter at @CECUed, that's @C-E-C-U-E-D. Thank you for listening.