27. Tom Stafford

Gavin Kelly
You're listening to beyond 1894, a podcast dedicated to updating you on research, innovation and Campus Life happening in Louisiana Tech University. In this edition of Beyond 1894, University Communications Executive Director Tonya Oaks Smith talk cybersecurity with JD Barnes, professor of computer information systems. Dr. Tom Stafford. He recently had a new article, platform dependent computer security complacency the unrecognized insider threat published in IEEE Transactions on engineering management. Stafford recently evolved the theory of cybersecurity complacency to describe the actions and views of well meaning but bumbling workers who unintentionally violate security. Learn more about what you should or shouldn't do to ensure the safety of your information on the web.

Tonya Oaks Smith
Well, welcome today to beyond 1894. I am here with Dr. Tom Stafford and he is the j. e. Barnes, professor of computer information systems in our College of Business at Louisiana Tech University. Today, we are going to talk a little bit about cyber and security and bad acts and bad actors with Dr. Stafford. So thank you for joining us today.

Tom Stafford
You're welcome. But it's the research is really about the opposite of that. We expect cyber attacks to be perpetrated by criminals. We don't expect cyber exploits to arrive arise from not paying attention or or not being worried, which is what my study is about, really, I, I was in the lab doing a study of the typical. Why do people do bad things at work and could not get an effect and started wondering why I wasn't getting an effect and learned it was due to a technological factor I'd not even introspected on I'm well ahead of your questioning. But the whole point really is that I by asking my respondents why they weren't scared of a cyber attack, they said, Well, I'm not a threat, I use a Macintosh off to the races. And that's what the article is about, really the fact that people get lulled into complacency by the platforms they operate on. So for example, if you worked at gbit over Mosher, that's a huge cyber security shop, you might be tempted to relax your vigilance and say, well, the boss has me covered, these guys know what they are doing. That's just the kind of behavior that leads to something like what happened to the colonial pipeline, a ransomware attack depends essentially upon somebody opening an attachment that they shouldn't mess with. Once it's open the the codes in the system. It's the the discipline to not open that juicy looking attachment. Got one today. Somebody's saying that a user in New Zealand accessed my Microsoft account, click here to log in and change settings, a clear phishing attempt. And it's phishing attempts that usually lead to these things. They issues how to keep people from doing that. Because by Gosh, it's just so easy, and they're getting very, very good. The one phishing attack that has impressed me the most since I've been here was one that looked like it was coming from Dr. Guys. And it was inquiring about my activity on Strategic Marketing Committee, which I was on. So I talked to Danny shields about a Danny sort of our guru of how to avoid all that bad stuff. He filters it out, you let him know if you see a phishing attempt. And he said, Well, you know, they're getting very clever, they're starting to micro target. They call that spear phishing, where they find somebody who has a particular connection, something they're interested in, in my case, they simply

wanted it to look legitimate by mentioning things they could find on the web that I had been doing with the university and influencing me to open a file, the file was a PDF, it wanted me to open the PDF and then open a PDF reader to look at the PDF. And that's when I realized, Oh, I have been fooled and shouldn't have because my computers are all equipped with PDF equipment, they'll open it automatically won't ask you to open a reader. It's a scary world out there because even the best of intentions sometimes are not equal to the sneakiest of attacks. And that's kind of what we're facing.

Tonya Oaks Smith
Well, I was I was this morning, I was listening to a reporter talk to a former hacker who is now a consultant Of course, that'd be Kevin Mitnick. I don't know. I don't remember what his name was sorry.

Tom Stafford
That would be backtrack. Oh, now Kevin Mitnick is the guy who was tracked down by the FBI and thrown in jail for very effective hacking. And what did he get he, he got the source code to the Motorola flip phone. That was his big exploit so he could then modify that and make exploits. But in exchange for leniency and other considerations. He became a consultant to the FBI. He spoke at you lm a couple of years ago, and I went over to watch him, took my stepson with me, and I'd been reading them already and Kevin's big point is I've never broken into anything by brute force, I always get people to give me the keys. social engineering is really what we're calling hacking now that the true hacking the the dictionary lookups of passwords, the brute force intrusions. Past firewalls are very, very rare indeed, because our hard defenses are very good, they're very hard to break, they take a concerted effort, they might take AI, and super computing power to get through it. Whereas getting somebody to give it their password by tricking them into thinking you're a friend is much, much easier. your Microsoft account has too many emails in it, you need to reduce your file size, click here. And that is the typical format is no longer the Nigerian prince that wants you to deposit a big sum of money is somebody saying, Well, you know, you're about to run out of email space, you better fix it here, we'll make it easy for you to connect. And it's just so easy to fall for that. I think vigilance is our own only solution really, that and knowing that we are at risk through sheer boredom and and attention.

Tonya Oaks Smith
Well, what's interesting is that that probably mid last year, when we were all at home, everybody in the office got an email from me. And these are not people that I have on my phone, as you know, contacts or anything, they got an email and it looked like it was from me. But when you looked at the email address that it was coming from, it will clearly was not from here,

Tom Stafford
the most important thing always check the return email address. And you can do that by clicking on the header up at the top where it says from and watching an expand out into its full address. Usually it'll just have its alias like my name. And then it'll have in an angular brackets, the true email address and the one from New Zealand actually, the one claiming I'd had my account access to New Zealand had an Austrian top level domain on it.

Tonya Oaks Smith
Not Australian. Yeah, Austria, Austria.

Tom Stafford
Yes. And the other thing that's interesting is we see a lot of this when you check those email addresses originating out of column the stamp stands the former Eastern Bloc of the Soviet Union. Here's the reasoning behind that, you know, when, when Gorbachev tear down that wall and the Soviet Union ceased to be I don't know how big of a percentage of the population it was. But it was a notable fraction of people were out of work. They were the people that were the watchers, the spies. And they had no other career that they were trained for knew how to practice other than going being watchers and spies and criminal and illicit behavior. So it's like a bunch of Vladimir Putin's being out of work and have nothing better to do but cause trouble. That's why we see so much of this coming from there. Now. We were talking earlier about whether colonial pipeline was a was a Russian government sponsored attack or not. And I'm following an item I just found on the PBS NewsHour where they think that it's not out of the question, you know, this kind of thing you can't really prove but you can certainly ask them to declaim it. And I've not heard a lot of that coming from Russia today. Other than there's that one quote that's in the news about dark side saying, well, we didn't intend to disrupt anything, we just wanted money. But if you look back to the solar winds hack that that was rather extensive, in fact, it was scary, extensive, it was into the government, US government agencies, you could almost make the rationale that we're seeing probing attacks, testing our defenses, and testing our willingness to respond. I see a certain sense in our adversary in that regard of being willing to push the boundaries to see what the boundaries are. And we haven't responded yet that I know of. We're not as public about it when our cyber forces, exact retribution. But nothing's happened yet that I would have heard about by now. And frankly, have to wonder what would be the result of an attributive attack. Anyway, that's the big challenge in this to disengage. This inset, an ex KGB strong man who's just naturally oriented towards trying to do this kind of stuff from trying to do this kind of stuff. It's his his way of life. So we have to expect more rather than less of this. Now, the flip side of that is the threat we face in China. They don't mean us harm. They want our secrets. I say that with certainty. But the fact is, the Chinese Red Army Faction is anxiously after in intellectual capital. Essentially, they'd like to get the designs to the Cisco routers, they'd like to get the source code to the Microsoft operating system, stuff that is not as easy for them to develop themselves as far easier for them to sneak in and take a copy of and make their own. Where does it end? I can't say that it does. But it sure seems to be giving a sense that our country's not as secure as we thought it was to these kinds of exploits. The safest will be is when everybody realizes Our ma shouldn't open another email attachment unless somebody I do know, phones me ahead and says I'm sending you this email, look for the attachment and the email says this is my attachment I told you about, then you have a fairly good degree of confidence that you're safe. But downloading an unwanted attachment is the typical infection venue for an attack of this sort. The the the ransomware attack, if you will. This happened to my ex once upon a time. Graphics are the big risks because graphics can embed a lot of active code. In fact, many graphics are active goes like GIFs. There was a time way back in the windows 95 year old and everybody was downloading comment cursors they could see the windows cursor streaming across this go comic cursor came with malware embedded in it. But the example I wanted to tell you about was when my exit watch the Grammys and Mary J Blige had appeared on the Grammys warned some really swift boots and she wanted to see about this boots. So she googled Mary J Blige, grammie boots. And the ransomware attack was immediate. When she followed the first link it, it started to grab ahold of her computer, I told her to power off, we'd boot up in safe mode, we'd scrub it with the malware system that was already on the computer and missed it by

that much. I mean, we we preserve the computer, we almost had a break. Because once it encrypts the drive, then you have to pay the ransom to decrypt. And sometimes they don't even send you the key to decrypt, they just want the money and leave you on your own dangerous world out there.

Tonya Oaks Smith
Wow. So you're really positive. They like your like your work sounds really positive. Say that was sarcasm?

Tom Stafford
Oh, no. It's it's a fact of life, people have been trying to take our, our computer data and secrets is encoded in them since we've had them. It's almost easier to do it now, because of the interconnectivity around the world. And because of the commercial applications of technology give you so many touch points to that. I tend to think that the research that's done in this field, when I hosted the dewald route information security conference in 2019, over booksure, most of the people they're presenting, we're taking the criminal justice perspective, most of the people in my field, take the perspective of there are bad people in the company, we have to find them and dissuade them from doing bad things. I've, I could follow that as well, because it's very popular, it's easy to publish that kind of stuff. But my sense was that there aren't that many bad people in the population, maybe one out of 100, who have truly psychopathic tendencies, and you have to really be on your guard against them. The biggest threat is not the bad people, it's the good people that don't know they're doing the wrong thing. And they feel good about the work and they don't realize they're bumbling around leaving trap doors open for bad people to take advantage of the company. Educating the normal use of the well meaning user to be more careful, probably be more effective than trying to find the couple of bad actors that are going to be there and and filter them out. My colleagues who do the other bad actor researcher probably disagree with me because the the exploits on a bad actor hits you are indeed dramatic. The things that happen when well intentioned users make password mistakes or download the wrong attachment aren't always as dramatic unless it's the one that ends up for example, encrypting the data center at the city of Monroe down the road, I told you about the ransomware attack over there, just opening the wrong email will lead to that. health systems have been particularly at risk when I talked to the CIO of Vantage recently said you know, on on the black web, one health record, one personal health record is worth more than one credit card number, because it carries links to information about prescription streams and people access health records, will they want to basically spoof prescriptions and get the drugs they're not entitled to get by pretending to be somebody they're not using the health record?

Tonya Oaks Smith
it so when you when you were you just talked about the value of a health record? I think that that's interesting. Because you have to really think about this seems like it's in order to utilize the the information that you steal on the web, you have to figure out how to use it and how to remarket it. Yeah,

Tom Stafford
where are you going to extract your value now the ransomware people just want the the money you'll pay them in exchange for decrypting your discs but as I say, you don't always know they're going to do that anyway, when it's an easy route back to them, if they interact with you any further past the original hack and payment so I've heard stories of people who paid and didn't get what they wanted. I've heard

stories of people paid and didn't get what they wanted. The principle seems to be don't get don't get exploited in the first place because it's a it's a question you wouldn't want to have to visit but at the same time, there is ransomware insurance out there now for companies that are worried about it. We could not operate if ransomware attack hit us here at Tech this week during advance We could not operate if our our data center was encrypted against us. We couldn't register, you're

Tonya Oaks Smith
not asking for somebody to try.

Tom Stafford
No, we're not. And I know the people that protect us from this, they are working diligently. And we do have some protections here because the technology we use is not the same technology that the hackers would be using. They're all probably on an open source operating system like Linux, we're running proprietary software, we have a lot of our operations centralized on a big mainframe. And it's not so easy to break into that if you didn't grow up in the mainframe era writing COBOL and doing mainframe stuff. So we do have that, that protection.

Tonya Oaks Smith
So let's talk about your your background, because looked at so you started out and your bachelor's degree is in interdisciplinary studies,

Tom Stafford
which is a way of not having a degree in anything in particular, except everything. It was a broad liberal arts,

Tonya Oaks Smith
you, you, you studied what you're interested in,

Tom Stafford
I was mixing sociology, psychology and mass communications and ended up going into radio for a decade and not liking how little I was paid there. And so going back to school and getting an advertising degree and not liking traveling and industry, so going back to school and getting a doctoral degree and doctoral degree in being a marketing professor for a period of time, but then the guy edited the Journal of advertising wrote an editorial he said, advertising is dead, the internet is going to make it all irrelevant. So I decided I better go back and get an internet degree. So I went back and got a doctorate in Information Systems. And that's what led me here. It actually led me to University of Memphis for 15 years, and then they hired me away from Memphis to come here.

Tonya Oaks Smith
So your work? You know, when we hear computer information systems, we think something Yeah, I don't know stuff. Yes, I sit in.

Tom Stafford

A really I class I'm teaching right now is all about training the future CIO, how to work with Indian outsourcers, or how to avoid being taken advantage of by Chinese factories, manufacturers. We spend a lot of time just lately focusing on what's happening with China. And I train them to think like a strategic executive, they have to find the threats before they manifest themselves. So they're prepared and guarded against them. Because the people who know the threads and avoid them gain an edge in the market as the rest of the market encounters the threats and have to deal with them. It's a competitive advantage, actually, to know what your competitors trying to do. If your competitors nation state like China. And I tend to feel that China is the primary competition we face both existentially and in industry, because they, they intend to win. And their culture is a cohesive one. So they intend to work together to win. So no mistake I'm having my students read the writings of the the ancient Chinese general Sun Tzu, it's it's generally reading and strategic management programs, like at Harvard. And they're they're learning a little bit about the Chinese mindset of how to engage with a competitor, which is basically be sneaky. Don't let them know you're attacking until you've already won the battle.

Tonya Oaks Smith
The Psychology of how we function in business influences how secure things are, and they influence our levels of trust in in the communication that come to us, you know. And so I think that how you talk about your background builds to what you're doing right now.

Tom Stafford
Yeah, I didn't intend to end here on purpose. It just sort of happened. But my broad interests have always been Why do people do what they do? And how can I learn more about it and help them understand how to do what they do better. So at center, I'm really a management theorist, because management information systems is really about how to manage programmers, that's a hard job programmers don't like being managed, they like to do their own thing. So like the Dilbert comic strip, that those are programmers. In my typical undergraduate class, it's it's even more challenging the the people that we need to manage who are programmers are also Indian programmers. And that's one more level of strangeness that we have to circumvent them teaching students how to be aware of the cultural differences and to understand that the way we'd manage worker here is not the same, that they'd be managed there. And that if we fail to know that, then we can't even start to make it better.

Tonya Oaks Smith
Well, that I could see how that philosophy could impact not just outsourcing but sourcing in a different area that has a different culture than the one that we deal with wherever we are.

Tom Stafford
The fact is, economics dictates we have to send a good deal of the basic work of production to department countries are standard living is high enough that even the people at the low end of the wage spectrum earn more money than the workers in the middle class. The way expect them to in places we outsource to. And so what we would pay what we want to pay for, let's say basic code work is enough to make us profitable. And to be profitable, we need to cut our costs on that if we can. So if we can find programmers in India, who are as good as programmers here, but work for half the price, we have to do it because we don't want our competitors will. same logic pertains to why this device I'm using here was built in a Chinese factory. Our workers can certainly build it but not nearly as cheaply as

as a Chinese factory worker will build it. The issue I have, and it's related to my cybersecurity interests is what are you giving away by having somebody in Russia? Did I say Russia, somebody in China, build this iPad Pro? I feel sure that I was in might be taking pictures and making blueprints and documenting the whole thing. So I could come up with my own version. And maybe they will one day. Yeah, I know, I sound like a conspiracy theorist. But adopting designs is is kind of the way those things happen. So security, we have a we have a NSA, DHS certified center of academic excellence in cyber defense, education, research and training, I think it is my hope I stated that right. And we basically do this kind of work just as a service to industry in the community. You know, we're in a huge part of the world here where security is essential, because just over there Mosier, you have the nuclear strike commander of the US Air Force, all kinds of state actors would like to break through that network and see what they're doing. GDI T is responsible for helping them keep that from happening. And they do a darn good job of it too.

Tonya Oaks Smith
So tell me about how having, having partners like GD T or global Strike Force, how does that influence the education that we offer our students? How does that

Tom Stafford
The main thing it does for me is it stimulates me to try to point all my best students to that company to go work there. They're they're hiring right now. And I've got a class it's half full of graduating seniors. And I know they could make a contribution there. I want our partner General Dynamics to have the benefit of our best talent. Here, we've got some very talented students, not only in my college, but also in Engineering and Computer Sciences. And our job basically, is to help them do their job, the way I view it, if they're doing their job, well, they'll continue to hire more people. And these people will work in conjunction with what's happening, Bowser, they'll get promoted up the food chain end up working in I don't know Washington DC is where GD is headquartered.

Tonya Oaks Smith
Because I'm sure that our listeners have heard really quickly, may talk about computer information systems, what's the difference between computer information systems, and computer science,

Tom Stafford
programming the computer, versus managing the people to program the computer. So you're, you're a project manager, in most cases in Information Systems, because you know how the programmers work, you could do the programming if you need to, but you also understand organizational theory, and how to get them motivated and cohesive and working together. And you're also skilled at the art of building milestones and meeting deadlines. We're about making sure that the technology function of the firm is effective and functional, hiring people who get their degrees in computer science as part of what we do. So the hiring and firing, the managing the incenting, the project management, and then people that do the work end up being people with very technical keyboarding skills at their programming or hardware skills, if they're building networks, or assembling computers, the disciplines all kind of flow together that way. In engineering, they're designing the systems in computer science, they're learning how to run the systems, using the software building the software, and an information systems were

focused on how to make all of that technological skill integrate into meeting the company's needs, as it manufacturers or markets, whatever its product is to his constituents. Okay,

Tonya Oaks Smith
that that's, that's helpful, because I think our listeners can understand there's a human aspect to this to this technical side.

Tom Stafford
And when you talk about what an Information Systems it is, it's three parts. stuff, we build software, hardware data, and one part the people that operate it people. It's not a system without people in the mix. It's just information technology. So when you hear the term it, we academics typically say, well, that just means the stuff you build. But when you call it a system, you're talking about how the people interact with it, and the work that it does and the workflows that it supports in the operations of the organization. There's a good rubric operations management information systems about making sure the technology function fits with the overall operations of the company, and generally it's manufacturing but oftentimes it could be service provision.

Tonya Oaks Smith
Okay. And to to come back around full circle, I guess. The addition of the humans into the system is the danger zone.

Tom Stafford
Because people get tired, and when they get tired, they let the guard down, the guard down, they don't think about not opening that attachment. And then that's if you get one message from any of this, it's don't open that attachment. There's nothing that you need to attend to that won't be sent. Again, if you fail to attend to it today, that you won't get a call about if you don't attend to it right now. Don't open it automatically. That's where 90% of the bad attacks really start. It's getting the code inside the firewall. And in the old days, you'd hear stories about people sneaking USB drives in and plugging them in. Well, that is certainly one way. But we've gotten wise to that universities do we typically? Well, at Memphis, for example, you could not run a jump drive in the classroom, they had the the USB interfaces all the activated because we'd had a terrible jump drive exploit in the classrooms. But leaving that aside the the notion that the people are the first and last defense against all of this, because the actions they choose to take or don't choose to take, determine whether or not the bad actors have an easier or more difficult avenues when they're trying to get inside the company.

Tonya Oaks Smith
So what do you see as being the next we talked a little bit about ransomware? We talked about this, the colonial pipeline hack. We talked about a couple of other hacks. What is the next thing that we should be concerned about?

Tom Stafford
We haven't seen what solar winds was intended to accomplish, yet they broke in, they're still in, we haven't cleaned them out completely. I don't know what that was for, we'll have to wait and see where the other shoe drops. But I got this from the folks over at Louisiana Tech Research Institute ltr II over at

the Bossier campus. And they said the thing to worry about artificial intelligence because now our nation state threat actors, North Korea, China, Russia, are using AI to engineer the exploits. And AI exploits are very difficult to counter at the human level, we're gonna have to develop AI protections. So it's the Battle of the robots that seems to be coming next. And I'm being an alarmist and futures by saying that the fact is, AI is already here. That's how come you can, I don't know you could be buying a, an iPad on your telephone. And all of a sudden, you start getting pop up ads for tablets on every app you use on that phone. Later that day, it's not even a very long delay. The power of artificial intelligence and data mining is what makes our technology so responsive to us. And it's also what makes us so vulnerable to it because AI, it doesn't know everything, but it has access to much of the data. And it can learn a lot of things about us that we would want to keep secure passwords. And well, they couldn't learn our passwords, they could learn stuff that would use to make a password. I don't know about you, but my passwords all have to be things that I can remember, or things that I will take the moment to look up on my 128 bit encrypted password file here. But the ones that I need to be able to remember right on the fly bank passwords particularly I combined from things that I consider to be memorable to me, but maybe might not be known to other people. Like inside jokes, stuff you would know stuff your other half might know but stuff nobody else would understand. I can't give you an examples of those without giving away my trades I

Tonya Oaks Smith
was gonna say. So we have to call do this

Tom Stafford
though with passwords. And really, there's the two threats we face open that attachment, it could be ransomware. So don't open the attachment unless, unless and until you can ensure that it came from who you think it should be. And don't be the person that send this sends this email. We need your help see the attachment. They do that here a lot. The intended communication is in the attachment and you have to open the attachment to find it. tell somebody what the attachment is going to be so they can decide whether or not they think it's worth the risk open. Secondly, passwords when you have a password even if you use familiar phrases, names and other aspects of the keyboard that might be useful for you to use because they're memorable. throw in a couple of things that make it difficult for a dictionary lookup to crack it. We call them wildcards IE like Asterix dollar signs, pound signs ampersands, any of those will fool a dictionary cracked because the dictionary looks up the 26 letters in the English alphabet and tries to find word combinations and cross references to what's stored on you in the databases about your birthday your kids names, where you live, where you went to high school things you might use for password throw wildcard to in and you can make that much safer. We we had a CIO at University of Memphis for I came down here required us to change our password every six weeks and to change it to something with 13 characters. uppercase, lowercase for numbers and end a and wildcard and they weren't easy to remember and it made me angry because on the one hand, yeah, it was good password to some of that. On the other hand, the only way to work with that was write it down on posted note and that's the third thing. Don't write it down on a post it note if you have to do anything. It's called on iPhone e wallet and It's it's a free download. And it transfers from iPhone to iPhone as you upgrade I don't know the Android example of that is but the the E wallet an iPhone now for 10 years going is where I store the passwords that I cannot remember that used to have to remember the password, a wallet, opened it up, find your password, and away you go my brokerage

account for example, I make difficult enough that I can't even remember it. So I have to open it up when it's time to use it.

Tonya Oaks Smith
And then you lose it. And you had to reset it.

Tom Stafford
Don't worry about resetting the password, just make sure you reset through the right link. That's another spoof that's very popular is to try to get people to reset a password Oh, we notice your password is expired. Reset at this link. You're giving them the credentials when you do that. Because you have to give them your log on identity. And then you set a password and they're probably just setting up a new account back behind the scenes in your name. You don't want that to happen.

Tonya Oaks Smith
Well, our our talk today has has certainly been informative and you've given us the the instructions to never open

Tom Stafford
an attachment have to know the attachment is legitimate. And the safest thing to do is not open it while you find out Don't open it automatically because the attachment if it's if it's an attack, the attachment is the payload that'll be the ransomware exploit. Once it's open, it's in the system, there's nothing you can do to shut the door.

Tonya Oaks Smith
And and the second was Be careful with your passwords.

Tom Stafford
Don't tell people your passwords. Don't write them down on post it notes. This I learned from a guy at KPMG who was ex CIA and he made a keynote at a conference and he said well, you know, hacks are really low, low level. This is what Mitnick said in his speech. It's not breaking into your system by sheer force. It's by doing sneaky clever stuff like getting somebody on your janitorial staff who simply looks at what's in the trash cans each night and can figure out stuff from that or her looks to see where the posted notes are because we all know where we keep keep them underneath the desk blotter keep behind this cabinet door I mean the fairly easy places to spot if you're a professional searcher for post it note passwords. I hate to say don't use a post it note because I will admit I've done it myself during advising my my boss pin. I have to look upon this. But when we're advising I basically put it on a post it put it in front of the computer so I can log in and out real quick because I'm always on the fly. That is bad practice. Physician heal thyself I'm doing the wrong thing exactly course I'm doing it in my office with no prying eyes. Nobody accesses my office, but at the same time is what we tell people not to do.

Tonya Oaks Smith
Right? Well, but we but but now listening to you, I'm sure all of our listeners will go. Okay, I've got to go and make sure that my passwords are more secure. I'll never open those those attachments that you got. And I will slow down. I think that that's part of the message stop and think

Tom Stafford
lay down promise in the modern workplace, we've got five things to do and four things worth the time. So we're always in a rush. But remembering that the modern workplace gets it we may not have a job to come back to if we can't be careful about not letting it get exploited by bad actors out there.

Tonya Oaks Smith
But thank you for joining us today.

Tom Stafford
We have a marvelous cybersecurity program at several levels here at Tech will teach you how to defend against brute force attacks with the the hackathons that computer science and engineering do will teach you how to manage the people who protect you from those hack attacks in the IRS program. And we all work together as part of the the Center for Excellence because the government has decided that they want to put their money behind something like this to have Centers of Excellence where we can teach people how to do this because we need more rather than less security workers going forward.

Tonya Oaks Smith
Absolutely. I think we did some research last year and that there were so many cyber jobs that we won't be able to fill them anytime in the next few years. You know,

Tom Stafford
there's there's one last point I'll leave you with. And this is my area of research, as I dabble in it anyway, because some of it is how to prevent an attack some of its how to get the right people into the profession. We're vastly underrepresented in the security industry right now. It's mostly young, white dude, hackers. It's just a natural thing for young white guys with computer skills to go in security. We've hired all young white dudes are going to go work in security we need women in particular, highly represented, they don't see that it's an attractive career trajectory, because it's largely seen as what the young white dude hackers are going into. And we're losing possibility of accessing half of an important workforce by not specifically trying to recruit women into this. The government has given lots of money out through National Science Foundation to study how to make people more interested in working in the field. And it all starts with find people who haven't traditionally looked at looked at this as a career trajectory. So that's my pitch for diversity

Tonya Oaks Smith
diversification.

Tom Stafford
Employed with the people who would naturally hire on its we have to we have to find ways to interest more people who would normally consider it as a career to become interested in. It's a very good career in this region. It It's a fabulous career in this region.

Commercial

Develop a prototype for the next big idea. Immerse yourself in the Internet of Things. Discuss with top CEOs the issues keeping them up at night, manage a real investment portfolio. pitch your best ideas to potential investors interned with fortune 500 companies across the world are right next door. Do all of this and more as a student in Louisiana Tech's College of Business. Learn more about how you can leverage technology to its fullest and lead innovation in any organization@business.latte.edu

Gavin Kelly
Thank you for listening to beyond 1894 Please Subscribe and rate us wherever you listen to podcast. For more information about this episode, check out our show notes beyond 8094 is produced by Louisiana Tech University's Office of University Communications