Good afternoon, everyone. Welcome to this month's toolbox Talk.

as you're getting settled with lunch,

I'm going to go ahead and do a quick introduction so that we can get started so that

I could give as much time as possible to our speakers here this afternoon for us.

But again, welcome to our monthly toolbox talk.

We've got, OIT with us today to talk about, security.

So with us today we've got, Chris Smith and Charlotte Russell.

So I'm going to do a really quick introduction of both for you.

So Chris Smith is the CIO and vice chancellor for information security and services.

And he's been an integral part of CU Anschutz since 2011 and has held several leadership positions.

He previously served as the campus technology strategy Officer and associate dean of Administration and Finance for the School of Medicine.

Before before joining

CU Anschutz. Chris spent 15 years at the University of Iowa, where he worked in the Department of Internal Medicine.

In his current capacity, he oversees a diverse portfolio of information and data services.

These encompass cutting edge technology supporting artificial intelligence, business integration, core infrastructure,

and development of solutions that are integrated with the university's mission areas and strategic priorities.

As an academic health care leader, Chris says.

Fostered collaboration,

Encourage innovative thinking, challenging teams to be proactive, nimble, and focused on continuous improvement to move us forward.

So we're excited to have him here again today.

If you remember, if you've been here before, he is also helped to do a talk on, AI, which was, really awesome as well.

Charlotte is also joining him today. She is our CISO and assistant vice chancellor for information security and compliance.

She joined CU in 2022 and oversees the connection between cyber security and the compliance missions of the university.

Charlotte has most, was most recently the ABC and chief information security Officer of the

University of North Texas System and also served as interim CIO overseeing the enterprise technology.

Excuse me. The enterprise technology. operations for the multi campus system.

She has served as a leader of information technology for over 25 years,

and is dedicated to collaboration and partnership in supporting our university mission.

So they're here today, as I said, to talk about security.

just so you all are aware of.

We we have your attendance or sign in capabilities.

It's on the screen.

But as you came in, there are also little cards that have the QR code that if you didn't pick one up on your way out, you can do that as well.

So it makes it easy. We're trying to find innovative and easy ways for you to do that.

And they're also on the little placards that we have at the end of the tables.

And we have plenty of lunch here for you and more chips. So please help yoursel, to that as well.

But with that, I am going to turn it over to our two speakers here today.

So please help me in welcoming them.

All right. It is great to see a lot of familiar faces. Thank you all for coming.

I'm going to jump in just to introduce us and turn it over to Charlotte.

we are going to try to move through these as quick as possible.

We'll make them available after, the talk or make the slides available after the talk,

because, we have a whole lot of questions that came in ahead of time.

And we want to make time, for your questions. we clearly think this is an important topic.

And based on the questions you've asked, you must, as well.

So, thanks, everybody, for coming both here and online.

All right, so what are we gonna talk about today? We're gonna talk about digital threats.

Personal. So we thought about this,

and we want to really talk about how can you all protect yourselves and thinking about it because it affects your daily lives.

And if you have your personal digital security compromised, it's a real challenge for you.

But then carry that over to here at the workplace.

And a lot of those same skills carry over to here.

So how does that help you here in protecting university data?

We're entrusted with a lot of data, from many different constituents,

whether they're students, whether they're research subjects, whether they're our own staff.

And that's a that's a high level of trust. So how can we help protect that data which we are entrusted with?

We're going to talk about, so campus digital security.

So how does that work in our positions here? And we have a, I can just, by all the folks I know here.

There are a lot of different positions, represented here.

So we're going to talk kind of top of the waves. But we can dig into that a little bit as we go there.

Best practices for a secure digital environment.

When we talk about security, we talk about levels of security or layers of security.

So we're going to talk about kind of those different layers you can apply that'll help bolster your, digital security presence.

And then building a culture of, cyber security awareness.

And where can I find as, both, a personal person and a university member?

How can I find more resources and how can I help enrich myself in them?

All right. So digital threats. And I'm sorry.

I'm usually the party pooper at most of the meetings when I talk about cyberthreats, whether it's an administrator meeting or stuff like that.

I don't mean to be the downer. We're just going to talk about reality today.

And how can we deal with the fun reality that we're in? Okay.

Phishing scams. Sorry, this is a little on the small side.

I tried to make it as big as possible. Again, we'll share this.

But phishing scams are a big deal, right?

So people send you an email, they say, hey, I need you to log in because your account got locked or you just won a new prize.

I want you to click on this link and log in. Now, what they're doing is they're trying to get your credentials,

whether it's trying to get into the university, trying to get into a bank account, whatever.

But they're stealing your credentials to then either lure you further or get access to that which is important to you.

And that is the number one way, cybercriminals basically kind of land a foothold or perpetuate cybercrime.

So that's that's one of our first focus, focuses that we look at.

And that's something that you all should be aware of. Ransomware.

You hear probably hear ransomware a lot. What does that mean? Somebody sends you.

Hey, this is a great image. Or this document's really important.

Double click on it. Turns out you didn't know the person.

It's not a document. It's not a picture. You do it and install something on your computer.

And what it does is it either takes data from your computer and sends it out to the internet, to a bad actor.

We use bad actor a lot. Cybercriminal, call it whatever you want.

Pain in the rear, it sends it out to them, or it encrypts the data on your computer and they say, guess what?

If you want us to delete it, not likely.

Or you want us to decrypt it. Also not probably likely.

You need to send us x number of money usually in Bitcoin so it can't be tracked or pulled back.

And we'll give you your money back. this is a multi-billion dollar scam.

Billion, billion, billion, billion dollar scam across the world.

And they keep doing it because they keep getting rich doing it, and it's not going to go away.

The thing you can do is protect yourself and know the signs of how to watch for.

So malware this is other types of, it's the new, I don't know, I'm older a little crusty here.

We call it viruses before, now it's malware because it does multiple different things.

Malware can be a program that sits on your computer and watches all your keystrokes.

So when you go to a website, it says, oh, I just saw the username, I just saw the password.

Good. I'm going to take that and transmit it to an actor. I'm going to watch what websites they go to to know they bank at this place.

They have a credit card here. They maybe have software here.

So that's like the new version of antivirus.

Thank you for calling me out. And then viruses.

Those are your traditional viruses. Get in, infect your computer, and then you get to share it with friends.

Just like the flu. Okay.

Latest trends in cyber attacks. So MFA phishing attacks.

You may notice this here. And this is why we've sent out, emails recently.

If you get a duo request on your phone and you say, wow, I didn't I didn't go to my.cu.edu, or I didn't go to HCM.

Somebody may be phishing for an MFA, which probably means they have your username and password,

and they're pushing and they keep pushing to your duo to see when you're going

to get tired of seeing that silly duo request and you're just going to hit.

Yes. Accept. And yes, that does happen here and it does happen with frequency.

Because people fall for phishing here and we see it.

So that is a big thing. Same with the banks. Oh you got a text.

Text text text. Like just make this thing go away and people make it go away.

And what do you know. Somebody now has access to your, your information.

SIM swapping cyber attacks. We've seen this in a couple of cases.

This is usually a much more advanced, much more targeted attack.

It's when they know this person has access to this thing we specifically want,

and we know they have multi-factor authentication, i.e. they get texts to release the information.

We have their username and password, but, we can't get them to fall for the phishing attack or the MFA phishing attack.

So what we're going to do is we're going to call up the cell phone provider, and we're going to convince them into switching the phone to us.

And yes, we've seen that the attempt on that happen on this campus for very, privileged individuals.

So it does happen. A way you can prevent that is by going and do what's called sim locking or locking your cellular accounts.

It's pretty easy. They'll basically just ask you for more information when you want to make changes to your cell phones.

Yeah. The SIM card was a physical thing.

Yep. And how did they steal it? I mean, they can change the data.

so what they're doing is they're saying a new SIM card is associated with my phone.

That's. What did you say? Oh, yeah.

So basically they're grabbing your phone number and applying it to a new device.

And actually for most phones anymore, they're not cards anymore.

They're all electronic. Okay, so recent security incident, we all had the opportunity to change our password.

I am going to say opportunity. The opportunity to change our password to a stronger password.

And just to be very crystal clear, a 16 digit password is what you would consider a contemporary

strength for password, eight digit, which is what it was previously, is not a contemporary strength.

So you'll see, when we, made those changes, we, you may have, may or may not.

Well, you've probably seen the password complexity. For instance, I use a longer password than 16, so it made no difference to me.

I just changed it again.

Some of you may have fallen into that category, and some of you may have had less than 16 digits, so it may have made a larger impact.

The other piece is we made some multi-factor authentication improvements.

Again, you may have seen it or you may not have seen it.

So we made improvements in some of our security measures to further strengthen the security of the university.

And in today's cybersecurity environment, we are going to continue to make planned

as our, as our plan to make planned improvements and cyber security measures as we move that forward.

And one of the best practices. And this is really something we're really pushing in the IT community, but it's in every community.

If you see something, say something. It's like the old TSA.

If you're in the airport, if something looks goofy, say something.

It doesn't matter if it is really an issue or not, but bring it up and let's look at it.

Because if your computer is acting weird, if you get a goofy email that you think, I don't know, this might be phishing.

Use the little phishing button on top and reported as phishing.

Because let me go back to the phishing piece. If it is phishing, you report it, they find it as phishing, it pulls it out of everybody's email boxes.

So that's like the best service ever. And it pulls it out of everybody's.

If it's not, they'll let you know. And let me tell you, I'm a proficient reporter.

And once in a while I get an email back that said, oh yeah, this was a totally clean email.

All right. Okay. My bad. And sometimes they're like, well, this was spam, not phishing.

And sometimes, and most of the time it is phishing. So it's just something to think about.

All right, Charlotte, it's all yours. You want this or you want that?

All right. See if I can do this well. So thank you, Chris, for giving everyone an overview of some of the threats and the incidents.

And how to manage those. I'm going to talk with you a bit about personal and digital security.

Personal digital security related to your personal information, and then also the devices,

your personal devices that you use on a regular basis that are not your university owned devices.

Here's some personal and easy to implement defenses to protect your information.

We recommend that you use best password practices.

So good password practices. So you heard Chris talk about the 16 character passwords that we implemented here.

You want to implement strong passwords as well with your personal accounts for your banking, for your online activity.

You want to ensure that they include a combination of uppercase and lowercase letters and numbers and symbols.

I know that's annoying to think about, but the stronger the password, the less likely an attacker or a bad actor is able to access your account.

So we talked about the eight character password that can be brute forced in a matter of hours.

If an attacker has your your your username, but a 16 character password takes years to brute force.

So strong passwords, use, consider using pass phrases so it's different words within mixed in or special characters in the numbers.

That's going to be really important for your personal accounts as well. And please don't use the same password for more than one account.

If an attacker were to gain access to one of your accounts, they're more than likely going to be phishing.

Phishing for access to any other services that you may have access to your bank.

they may be guessing if they have the username and the password.

It's fairly easy to to try and guess and just see what works. Credit freezes.

Okay, this is a great one. So everyone has credit and you have a credit file with the credit bureaus.

You should freeze your credit when you're not using, not intending to use your credit.

Most of the time we're not using our credit to open up large lines for purchases.

So freeze the credit until you need it. You can unfreeze it.

It doesn't take very long for the period of time that you need it unfrozen, and then freeze it again.

It's like protecting your account and your identity.

So it protects you from individuals that are attempting to steal your identity, restricting access to your credit.

And it also prevents future accounts from being, accounts for being opened up in your name.

So if you haven't done it, I recommend that you do that as soon as possible. Freezing your credit is easy to do.

It doesn't harm your credit score at all. In addition to that, recommend, purchasing identity theft, monitoring protection.

So this can be done through financial services or other service providers, your credit card companies as well.

This protects you from potential threats because these services monitor activity.

And they will alert you if there's some unusual activity with your accounts.

And consider also, purchasing, let's see, insurance coverage as well.

In the event that someone does obtain your information, you're a victim of identity theft.

The financial impact can be very significant.

It can be in the thousands, hundreds of thousands. It can be very significant, depending on how far they're able to go with

stealing your identity and purchasing things or using things to disrupt your life.

So you really want that insurance. It doesn't cost very much per month.

A few dollars, depending on the type of coverage.

You can get individual, multiple, adults, family coverage to cover even your children, so consider doing that as well.

Well, I'm not, I'm not an expert in that area.

But I can say that we have looked into several services, like aura.

I know that McAfee provides some services, some legitimate services, but we will.

I'll get, if I can get your information after this, I will provide some recommendations to you.

Okay. Go to the next slide. Safe browsing and email practices.

Okay, here's a here's a let's get. Here we go.

So when you're using your browser on your computer, you want to make sure one of the first things you do is ensure that that browser is kept current.

It's updated. I know if you're using some browsers there, it feels like there are updates every day.

It's okay. You want to go ahead and allow those updates to occur.

In most cases, you can keep your tabs open, keeps your sessions open.

You can go back to them without doing so much disruption to your works, to the work, the things that you're working on.

So please update those browsers. Do it regularly.

You want to avoid suspicious, this says links, but websites.

So when you're browsing, if you see a link to a site that's just a little bit worded, a little bit strangely, it's not a normal site that you visit.

I would avoid it altogether. like an email, don't click on links to websites that you're not familiar with.

If you want to visit a website, I would, that you think is legitimate.

I would suggest you do a search,

and or go straight to the website to obtain the information that you're looking for rather than clicking on the link.

Email, practices. Again, don't click on links in emails.

We talked about phishing. you hear us talk about phishing. Remember, this is in your personal email as well.

We're not just referring to the to your work life here.

It's really important that you don't click on those links because they could lead to infections of your phone or the device that you're using.

It could introduce malware. It could introduce what Chris mentioned as keystroke loggers which record everything that you type.

Or any other malware that can perform any other other types of malicious activities.

Okay. So more about your devices.

For those of you that don't use device locks. I'm going to encourage you to do that.

Highly recommend that you. That's a form of physical security that protects your device from others, should they gain physical access to it.

This means locking the device through the screen protector.

Screen saver that's comes up, and it requires some sort of a login or authentication before you can access the files on your computer.

You're going to want to consider biometric if it's offered as well with your device.

So that could be finger print or it could be facial recognition.

But you want to enable that on your your personal devices to protect them.

It's another layer. It's a second layer protection. Software updates.

Again, make sure your software is current.

It's really important that you update not just your browser, but all the software that resides on your computer for a number of reasons.

First, your computer will perform much better.

You will be able to use. It'll be faster.

You'll have the latest updates and features from the service provider, and you may learn they, may be able to access new services.

But what we are here to focus on the security.

Because if you're not updating those devices, a bad actor could scan the network, which you're sitting on.

Find the vulnerability that's associated with the software that hasn't been updated,

and use it to attack your computer or gain access to your computer.

Those updates are really, really, really important. So please do enable those and enable automatic updates if you can.

It makes it a little bit easier for you to manage those. Okay.

Anti-malware software. So anti-malware software.

Antivirus, anti malware software is used to protect your devices from relevant, from being infected with viruses.

Data stealing ransomware. Which

you heard Chris talk about. Adware, those junk ads that you may be, you could potentially receive the keystroke loggers, or other malicious software.

So go ahead and purchase that from a reputable provider and install it on your devices.

It's going to make your life a lot easier. It will block threats so that you never see them, and it will also prevent,

it will help the performance of your computer as well, or the device that you're using.

Personal digital security. So usernames and passwords.

This is one that troubles me when you, if you have ever been a victim of cybercrime or identity theft.

You may have received a notice from a provider or an online, your bank saying that your credentials were, or your PII was released.

It was found on the dark web. Well, that information lives out there.

It's sold and it's resold, and it's used to continue to attack the individuals that are victims of those crimes.

So it's very important that your usernames and passwords are strong and that

you use multi-factor authentication if it's offered by your service provider.

It will. It's another layer of protection that will prevent an attacker, as Chris mentioned, with Duo as an example,

prevents an attacker from just being able to brute force your username and your password.

Typically, they're not going to get past a duo prompt or a multi-factor prompt because it's typically

something that you have with you or something that you know or as your physical,

it's part of you. Okay, so that's what that multi-factor or that dual factor or five factor authentication will provide to you.

Public places and USB devices. This is a favorite talk of mine.

So when you're in public places or you're in the airport, you have your USB device and you're going to want to charge your device at some point.

If you're low on battery, don't shut. Don't plug in the USB device directly into the the outlet that is provided there.

You want to plug your power adapter into the outlet.

When you connect your USB device to those sources,

there's data being transferred from your device to the online or the service that you're trying to connect to.

There are also other users of that network that may have introduced malware in that network,

and that malware can be connected to your device through that USB connection.

So always use the power adapter. You can plug your USB device into the power adapter,

but make sure the power adapter is where you're you're charging from and not using

your USB device to directly to receive the power and charge your devices.

Okay. And last but not least, on this slide.

If your device is no longer needed, perhaps you've upgraded.

You have something new. You may have an old device that you don't know what to do with.

First thing you do if you don't plan on using it is restore it to factory default settings.

It will erase all the data. It will erase all the settings and any other information that may have been stored on that device.

If you don't do that and you hand that off to someone who's going to maybe,

resell, it's a resale, you're getting some funding recovered or you want to donate it.

Whoever receives that device has access to your data, all the information that you left on that device.

So always restore to factory default. How do you say sales use?

nowadays they have the public like USB charging ports, where it's just the one to say, I believe your phone is connected to USB.

I know you said like at airports, don't do it, but like in schools, I've seen it like in universities or in doctor's offices.

They have that. I would not recommend it.

I love your question, but it's still a place where the public, if the public can gain access to it,

you're not going to be aware of the security controls that they have in place with that network.

Can you repeat the question for them? I'm sorry.

The question was when you go into a place other than an airport and you have a they have the USB devices where you can connect your device to that,

that outlet or that connection point to, charge, is it safe? Would we recommend doing that?

And I wouldn't recommend that unless you are really confident in the security of that Wi-Fi network that you have just connected to,

if you're not aware of the security of that WIFI. Yes.

Yes. Yes. USBs and Wi-Fi. Okay, so the USB connection, I wouldn't.

You're basically going to be connecting to power and connecting to other networks through that source, right?

Whether it's Wi-Fi or the, the wired network.

I wouldn't recommend it unless you know the security of that environment, because you don't know with that,

because you don't know, I'll call it that portal is connected to.

Right. You don't know what's on the back end. Unless you know the technology team and they've explained it to you the security.

So let me throw out one more thing. Sure. So I think that's a good question.

And that one comes up a lot. And for anybody who is at the block party and we had our booth, which there is a lot of.

I don't know. Swag, I think is what you call it.

One of the things was, that we had actually we ran out of, I think, pretty early, but there were USB blockers and you can buy those on Amazon too.

So all it is, is you've got your iPhone or your, droid or, I don't know, Samsung charging cord.

Right, usb-C or lightning charging cord. And you can buy this little adapter that you drop on to the end of your USB cord.

And it basically blocks the data and only allows the power leads through.

So you can put that on the end of your cord and you can use that there. Or the other thing is,

I have to travel a lot for family things. Like if you're on an airplane and a lot of folks are like, gosh, the airplane plugs are garbage.

So the easy way around that is there's two ways.

Either you buy a really short little three prong extension cord, which is nice because then your power port isn't always falling out.

And three prongs hold on really well to those. And actually, like when you have to go to a classroom or a doctor's office or something like that,

they hold on to the wall pretty well and then let your, you know, it's only like six inches.

That's like the one that I have. Or this sounds super goofy as well.

The international adapters work really awesome on airplanes.

so you just bring if you ever have one of those, like a UK adapter, you bring that and then plug it in.

So there's a couple ways around it that will prevent you from having to plug directly in.

But those little tiny data blockers you just type in USB data blocker on Amazon.

And let's face it, I lose one of everything.

So, you know, buy a couple pack, and then you can throw that on the end of your usb-C or USB adapter, and then that'll help.

And you can feel much safer plugging in. Does that make sense?

Okay. Sorry to jump in there. Good information.

Great information. Okay, let's see what time of year.

Okay. Let's move quickly. I'm going to go very quickly through the rest of these slides, because we have lots of other information to share with you.

So, next up is let's see, social media.

Yes. Be careful in sharing your information on social media.

We talked about your data being sort on the dark web.

If you've been a victim of identity theft, that information can be used to attack you and crafted to attack you,

to build identity where they attempt to build your, steal your identity.

Protect your primary email address. I'm not sure if you've heard about this one before.

So using your primary email address for trivial things that are not relevant are really critical to your identity or your personal life.

I wouldn't recommend that you use that. Just create, find another junk, even create another junk email address.

Use that for those things that are not really critical, but for your banking and other sources where they require you to use,

provide an email address, make sure you protect that and guard that more so than you would any other type of address.

Be careful what you click. We talked about that. And then backup your important data.

If you can, try using a cloud service provider rather than trusting that your device,

your data on your device will always be there will be the integrity will be there just to provide,

get a third party, external source if you can. Trusted source.

Recognize and avoiding phishing scams.

We kind of talked about this a lot, so I think I can probably skip over this unless you all want to walk through this.

But we'll provide this presentation afterwards so that you can walk through these.

But you hear a lot about this from us through the training that you received.

So I'm going to skip this slide. And a couple of other things related to personal devices.

When your webcam, the webcam on your, computer, your laptop, that device, you want to make sure you cover that when not in use.

Just another measure of protection. in case your device is infected with malware, that malware may be, recording,

information from your monitor or taking images of your face in your likeness.

Avoid public Wi-Fi.

We've talked about that. Deleting emails from individuals that you're not aware of, that you don't know, and also not clicking on links to it.

Attachments. We talked about that. Research data.

Your research data is very valuable. It is highly sensitive and others want it.

They want it and they will do whatever they can to take it.

So we want to ensure that you have the good information to, the knowledge to protect that data.

When we talk about research data here, we're pulling back to our university environment versus personal.

So we hope you're not storing your university data on your personal, your

personal accounts and other places that aren't authorized by the university.

So protect that data by ensuring that you have it backed up through a university approved storage locations.

Use strong passwords, which we require here. keep the software up to date.

And again, we talked about the storage solutions. And then collaboration with your IT teams.

That's a really important factor in helping to facilitate good technology support as well as security.

If you haven't done so, connect with your local departmental IT teams, your school, college, IT staff

they play a really critical role in helping to support you, to help you identify ways to better protect your research and your environment.

And they also play a critical role in ensuring that the digital security and the campus physical security of our campus environment.

So I recommend that you talk with them. They can help you.

They do many things to protect our environment, including blocking cyber threats and also ensuring the integrity of our network.

So if you don't know your I.T teams, get to know them. They're a really great resource and they're very knowledgeable.

Okay. Oh. All right.

So we actually had a lot of questions come in on artificial intelligence.

So we're going to touch it a bit. And then we'll come to some of the Q&A as well.

Best practices for using AI applications.

I'm going to stick a little bit more to the university perspective, but I think it actually kind of goes both ways.

And like I said, we'll come to a bunch of questions around that too.

So use university approved AI software.

Just to be blunt, we see a lot of software that's not approved by the university that's still being used.

A, otter AI, bubble notes, things like that

in zoom meetings. Those are not approved by the university.

And that means university data conversations, which are considered university confidential

and data classification is going outside of the.

Sorry. Outside of the university, which they shouldn't be going outside of the university.

That means it technically could be public data. which is not a good thing.

That's why we have zoom AI enabled, and we've gone through all of the data protection practices there.

Technically, if you have, advanced copilot license, you could use it for teams.

Most people are pretty clear that they like zoom better than teams.

But, you know, to each their own. AI one of the really important things, whether using it personally or here, can not forget your data.

Once you put something in there, it's there forever.

So if you say, gosh, you know what, I got this medical note from my doctor.

I want to know what it means. I want to summarize it so I'm personally at home.

Let me be clear. I'm personally at home.

So I'm going to go to the personal version of copilot or the personal version of ChatGPT, and I'm going to upload it and say summarize it for me.

All your information is now out there and it's theirs.

Full stop. You can't say. By the way, I'd like my information deleted.

I'd like that not to be there anymore. It's gone. That's it.

You sent it off into the cyber world. Now, the benefit about our instance of copilot here at the university is at least it's protected data.

So we're not putting it out there. So that's why we can use it for confidential data and what we call university public data.

So when we say, oh, I would like it to summarize this email or I'd like, I'm sending this email to so-and-so,

help me make it sound, more concise or more professional or more empathetic.

Sorry. There's a there's a study, actually, where they learned that AI, helped physician notes come across as more human readable.

No, it's actually really awesome.

There's some really cool research here, and they're trying to figure out how to make it work in medical practice,

but also be, applicable so the patients can trust it and say, well, that's not my doctor.

You know, there's there's a balance both ways.

I mean, there's some really awesome research that's happening both here and elsewhere around the country.

and then just don't put personal data in there, especially, especially outside of here.

Now, here, we're protected in our approved applications.

Let me say it again in our approved applications. Copilot.

Zoom. Those are the key pieces. If you use the advanced version or the pay version of copilot, that's covered.

The free copilot for here in the university as long as you're logged in is covered.

If you're not using those, you are not protected. That is a, that's a big deal and we cannot be leaking university information that way.

AI is cool, but it's not cool to really spread that.

And we actually have guides on using this and applicable ways of how to make it more useful.

out on the website and if you want more, hit us up.

We'll figure out how to do it. Or if you found a really cool way to use AI.

Let's figure out how to document that and put it out there for others to use, because there's some really neat stuff going on with all of you,

and the ways you're learning to use AI too that are way beyond the stuff we found today.

Okay. Protecting AI adversarial model.

So I got to meet with a group recently. So what will, why does it matter if I put my,

If I put my, medical chart data in there.

Why does it matter if I put university data in there? Because you can actually write prompts to get that data out.

To be able to to basically poison it and inject it to what they call poisoned, prompting to be able to get that data back out, to get.

If you think of the AI engine as a person to get it to spill its secrets, which okay.

It's kind of a fun game, but that's what, cyber adversaries do to get it to spit out.

The other kicker is, is if we're going to implement AI solutions,

we should be also very careful because by playing with the models and tricking the models,

because they're basically just very advanced scientific algorithms or mathematical algorithms,

you can actually get them to respond in ill formed ways, no matter what your questions are.

So you have to be really careful of that. And that's why I ethics and safety is now becoming a much larger thing, because, you know,

whether it's the airline that offered the dollar tickets or the abuse of chat bots or whatever,

you have to actually be really careful of these things. And then the other piece is when we look at it from a cyber perspective,

we have to look and try to break into these models and try to break these models and look at them over and over.

You can't just release something out, expect it to work and then never come back to it.

a lot of folks that think that's how IT works and that's not. Okay.

Transparency.

I think we really talked about this, but it's we have to be able to explain our models, audit our models, and ensure they're trustworthy.

So really, the thing you should know when you're using AI is.

Expect AI just like me. Just like you, to make mistakes.

Just because you're asking AI something doesn't mean it's going to be right.

You should always bring a level of skepticism to the table and say, all right.

And the best way to do that is ask it the same question a couple times.

You'll be like, what? You told me something else before. It's like talking to a teenager.

So I mean, it depends on the model too.

You know, as some companies are getting better about this by creating those, those ethics and safety groups.

But that's kind of how they're approaching it. So again, you know, the way at least we think about it right now.

And the way we're going into it is AI is an assistant. AI is not autonomous.

AI is not, does not have the steering wheel.

We're not using full self-driving here. That's a whole different story.

Okay. I'm going to flip through this because I want to get your questions.

Okay, so what does this mean?

See something? Say something. We're here to support all of you.

Right we are. And we have distributed I.T. everywhere, and we have central IT.

But we're here, all of us, to support all of you. So something looks goofy.

Raise it up. We'll help figure it out.

We might not have the most satisfying answer all the time, but we'll dig on it and we'll try to figure it out.

You should always feel, encouraged to report something.

And if anonymity is important, you can call one of us.

Leave a message to. If that's, like, an easier way to do it. Send an email, whatever it takes.

We respect that privacy as well. But. Just say something and we'll help you get through it.

Okay. These are resources. And again we'll send this out.

There's a whole lot of resources here. I think the most important thing we think about is continuous improvement.

So where you see gaps, where you see, you have ideas or where you, anything else just hit us up and we'll improve it.

Okay, so I want to go through a few questions, and just try to blast through these and make time for your questions as well.

If that's okay. And then I think what we'll do is create an FAQ site, so people can go out and refer to this.

So what's the best way to keep track of our different passwords?

I thought that was a pretty good one. So University hat on.

We have single sign on. You should have one password.

You should memorize that password. It's not on your desk.

It's not on a post-it. Please remember what that password is.

I'm sorry. We went to 16 characters, as Charlotte said, a passphrase is a really great idea.

It helps you remember it doesn't have to be 25 random characters.

Passphrases are really good way to go. You sprinkle in some different characters in there, and that helps you move forward from a personal one.

Now, I wrote this down because Charlotte is really nice and I'm not as much of that.

She said, please don't use the same password. I'm going to change that.

Don't use the same password. Don't use derivations of the same password.

Right? That is going to absolutely clip you when you're in.

Your data will be breached and leaked on the internet as soon as you start doing this identity monitoring and all of that,

you will be horrified how often your stuff is leaked on the internet.

Who does this right now? Just out of curiosity. Okay, one two, like a few people.

And, how many of you get basically leak notices probably every couple of weeks?

Okay, so those of us who monitor get a new leak notice every couple of weeks.

I'm going to give you a rough idea. I've got. I think right now in our family, we we have our family accounts.

We have 850 accounts, every one of them with different passwords.

All of them are 25 character passwords. And we use a password manager.

So. You may say, why would I pay for a password manager?

Because that's not manageable any other way. So think about it.

So if you have New York Times, New York Times Wirecutter does reviews on it.

Right now one password is there.

Recommended, whatever the heck it's called. You can go read reviews anywhere, right?

You type password manager best review on Google.

It'll tell you what to do. Like one password is pretty much the top one right now.

There's another free-ish one. LastPass used to be it, but they got breached, I think twice, maybe three times.

Not sure I would use that one, because that means you go change every one of your passwords, which doesn't sound like a good time to me.

Next one is use MFA. So here's why MFA matters.

Multi-factor authentication. If those get breached, at least you still have MFA covering you.

Right because somebody tries to log in. And this has happened.

When one of those is gotten breached, all of a sudden I get an MFA request.

I'm like, what is going on? All right, I'm going to go change that right away.

If you get an MFA request from something that you didn't request, you should go change that password right away.

Okay. Best way to keep passwords. What's a top priority for university

cybersecurity right now? So layers of protection is how we think about it.

And increasing the coverage of those layers of protection is what we're looking at.

And really the top two focal points right now are

Phishing attacks and how to better educate our user population how to prevent phishing attacks.

Because when we look, we've done phish testing. Our pass rate isn't where it needs to be.

It's actually really far from where it should be. And that's okay.

That means we'll get better at it. And what's called endpoint security.

So when Charlotte talked about anti-virus and managing computers and all of that, really boosting our endpoint security across the university,

those are two big pieces because we don't want people to take control of our computers, which then takes control of our network.

And we don't want people to take control of our networks, which then allows to take control of our network,

take control of our accounts, which then allows us to take control of our data in our network.

So really increasing those, which increases those levels of security.

Let's see, let me go to the next one.

Charlotte jump in too, what are the best options for dealing with personal data?

So you show up on one of those lists and you see your passwords been compromised.

Change your password. Change anything that was the same or similar.

This is like half of my family I've spent a full weekend on

changing all their passwords. It's really fun. Raise your level of vigilance.

So if you see anything that looks goofy, just go proactively deal with stuff.

Have monitoring services if you don't. And I want to think about that insurance because, you know, if they go after your

financial institutions it'll at least cover a gap, or you have to read the details on it.

and then to be blunt, oh, freeze credit and work with your financial institutions.

They should know what's going on. And then, I know I said this before.

Double down on your skepticism. Right. Oh, I got that email.

If it's too good to be true, it's probably too good. So just double down on it.

We talked about identity monitoring and mitigation.

A few examples of AI assists in daily tasks.

We kind of talked about this. You know, summarization is a really. AI does a, does an amazing job on summarization.

So if you get at a whole large body of text and say, hey, summarize this or summarize this concept for me,

like, I don't know about this concept, tell me what this means. Boom.

And I always say in bullet form because, I'm a bullet form person.

Anybody gets emails from me, they always get it in bullets because I don't know I'm anal retentive that way, but that's the way it works.

So it does a really good job on that. If you say please summarize what I've written, it'll do that as well.

Zoom does a pretty dang good job on summarizing meetings, as long as all the speakers are basically labeled.

Zoom has another nice feature that allows people that come to the meeting a little bit late to say, hey, catch me up.

And one of the other things that's really great for what we're doing with accessibility is you can have closed captioning on zoom.

It does. It's and now that they've added the AI features as much further ahead.

Copilot and ChatGPT.

I love this one. I kind of don't. But, ChatGPT is not approved here.

It's not. We can't secure the data yet. We don't have an enterprise agreement.

We're actually looking at it. They want you to basically license everybody, which.

We're talking millions. So it's not a priority for the university at the moment,

but we are looking at it to see if we can build a model to where people can buy into that chat.

The chat bot engine to see how we can do it, to where we can secure it.

Because there are there there are good differences between the two.

It's just we have copilot right now, and we're trying to negotiate with ChatGPT to see how we can do it in a safe manner.

Let's see how.

I think we covered them. Okay. What questions y'all have. Those are really great questions.

So the people who submitted ahead of time, I really appreciate it.

That was, I had to sit and think. I know Charlotte did too.

Go for it. Yeah. This is from online.

Okay. Um. What password manager do you recommend?

And I know you said that you can't specifically recommend any one.

Manager. Or can I ever solve for the work of people buying, or get recommendations?

Okay, so I can't recommend one on behalf of the university,

but I can tell you that I follow what the Wirecutter recommendation is, and I use, one password and I don't remember what the.

Honestly, it's really all that's kind of left after that, or after LastPass took a dive.

Although, you know, for people in the apple realm, with the new iOS and the new OS,

they've integrated password management with a lot of their biometric tools.

So folks may want to look at that, but that is that Apple specific.

I can't speak to Android. Okay. No problem.

Did somebody else have a question? Anybody else have a question?

Up. Go ahead. Is tap to pay any more or less safe than using a physical credit card.

So tap is more, is safer than using swipe.

I don't know. Is tap to pay like Apple Pay or Google Pay is safer than using card.

I would that it does encrypt it doesn't it?

And isn't. Yeah.

Yeah. Yeah. So I tend to use anytime I can because I don't like taking the card out.

And you know, they can't scan the stripe especially.

And it never leaves my hand. So like, there's a benefit, right?

When you're in Europe, your card never, ever leaves your hand, which is an important thing to make sure it's not skimmed or anything.

I always tap when I can, but in the U.S. at least.

Chip. Like. It.

It is secure. Okay. It's better than the swipe.

but if that's all they offer, Chip is fine. Chip is an older technology, but it's fine.

It's secure. Yeah, I think in terms of security, it's tap, then chip, then swipe.

We can look that up though. I think that's a really good question.

We should know that with PCA, shouldn't we? But I don't think our piece.

Sorry. we have to do what's called credit card compliance for our campus, but our expert is not here.

So we will actually add that because we can ask. Can you.

Can you stop by so we can reach out to you afterwards?

Okay. If you want to use.

So I haven't. I'm not using any AI right now on campus, so if I want to start using something, how do I start?

Like, how do I. You said you have to have a different kind of login or something for copilot.

That's not personal. Yes. So which we have the link on here, the links on I, I can send those.

So what we will do before we send these out is we will append on the resources page

right here we will append the AI link or the AI resources link to the bottom.

So you can go to that and it will talk to you all the way through how to login to that.

So that sounds okay. And it will show you how to ensure you're logged in.

So you're now and you're in the safe spot so you can get to the copilot chat bot.

Was there another? Oh, sorry.

That question was how do I get. Were you on the mic I don't remember.

No. Okay. Oh, you are okay. Thank you.

Have to turn it on. quick question, I so I received junk mails in my, you know, outlook folder from time to time.

And oftentimes the junk mails are basically the same content but from different addresses.

So, you know, you have that button where you can report or report phish or junk mail and you do that.

And so thank you for reporting. And the next day I would receive something very similar to the one I just junked or phished.

And then I would do the same thing and wash, rinse, repeat kind of thing.

Do you have any suggestions on being able to block similar content of junk mail as opposed to an address?

Does that make sense?

So is it in the summarization email that comes from defender that shows you have these messages that are suspected phish or suspected junk mail?

No, it's actually my inbox. Okay. Let's do you have one up?

No, I, I haven't actually received it in about a week or two, but all the ones that I've received, I have reported.

Yeah. So I just wondered, okay.

Like, as opposed to one blocking an address, it should be reducing those.

But we can take a look if you, let us know your name before we before you leave.

Okay. And we can reach reach out to you. Happy. Thank you.

Appreciate it. Thank you. We want to reduce as much email waste as possible. Wasted time on email.

So I'm totally with you. And you may have noticed, actually, a lot of you,

you may notice that there are emails that now come to you that say suspected high confidence phish or phish, or high confidence spam in your email.

And what that was is we basically turned up the detection settings on phishing, etc.

So yeah, that's called quarantine.

So basically it doesn't hit your email. And for the most part, I quit looking at those anymore because they're always spot on identified,

which means it just took that level of volume out of my inbox, which is nice.

And we should look to see if it's happening for you or not happening.

Hi, I have another question.

there was a slide about covering your, you know, camera when not in use, does that apply to university devices as well?

Is there a risk when we? Yeah.

So university devices you know I think this this is an important point that I don't think we probably clarified very well on the slides.

But university devices are to be protected by what's called defender,

on PCs or anti, or actually defender on Macs too which are anti-malware devices.

So that makes them considerably less, susceptible to anything like that.

I've seen some people that do cover their cameras and some people that don't cover their cameras.

I'm, don't care about my camera coverage person.

And then I know other folks that just use the post-it to cover it and other people that have the sliders and like Dell's,

for instance, almost all have shutters built in.

And I know that because most folks are like, why doesn't my camera work?

And then you show them that there is, that there's a slider on top.

I think most people here might have experienced that at one time or another.

So, you know, is it a good safety thing? Yeah, you can totally do it.

I. It's a preference, I think thing.

University computers. Yeah. For you, it's a thank you. It's a preference for university computers.

And I think the other piece is. You know, on the one slide we said back up your data.

You know, the important thing to remember about university computers as long as you're storing on

the university enterprise storage or you're storing on OneDrive, that data is backed up.

So it's not something you have to think about which, to be completely clear,

you should be storing on either one of those, or it's not actually insured or covered by university policy.

And that's why those those are enterprise storage, and they're actually backed up offsite as well.

If we'd have a major, catastrophe. Other.

Go ahead. Yeah, but time is off.

Is my camera. Does it? Do I still need to cover my camera? So if your laptop is off, off.

You don't have anything to worry about with regards to the camera.

And, uh. Sorry. Thanks. just throwing it across the room.

don't tell Anna. yeah.

So you'll be fine there. And again, if you, most Dells, for instance, have the shutter on the top, which makes it super easy.

Yeah. It plugs into, but I have, office set up, and I have a, no, it'll feed back to my hearing aids, and it'll be bad.

I'll repeat it. That's okay. So.

So I have a, uh. A thank you.

I have a docking station at home and a docking station in the office that I plug into.

Yep. I have my old laptop that I plugged in to the docking station when I'm not using my work laptop.

each of those has a camera, but then I have a separate camera.

Yeah, but as long as the system is off I'm ok? Yeah. That's fine. Okay.

Yeah. So the question was, you know, if you have a laptop with a docking station and a separate camera,

if your lid is closed on your laptop, you're fine because it's by default covered.

But you may decide to close the shutter on the external camera or just put something over it.

That's your choice. Any other questions?

Okay so this has been awesome. We're going to create FAQs

based on what we've heard. Do not hesitate actually to reach out to Charlotte or, I,

I probably won't be answering the questions, but we will find somebody to answer the questions.

No, but seriously, if there's more we can do, absolutely reach out to us.

Tthis has been really valuable, and especially to see the depth of the questions that have come in.

We really appreciate, the interaction here today.

So thank you all.