00:01

Good morning everyone and thank you for taking time out of your day to come and

00:05

Listen to what we have to say.

00:08

Our goal today, I'm here with Rachel Hayes, our goal today is just to

00:14

Raise awareness for you on email and data security.

00:18

share some tips and tricks, maybe, maybe some best practices things to think about. Um, and then were gonna leave time for any questions that you may have. So the topic today like it says email and data security training.

0:33

Alright. So today's agenda, we just wanted to talk a little bit about phishing emails, how you identify the suspicious email what to do, what not to do. I'm going to talk about securing your data and then we're going to talk about data security while traveling

0:47

Again, some tips and tricks that we want to share and some helpful links along the way.

0:54

So identifying phishing emails.

0:58

Pose kind of pose these questions, because these are things that we get quite a bit like how do I identify

1:05

A phishing or potential spam email. So one thing that I want to caution you all on is

1:13

If you get an email and you're like, I don't know about this, looking at the address that's showing and the from field look at the full address, not just the display name, but the full email address. There's a little example below that.

1:28

Does it look like a valid address. And so many of you were around last spring. And you remember the barrage of emails that were going around several different occasions, actually, that appear to be from our dean Carole Basile

1:44

In the display name it shown as Carol Basile so there was quite a few people that

1:51

Automatically responded to that email, because it came from Carole. If you take a closer look at that the email address that it was coming from had been spoofed and was showing CaroleBasile223@gmail.com and there was actually several different

2:09

renditions of this. So there was a few different emails that they were using for this. There were also some emails that went around that appeared to be from Punya Mishra, as well as Sarah Polaski kind of along the same lines, so

2:26

the other thing when you're looking at your email from your computer is pretty easy to see the full address that that's coming from

2:36

If you're looking at it from your phone. However, it's going to be more difficult. So if you're viewing. If you have outlook.

2:43

Installed on your phone and you're reviewing emails, you're only going to see the display name that it's from

2:52

If you are suspicious about an email and you want to see the full address all you have to do is just click on that person's name so I'm sorry I didn't include a screenshot or anything like that but

3:07

If I happen to go in one. I know you're not gonna be able to see this but

3:11

It's going to come up and it's going to tell you who it's from. It's going to show you like who it's too if you just click on that person's name right below that it's going to populate the addresses that are associated with that email. So just an extra

3:26

Layer for caution I guess for you to use.

3:32

When looking at that. So the next question is always, what do I do if I receive a phishing or a suspicious email. So the first thing that we want to tell you is

3:40

Do not click on any embedded links that may be contained in that body of that email. So as an example from this from these that we're going around, Carole. They started out by just saying, hey, are you in the office. And so people got that. And they were just like, yeah, what do you need

3:58

And then it went from there and ultimately what they were wanting is they were wanting somebody to go and purchase.

4:04

Gift cards in an electronic format and then sending those off. But there are other emails that will have links embedded that ultimately you can contain malicious material activity. And that's how through those links, that's how people get

4:24

Access to your computer to your files to your contacts to

4:29

credit card information bank accounts, all that stuff. So never click on any links that you feel

4:36

Are in a suspicious email. The other thing is don't reply to the email.

4:43

going that route and refer back to this email from Carole. Quite often, but if you do happen to reply, don't don't include any personal information such as a phone number.

4:54

You know we got a few instances where in regards to that email people would say, Yeah, I’m here call me. Here's my phone number. So now you've given out a piece of your personal information and your phone number, where now they can start

5:10

bugging you know harassing you calling you even trying to take out your phone, potentially. So just don't give up any personal information. If you do happen to reply.

5:21

Um, if you are unsure if the email is legit.

5:26

When appropriate or when possible call that person that it appears to be from the say hey, just got an email that looks to be from you. Did you send this

5:36

I know that's not always possible like again this example, people are going to pick up the phone call and ask, you know, Dean Basile, hey did you just sent me an email.

5:46

So it's not always possible. But really dig deep in and look at that, before just automatically replying, and I know when you get an email, especially with somebody names such as hers positions such as that you're, you want to be very on top of things and responsive, but

6:04

Just be careful. I can't say that enough. Just be careful.

6:08

Also included a couple of links, I don’t know how many of you may be aware that ASU does host a site that is specifically related to security it is named get protected in ASU or get protected dot ASU.edu

6:25

They have several different areas on there. It's a very informative site. So I will refer you to that. I also included the link that takes you directly to information on phishing and what you would need to

6:39

Be aware of what you can look at steps that you can take to report things. So we'll make sure we get this published out to everybody.

6:48

Okay.

6:54

Alright, the next piece of this is if you do get

7:00

If you do get a phishing email. We want you to report that. So how do you report back. So if I was to get an email from Carole what in that particular instance, you're going to want to report that email to

7:13

Folks that you to. You don't want to do that by just forwarding the email that's the other thing that I probably should have put in this slide it as a don't is don't ever forward an email that you feel is suspicious. Because when you do that you

7:32

You're further putting your you're expanding the vulnerability that's already there to others. So never forward that and I will go back and I will fix that in the presentation before we send this out.

7:45

Let me make a note.

7:51

Okay, so

7:54

The way that you would want to report it email is you want to copy all the texts that appears in the internet headers box and pasted it into a new email that you send to infosec@ASU.edu with the subject line of phishing email.

8:09

So down below that I've given us some information on how you locate the game, you know, Internet Heather's

8:17

Because it's different on using Outlook on Windows vs outlook on Mac and it's even different on other email applications such as Gmail and such. So I'm giving you a link to that, um,

8:31

The other thing that I want to make you aware of is if you do get

8:35

An email that appears to be suspicious, please don't hesitate to reach out and contact us because we can help you go through this process as well and

8:47

Once you reported the email. And once you've sent off to infosec@ASU.edu. What that does is that opens up a ticket with the security team at ASU.

8:58

They can take that information that is in that headers box and they will and research that and they will block the sudden they will be able to, in most cases they are able to identify the source of that email and they can block that Address

9:16

And then you would get a response on that ticket and we're working on a separate document as well that will have screenshots on exactly how to do this on each one on Windows and Mac. So we'll get that to people as well.

9:33

Before we go on to data protection and security. Do you guys have any questions on the phishing emails

9:41

Oh,

9:44

Alright, so I'm just going to look at a time talking about data protection and security. Um, one of the big things is secure your data. So the

9:53

First tip that I always going to tell people is never walk away from your computer, your phone or your tablet without locking that screen so never walk away with your screen just open because if somebody comes in behind you.

10:05

They have access full access to your system and ultimately you're the one that's responsible because you're the user that's logged in, you're the person that's going to be held responsible for any malicious activity that was

10:19

That could potentially happen.

10:22

So always lock your screen.

10:25

And the other thing is when you're working with data don't store sensitive or personally identifiable data on your computer, all that data should always be stored in a approved.

10:39

ASU.

10:42

Storage system, whether that be Dropbox OneDrive a secure network drive. There's a multitude of storage of options out there. That ASU offers

10:54

If you have questions about the storage of giving you a link in here to an HR data handling matrix.

11:03

And if we have time, we can pull that up. But basically, this takes you out to a Google document.

11:09

That UTO has put together and it will tell you the source. So if you look at Dropbox. If it spans wide and it will tell you, can you store personally identifiable data can you store.

11:25

Credit card data can you store HIPAA data is going to tell you yes or no or whatever the limitations may be so some of these may be approved.

11:34

To store if with approval of IRB. Some of these are not approved as storage systems for certain types of data. So it's going to be important that you know the type of data that you are going to be working with and needing to store.

11:50

If you're working with this type of data and you need to store on your computer for a specific reason.

11:56

As soon as you're done with that delete that data. Get rid of that data. Same thing goes on if you're storing this data on on one of this to approve storage methods, if that data can be replicated.

12:08

Again, and you no longer need it for this particular project. You don't know when you're going to need it, again, get rid of the data don't store it on even on secure methods don't store that longer than what you need to. Okay.

12:22

Also you want to make sure that your device is encrypted, which all issue equipment is encrypted before it's handed out to anyone for to sign to anyone.

12:32

So you should not be working with sensitive data, you should not be working with ASU data on a non ASU computer. And I know that's going to open up questions in regards to like student workers and all of that. And we need to handle those on a case by case basis. Okay.

12:57

I'm thinking about the audience.

13:02

Most of you in the room are not going to be working with K 12 students or parent data, but there is a level of awareness that needs to be there for researchers and faculty members that are

13:12

Maybe partnering with a school district or on a specific project related to that because K 12 has its and each district is going to have its own

13:24

Policies and procedures for that type of data. So they would, we would just be for faculty to make sure that they're going above and beyond in securing that type of data.

13:34

Um, the other area of security that we wanted to talk about a little bit is the security review process for software and hardware purchases

13:43

As many of you know that ASU has implemented the requirement of a security review for all software and hardware.

13:53

For all software that includes paid and free versions of all software and we have to go through a process to understand how are you going to use it. What type of data. Are you going to be using with the system.

14:07

How are you going to be using the system like how many records are going to be in there because if for some reason that was breached we need to know how many people will need to be contacted um

14:20

There are different levels of US software security review. Some are not as involved. Others are very involved and basically what drives that is

14:32

Not only the type of data that you're going to be using within that system, but also does it integrate with any other ASU systems such as canvas or maybe a PeopleSoft or another system such as that.

14:48

On the hardware side on it does. These are required for most of hardware. The exceptions are items that

14:55

Get cannot operate without another device such as a mouse or keyboard and as technology continues to evolve many systems are smart devices now so

15:06

We really have to look at what's being purchased and why it's being purchased and that will again drive that the type of review that has to be done.

15:16

Security review request can be requested by sending an email to edops@asu.edu and I've listed some information with what would help us.

15:26

Work through that review in order to get to an approval level. So the purchase can be completed.

15:32

You can also work with your business office contact of these items because they will reach out to us, letting us know and and gotten this request and does this data security review, etc. So that's another resource for us.

15:49

All right, at this point, I'm going to toss it over to Rachel Hayesand she's going to talk to you about data security while traveling

15:57

So,

15:59

Data Security with traveling. I think that

16:02

To tell a story first before we get started, as why this is important. There was a different unit that was working at and any issue.

16:11

And kind of work one day and everything was just a bus away and I didn't know what was going on.

16:19

I found out later that we had a faculty member that had visited a country that was a sanctioned country. And it was found out later that

16:33

It was highly susceptible that he had shared data with people that he should not have, the result of that, though, was that ASU took his computer and they kept it

16:49

Didn't matter what was on there, they needed to see everything that he had access to everything that was involved, anything that he could possibly have shared with other people, while traveling

17:01

And so, as, as I continue to work in research, I, I get concerned about those things, especially when we're traveling globally, or even just traveling in general, it's good to know.

17:15

What we can do to secure our data and what processes we probably should go to before traveling to a country that's overseas.

17:24

So the things that I like to talk about today are identifying the sanctioned countries. So those are countries where securities have been in place by the US government. So that would be do not share

17:37

Data with them without approval. I'm going to share with you a link to go ahead and get two steps for control wizard. So you can put in the information that you have. If it says that you're supposed to reach out to us management and you do it says that you're okay. Then you can travel

17:53

Without having any extra approvals.

17:57

Kelly brought up the Go get protected. There's a couple of things that I'd like to share from that website that also talk specifically about travel

18:06

And other responsibilities that you have personally, you are being mobile and they were good tips, not only when you're on business, but also for personal reasons as well so

18:22

So this is a link and a picture of the page that brings you to the US Department of Treasuries sanction programs and country information if you will be traveling or if you know any faculty that will be traveling

18:38

It's kind of good to check this list, it does change and it is updated. From what I understand,

18:45

And if it does show up, then I would highly recommend that we have some sort of conversations or you know do again some extra digging to see what we need to do to keep ourselves protected.

18:56

The next slide will show you a link to going to do the export control wizard, and this is on our research integrity. So this is sponsored by orspa and you would put in your information.

19:10

And it will tell you exactly what your next steps are. And I said it was a sponsored by orspa. The, the link the main link is worse, but they do direct you to the research integrity and insurance.

19:24

Oria is what they are called and you can also contact them by phone at any time. If you have any questions I've spoken with the ladies there.

19:34

And just as a note. They were super helpful.

19:39

They we talked. I talked to on the phone with Kelly with them. So we had brought up the different scenarios that we see within our college

19:47

They felt that, again, that that was the data that we put for us in the college and nothing would be to the extent that we need to get expert approval beforehand, but it's just good to be aware of these things as as our as our after we've reached out farther across the world. So

20:07

Next slide. This is the get protected building mobile slide. And as you can see there's a bunch of different

20:17

Things that you can look at with any here. It is very extensive as as Kelly mentioned. And that's the link that we will be able to share out to you.

20:25

Some things that I do want to point out, though, that are specific that would be probably very helpful is on the next slide. We can see those things. So

20:35

Things that do stand out for your electronics is to make sure that you have something that's encrypted ahead of time. I remember not too long ago and ASU put for us

20:47

To make sure that we were using using your phone's you kind of have an encryption. If you're an Android, I think they said that Apple automatically encrypted. So there was nothing there. And, you know, if you're going to be

21:02

If you're going to be using things, just think about how how hackers can get in there and you know they're getting more and more creative each time. And as Kelly mentioned before, remove the sensitive data that you don't need.

21:17

I don't know if any of you have been in a position where you've lost your phone or you know people that have lost your phone even on a personal level, and oh my goodness, what happens when you think about all the pictures that you lost or wow you know I had that saved on there

21:33

Face links again. Oh, absolutely. You know, I mean just it causes so much stress. So if we remove those things, then that those are things that we can easily recover at a later time if if your devices are stolen or to lose them from them in the trash bags.

21:53

Things out of my travel and then one of the one of the main things that I know that we do not do.

22:01

That they brought up that I felt was really interesting is to take a loaner or an alternate device that contains no data and can be wiped afterwards.

22:12

I know our faculty take out their laptops to go ahead and work on their plane when they’re at the hotel and they're doing different things. And so I don't know how how

22:23

how happy they would be about coming in to get a loner and saying, Hey, I'm alone I'm out a laptop. So I want to take my own, but that is something to go ahead and think about that. That is an option that's available.

22:36

To us to go ahead and keep, I guess, I guess, the greater conversation is to make sure that we're keeping those things, not on the main computer itself, but in the cloud that you can reach and then always use the VPN when connecting

22:50

Next slide. And another slide, I'm going to talk about hotel travel. And I think that that's really important if you are in a hotel or if you're at the airport or at the cafe. Those are not secure

23:02

Internet sites, which means that anything that you do can be seen by whoever is running those sites.

23:13

Or those those connections and. So something to think about is if you are in an airport or if you're at a cafe. If you have haven't logged

23:23

If you haven't downloaded the Cisco connection. I think that that would be something you might want to reach out to your to people about today, you can get that onto your computer, but I highly recommend that to keep everything safe.

23:35

And we will continue to move along. What happens if things are stolen.

23:42

So I'm going to back up just one second. No, it's fine. My thought process is going to back up on my thought process.

23:50

We always are talking about putting your travel request put in your travel request put in your travel request.

23:54

And why is that so important because if you are on edge to business and something were to happen to your body.

24:04

To your personal belongings. We then have the capability of getting you medical attention evacuating you out of the place that you are at

24:17

We have the ability to make sure that if you are on insulin, we can provide places for you to get that medication if you get hit by a car.

24:28

You can go ahead and use ASU’s insurance if you are being if your back pocket stolen and you have a cell phone that belongs ASU, a laptop that belongs to ASU, we can put in a

24:45

I lost my train of thought, we can go ahead and put it in a request to get that that insurance and insurance claim to get that recovered. So with about that that is leaving not only you yourself, your body, but also your belongings.

25:01

At risk. And so then I come to this if something does happen. If your laptop or if you have a another device that belongs to ASU. I've had to email.

25:12

The information security office which Kelly previously they will submit a ticket, they will get the process going. I would also recommend that we email the business office that we can also

25:23

Track what it is that you know find those security or the serial numbers that are attached to those devices so that that's just my thought to

25:37

So also that good protected the mobility side, one of the things that stood out to me beyond anything else I i remember attending and training.

25:47

And that training provided me access to a lot of personal information across the university. And one of the things that have had enough spider man sitting there and, you know, with great power comes great responsibility.

26:03

The data that we're keeping the information that we have

26:06

That holds great power. And I think the thing to think about is that it is everybody's responsibility to keep this information, safe and secure and confidential, regardless if we are working in the data.

26:19

Itself, or for working with parents or children or even our co workers, just to be mindful of that.

26:27

And so one thing to do in case you're not quite sure where your data falls into ASU’s security, there is a

26:38

Matrix link that I saw the Kelly had one of her slides. But within that matrix link, it has, you know, refer to data handling standards and this is the link that that refers to it.. It gets you to those Google Doc.

26:52

And within this Google Doc, it defines the different classifications of information that we have an ASU, and also provides standards or requirements that we have for handling all those different

27:08

Classifications so that'll be something that you can read over as well just to say, Okay, you know what, where does this fall as far as you know vulnerability and you know how, how, how, how powerful is the data that I'm using. So

27:28

And then just the last little slide here, there's just some information that is also available that I'm not going to go into great detail about, but it does give you

27:40

Information on using the Wi Fi at public locations, which again I come back to the using the VPN.

27:48

It gives you a checklist for your mobile device. So once again, we talked about making sure you have things encrypted, making sure you have some sort of pass code to get into your phone. So it gives you a nice set of checklist, they're

28:05

Going to be very interesting and I looked it up even have a link to the FBI business travel brochure that is very interesting. I

28:15

found it interesting to look at some of the stuff that they were saying in there so that that might be something that

28:22

Again, or share with others. And then it also gives you another checklist on what to do, is comparable storage devices security. So how many times we travel around with

28:31

Flash drive or comments or backpacks with our key chains. And so those are things to think about. Like power. We keep secure and with that

28:43

If you have any questions, we encourage you to email the Eops@asu.edu will be checking that for any security related questions and follow up with some sort of ways to get you to to the answers that you're looking for and

29:05

I suppose at this moment I shall end with do we have any questions