RAW Cybersecurity Training Webinar Transcription

Not quite a minute, but I guess now's as good a time as any so we'll go ahead and get started today.

So I'm kicking everything off.

I want to welcome everybody to our first webinar of the Year.

This is going to be a regular occurrence.

We're going to do be doing these typically the last Thursday of the month

unless otherwise stated we felt like the best way

though to kick off 2021 was really to seduce some baseline cyber

security awareness training hence the discussion today.

Now there are a number of people may be on the line today who have

been through similar trainings either with us

or otherwise and then there are those individuals that have never been through this

so we welcome all I'm sure that there are things that can be Revisited here

and just some handy reminders and best practices.

And for those that have never been through any sort of training like this.

Hopefully this will get you up to speed

and provide you with a good solid foundation on cybersecurity

what it is and what it means to your organization and best practices.

What you can do to ensure that you do in are adhering to the highest standards

when it comes to cybersecurity at least within the best of your ability.

So getting things started today,

my name is Chris Montgomery. I am the director of sales here with throttle out who the

organization now going on about a decade this year with me on the call today.

I also have AJ Roger she will be Fielding our Q&A.

So if you guys do have any questions,

please feel free to any of those questions in the Q&A section of our Up,

and we will do our best to answer those either

as we go or towards the end and if we have to get back with you on something,

of course, we will as we outline our agenda for today.

We are going to be covering a number of things first

and foremost are going to talk about the state of cybersecurity going into 2021 essentially

outlining why it is that we are doing this today in the first place.

We're then going to talk about most common types of cyber attacks

and some security definitions not necessarily in that order.

General best practices and how to safely browse the internet

and securely check email and then we'll wrap up with any questions that might be out standing still

or we will talk a little bit about how throttle that can help organizations to address some

of the needs that you're going to be reviewing this morning.

So in kicking things off, let's talk a little bit about the state of cybersecurity right now

and 2020.

There was a new ransomware attack roughly every 14 seconds

and they expect that to them being roughly every 11 seconds going.

20:21. So needless to say that is why it is

so important that organizations have here to good best practices

as it relates to cybersecurity the weakest link in any network chain is typically going to be the

use so if the users can be updated

and and aware and educated on exactly how to protect their organizations from outside attack

and what to look for in the event of a phishing attack Ransom or attack or otherwise,

they're going to be much better prepared to deal with those issues

as well as to get ahead of them before they really create some problems for the organization.

Cyberattacks overall have cost organizations ten point

two billion dollars in victim losses reported.

Now, there's a very specific reason at that word reported is an italicized print.

That's because a lot of these things go unreported.

We're going to talk about that momentarily,

but all those that have been reported ten point two billion dollars has been

reported in losses due to things like ransomware attacks

and Bad actors compromising the networks that are out there that are organizations

and other organizations.

Use so we can go through and talk corporate data breaches personal data breaches credit card fraud

and everything else and a lot of this is coming in obviously through email accounts identity theft

and investment fraud,

but our core today again is going to be really just around.

How do we securely surf it on the internet

and how do we identify phishing attacks via

email and in general as far

as business email speaking of which what you're seeing here is a pretty substantial increase.

In the amount of losses due to business emails being compromised.

That's why the vast majority of our discussion today is going to be around email

but again fraudulent transfers a money

as well as obtain PII personally identifiable information that can be used for future attacks.

As you can see here essentially since about 2017.

This has been on an upswing with a bullet to say the least one from 5.3

billion all the way to twenty six point two million.

Now industries that are consistently under attack When I Was preparing for today's webinar.

I'm not going to not going to lie. I was a little surprised by what I found here.

I always knew that finance and Healthcare were consistently and constantly under attack.

However, we talked in terms of those two verticals.

They are typically subject of third-party governing body specifically financed through the SEC

and the cybersecurity checklist that they have assembled

and Health Care through HIPAA

and the different cyber security requirements that HIPAA puts in place to ensure

that your personal Healthcare Phi information is protected.

So it was a little bit surprising to see that Manufacturing legal and construction.

We're also in this top five, but if you think about it,

it shouldn't surprise anybody when you talk in terms of manufacturing.

I work with a number of manufacturing companies in the st.

Louis area and in working with them I could tell you that they could tell you

for every minute they are down exactly how much money that is costing their organization in output

and productivity because of that.

That's why it's all the more important

for those organizations to get back up and online quickly at actors understand this.

They know the ramifications

and the potential cost to manufacturing facility and they figure will be a quick transaction.

So these are organizations that we probably want to Target

when you talk in terms of legal or law firms in general and a lot of cases.

They are small or you know, five ten fifteen user firms.

They don't have the same protocols

in place as a larger firm might have

but they're still dealing with pii personally identifiable

information Social Security numbers names date of birth all that.

Staff that if a bad actor were compromised a server or network and collect that data.

Obviously that could be used at a later date

for attacks against those individuals that the data was collected around

or more specifically to be have it then

for resale on the dark web and then finally with regards to construction again,

very similar to manufacturing. You have a lot of folks that are out in the field you take down a

network you've put a construction firm pretty much at a dead stall

and as a result they are.

Probably going to be willing to do whatever it is that you ask

as far as remittance payment

or otherwise to get their organization back up in online as fast as possible.

Now, why don't we hear about more attacks in the small in the SMB space in general?

There's a variety of reasons first off.

It's not really news worthy. I mean, you know Channel 4 channel 5 Channel 2 is typically not

looking to report on a Cyber attack that occurred within a law firm

or a financial services company here in town unless that firm was a large,

you know, multi-state multinational company of some kind or unless it was a large retail.

Organization like a Target Snooks year Birds those organizations.

You always hear about it, but for the run of the mill,

you know, what comprises 89 you spent percent of the businesses out there and your SMB space.

It's just not newsworthy and it's not really going to see itself,

you know, getting a lot of reporting in addition to that is really embarrassing to admit.

I mean, nobody wants to admit that they were compromised

and I can understand why there

were so many things that can come with this whenever something like that occurs.

For example, the pr is an absolute nightmare.

Obviously, you do not want to get this in the paper on the news

because the clients and organizations

and individuals you might do business with they catch wind of this may have serious

concerns around exactly who they're doing business with.

So again, the pr is just an absolute Nightmare

and as a result of that then you potentially have legal ramifications and the next thing you know,

we potentially have somebody willing to take you to court

because they feel like their day Information may have been jeopardized

and that was a hundred percent on you.

So as a result again, you typically do not hear about these things and they go unreported now,

why is that well for the most part people in the SMB space just

don't think it's going to happen to them.

They feel like look they are coming

in and targeting a very specific type of client and that client is not me.

I have got 10 or 15 employees,

you know, I do five ten fifteen twenty million dollars in gross annual sales or in business.

Yes, and at the end of the day, that's really not who they're targeting you're looking.

Well, you're right. They're not directly targeting you

but as we talk through some of the definitions and different types of attacks that can occur.

They are still targeting you but just in a different way in addition expensive.

Okay, they look at it and say well, you know what?

How much is it going to cost me to make the investment needs additional security features

and functions the hardware the software whatever might be required

and in so doing is that going to outweigh You know the investment that the potential

for something like this actually taking place.

So again, there is a cost associated with it means how you put in place strong security measures.

You are potentially looking at increasing your spent in order to do so and just like Insurance.

It is one of those things. Where do I make this investment

and feel confident that if something were to happen?

I'm covered but it's always going to be a balance.

You know, those the investment outweigh the concern Vice.

Versa, so again, it makes sense as to why folks.

Look at this way. We want flexibility,

you know free and inexpensive and you want unrestricted resources again,

I fully understand but as an analogy

or as a discussion I used to have when I used to be in a different industry,

which was very specifically the security industry residential

and Commercial alarm systems back 20 years ago.

One of the questions that I would ask folks

and ever they would tell me that the competitors come in and giving them the alarm system for free.

Is how much Faith would you put

or do you put in anything to receive

for free and the reality of it is the answer was almost always will know Chris.

I mean it was free. I would never put that much stock in something like this

and when it comes to your network as a business,

you don't want to use free Solutions. If you can help it they might be finding the short term

for a smaller organization.

But as the organization grows, you typically do not want to use free Solutions.

You want to get in in place best in class or enterprise-grade.

Ins that are typically going to have some sort of recurring

or one-time investment in order to get that solution in place.

And then finally trust that your IT company is providing you with

everything that you need to protect against cyber security

or I should say to protect against Bad actors and cyberattacks that said we as an organization,

of course, we have firewalls in place. We have antivirus in place.

We have ransomware detection mitigation Tools in place.

We have a lot of Tools in place to assist organizations

and preventing attack identifying

attack or eating attack or over the case might be

but there is no 100% foolproof scenario where you put together.

This is the package once we overlay this you are completely

and totally protected from any Cyber attack

or bad actor attempting to compromise your network because at the end of the day,

even if all these things are in place,

you still have the people element associated with this.

This that ultimately can compromise your network unknowingly.

And once again, that's the reason we're having the discussion.

We're having today, so 46% of smbs have been targeted by ransomware

and 73% of those have paid that Ransom

and cyberattacks now cost companies about two hundred thousand dollars on average.

So once again all the more important

as to why we're having this discussion

as far as just a general case study of an organization a small Law

Firm that was actually affected by a ransom

or attack this firm.

All I actually had crowdstrike come in to investigate the ransomware infection

and Covered this I know crowdstrike has been in the news because this was from 1 December of 2016.

And I know that in the last year or so, you've heard different things about crowd strike.

But either way they are still reputable organization.

And as a result they do do some some Diagnostics

and forensics what they found was this organization have five million encrypted files.

They pay 25,000 dollars plus in Ransom.

The backups were corrupted because any time a ransom or attack occurs.

Typically, the first thing they're going to do is go out

and corrupt or encrypt the backups to ensure that the

organization has no place to restore from they were down

for two weeks again,

I don't know of a lot of organizations out there that could

survive two weeks of being just completely

down and dead in the water and finally based on how much data they had to restore.

It took 39 hours per terabyte to restore everything and get them back.

Back to even again hence the fact that it took them two weeks to do.

So. So again, this gives you a pretty good idea leading up to our next phase of discussion

as to why we're having the conversation today what's going on in the marketplace

and the reasons that organizations need to be concerned about cyber

security and potential for Cyber attack.

So we're going to save way off now to security definitions.

I want to provide you guys with a just a general understanding of

just some general definitions around security

and we're going to talk also about Different types of attacks that

occur in the with the one that we see most common.

So we talked in terms of definitions. We're going to start with encryption.

Okay, essentially. What encryption is is you have

point a and point B this being you the user let's say and wherever the network or whatever it is,

you're communicating with happens to be located

as that information for versus

back and forth you want to make sure that data is fully encrypted

as it goes back and forth with this.

Does is prevent somebody from essentially inserting themselves in the middle

or listening into these conversations and as a result lean that information.

So again encryption is just the act of everything being encrypted in a certain way

or it just looks like gobbledygook

ones and zeros or what have you

as it goes back and forth in turn not offering up any personal information financial information

or otherwise data Integrity ensures that

as this data is going back and forth in this encrypted state is that it's not corrupted.

Okay, the data is it has good solid integrity

and if the data is not being manipulated managed

or changed in any way shape or form as was traversing back and forth.

Authentication is that process of identification is you are who you say you

are so you go out to a website you go out to your banking or financial institution.

They want to authenticate are you in fact the individual that you say you are.

So again authentication protects against man-in-the-middle attacks

and builds the trust between the user

and the organization that they're actually communicating back

and forth with and then finally to factor otherwise known as multi-

factor MFA authentication.

Okay, two-factor authentication is something that you are going to see

more and more of and you're going to see more

and more organizations beginning to adopt multi-factor authentication for those that are not aware.

You've seen it you've used it you probably use an everyday

and don't even think of it in these terms multi-factor authentication can be defined

as using your thumb print scanner on your phone that could be a for multi-factor authentication.

It could be the facial recognition feature on some of the different.

Current iPads and Apple devices that are out

there for people to be able to login in addition the old RSA tokens.

I haven't seen one in years,

but I'm sure there were some on the call today to remember

what I'm talking about that every 30 to 60 seconds to change the number

and whenever you go on you have to key in whatever number was up at the time.

So again, multi-factor authentication is a way a redundant way

if you will or a secondary way to identify you are in fact who you say you are.

I'll find a way that I see it happening is text message.

You know, really? I log in to my website

or something along those lines

for my bank and they send me a text that I then have to key in a six digit code that

they provide random that then identifies that I am.

In fact who I say I am. So again,

you're going to see more and more of this

as time goes on because this is one of the primary ways people are

securing against Bad actors in cyber attacks.

Now, what are some of the most common types of cyber attacks?

I'm not going to bore a with a bunch of these

but but will scan through a handful

but we'll get down to the real meat and potatoes things here towards the end on these.

So you'll hear these thrown around occasionally a denial-of-service attack is going to be

one where the system that you're logging into Network whatever it might be is convened

completely overwhelm the system resources been overwhelmed

and it can't respond and basically a shuts everything down prevents it from doing everything

anything and freezes everything in a point in time man-in-the-middle attacks.

This is where we talked earlier. About encryption

and data Integrity is that data flows back

and forth that prevents against things like man-in-the-middle attacks.

These are attacks that occur again,

when a hacker inserts himself in between the user and whatever it is,

they're communicating back

and forth with and then in turn gleaning information off

as that individual is communicating

back and forth password attacks two different kinds a Brute Force

password attack really just means more of a random approach.

You notice it. In there and essentially going through

and trying different password combinations based on things like a

person's name their job title things along those lines things.

They may have picked up over time to ultimately try

and figure out exactly what that username

and password combination is going to be and then there's a dictionary attack.

This one is one that you know is a little bit more complex in nature.

It's basically using a dictionary of common passwords to attempt to gain access,

but then there's also a way where you can kind of Bounce This dictionary off of other things

and do a compare and contrast

and that's going to filter out some potential username password

combinations that a bad actor might be able try

but the ones that we typically see are going to be Brute Force attacks things along those lines.

So an example and why Brute Force attacks are

so simple is that even eyes the sales person could go out hypothetically looking

for email addresses and I can type in three

or four different combinations of email addresses just guessing

and inevitably Probably 80% of the time I'll find it out there somewhere on somebody's website.

So again going in and Keen in the manipulating.

Those things can ultimately result in a Brute Force attack.

And again, that's an easy thing that we can overcome.

We talk a little bit more about complex passwords

and some of the things we'll get into around best practices.

Later. Eavesdropping the tax these are where they're basically listening in again.

This is why data integrity and encryption is so important again,

it's prevent somebody from eavesdropping

and listening in conversation as that information for versus back and forth drive by a tax.

We're going to talk about this today

as well. These are typically attacks that occur unknowingly to the user

because they go out to a specific

website and they end up Contracting some sort of a malware infection without even

clicking or doing anything

and we'll get in that in a few minutes here

as to exactly how that occurs it can also occur

when somebody downloads things from a site that has been compromised

and usually those sites are compromised in large part

because the user or I should say the hosting organisation

or the organization the business that actually has that website

has no idea that that code has been compromised

and that results in things that a lot of us are familiar with which our malware

attacks now we're attacks occur again via Drive-by download

but they can also occur when you go out.

For example, like I have in the past where I went out to download a specific font,

when I downloaded the font with it came a bunch of other minutiae

and then when I went to get online the next time I have pop up,

once you pop ups coming up and everything else to the point that I could even see my screen anymore.

So again, that is a form of a malware attack that ever occurs.

It's a very easy fix and easy to clean up at the end of the day can be a real pain

while it's actually going On spear fishing

and then finally regular fishing

and I really want to talk about this one

for just a couple of minutes

because this is the one that people really believe is it is what's happening to them.

So when they say Chris it can happen to me what they Envision is.

There's a guy out in the parking lot or there's a guy sitting in a basement somewhere in dark room,

and he's just decided he's going to Target XYZ company

and he's going to go about collecting as much information about them.

Them he's going to start scraping the bottom of the barrel just really get

deep into this organization to understand how they

operate and better understand exactly

what they're doing and these can be very hard to identify

because the end of the day these fear phishing attacks the ongoing

for a very long-standing period of time again,

this I think is what comes to mind for a lot of organizations and business owners.

Is that all you have there's some guy out there with directly targeting.

Here's what I can assure you

for your small to medium-sized businesses

and less In financial services or otherwise chances are pretty low that that's what's happening.

What most people are subject to is the next iteration which is just a general phishing attack.

Okay General meaning that they are just sending out

as many emails as they can with attachments

or links contained within hoping that somebody will click on it

or do something with it and ultimately get caught up in their net.

And as soon as they do that's

when they start interacting

and engaging with those jewels in organizations and ultimately that's when the problems occur.

So again to be abundantly clear spear phishing is an organization

or an end up bad actor that is targeting organization very specifically

and going in and investing a lot of time doing research in attempting to gain

access to that Network in some cases gaining access

and just sitting back and collecting data over a long period of time

or as a phishing attack or going to Target our discussion around today is very Broad in nature.

And can apply to anybody and is probably the most common type of attack that we see out there.

So before we get off into best practices,

I'll pause for just a moment here and make sure that we don't have any questions.

It does not appear that we do

so we will continue to move on here and to how to safely and securely use the internet.

All right, so in getting things started here first thing we want

to do whenever we're out on line is we always want to make sure Sure,

especially if we are communicating any Financial

or personal information or data that you are in a secure website

whenever you do that your banking sites are always going to be secure.

Most of your payment sites are going to be secure.

So again, you want to make sure that you are in a secure site

every time that you're communicating back

and forth with any data that if it were to be compromised could cause a serious problem

for either you as a user or

for the entire organization itself that said the To identify this is you always look

for the ask the end the HTTP

when you look at your address

bar or you're going to see a padlock typically somewhere in the browser window.

It's going to be to the left or right of the address bar may be down in one of the corners.

But again, make sure that you are on a secure site in addition of the abundantly

clear if you're ever on a non-secure in Secure site

and you want to make a purchase on that site where you want to transact in any way with

information that is of age of a secure of a personal nature make sure that they offer

a secondary option to make payment

or submit that data.

So for example, if you're wanting to make a purchase usually sites,

they're not secure one through something like PayPal use PayPal use

that as an option when you're making your purchase

because PayPal is going to take that out of their sight to a secure site

for your transaction and then back to their site to complete

it but none of that is happening within their insecure or unsecured environment.

Browser ads essentially pop-ups.

Okay. That's what we're talking about here. I don't

see as many pop-ups as I once

did but again pop cups or something that can be very malicious in nature.

They can be in some cases just a form of malware

or they can be pop-ups that occur on specific websites that

you might visit we would always encourage

folks if they can a try not to interact with these if you can help it

but more importantly put in place some sort of a pop-up blocker to block those Coming up.

It's been my experience that typically when a pop-up comes up,

there's usually not a significant amount of benefit to it.

However, there are those times

just so folks are aware that you might be on the financial side

or something along those lines where you have to enable pop-ups

just for that site in order for a login pop up to prompt or something along those lines.

So there will be instances where that's the case,

but we would always encourage folks to use Solutions like you bought

or Adblock Plus 2 block these pop-ups from actually occurring and cause a potential problem.

Varying your passwords. I have done a number of these trainings over the years.

I can't even really tell you how many times I've asked the question

which is how many folks use the same username

and password across all or multiple sites.

They visit inevitably the number of hands that go up in the room

or in direct relation to what the studies show

60% or six out of 10 individuals use the same username or password.

Nation across all or multiple sites,

they visit that means is if a bad actor were to figure out your username

and password combination for one of those sites.

They could in turn have that information

for every single site that you visit and obviously that could be a major problem.

So make sure to very those passwords. Now

what I hear consistently and I understand because I'm in the same boat.

I can't even begin to tell you how many usernames and password combinations.

I have just for email that doesn't include just trying to get into my phone.

All the different accounts that I have. It is absolute Insanity.

So what I would do is encourage people to do is to look at a password Vault like LastPass

or - Lane the nice thing about these password vaults is that a they

give you the ability to store all your passwords

and once secure location that you can access with 1password

where you can access with just a thumb print scan

or something along those lines to get in in addition those Solutions can also create passwords

for you and the benefit to that is Is that

what you in a position where a lot of cases you won't even know what the password is.

It will just pre-populate in advance using that solution.

They do have browser plugins as well that in the event you're online.

You can also access the same password Vault

and it will pre-populate your username

and password in those different sites that you visit in which case they have the information.

So again, that is one way to kind of manage what has become a bit of a management nightmare,

which is how many accounts do I have.

I'm going to use a names I have how many passwords do I have

and you're telling me I have to vary all of these if I've got 20 or 30 of these.

So I feel like I have that is almost impossible and I understand that.

So again leveraging a third-party password Vault application is always going to be helpful in that

regard and being creative with those passwords again,

making sure that they are complex in nature

what I mean by complex is they usually are going to have a capital letter.

They're going to have a number they're going to have a symbol those are the

kinds of things that Make it a complex password.

But in addition to that Studies have shown that you typically want to have a password.

That is at least 16 characters long in order

for it to be at the highest level security

and limit the potential for the password to be compromised or cracked.

All right. Now how do you create a complex password that 16 characters

that you're ever going to remember in my experience?

What I have found is the things like movie lyrics song lyrics are see a movie line song.

Eric's I tend to use things like positive affirmations

so that way when I start my day and actually log into my computer,

I have something nice to say about how the day is going to go.

So again, you can do any of those things.

But when you do it make sure that it's always start with a capital

letter that has all spacing in between each word.

And then it has proper punctuation at the end.

This will allow you to achieve a complex password that is easy for you to remember going forward.

So again, make sure though the real takeaway here is that the

password is at least 16 characters long

and then includes a capital letter if ideal if it can a number

and a symbol and in some cases I'll see people do is I'll use like the letter

e and turn it into a three or something along those lines.

So again, that's practices make sure it's 16 characters are more make complex.

Do not use autofill. Okay autofill can create a variety of problems largely

because this information can cash.

Your PC essentially be stored on your PC.

And in the event something is compromised.

You could find where those passwords could be located by an individual or a bad actor.

So as a result again, this comes back to either leveraging you third-party

solution like last past help you remember those passwords

or pre populate those passwords because again,

if those passwords are stored locally on the machine,

it can cash and as a result of that cashing it could be compromised in the future.

In the event that machine itself will be compromised.

Do not click it. This is one as we click through here.

I know everybody is seeing this. Excuse me,

go ahead of myself with these pop-ups.

If you ever see this happen, this is most likely a malware infection of some kind so when it occurs,

first of all do not interact with these pop-ups,

if you think you're closing it by clicking on the Red X up in the right-hand corner the folks

who have come up with these have gotten smart enough to know

and they just basically anything that you click on within that window is going to start Actually

causing problems downloading something in the background otherwise,

so if you ever have an instance like this where you're getting pop-ups

just because you're online you need to really pretty much just shut your browser down

and if you're a man and services or just any client of throttling it reach out to us,

we can remote in and clean up that malware infection or whatever it is.

That's reside in their local desktop laptop or otherwise to get you back to even again,

but again, that's your takeaway here is do not run this

we as an organization provide all of our clients that are on our

managed Services Program with an antivirus

and malware and spyware solution

and is not going to pop up like this asking you to run a new updates

or telling you that you unprotected.

We monitor manage and maintain that solution for you in real time.

So again, I say that because don't ever think that it's also our solution

and is popping up is inevitably a malware infection of some kind that is creating problem.

Couple of other tips just be safe

and just be sure that you pay attention

when you're on a search engine

as to what the results are that you're clicking on

and always keep an eye out for shortened URLs numbers,

hyphens and special characters stuff like that.

What I would tell most folks is this when you're out doing your research online,

we in the u.s. Here familiar with things like.com dotnet Maivia dot TV or got Moby.

These are all here in the United States.

States however, if you're out online

and you inevitably come across a site that's dot edu dot a u CN those

types of domains those are from overseas.

And that is typically where you're going to have problems like the drive-by

downloads that I talked about earlier things along those lines.

So if you're ever in a situation like

that and you're doing some research

and you happen to come across a site and you notice that it's a DOT C in dot EU or otherwise,

see if you can't locate the information. Shouldn't L.

Swear. We do provide some filtering

or at least protection against that forearm

and services clients prevent them from going to malicious websites that have been blacklisted.

But again, there's never a hundred percent guarantee

and we would always encourage you to get your information domestically as opposed to going abroad.

Okay, so that gives you guys some general ideas on just best practices around getting online

going out visiting websites how to vary your passwords how to interact

and engage online and what you should be paying attention to but again,

you do have a fraction or a portion of Bad actors

and cyber attacks that do occur just through General online browsing

but the vast majority really take place

as indicated in the earlier slides outlining the launch

into compromise business emails through email.

So that's what we're going to say way off into right now take a look here

and see if we have any questions does not appear that

we do so moving on we will talk then about how to identify.

It attacks when using email

so we need to establish before we go there with social

engineering is our in a room full of 50 people

right now able to ask by a show of hands with social engineering

is but since I'm not although I can do is really provide a definition.

The best definition that I can give are examples of social engineering makes a lot more sense

when you know what it looks like

as opposed to just the definition

what happens to be examples of social engineering Nearing

would be you're in the middle of a really busy day

and your phone rings you answer the phone and on the other end of the line.

The individual says hey, I'm Chris Montgomery.

I'm with your IT company. I'm doing some updates and patches today,

but for whatever reason we don't have your password on file here.

Can you give it to me real quick again?

You're busy. You're trying to get on with your day.

Yeah. It's abc123 anything else.

Nope. That's it. Great. Thank you. And you hang up?

Okay, you don't even know who you talked to.

All right. You were just hurry. Ross they were taken advantage of this fact,

they knew full well that you had a lot on your plate that you weren't going to question

it and as a result,

they now have your products. Okay, another example in more of a physical sense

would be you come walking up on a large building you you work

for a company that employs two

or three hundred people and

as you approach the building its card access only

so you come up you swipe your card

and right behind you as an individual holding a whole stack

of boxes that can't get to their key card

and they say would you do me a favor

and hold the door for me and I am My hands full

so you go up you hold the door for them you let them in and you don't you think well,

I'm just being courteous.

But at the end of the day, you don't know if they were authorized to be there in the first place.

You don't know if they actually did have a key card.

But again, they were taking advantage of human curiosity.

So that's what social engineering is. It's taking advantage of people's curiosity

is taking advantage of just them being respectful to others.

It's just taken advantage

and just general human nature and using it to their advantage in a bad way.

Final form of social engineering that we see out there,

especially online or phishing attacks.

Okay, and that brings us into why we're talking about phishing attacks today

and how to identify them.

So when identifying a phishing attack,

there are some pretty telling signs that most likely this is not legit.

Okay one step sign is the from address is odd now,

you'll see over here to the side that this shows

as Rackspace but what it also shows is this this Weird info dot

912 so on and so forth when you would expect it to maybe say info at Rackspace.com

or sales of Rackspace.com.

All right. Now the reason for this is this email address has been spoofed.

So on the surface it appears to be from Rackspace.

But if you hover over the address, you're going to see a completely different

address that is one of the easiest ways to identify

whenever in question or in doubt whether or not this is a ransom or attack.

So my point is is that if you can go out In your questioning

whether or not this is from it who it says it's from just hover your cursor over it

and it will actually show you the actual email address if that

email address looks like a hot mess like this

and chances are that is not actually from Rackspace is from

some sort of a bad actor trying to compromise

and secure some data inevitably.

There's going to be some unprofessional punctuation again

A lot of times these are performed overseas.

So as far as how they are communicating to be slightly different

and as a result that is Is usually a tell there are a lot of times errors in the

grammar of the capitalization is off Punctuation is off.

Something's just a little odd about the way that was written There is

almost inevitably a link to an external website

or there is an attachment one of the two

and then finally there is going to be the use of a threat to promote an immediate action.

If you don't do this and this case within 24 hours,

it's linked won't work anymore. The one ones that I've also seen is,

you know, we're trying to reach you to collect money.

And if you do not click on this link within the Amount of time some sort

of legal actions can be taken against you.

So again, there was always some use of threat to promote action on the part of the user.

So in talking in terms of just some examples of

what we have seen over the years one is an example is would be one with an attachment.

Okay, and this case what they're trying to do is to prompt me to click on the attachment

because it says see attached the payment report from to funds Express.

We would see this or somebody might see this and say oh,

this is a payment. I need to make sure that we look at this.

Maybe I should forward this on to accounting

and then that point now it takes on a life of its own because they look at it and go.

Oh this must be legitimate. It came from somebody within the organization.

So if you ever get something like this take pause

for a moment and think who is this person and why would they be sending me money?

And should I really click on this attachment

or should I just go ahead and disregard it and go ahead and sleep this thing altogether.

I would encourage you to just Believe all together again that attachment

is when most of your problems are going to occur.

So if you can avoid clicking on it at all costs by all means do so.

Another example would be what you see coming from trusted sources these days.

I mean, let's face facts. There's there are some people I hope not on the line today,

but there might be a few you know,

that haven't been out much or the last nine months.

I'd say most of us haven't been out much

or last time on so I wouldn't do for a night of the concert or something or a movie right now.

I can't even begin to tell you

but because of that we are using things like am On ordering a lot more online

or using services like FedEx USPS and ups and over result.

We are constantly getting updates from these organizations on the status of our purchase the status

for shipment all that stuff and as a result,

it's very easy because you're getting

so much stuff these days via these VIA mail and through different carriers.

Just go ahead and click on the link that they send you

or click on whatever attachment they send you all.

Ultimately, that's where the problems can occur these Bad actors have gotten very good at taking

what you see on the screen here from FedEx UPS USPS

and otherwise and creating emails that look identical to those that you would normally see

for an update on tracking or otherwise with the idea.

They know full. Well you are receiving a lot of stuff in the mail

or via these different carriers

and then inevitably somebody's going to click on that link to

see what the status of that respect and purchase happens to be And then of course,

that's when your problems are going to occur. So if you receive something like this,

I would always encourage folks go to the website itself.

He in the information. They're the tracking information that you

have and do the tracking through that in addition.

And as most know in order for you to get tracking updates,

you typically have to say that you want them.

So especially with USPS FedEx and UPS.

You have to actually click on it. I want these types of alerts.

I want to know when it was shipped. I want to know what the transit status is.

I want to know what was delivered. I want to know where it was delivered all that good stuff.

You typically have to go in

and choose those as well as

what form of communication is going to be used to notify you text messaging or via email.

So again, if you have not done that

and then you get an email like this we can pretty much rest assured that's officiants hair

and you want to avoid it at all costs.

So again, I would always encourage folks if you're ever going to need email like this.

Take pause do not click on the links

or attachments the men go out to the website for that organization,

Keen your tracking number there

and get your information directly from the website because we know that's a trusted resource.

Okay? Phishing attack from overseas.

This one again is why I talk about being conscientious

of what the domain or the address is

and I realize that this is an older one and it seems pretty easy to identify,

but I have it up here for a different reason. First off is that I wanted people to see the dot C.

And because again, you see the.com dot CN s coming from China.

I think you're goes without saying especially when you see the characters that are on here.

That's most likely coming from somewhere in Asia in addition to that.

Excuse me. And the reason I always bring it up here is because people ask the question.

Well, why don't you just block it? Why don't you just put it up there

and block it all together with your spam filter,

otherwise and the response that I would give to that is I can't because they used numbers here.

I tried to block this thing more times than I can count

and every time that I did they would just change one digit

and obviously numbers go on for Infinity so they would go from at 8730 328 7:30.

For 556 3738 and this can go on

for Infinity now eventually it just stopped

but I got one or two of these a

day and would block it every time

and inevitably it would resurface again with just a slight variation

and email address that it was sent from.

So again, there are times when it just doesn't work.

Okay largely because they're using numbers

as opposed to just a standard domain name using letters that you would normally see.

This is one that I hear about more often than I'd like to admit.

I've actually got an example towards the end here of somebody who tried to do this with me.

In this case. It's where a phishing attack requesting a wire transfer

or gift card request inevitably.

What they're trying to do in this case is is that they are collecting information

or they are trying to get you to take action and see what you'll do and listen,

let's start the conversation.

Once they have somebody engaged in the discussion at that point what's going to happen is Then

they'll start to engage you in the process of doing the wire transfer to

them as opposed to an organization that you may have thought it was going to in the first place

in addition how you could tell hypothetically at this was not legitimate is my Kyle is the

president of the Congress CEO of frontal map.

So if I saw this and just saw the name,

I would say, oh, it's from Mike. I mean, of course I can help him.

Here's the thing. If you look at this in more detail,

you'll notice that it are named throttling that is spelled.

Thr o TT e l NE T is opposed to Ellie any tea.

So again the way that our minds work

and I know that people have done this over the years you tend to fill in the blanks on

what you expect to see so that's why it helps you to take pause

when it comes to these things take a moment to really look at the email that it's from,

you know, notice the slight variations in the characters

that at first glance might appear to be fine.

But at the second look, you know, wait a minute something's not quite right about this so Yeah,

that's how these things happen and then tough folks get compromised.

Now this is the one that's attempting to gain information for a future attack.

Okay. So here's one where again now it looks very legitimate.

I mean my cat fraudulent.com that is his email address.

Okay. And in this case, he's asking me I need you to take care

or he was asked I need you to take care of a financial obligation for me today.

What do I need? Okay.

This is what they're looking

for account numbers routing number so that could be credit card numbers,

whatever it might be. Be so again you ever receive an email like this pick up the phone

and call the individual that it's from and make sure that they in fact requested this information.

Now, here's the rub these Bad actors have figured out that you're going to pick up a phone

and call to find out if this is the information that was requested or not.

And they're even going to say in the email do not pick up the phone

and call to find out because you know what?

I'm in the meeting all day.

Don't heed that, pick up the phone

and call. The reason I always encourage this

because I do not know any business owner on the planet who wouldn't rather pause

for a moment and take that call to verify

and confirm who they are as opposed to you take an action taken the company AMEX

card by $2,000 an Apple gift card scratch them off

and vitamin to an email to a bad actor.

So again take the time make the call make sure it is Su they say they are

and that this was actually a legitimate request that was made.

And now to save way off I'll give you an example of how incredibly Petty these individuals can

be and how much they just will not give up.

Okay, right before the holidays right before Christmas.

I actually had somebody try to do this gift cards TM on me.

All right, they pretended to be George Rosenthal George is actually on the call today.

George is the president of throttle map.

But as you'll see here in the highlighted area.

Yeah. I came across the stores Rosenthal

but it was from manager executive

12:10 and Gmail.com they were just goofing George so that hopefully I wouldn't pay attention to it.

Now as I was having this conversation. And since I knew out of the gate,

this was not George. I got a little snarky with the guy his first thing you ask me

for is to sell my cell phone number and of course I come back to him and tell him you know,

what I've worked here for better part of a decade

and it's really insulting to me that you don't even have my cell phone number.

Okay. I think I'm just going to quit. I don't want to work here anymore.

He goes into apologies and tells me I'm sorry is I tell them still that.

I'm quitting. And I tell them you know what it's okay,

man, you know, I've calmed down now, you know,

I went out for an afternoon happy hour now back to my desk.

I think we can get this done today. What do you need?

Okay at that point. Oh,

I need a gift card from you. Oh great.

Okay, that's fine. I can get you a gift card.

That's no problem. You know, but I'm busy what can I do for you?

And then from there he asked me to go out

and buy a thousand dollars in two hundred dollar increments of Google Play gift cards come back

and basically take pictures of them and send them over.

Of course. I didn't question that because well,

I just don't get I can't I can't do that.

I don't have any money in my bank account, you know,

what reimbursement stuff so he goes so far as to say to me.

What can you do? I tell him a hundred bucks.

He doesn't care. It's like great.

Can you arrange that for me the next 10 or 15 minutes?

I'll take the hundred dollars. So again, they do not care what the amount is.

They just want to start the conversation and even $100 is Nothing at all.

So as we continue we pretty much just end with me divulging the fact

that we are in fact a cyber security organization

and at the end of the day,

I know exactly what this individual

is doing and all that I can hope is that I prevented him from doing it to somebody else

because this went on for about three

or four hours of us going back

and forth at the end of the day he disappeared never to be heard from you.

All right a couple last items ignore unsolicited links in Al's so again,

this comes back to that idea of any time that you receive an email with a link

or attachment contain within avoid it at all costs.

So in addition to that do not log into accounts were either a link

was received in an email on instant messaging

or social networking.

So for example, you don't see it as much anymore but on occasion,

you might get a message from a long-lost high school buddy that you haven't talked to in years,

but some sort of article you really don't have any interest

in but they think that you do

and then when you click on the article The pop-up comes up that says hey,

I need you to login to view this you're already logged in in the first place.

Why would you need a login again? That's

because they're willing to collect that data that information right username and password.

Why because they know on average 60 percent of the population

is using the same username password across

all or multiple sites that they visit

and they stand a pretty good likelihood of figuring out your username

and password combinations for other sites.

You might visit. So again, if you're already logged into a site

or otherwise don't go Go back and log back in again.

Just recognize that as most likely some sort of bad actor out there trying to collect

or glean data from you.

And as a result, just go ahead and close it out about the last thing you can do there,

especially on social medias send a quick message back to your friend and say hey,

I think I've been compromised a quick fix of that is just changing username and password again.

Once they do the problem typically just goes away altogether,

okay. And then finally do not fall for it.

Okay, I have had these calls made to me on more than one occasion here at work.

I've had them at home, but they are inevitably the same.

It's a call from Microsoft tech support saying hey,

your computer is doing some weird stuff.

So we're reaching out to you today to see if we can't remote

in and resolve whatever the issue happens to be.

Okay. The reality of it is Microsoft is never going to reach out to you.

You to do a scan of your computer

to try and identify problems

or anything along those lines

for anybody on the line today who's ever called Microsoft for technical support,

you know full well that you're going to be on that

call and on hold even at two in the morning probably for a few hours.

All right, the likelihood that just one day they've gotten

so far ahead and call Q that they are now proactively reaching out to all of their users,

which is pretty much a danann 90% of the population is pretty low.

So again, if you ever get a call from somebody In to be from your helpdesk

or claiming to be from Microsoft hang up.

Okay, if they say the from your help desk in your throttle neck client.

Say listen, can I call you back? What number can I reach you at?

All right and then call back

and you will inevitably be able to find out pretty quick

whether or not that was a joke legitimate call or not.

Okay, so that gives everybody some ideas on best practices at

least 12 around how to safely surf the internet

as well as how to identify phishing.

Tax and how to safely and securely check your email

as well as some additional items on top of that around

what you should or should not do and a few calls from Microsoft tech support or otherwise,

so as we wrap up here and hopefully it's been beneficial for our Bay on the line today.

We'll just cover briefly that of course we can help at any point in time.

If you ever have any concerns about any of the things that we've covered today,

we most definitely helps give us a quick call toll-free at eight six

six eight to nine 55 57 we've been Than happy to

assist in addition to that how we help organizations out there in the

marketplace is through a variety of different

solutions than we offer everything from managed Services.

We service the full-time it department

for an organization providing you with antivirus

and malware and spyware Solutions backup checks remote maintenance monitoring management

and much more.

We also of course provide hosting Solutions

and Standalone cyber Security Solutions such

as mock phishing attacks get your users to to identify these attacks

when they occur and to give them additional training

whenever they come up as well

as things like enhanced Advanced threat protection through spam filters

and a variety of other different solutions and services that we offer as organization.

So in closing here and I see we have a couple of questions and I'll dress those in just a moment.

We if you ever have any desire to learn more about us,

of course check us out online at throw them in a.com

or once again even call us today 668 to 59 66 another number that we use on a regular basis

and we are more than happy to help with any needs that you guys might have.

So as we wrap up here, we'll just take a quick look at the questions here.

Looks like one question that we had came in was is there a certain way to remove a suspect email

or can it just be deleted so build answer your question.

Just delete it. Okay. Now when you delete it,

it will go into your deleted items. You have to delete it from there as well.

But again the only way that it's really going to cost. A

problem in most cases if you interact with it,

so don't click on any links don't click on any attachments

and definitely don't do what I've seen people do in the past

which is don't forward it to the company

as a live link and say hey,

this is a phishing attack don't click on that's just inviting people to click on.

So again an easy way to do it is just delete it

and then delete it from your inbox

and there was no likelihood

or probability that's going to be so hopefully that's given you an answer.

That one aside from that.

I don't think I have any other questions only take a look here.

Looks like anything else that I'm getting is just tips

and tricks on how I can improve my webinar going forward.

So these are all be heated going forward.

Again. This is our first one of the year. Unfortunately.

I have a lot of sun come in. I think it's washing me owl that on the screen.

So I apologize for that. But I can promise you

as I'd said these will continue we will be introducing these every the last Thursday of each month.

The next one is going to be on active directory. After he's okay.

This is going to be a pretty important one for those individuals and business owners out there.

They're not familiar because we're going to be talking about is how active directory which

ultimately dictates who can access your network is being compromised these days

and what you can do about it to protect against it.

So so without further Ado we will wrap up here today.

I do appreciate it on behalf of George AJ and myself.

We certainly appreciate you participating today and joining us.

And again, if you have any questions needs or anything else feel free to check us out online.

Line at throwing that.com. You can email us at sales at fraudulent.com,

or you can get us on get us on the phone. Again 866 826 5956 on once again,

I think for your time today,

and I look forward to seeing you again here in a few weeks to talk about active directory

what you can do there in the meantime.

I hope you have a great day.