-So without further ado,

let me introduce Courtney.

You know, we've been partnering

with Microsoft ever since,

really, I worked at AARP

on various things,

but we've never had a better

relationship than we do now,

and I think a lot of that

is due to Courtney Gregoire

and the Digital Crimes

Unit, which has really

made fraud prevention,

fighting these tech-support

scams, a top priority.

And Courtney comes to us

with a lot of experience.

She's worked in Washington D.C.

for many years.

She is a Court Commissioner,

which I didn't,

until recently, realize,

and is now an

Assistant General Council

for Microsoft's Digital

Crimes Unit.

And more importantly,

I can tell you that I call

and talk to a lot of

U.S. Attorneys and AGs

around the country.

They all know her.

They all, "Oh, yeah, Courtney.

I know, sure.

I talked to Courtney yesterday,"

you know?

She is really on this

is really passionate

about cleaning up this whole

business of people not trusting

or trusting their computer

and the tech-support world,

so please help me

in welcoming Courtney Gregoire.

-Come on up,

and we'll get you going.

-This is legitimate tech support

by the way.

-You know, here I am.

I'm working on a mic

without thinking,

"You should be doing this."

And did somebody

steal the clicker, Chuck?

Oh, no.

Wait.

Here it is.

There it is.

All right.

You're all set.

-Thank you.

Thank you.

Well, it's a pleasure

to be here,

and it's really a pleasure to be

here with some great partners.

The AARP, the Washington

Attorney General's Office,

BECU, and of course, Chuck

in the Federal Trade Commission.

Before I step into some of our

online safety tips and tricks,

I wanted to share with you

a little bit about why

I have one of the greatest jobs

that I could possibly have,

and that is my responsibility at

Microsoft's Digital Crimes Unit

is to fight cyber crime

that is impacting

some of the most vulnerable

across society.

So first and foremost,

I do some work

on our online

child-exploitation front,

and I get to focus

on chasing down these folks

who are engaged

in tech-support fraud.

Let me tell you, I'm hoping

Chuck shared how tremendous

of an announcement

we had last Friday,

and this is...

I know I'm speaking to a room

who is not engaged

in this behavior,

so this is my notice

to the criminals out there.

We're coming,

and here is how we're coming.

By collaborating with law

enforcement,

Microsoft's Digital Crimes Unit

is able to take

an individual report

that a couple of you give us,

and run really smart data

analytics and machine learning

and say, "What is the pattern

and practice here?

Have we seen

this phone number before?

Have we seen

this website before?

Can we scrape what these pop-ups

are looking like out

in the wild out there?

And by using that

smart-data team

that I get to collaborate

with daily,

we can collaborate to make

the big impact of last Friday,

in which 16 new actions

were filed by Operation Tech

Trap, where seven individuals,

I'm very happy,

are facing

federal criminal charges,

including a prison term

for wire fraud, and guess what?

If you didn't think it was

important to report

before I spoke to you,

I hope you understand

why it's really important.

They will see longer sentences

specifically

because they were victims

over the age of 55.

So I love what I get to do,

and you can help me

ensure that we can make

the impact

by doing a couple things.

One, sharing your experience

with us

on our online survey form.

We want to encourage you

to report

to law enforcement directly

and tell us at Microsoft

what happened.

This is, of course,

you're going to tell us

everything that happened to you,

and then you're going to hang up

before you lose any money,

or you're going to

disconnect your computer

before you lose any money,

but I still want

that information

so that we can go after them.

We're also going to take that

to build that into our products

so that our products

are safer for you,

so our products block

those pop-ups

before you see them,

so that we know how this pattern

and practice can change.

And lastly,

on the education front,

which is really what I want

to focus with you on today,

and how you can share what's

going on with your friends,

your family

and best protect yourself.

From a Microsoft perspective...

Really,

from an industry perspective,

we've been focusing

on tech-supper fraud

because it's really concerning

when folks give access

to their computer,

or their smart phone or

their iPad over to a criminal.

Let me just be perfectly clear.

You may see that 300 or $500

that they stole from you,

but you don't see what

they've dropped on that device

to come back and try again,

or what they've taken

when they had remote access

to ensure

that they can come to you again,

and that's personal

identifiable information.

At the end of the day, I work at

a place called Digital Crimes.

We talk about this

at Cyber Crime,

but you've heard

from folks before.

This is the same scheme.

They've just changed the script.

They are trying to get

information out of you,

and they are trying to dupe you

by scaring you into believing

your computer is at risk,

your device is at risk.

So we want to talk a little bit

about regardless

of how they come at you,

it's that same scheme.

We are receiving some 10,000

customer complaints per month,

and we are using smart data

to figure out

how to go after those folks.

They come in because someone

just called you on your landline

or your cell phone,

and I am one of

those lucky recipients

of about a tech-support

call a day or two.

That tells you they share

that information.

They share it in the dark web,

and once you're on their list,

it's very, very difficult

to disconnect, so be vigilant.

We talk about web advertising.

This is if you happen to go

to Bing or Google,

wherever you do your search,

and if you went and searched

for tech support,

how are you going to know

that's accurate?

This can happen from e-mails,

and it can happen

through chat as well.

So when we're talking

about cold calls,

particularly in the tech-support

fraud space,

they may try to make

a connection

that sounds reasonable.

They may say they're calling on

behalf of Microsoft,

or Windows, or Apple or HP.

They will try to give you

a piece of information

that they have totally made up

to see

if you will illicit and share,

"But I use a Dell computer.

But, actually,

I use an Apple computer."

They will them pivot,

but believe me,

they've taken that information

down for future use.

They may ask for your e-mail,

credit cards.

Those are no-nos

and non-starters as you know,

and we definitely want

to discourage from that.

I need to just highlight,

Microsoft

Support does not call you

to tell you you have a problem

with your computer,

so that's easy, and that's why

you need to be very, very weary

of any of those phone calls.

The lens I say is,

"Did I seek out help?"

You know, if you actually had

sought out help,

then they may be calling

to follow up,

but then they'll have

a very specific information,

but if you get this call

out of the blue

and

you didn't initiate it, hang up.

Here are some of those

big red flags.

They don't know your name.

They have those

vague descriptions,

and I'll be honest,

I'm an attorney,

not a software engineer,

so if they say

they've got malware

or a zero-day,

that's still vague.

And it sounds like gobbledygook

to me sometimes,

and it will sound like

gobbledygook to you.,

but that is not specific,

and it is not specific

to be addressing your issues.

They'll avoid answering

questions when you say,

"How do know that?

How do you have access

to my device?"

"Oh, Microsoft does that."

No we don't.

The bad phone connection,

primarily because it's usually

an international calling center

that's the back up there,

or they may ask you

to call another number,

and that is a nice new tool

they're using to make it

a little harder for those of us

who are on the trail

to track how they are operating.

So the real thing,

you solicited the call.

They know who you are.

They have either

a customer ticket number,

and they will clearly

introduce themselves

and it won't be confusing.

It's not going to sound like,

"I'm Windows Defender,"

which is a legitimate service.

If we're Microsoft Customer

Support,

we're calling to follow up

on your conversation with us

at a specific time

with a specific number,

and we, by the way, are just

Microsoft Customer Support.

That's clear.

So we'll talk a little bit

about web ads,

and this is when you've

gone out on the web

and

you've searched for something.

You could be searching

for tech support.

You could be searching for

that warranty on your computer.

You could be searching

for any type of information,

and we all know those

search engines are great,

but you also need to know

that folks have the ability

to promote their services

in the background there, right?

They are paying money to be

in the auction

to have their search results

be top and center.

Bing, very clear.

You do not get to bid to offer

Microsoft Tech Support,

Apple Tech Support,

HP Tech Support,

unless you are Microsoft,

HP, Dell.

That does not mean they won't

show up on there,

but they should not be

the most relevant,

and we will clearly

identify where we are.

Web ads are really

challenging sometimes

because they will

be disguised as promotions.

I find more often

they are threats.

Beware this malware virus,

call immediately,

and so the first question

I have

is what should you do

when you see this?

What looks like

an anti-virus alert,

and I want everyone to think

a little bit about this,

and now we'll talk a little bit

about the red flags.

See, what's challenging here

is that anywhere in that box

may activate

what they want you to do.

It may take you to their URL,

and so even though

they've given you

these nice buttons,

more options or close.

That close, which is green,

which makes you want

to go there.

It's their code.

They're intentionally

sending you to somewhere

they want you to go

that you don't want to be,

and so we absolutely want...

The best thing to do,

but I know this is hard,

is to hard close the browser.

Get out of that browser

and start again.

That green X box up there

is usually safe,

but is not longer

a fail safe,

so we really do encourage

you close the browser.

They want to direct you

to a URL.

They want to direct you

to their website,

and that can trigger downloading

additional software

to your advice, etc.,

so be weary of these alerts.

So the most common thing

we're seeing right now,

and I actually want to give

a little bit of the backstory

because I think

this is interesting,

is these pop-ups tell you

to call a phone number,

and I'll be very clear.

Microsoft Customer Support

does not

deliver information like this,

and our Customer Support

does not tell you

to call a phone number.

It takes you to an online tool,

so this is really just

a lead-generation device.

They are just trying to

get you to call,

and then that fraudster

will take you.

What I care about saying

to this room

is this is just the next

evolution of the same scam.

The tech-support fraud was cold

calling for several years,

and we were really

tracking that.

What was interesting

is just last year, last summer,

we went out

and did a global survey

in 12 countries

around the globe to ask,

"Have you had experience

with this tech-support scam?"

And the answer, two out of three

people had had some experience.

They'd seen a pop-up.

They'd gotten a phone call.

They'd seen something.

One in five had continued

with the fraud,

but what was really interesting

is that because of this shift

to pop-ups,

Millennials were being taken

at a higher

than our senior citizens.

They trust those devices.

They live on those devices,

and they just executed

without thinking,

and so we are seeing

this evolution,

and they are continuing

to make these pop-ups

more sophisticated.

So as I was mentioning web

search.

You want to be very thoughtful

when you think

about search-engine results.

They can feature

third-party ads,

and we do everything we can

to ensure it's crystal clear.

Where is the legitimate answer?

Where is the legitimate

Microsoft Support?

Official support information

is prominently displayed

in both

Bing and Google here,

but you do need to continue

to look and pay attention.

In this example from Google,

you know, Microsoft

Support's legitimate information

is really high up there,

but there's a box on the top.

A box that says it's an ad,

right?

There's a nice yellow,

"This is an ad."

That means it was paid for.

It is not an organic

search result,

and you want to be

a little skeptical about that.

The other things are, really,

you know that this is typical

in fraud,

overly-complicated descriptions,

overly-complicated titles,

or what we call it,

a URL that doesn't look

just clearly

Microsoft and Microsoft Support.

So you want to look at those

because,

again,

this is another mechanism

where they are trying

to get you to their website.

So there's a legitimate

one here is green.

There's no ad tag.

There description is official

and very, very clear,

and you want to be vigilant

throughout this.

I am proud to report that

after we, last year,

took a policy change at

Bing informed by that great data

work that the Digital Crimes

Unit can do, Bing blocked

17 million tech-support fraud

ads from being entered

into our search results,

but that tells you how many

there are out there,

and how they are

highly incentivized

to continue to try

and put information out there.

So e-mails.

This is a significant challenge,

and one where you want

to honestly be

as cautious as possible.

You hear a lot about

cyber crime these days.

We hear about attacks

are are sophisticated.

We talk about malware

and viruses.

The reality?

Seventy-five percent

of cyber crime

starts with a phishing e-mail.

These criminals are very,

very astute.

They may try to find information

to send a phishing e-mail

that looks relevant to you.

It's from an organization

you're a member of.

It's from an organization

that you have publicly stated

that you support,

or it may look like a friend

who unfortunately has had

their credentials hacked.

And when I say 75 percent

of cyber crime

starts with a phishing e-mail,

that happens everywhere.

I'm not going to give you

the citations about

how many Microsoft employees

have fallen victim,

but it's common.

So we want to look really hard

at these e-mails,

and you want to look

at these e-mails.

Phishing e-mails are often

disguised as office newsletters.

They are claiming, "Just enter

your information

to make sure your

credit card keeps working,

to ensure your

Microsoft account stays open,"

but we really want to look

at some of these key elements

to detect a fraudulent

e-mail or website.

I'll go through these

visual hints,

but let me be perfectly honest.

You can get rid of this e-mail.

You can separately go seek out

Microsoft Customer

Support and see

if you need help.

Your credit card,

phone call or e-mail.

I hang up.

I call back on my own terms

and start re-entering

into my account

on my own terms.

That is the best

and most secure way.

You want to be on the look out,

and you want to report

phishing e-mails,

so there are some visual hints.

Taking a look at this

quote-on-quote e-mail

from Microsoft Account,

you see that the @ blah, blah,

blah, is not @Microsoft.com.

That's a nice way to ensure

these are not legitimate folks.

Two, although they're

really good,

they often do have

strange characters,

grammar mistakes,

spelling mistakes.

I'm not asking all of us

to become our second

or third-grade teacher,

but take a look.

What looks odd?

I do promise you

that we proofread

many of our Microsoft Account

e-mails before they go out,

so you're not going to see

these strange characters.

Threats.

You know, "Your account may

shut in 30 days.

If you don't take action,

you're not going to be able

to access your account."

Those are threats.

That's now how legitimate

companies behave.

That typically doesn't make you

want to be our customer,

and so we do not engage

in those types of threats,

and neither do banks

and legitimate companies.

Low-resolute images.

That absolutely looks blurry

to me.

That indicates a little bit

of a risk,

and then the old trait

that we always encourage folks.

Hover your mouse, your cursor,

over these hyperlinks, right?

Those links that take you

to somewhere else on the web.

If you hover there, it'll tell

you what is the destination URL?

Where is it going to take you?

If it's going to take you to

XPZTechSupport247Fraudster.com,

you probably don't want

to click on that,

and go revert back to it

should be a clean hyperlink.

Lastly, there's one thing

we absolutely get right,

is our copyright information.

That's to protect ourselves

legally,

so that's a good place to go.

So what to do?

Delete it.

Alert family and friends

that you may have been

subject to a phishing attack.

Do not open an attachment.

It's very, very important,

and I say that,

and we have to operate

that way quite often.

Don't click on links

in a phishy e-mail,

and report it.

It's, you know, again,

we improve our products

based on the information,

so report to us or report

to your e-mail provider,

whoever it is, phishing e-mail,

fraudulent e-mail.

So the flip side,

here are the goods.

You got an @Microsoft.com.

We know something about you.

We've shown a legitimate reason

that we're contacting you.

We've taken action your behalf.

As opposed to threatening,

we have taken action

on your behalf,

and the hover tells you

this is a URL

that looks legitimate and clean.

So the next phase

that you of course

want to be weary

of a little bit is chat.

I love chatting with my parents

and my grandmother.

They do have a different style

than I use in chat.

They also then have

a very different style

than my sister who is

7 years younger than me

and probably has texted 14 times

while I've been

standing up there.

It's a generational...

We're all learning about.

Chat is a really...

It feels like it's personal.

It's in a box.

You can chat back and forth.

It feels a little less informal,

and it's a great way

for fraudsters

to continue that phishing,

to try to find information

about you.

So how do they do that?

They look at your

public profile.

So if you leverage Skype,

if you leverage LinkedIn,

if you leverage these great

tools that can help us connect

and be more efficient,

look at your privacy settings.

What am I telling the world

about me?

I definitely don't need to tell

them by entire birthday.

I definitely don't need to tell

them my Social Security number.

I want enough in that

information so that

a long-lost friend

from high school

might be able to reach me.

I don't need to be telling the

fraudsters my entire life story

so that they can use it

for other purposes.

So take a good look at what's

being kept private

and what is in public

in your profiles

of all the services you use,

and absolutely

the phishing e-mail scam

that I talked to you about

is exactly the same

as the chat scam.

They may have gone

through your profile.

They found what university

you attended.

They are posing as

the Alumni

Representative

for your university,

or a charity that you

have previously supported

and promoted

on your public profile,

so make sure that you

actually know the individual.

Don't trust a claim

of an organization

because that is information

that is readily available

and is the greatest way

that they can reach you.

So last, I adore video chat.

I've got two little kids

and when I'm traveling

on the road,

it is the greatest way

to connect with them.

It is absolutely crazy

how intuitive it is

for a 4-year-old

to use this technology,

but we do want folks to be weary

of the different types of video

chat you can use.

Skype does not record video,

but other third-party apps can,

and just as you may have heard

the cold-calling scam,

that they're calling you just

so that you can say

a couple of words

that they can leverage

in the future,

video is very, very effective.

Some of my colleagues

actually tracked down

some criminals

that were behind...

Who were using

pre-recorded video chats

to pose and open bank accounts

of those individuals.

They had the voice recognition.

They had image recognition,

and so be thoughtful

about how you're engaging,

and on the other side

of it is, of course,

you want this to be

a two-way video chat.

Be a little weary if it's

just a one-way video chat.

You're providing video

and they're not,

but know that they can

also change their identity.

Technology is great

for a lot of things,

but the tools that are out there

that I see too often

in the online child-exploitation

space of fake video images

to recruit and groom

are very, very sophisticated,

so use a trusted,

trusted source.

Am I going backwards?

I am now.

Great.

So you've heard me try to say

this throughout today,

but sometimes we all lapse.

This is not just a computer,

laptop problem.

We've now got all of these

great smart phones.

We've got smart phones.

We've got iPads.

We've got printers

which save information,

and so these are

the smart devices of today.

We all are hearing about about

the smart devices of tomorrow,

so when we say,

"Secure your digital self,"

we want you to think about

all of the digital information

that is being collected,

and how you take care of that.

I envision, and forgive me,

Doug, if I'm jumping out there,

but the shredding party

of before

is now going to have to be

the device-destroying party,

or at least

take out the chip.

Take out the memory

of your printer

before you are recycling that.

Those are important,

important elements.

So it's hard for me because

as I give these remarks,

it sounds like

I'm just scaring you,

which is not the intention.

Technology clearly has made our

lives better in a lot of ways,

and in fact, the best way

to protect yourself

is to use

your devices frequently.

The more familiar you are...

This is how

it's supposed to function.

I know I use Skype with my

children or grandchildren.

The more you will understand

when there's something fishy,

for lack of a better term,

so be active and stay vigilant.

If it sounds too good

to be true, it probably is.

The flip side of that,

if it's threatening,

it is probably

overly exaggerated,

and find a different way

to address this.

Something we have to tell

everyone,

"If you wouldn't do it

in person, don't do it online."

And my pledge, and my, actually,

request, is report the bad guys.

Do not be afraid or embarrassed,

and please tell your friends

and family to do as well.

One of the hardest things in

almost all of these fraud scams,

but we hear quite often

in tech support,

is people aren't comfortable

in this space,

and so they got a call.

They were told there

were malware and viruses,

so they paid the person $300,

but, "They cleaned my computer.

I am not a victim."

Folks want to be vigilant,

and we need to know about

these patterns and practices.

Report it to us.

Let us help unpack that,

and encourage your family

and friends

to do so

and be an ambassador.

Share these tips and tricks,

and as Chuck said,

I will also be in Kennewick,

so tell your friends to join us

in the Tri-Cities next week.

I have...

At the end of the day,

there is literally no difference

to giving remote access

to your computer

as giving a key

to your home.

You wouldn't let a stranger

have that extra key

or the access

to your back door.

Don't give remote access

to your device where you store

images and personal

identifiable information,

and there's a financial

traceable thing.

There is truly no difference,

and we should be vigilant

on both fronts.