-Here is what we're going

to do today.

I'm going to talk about

some of the trends.

"Why are we talking about

impostors so much?"

you might ask, and Bob alluded

to this, so did Mike,

but I'm going to give you

a couple more just data points

about how this is really

the type of scam

that's most likely

to target us these days,

and then we're going to go

a little bit deeper on --

Bob already talked

about the IRS.

You'll hear a lot

about the IRS today.

You're going to hear from a guy

who actually worked

in one of these scam rooms

in a minute,

though and, likewise,

with tech support,

I know Courtney is

going to talk about --

I mean, I know there is some

overlap to our presentations,

but we believe that repetition

is the mother of learning so --

And then just sort of tips

on how to avoid this.

Well, here is how we define

an impostor:

a scammer who is pretending

to be someone

they are not in order

to trick you out of your money,

and, you know, you could argue

that that's been true forever

with swindlers and con men

that's what they do,

they pretend to be

somebody they're not,

but there are these

three trends

that Mike already

alluded to them,

but I'm going to go

over them briefly again:

technology, the globalization

of the economy

and this fear and anxiety

because we really believe

these are the drivers,

and all of this

is designed --

As Mike said, you folks

are not going to fall

for the IRS scam, right?

I mean, you've heard about it

and so forth

or the tech support or any of

the things we're talking about,

but not everybody who could fall

for this is in the room today,

so we really do hope

at the end of the day

that you'll take this out

and warn others.

What do we mean by technology

driving things?

To me, I've been studying fraud

for 30 years,

and the technology --

I mean, one con artist said,

"If you're not using the

Internet to commit your crimes,

you should be guilty

of malpractice"

because it is just so easy

to pretend

to be somebody you're not,

whether it's a romance scam

or something else,

and, you know, you can --

The number of robo --

How many people have gotten a

robo-dial call in the last week?

Everyone, right?

Everyone.

It is so easy to just press

a button, as Mike said,

and, you know, 500,000 calls

come in, and so it behooves --

You know, it's up to us

to come up

with sort of defenses

to these things.

The other thing is just the

globalization of the economy.

You could be calling

from Malaysia.

You could be calling from India.

It doesn't really matter.

You can e-mail

from all over the world.

It is really,

truly a global economy,

and this makes it really hard

for law enforcement to stop it

and puts even more pressure

on those of us

in the prevention world

to get to people ahead of time,

and the last piece

is fear and anxiety.

You know, we live

in the age of anxiety.

There's a lot to be anxious

about, and as Mike alluded to,

there is a lot

of good research now

that shows

that when we're anxious,

we just don't make

good financial decisions

or any decisions, really,

and the con artist knows that.

They will ratchet up

that anxiety,

and you're going to see

how they do it in a minute.

The data doesn't lie.

These are statistics

from Consumer Sentinel.

This is Chuck's organization

that shows

just this meteoric

rise of impostor fraud

reported to the

Federal Trade Commission

over the last 5 years,

a huge increase.

In Washington State,

this is the data

from reports

they got from Washington State.

It is by far the number-one

thing followed by

debt collection,

telephone, banks and lenders.

We just did a survey,

and I'm going to report

we're releasing that today

as part of the launch

of this campaign,

called "Are You Real?

Unmasking the Impostors."

This was done by Karla Pak,

who is sitting right here.

Karla Pak is our research guru,

and so I hope I don't get

any of this wrong, Karla.

We surveyed 800 people

really recently, like,

March 28th to April 21st,

and one of the things

we asked them was,

"What kind of calls

do you get?"

and a huge percentage

of the stuff

that we're talking about today,

that's not an accident.

The number-one thing

people reported

was that they have gotten

the tech support scam,

which you'll be hearing

about quite a bit today.

Whether it's a pop-up

that says you've got a virus,

whether it's somebody

calling you saying

they're from Microsoft,

56% of the people we surveyed

said they've gotten this

in the last 12 months,

and that was by far

the number-one thing

they were targeted with

followed by phishing scams,

there's something wrong with

your bank account from a bank,

you know, fill

in this personal information,

and that's what

they're in it for

is your personal

identifying information.

33%, one out of three people,

lottery scams, IRS and so forth,

so you can start to see

how this breaks down.

We also gave people a quiz,

"What is your impostor IQ?"

and let's just go through this.

You don't have to raise

your hand or just --

But see if you could answer

these questions yourself.

Question number one, commercial

telemarketing robo-dials,

which everyone gets,

from companies you don't have

a previous business

relationship with are illegal.

How many people think

that's true?

How many people think

it's false?

How many people don't know?

A lot of people don't know.

It is actually true, and 73% of

the people we surveyed

were either not sure

or did not know.

Here is another one.

Caller ID is a reliable way

to know

where a telemarketing call

is coming from.

True?

False, very good, false.

38% didn't know

or got that wrong, so we think,

"Oh. Well, if I've got

a caller ID thing,

it says it's calling from 206."

We all know, but not everybody

in the state knows,

that that's spoofing.

Very few telemarketers

use their real phone number now

because you can

just buy a number

and make it look like you're

calling from the 206, right,

but not everybody knows that.

We know it,

but not everybody knows it.

This is an example of a fact

that would be great

to share with your neighbors

who may not know this.

Technology companies

don't notify customers

when a virus is spotted

on their computer.

True?

False?

That's true.

They don't.

44% didn't know

that or got it wrong,

and, finally, the IRS

is allowed by law

to call you

about back taxes you owe

without sending

written notice first.

False, very good,

and a lot of people did --

Only 23% got that wrong,

so we'll talk more about that

IRS thing in a minute.

So of these 10 questions,

77% of the respondents

got 60% or less

which is kind of a D.

There's -- It's an F.

It's an F.

It's not good.

Yes?

-Could you e-mail me

your presentation?

It's going really fast.

-Is it going too fast for you?

-Yes.

-We could probably

post it online.

-Okay.

-Yeah.

We don't want to --

I'm not trying to hide

anything from you.

-No, no, no, no.

I just want to go back to it.

-Okay, but you reminded me

to slow down.

I appreciate that.

No, really.

I tend together too revved up

about this thing,

and so part

of the other survey --

So we sort of have

this general conclusion

that not everybody knows

the tactics impostors use

to defend themselves.

Yet when we ask them,

"How confident are you

that you could spot

one of these scams?"

87% said

that they're pretty confident,

and another 85% said

that they're pretty sure

they won't fall

for a fraudulent pitch.

So you have this confluence

of really showing

that they don't really know what

the tactics are exactly to spot

but a lot of confidence

that they won't be taken,

and this is something you will

encounter as our fraud fighters

now going out into the world.

Nobody thinks they're going

to fall for any of this.

It's known as the illusion

of invulnerability.

In the health psychology

literature,

this has been true for years.

People say, "You know what?

People get cancer,

but I won't," right?

You don't want to think

about it, whether.

You're in denial.

Well, if you never think

you're going to get cancer,

you'll never do anything

to prevent it,

and the same is true with this.

If you never think you're going

to be taken,

you'll never take steps to avoid

it other than this general idea

that I'm just not going

to fall for it

because I'm too smart,

and my pet peeve --

I won't go into too much detail

about this,

but you know this phrase,

"If it sounds too good

to be true, it probably is?"

I hate that phrase.

Why?

Because it assumes --

It's a perfectly logical thing

to say and to think,

but that assumes that

you're thinking logically

and rationally at the moment

you make that decision,

and the con man's great gift

is to put you

into an emotional state

so you don't think logically.

So if you're only relying

on your rational mind

and not managing your emotions,

managing whether

you're vulnerable or not,

it's like locking a safe,

you know, you're locking

your money in a safe

that the con man

has the key to really.

It's really more and more

about managing people's emotions

in their vulnerable state,

not about intelligence

or brain power.

So let me introduce you

to two characters

that we recently interviewed.

One of them, Jayesh, the guy

on the left, is from India,

and the other guy, Dan,

is from South Florida,

and both of them worked

in fraudulent boiler rooms

that did various bad things

to people in the United States,

and the one thing I want to say

about these two

by way of introduction,

we've interviewed

a lot of con men.

Usually -- Bruce and I,

for years,

have gone into prisons

and interviewed guys

in orange jumpsuits.

These are really bad guys,

drug dealers, you know,

and they tell us how they did

it, and that's the thing.

There is this growth in people

like these two guys

who aren't really --

These two guys were never

charged with any crime,

and they were never

convicted of any crime,

yet they did the work.

They did these calls,

and increasingly you're seeing

boiler rooms in South Florida.

They have hundreds and hundreds

of these people

who are just young people

looking for a job,

and they get caught up

in these rooms,

and what I'm going to take you

through here in the time

that I have

is to go a little deeper

into both the IRS scam

and the tech support scam,

and I know both Chuck

and Courtney

are going to touch on this.

Courtney, in particular,

is sort of the tech support

expert from Microsoft,

and she's really,

really an expert on it.

We're just going to take you

through

what these two guys

talked to us about for a minute,

so you can get a real feel

for how they do it

and especially how they focus

on getting you

into a heightened

emotional state

which, in both cases,

tends to be fear,

fear and anxiety,

fear that something

is terribly wrong.

So let's see.

Let's see.

I'm going to play this tape,

and you've probably

all heard it before,

but we're going

to play it again.

This is a call

that came in recently.

How many people

have gotten that call?

Half, at least, of the audience,

so that's out there,

and, you know, we've heard

these reports from TCA

and other places that

they're bombarding Americans,

but who is the person

on the other end of the phone?

Who is that person,

or who is the person

you end up talking to?

And this is where we want

to introduce you

to one person who we interviewed

who actually worked in one

of these boiler rooms in India,

and this is the first --

You're the first people

to see this

since we filmed

this guy in India.

-Meet Internal Revenue Service

officer Adam Smith,

better known to his family

and friends as Jayesh Dubey,

a 19-year-old in Mumbai, India.

Jayesh

and his friend Pawan Poojary

were looking for work

when they heard

about an opportunity

in one of Mumbai's

many telephone call centers.

He was impressed by the office

and the size of the operation.

He was especially impressed

by the salary.

Jayesh started off just

answering calls from America,

getting basic information

and handing the victim off

to an experienced closer.

As he gained skill on the phone,

he handled

the whole call himself,

getting the victim

to hand over the money

to pay

their fictitious tax bill.

The phone room reached out

all over the United States

every day.

As he talked to more and more

Americans, he and Pawan

began to feel bad for the people

they were stealing from.

They decided to quit,

and they were fortunate

not to be at the office

when 200 Indian police officers

descended on the operation.

Police blocked the exits,

detained more than 700 people

working that day

and seized everything inside.

Authorities

determined the office

was just a branch

of a larger operation

that made over 1.8 million

calls to America

and stole hundreds

of millions of dollars.

Today, Jayesh is speaking out

about his experience

and the tactics he used

in the boiler rooms of India

to defraud Americans,

and he has one message

above all.

-So there you have it.

That was Bruce Carlson.

Bruce, nice job on that video.

Yeah. Good job.

[ Applause ]

Thank you.

What we want to do now,

now that you've met him,

is go -- Oh, there's Bruce.

He's in the back, very shy.

He's very shy and withdrawn.

We want to take you through

just for a couple minutes --

go a little deeper.

What happens if you call back

the number?

How many of you who got

that call called the number back

to find out what it was?

Not very many, hardly any.

Well, you heard him say

that they were doing

50,000 calls a day.

10,000 people called back.

I mean, if you get one

of these calls,

you're not sure what it is.

I mean, the IRS is scary, right,

and so what do they really say?

And we are going to --

We had, you know, one of our

super-duper fraud fighters,

I won't say where they were

or who they are,

talk through, call back

and see what they really say,

so let's listen,

and then we'll hear

Jayesh comment about it.

That's pretty scary, right?

One of the things that Jayesh

told me when we interviewed him

was this works

especially well for people

who live by themselves,

who don't have another adult

living with them who can say,

"What? Come on.

What do you mean?"

Section 7201, Chuck,

correct me if I'm wrong,

is an actual part

of the tax code,

so they're doing their research

about this, and it's --

You know, the best lie is based

on some degree of truth,

and so --

But that gets very scary

very quickly for people

who live by themselves.

Let's hear what Jayesh

has to say about it.

And could you imagine

just hundreds and hundreds --

I mean,

when they busted this room,

they detained 700 people

that were in this building

in downtown Mumbai.

700 people were doing this,

and I don't know where

this call came from.

It might have been Mumbai.

It might have been Malaysia.

It might have been, who knows,

South Africa,

but all of the tactics

we've identified

before about source credibility,

pretending to be --

Oh, look at this.

He's talking about being the --

working with

the attorney general.

I wonder if Bob knows this.

Let's...

So as you resist --

This is one of the dangers

of even calling.

As you resist more and more,

they ratchet up the threats,

and this is --

Let's hear from Jayesh

about this.

Yeah, so we know

that it's not true,

but hearing it from the guy

in the room

saying,

"No. We weren't recording it,

and no, we don't know

any attorney generals."

I mean, we now know an attorney

general,

but so, Shannon, I hope

you're listening to that one.

Then as you resist more and say,

"How do I know

this is even true?"

they ratchet up the pressure

even more to the point of,

in this particular call,

they had the audacity

to tell the victim,

"You don't believe me,

so what I want you to do

is go down

to the police station.

I'm going to fax your documents

to the police station,

and they will arrest you,

and then that will prove

that I'm real," so let's listen.

Confident.

That's a confident --

I guess that's why

they call them con men maybe,

but you could imagine somebody,

an older person living alone,

having this conversation,

trying to resist,

and they just

ratchet up the threats.

So what does Jayesh say?

Is any of that real?

So, again,

for this audience here,

who never would fall for this,

you say, "I know. I know.

I know," but part of the reason

we make these videos

and try and distribute

them online, in person,

is for that person who may

be alone getting this call

and doesn't believe

that it isn't true.

The conclusion to this --

Well, one conclusion is this

is the mastermind

they just arrested,

and our guy, Jayesh,

actually met this guy,

Sagar "Shaggy" Thakar,

a 24-year-old entrepreneur

who was the mastermind.

He had multiple boiler rooms

all over India and Malaysia.

The reason he eventually

turned himself in,

and this is just last month,

according to news reports,

was that his girlfriend

threatened

to break up with him

if he didn't turn himself in,

and that's the only reason

he turned himself in I guess.

It's the power of love,

you know.

[ Laughter ]

But the thing that really

kind of boggles my mind

is how they actually got

people to pay the money.

Remember how he said,

at one point,

that,

"You owe $7,212 exactly?"

They have them go down

to Walmart or a department store

and buy iTunes cards,

you know, like $500.

"Put $500 on an iTunes card,

then call me and read me

back the number."

Once you read them back

that number,

that money,

they can cash that money,

and it's gone forever,

and you can't trace it,

and how they convince them

to go from,

"You owe the IRS money,"

to, "You've got to buy

an iTunes card,"

we explored this

with Jayesh at length,

and it's this convoluted

thing about,

"Well, we have a partnership

with them,

and it's an electronic

transfer system,"

and it really doesn't

make any sense,

but remember, again,

us sitting on the outside

of this transaction,

you're not under the ether,

the emotional vibrations

they've created,

the fear they've created.

You're not thinking rationally.

You just want to get out of it,

and they give you a way

to get out of it.

They'll even hire a cab

to come to your house,

take you down to the local

Walmart to get these iTunes --

You know, it's just crazy

how they can be convincing.

So the IRS has warnings.

You will hear this over

and over again.

Obviously they don't --

You don't pay your tax bill

by getting a green dot card

or wiring money

or anything like that.

We all know that.

We need to keep

warning people of that.

IRS will never call or robo-dial

you

without first

sending you written notice.

The IRS did just recently

announce

that they will be contracting

with collection agencies

to do some of the collection

of back debts, which we have --

is worrisome to me

because the con artists

will be able to pretend to be

those debt collection agencies,

but, nevertheless,

they won't call

until they've written to you.

You should know about it first.

You shouldn't just get a call,

and if you do get a call,

obviously call independently

and see what your tax status is.

So that's the IRS scam,

taking you inside

the boiler room,

trying to unmask

some of these people

and show you who they are.

The next one I want

to get to is,

and again, you'll hear more

about this from Courtney

because she's really the expert,

but the tech support thing,

you saw that 56%

of the people

in the state of Washington

we surveyed

had some kind of tech

support scam experience

in the last year.

This guy worked --

Well, let's just play the video,

and we'll introduce you to him.

-Meet Dan Goldstein.

Posing as a computer technician,

he was part of an operation

that sold phony computer

support services over the phone.

-The consumers would end up

on the phone with me

by either seeing

an advertisement

or by actively looking out

for a PC cleaner,

which was a downloadable

software

that they could put

on their system

that would clean the background

of their files

and speed up their PC.

-Dan's outfit operated

a boiler room in South Florida

under a variety of names.

The company and its various

aliases were all sued

by the Federal Trade

Commission in 2014.

-It was just a very large

open area with approximately,

I'd say, about 12 or 13 tables

that were probably 40

to 50-feet-long each,

and each table was packed

with computers

and people sitting in front

of every computer.

The first couple of tables

were called the bone pickers.

Their job was to pick the meat

off the bone,

essentially try

and get as much money

that we couldn't get from you

at the beginning.

-Dan's job was to get the caller

to give him control

of their computer

and then sell the victim

a variety of computer

tech support services,

none of them

with any real value,

that could add up

to thousands of dollars.

-I didn't go in, again,

knowing that it was a scam,

but when the FTC

brought it down,

by that point, I was well aware

of what the company was.

It hit me that what we were

doing was, indeed,

very dishonest and immoral,

and you started to really see

that what was happening

was not exactly

what we were presenting.

-Pleased, right?

So how does this work?

And, again,

I'm going to describe

just one iteration

of the tech support scam.

I think Courtney is going

to talk about other examples,

but in this particular case,

he's talking about

the Federal Trade Commission,

Chuck's organization,

and the Florida AG's office

brought suit against

this company.

This was in 2014,

and essentially

what they were alleging

is that you'd go online.

You're worried that your

computer is running slowly, say,

so you'll

either see a pop-up ad,

or you'll Google, you know,

how to fix my computer

or how to clean my computer,

and something like this ad

will come up, PC Cleaner.

You can fix, clean and speed up

your PC in minutes.

There is a free scan,

they'll say, you know,

so you click on it

to scan your computer

to see whether there's

any problems with it,

and one of the things

the FTC did in this case

that I thought was very creative

is they hired a computer expert,

and they set up the company

by first buying a new computer

that had never been used,

having the expert look

at it in detail.

It's running perfectly.

There's no problems with it,

and then they clicked

on this software,

and this is the screen

that always comes up,

and this screen says

that you've got 8,056 problems

with your computer.

There is 928 problems

about viruses.

There is 6,800 and --

There's traced temp files.

This is counting all kinds

of things on your computer

that are on everyone's computer,

and doesn't mean that

there's anything wrong with it,

but you look at this,

and you say, "Oh, my God.

There's 8,056 things wrong,"

right?

So then they'll say, "Fix all."

See the button that says,

"Fix all"?

You'll click that.

You pay them $30, so now

they have your credit card,

and it downloads the software,

and they say,

"To activate this software,

you have to call an 800 number."

You don't, really, but everyone

calls the 800 number.

425,000 people called this over

about a 2-year period,

and when they call,

that's when they get this guy.

He's in the room,

and then he takes us

through what happens next.

-My job then would be to access

your computer remotely.

The first thing I would do would

be to pull up your task manager.

We would go right down here

where it says,

"Processes: 94,"

and I would tell you,

"Oh, my God.

You have so many things

running in the background.

This is insane.

No wonder your computer

is moving so slowly,"

and you can see even though

it's 94 processes,

it's really not using

any of your computer,

but people don't know that.

All they see is

this giant number here,

and I say, "You shouldn't

have anything more than 10."

-He'd say, "10" if it was 94,

but if there were 340,

he'd say, "39."

He had this formula

where whatever the number

of processes running were,

I would just say,

"You shouldn't have more

than 10% of that," right,

which means it's not

really analyzing anything.

He's just making it up,

and so --

But this starts to scare

a person, right?

Not only were there

8,056 things wrong,

but now there's this problem

with the processes,

the task manager,

and then he takes it a step,

another step.

All of these are fear tactics

that get you, again,

into the ether

of fear and anxiety,

so you're not thinking clearly.

Then he goes to

the error log tactic.

-Without question,

the scare tactic

that worked best

was the error log.

It was the cherry on the icing

of the cake, essentially,

is all of a sudden

this error log would come up,

and for most people's computers,

it would have thousands

and thousands

and thousands of errors from

the day they owned the computer,

and that was certainly

an eye-opener

for a lot of people

to think that

there was definitely something

going on behind the scenes

that they didn't realize

was happening with the computer.

-But what are those error logs,

right?

You get these screens.

Everybody has these.

It's another one of those things

on a computer

if you tried to log

onto a website,

and your Wi-Fi wasn't on,

error, right?

Your virus might detect

a bad website, warning, right?

That's warning you of people

like him, not warning you

there's something wrong

with your computer,

but they use stuff

that's on the computer

that's benign to get you

to think

that they need the problem,

and, of course,

all of it leads to the --

what it really leads to

is you buying,

spending $300 to get it fixed,

and one of the questions

we asked him was,

these people in the rooms,

were they really people

from Microsoft?

I mean, are they digital

crime unit work?

They link them up

to the digital crime?

No, probably not.

Here is what he said.

-Nobody in that room was

a certified computer expert.

Anybody that you would actually

ever get on the phone

with as a consumer had no actual

background in knowing computers

and, you know, really being

what you would consider

a "expert" of computers.

Most of the people

that I would say were in there

were current or ex-alcoholics

or drug addicts,

and a very large chunk of them

actually were currently living

in sober facility

halfway houses.

If people knew the inner

workings of who they were

actually speaking to

on the phone,

there's no doubt in my mind

that 95% of those people

would have hung up the phone

as soon as they got on with us,

without question.

-And, you know,

one of the things --

I can verify this because we

were getting lists in Florida.

When you have

a telemarketing room,

you have to register

all of the people

who work in that room

with the state,

so we were getting Freedom

of Information Act requests

from them, getting names

of hundreds of these people,

and a lot of them

had criminal records.

You can look that up.

These are the people who you're

getting on the phone

who take over your computer.

You know, in order to do this,

you've got to give them

permission

to take over your computer.

The bottom line is it's just

something to really avoid,

you know?

FTC filed a law suit,

got a temporary injunction

against them.

This company took

in $120 million in about 2 years

doing this thing

that we've just described,

and there are many

more out there.

Courtney is going to talk

more about them.

I have to say, we've been

working with Microsoft on this,

and I know they've been

working with law enforcement.

Every time I call an AG,

they go, "Oh, yeah.

We've worked

with a digital crime unit,"

you know,

"They are really trying"

because a lot of these companies

will wrap

the cloak of legitimacy

around them by saying,

"I'm a partner with Microsoft,"

and that's an abuse

of Microsoft's logo,

but they will --

or some other company, Apple,

"I'm working with Apple,"

because that legitimizes them,

and it's really hard

to keep control

over all of those claims,

but that's what they do.

So how do you avoid it?

Don't download free software

to clean your computer.

If you think it's going slowly,

take it down to Best Buy

or some retail store front,

a Microsoft store

where you've got a technician

who is certified

and who can look at it.

Don't click on pop-ups.

A lot of these pop-ups --

One of the other

versions of this

that we wrote about

in the AARP magazine

was there is this

cloaking device that they use.

So you click on a pop-up for,

say, dog food.

You're looking for dog food,

and it's benign.

You're looking for dog food,

right, you Google it.

You click on it.

It's not really an ad

for dog food.

There's a cloaking device

that makes it look like that ad,

and behind that is this thing

called the blue screen of death,

and this thing comes up,

and just all of a sudden,

there's a blue screen,

and it says,

"Your computer

has got a virus," right?

Well, all you did was click

on a dog food ad,

and now your thing is shut down,

and, "Oh, what do I do," right?

So there's a lot of that

going on out here,

and it's really

just hard to --

You know,

it's just hard to know.

You can't completely

avoid it all the time,

but on this cleaning your PC,

clearly the thing to do

is to not respond to pop-up ads,

and if you're concerned,

as I said,

about the speed

of your computer,

take it to

an authorized repair place.

Other impostor scams

to watch out for --

I'm not going to go

into detail here.

I could talk all day about them,

but the grandparent scam,

how many of you

have ever gotten that call?

Have you?

Someone posing as your grandson

in Mexico,

anybody want to give

an example of that, anybody?

-I got one for my nephew,

and they had

the right first name,

but the voice was not right.

-Yeah.

-So that's what's what threw me.

I wasn't able to --

I did talk to him a while.

I said, "Oh. How is Larry?"

his dad, and he made some,

you know,

comment about how he's fine

or something like that,

but the more he talked,

the more I was able to realize

this was not my nephew.

-What did he tell you?

Was he trapped somewhere?

-Yeah.

He was in Seattle,

as a matter of fact.

He was in the police station,

and he needed

X number of dollars

to get himself out

of the police station.

He was in Seattle, you know.

-Yeah, and so you eventually

just hung up on him?

-I did. I did.

Yeah.

I felt -- I mean,

I even felt guilty for doing so.

-Did you call --

-He's my nephew.

-Did you call your nephew

and verify that he wasn't --

-Well, I wouldn't have

called him.

I would have called his dad.

-Yeah.

-I don't remember.

It's been a while yet,

but I got another one.

The jury -- The not --

-That was the next one

on my list.

Look at this...

-Yes, that one.

That one, they got it.

-...fake jury duty.

-They got me there.

I -- just exactly what you said

about the emotional, the fear.

The sheriff was going

to come to my door

and put me in the back seat

in handcuffs.

I could not stand to think of my

neighbors watching this happen,

and I race out

to my credit union in Tukwila

to get money for a PayPal card,

bought it, sent it off,

and as soon as I sent it off,

I relaxed,

and I realized

what had happened,

and I called

the police department,

and they said,"Yeah,

that's happening these days."

-So on the one hand,

you were relieved,

and then right after that,

you felt horrible that

you had been scammed kind of.

-Yes.

-It's kind of a mixed emotion.

-I still feel terrible.

-Yeah.

-I'm still angry with PayPal

for not getting my money back.

-Yeah.

Yeah.

Yes.

-That was a terrible one.

Sorry.

-Great story.

Thank you for sharing that.

Yes, ma'am?

-The grandparent scam happened

to my dad

when I happened

to be visiting him,

and one thing that my son,

supposed son, said was,

"Please don't tell my mother.

Don't call them,"

and even though my father

had read about this scam

in Consumer Reports,

he still fell for it.

-Oh.

He did?

-He went to Western Union,

and luckily he had wrote down

the wrong phone number

or something,

and so he didn't

send the money.

-Oh.

-But he --

What amazed me was

he had heard about this scam,

but he still thought

this time it wasn't a scam.

It sounded so much like my son.

-Yeah, and they have different

ways of doing that, like,

"Grandpa,"

and then you say the name,

and now, they're, "Yes.

This is David.

Yeah. My name is David."

Right, right, very clever.

Yes, sir?

-I even had a call questioning

the last name of my mother.

Well, I don't know

how they got my name,

and they wanted to have more

information about my mother,

and I says, "You know,

she was born in the Ukraine.

She immigrated

to South America,"

and "What was her maiden name?"

So I said to them, "You know,

the maiden name was Lenin.

She was a cousin, you know,

of Vladimir Ilyich Lenin

who ran

the communist revolution."

[ Laughter ]

-Now you're playing with him.

You're playing with him, right?

-And the guy said, "Actually,

you know, my name, Louis,

well, thank you very much.

It was a pleasure

to talk to you," and he hung up.

-So you saw that coming,

but what were they doing there?

Why did they want

the maiden name?

What do you think?

-I don't think they got to that

because

they couldn't get to the maiden

so they really asked me,

and I said,

"I'll give them the story."

So when I assumed there was more

than that,

when they heard the story,

they said,

"Well, this guy probably won't

work with this guy," you know.

-All I was going to point out

there was that's a phishing scam

because --

and the reason they want

the maiden name is often that

is a security question

on your Facebook account

or some other

social media account,

and, you know, we had

this conversation last night

when I was talking to some folks

about David Morros --

Raise your hand, David.

David is a new volunteer

from Tennessee.

He's going to volunteer for us

for the Fraud Watch Network

and an expert in cyber crime,

and we were talking

about Facebook,

and he and I were both going,

"Yeah. We don't use Facebook.

It's just --"

because Facebook is where

a lot of personal

information gets posted,

and if you don't have

your privacy settings right --

I'm not an expert on Facebook,

but I can just tell you

as a crime prevention person

a lot of the scammers --

I mean, we interviewed an ID

thief a couple years ago

who would just go on --

That's the first thing

she would do

when she was trying

to target somebody

is go onto their Facebook page

and find out birth dates,

names of relatives,

maiden names,

all things that you want

to share about yourself

just because it's Facebook,

and you want to share yourself,

but they can use

that then to hack in,

so Face --

I don't know how we got --

Thank you for those stories,

though, very helpful.

A lottery/prize scam,

anybody know someone who's

gotten a lot of these mailers?

I continually worry about these

older folks, in particular.

Our research has shown

that that's --

A lot of older folks

get these lottery scams,

and then the last on

is the government grant scheme.

You've just won, you know,

an $8,000 grant for free.

All you have to do is pay,

you know, $250,

and we'll send you

your $8,000 free grant money,

so that just preys on,

you know, gullibility.

Most of them are trying to get

you into the emotional state.