[music playing]

[Narelle] Hi,

and welcome to another episode
of the Digital Access Show.

I just had to look see
where the camera was.

Okay. I can't see properly.

I think I'm looking
straight at you guys.

Listen today, I want to
approach the operability…

principle, but we're looking
at one particular area,

navigability.

But we're going a
bit more in depth.

We're looking at navigability
and cyber security.

Why?

Everyone gets hacked.

This really is aimed
at the developers,

the designers,

anyone that's doing content,

and just some thoughts for you

on how to make your
website more secure.

So to do this, I've brought
along a friend of mine,

Luke Irwin from
Aegis Cyber Security.

Luke, thank you so much.

[Luke] Hello, Narelle.
Thanks for having me.

[Narelle] Luke, can you
tell us a bit about yourself

and how you got
into cyber security?

[Luke] Yeah, certainly.

So I've been in tech
now for 23, 24 years.

Been in cyber for about 10.

I started off doing tech when I was
with the Royal Australian Navy,

where I was looking after a

fairly significant
database system.

And over the last 20 odd years,

I've simply worked
my way through

and up various tech
and management roles.

Where about a decade ago I decided
to transition towards cyber.

And now I run a security
consultancy working with firms

to help them address their gaps,

their vulnerabilities,
their risks, and

get them on the right path

so the bad guys don't
essentially destroy

what they've put all that work into.

[Narelle] One of the things,

and you and I have just keep
having conversations about it,

because, obviously, I'm passionate
about digital accessibility

and you're passionate

about cyber security.

There's an interconnection
there, isn't there?

[Luke] Massively.

So many of the systems
that exist nowadays on like,

you cannot live without
the internet nowadays.

You can, but life's going to become
really difficult, really slow.

But everything nowadays,
it's so interconnected,

and it's so dependent
upon being able to access

and use technology
appropriately and securely.

When you look at how many of these
systems are configured online,

even looking at, say, bill
payment portals for your power,

your water,
your gas, your phone,

they're not necessarily
easy to navigate

from a vision impairment,

hearing impairment,

processing impairment. That…

simple design makes it harder to
participate in day-to-day life.

A classic example is you look
at the puzzle-based CAPTCHAs.

How is somebody who has a vision
impairment supposed to realise

where to put that puzzle
piece in a mixture of colours?

If you look at the options,

which Microsoft,
to their credit,

they've given a vision-based
and a sound-based approach,

but when you push the speaker
button to make it play back

what is on that CAPTCHA,

it may be distorted.

If you've got a hearing
impairment and a

vision impairment,
you can't see it,

and your hearing aid,
or your hearing,

cannot make out
what is being said.

So there needs to
be a better third way

to be able to
secure and validate…

who is accessing the system.

[Narelle] What is, what's
something that people can do, Luke?

What's something,
briefly, that people can do?

[Luke] A lot of other
systems will fall back

to either an SMS-based

or an email-based multi-factor,

and while having that

as a multi-factor is
better than having nothing,

I just want to
make it clear that

tht is, that's not very secure.

It's about the
equivalent of putting a...

I can't think of a good example,

putting a $2 lock on a
$1 million bank vault.

That's... it'll stop
the honest people.

It won't stop the people
that really want to get in.

Things like the
multi-factor authentication

via the authentication apps
from Microsoft and Google,

and a couple of
others out there,

they are much better.

But the challenge with
that is to set them up,

you generally need
to have good vision,

because you need
to be able to navigate,

you need to able
to position the QR

codes, put in the details,

read back these challenge
responses they make you go through.

So there's a gap between
the need for security

and the need for accessibility,

and I feel the industry
hasn't yet hit that

good middle ground.

That's probably the best way I can
answer that one for you, Narelle.

[Narelle] That's interesting,
because I've never,

you know, for me, I thought,
multi-factor authentication.

Suppose, being a coder,
I'm not cyber security.

I will make that clear.

I wrote code for 40 odd years.

You know, I was in databases.
I was in desktop, bit of web,

web development.

Not cyber security.
-[Luke] Yeah.

[Narelle] To be honest,
I only just passed

the cyber security section

the second time I went
back to do my degree,

because it just, because of the…

the way you have to change your
thinking completely to do it.

The… other thing
that I'm noticing,

and look, I'm getting a
ton of SMSes at the moment,

where and that they're from,

they, they pretend
to be from the bank.

Or the latest one yesterday
was Australia Post.

Now, I know there's no
parcels being delivered to me,

but they look…

they look real, because it
just uses words like "click here"

or, and that's
one the things that

digital accessibility
stresses about.

From a cyber
security point of view.

What's the dangers?

[Luke] What you're describing
is called a phishing attack,

and that's P-H-I-S-H-I-N-G.

So it's trying to trick
you into doing something

or giving up something
you don't want to do.

I have lost count of the
SMS as I get from Toll,

or Linkt, or Australia Post
going, "You have a parcel".

Your Toll fees are overdue now.

[Narelle] Yep.

[Luke] Now wone, is that a
normal communication method

for that organisation
to reach out to you

and 90 percent of the
time, the answer is no.

If you have a screen reader,

you may be able to
hover over the button.

[Narelle] That's if you
can use a keyboard.

[Luke] If you can, yes.

[Narelle] If you
use a mouse, sorry,

people that use a
keyboard can't even do that.

[Luke] You are…

generally speaking,
you're correct.

Yeah, that if the
developer has done it well,

you can push tab to
navigate to things,

but again, if you can't
use the keyboard,

you've got a whole
other problem.

[Narelle] Yeah.

[Luke] That's where
one of the issues of

compatibility
between accessibility

and cyber security essentially
butt heads to a certain extent.

Because cyber security,

they want you to
slow down and think

and use all the
tools available to you

to determine if something
is safe or not safe.

But if you have an
accessibility issue,

you might not be
able to use the tools

to determine if it's
safe or not safe.

So there's this
expectation that you can

against an existence of
capability that you can't,

because of vision

or hearing or tactile.

That's one of the questions
that hasn't been answered yet

by the industry.

What you, one of the things that you
need to do when you're looking at

or clicking on any link is
understand where you're going.

So if you look at the link, you
want to look at what's up front,

look at what comes
after the slashes,

and look for where
you've got things like,

after the first section,
you can see like, might be…

telstra.com.au/gibberish,

and then /aws.ru.something.

That's where
you're actually going.

You need to know how to
be able to read those links

and work out where
you are going. Now,

I understand that…

many of the disability
support tools may not

be able to appropriately
handle those,

and that does create a risk
for people with a disability.

And I'm sorry I don't
have an answer for that,

because I'm yet
to come across a…

a set of systems or tools or

products that can actually…

correctly address
that risk for you.

[Narelle] You know what?

This is bringing up more
questions than answers.

[both laugh]

[Luke] Yeah, this is one of the
one of the things I both love

and sometimes struggle
with, with cyber security.

Every time you get an answer,

three or four more
questions pop up,

and you end up going
down a rabbit hole.

It's one of the things I
love, but with limited time,

there's only so far down
the hole you can go.

[Narelle] Yeah.

[Luke] When you're also
looking at these links.

Well, the first question is,
you need to understand,

why is this person
sending it to you?

Now I'm not saying everybody that
sends you an SMS, trying to scam you.

That's just not accurate.

But if your phone is
filtering it through into junk,

then there's a high
likelihood that is junk,

because Google and Apple,

with the support of the

telcos like Telstra and
Optus and Vodafone…

work to detect when these
types of SMSes are sent out,

then match them
against other types

and push them
into the junk folder.

Now, if they're there,

it is possible that
valid things go in there,

but it is less likely
that they are valid,

strongly less likely.

So if it's in your junk,

please be careful.

If you get an email,
sorry, an SMS,

or even an email from your bank,

Toll, Linkt, Australia Post,

a courier company,

do not click on the link
in the email or the SMS.

Go to Google,

look up the website,

and then go into that
website and put in your details,

or the details that have been
provided to you in that message,

your tracking
number is whatever.

It's not great,

because you might be

looking at a 25 character…

long string of digits which
could be challenging.

But if you do it that way,

then you know that you've
gone into a secure system,

and you haven't
clicked on a link

that is taking you
somewhere that's going, hey,

to release this package,
we need your credit card number.

The question is,

if anyone asks for
your credit card number

and you're not actively
trying to buy something,

please don't put it in.

[Narelle] Yeah.

[Luke] It's…

that's one of the, it's one of
the risks that exist, and it's…

people want to believe what they
receive is true and accurate.

They want to believe that they're
trying to help them get what is…

theirs.

But in most cases,

with the cost of execution for
a digital attack being so low,

the bad guys that send out tens
of billions of these messages,

and see what sticks.

If only .01 percent
actually result in revenue,

cool, that's still a million
people we've gotten.

And if we get a million
people for $5 each,

for something that had
no cost and very little risk,

then it's a,
it's a positive for them.

It's the same way the old spam
emails used to work so well.

[Narelle] Yep.

Yeah, I remember them.

Luke, one of the things,
when I go onto a web page,

and it could be like…

could be anything.

And again, you get those,

that generic wording, like…

"Learn more here" or "Click here".

Again, how does a person…

guarantee that the web
page hasn't been overlaid

by another web page,

hacked into or anything else?

Because it's, yeah.

[Luke] Okay, so
with those types of,

so what you're describing there

by putting an overlay in is
a fairly sophisticated attack.

So that means someone has
to have taken over the website.

[Narelle] Yeah.

[Luke] Generally speaking,
the more successful,

popular and used websites

are going to have
good website security.

That's not 100 percent
across the board,

but one of the best
ways to tell is, um,

up in the top left hand
corner of the address bar,

there will usually
be a little padlock,

or a shield or
something similar,

that indicates that you're
communicating

via what's called HTTPS,

which is Hypertext
Transfer Protocol Secure.

[Narelle] Okay, but if you've
got a vision impairment…

[Luke] Exactly. Then again,

this is one of those gaps where…

cyber security versus
disability accessibility.

-[Narelle] Yeah.
-[Luke] There isn't an answer yet.

I don't know if a screen reader
can successfully read that.

But, if as long as it's HTTPS,

and you've got that padlock,

then the site is who
they claim to be.

[Narelle] So, the screen reader will
read the address bar. So that's good.

[Luke] Fantastic.
So if it says HTTPS,

then you're good.

Now I want to call out there
is a bit of a risk there still.

Because that's on the assumption
you've gone to the right page.

We'll pick Google, for example.

So G-O-O-G-L-E.

-[Narelle] Yeah.
-[Luke] Let's go G, triple O,

G-L-E.

That isn't Google.

You can register that
and say who they are

and get a certificate
saying that.

Now Google would have registered
addresses around that.

But as an example,
you aren't actually on Google.

You're on Gooogle,

-[Narelle] Yep.
-[Luke] So,

anything you put in isn't going
to who you think it's going to.

So you need to make
sure where you're going…

is actually where
you're supposed to be.

And you've typed in
the address correctly,

or cut and pasted the address,

you've put, you've gone
to the correct address.

[Narelle] Yeah.

One of the tips that I like
to use as well with the link,

the naming of links and things,

I always say, use five
words or less but be concise

about where you're
taking them to.

Don't say, "Learn more".

[Luke] Exactly.

[Narelle] Because screen
readers read out of context.

[Luke] Precisely. The
use of alt text is critical.

You need to use alt text
on buttons, on pictures,

on links.

Make sure that the if you've got
a button or a link that says,

"Click here",

that if you hover over it,

the alt text actually
tells you where it's going.

[Narelle] Yep.

[Luke] If you just
say, "Click here",

how is somebody who has a vision

impairment supposed
to understand

and see where they are going.

By not doing that,

the developers and the,

the web devs are

introducing risk.

They're potentially
creating a problem.

Yes, they know where
they're going to is secure,

but how does the person who
wants to go there know that?

So there needs to be better
accessibility on these websites

to support people
with a vision impairment

or any other form of disability
to be able to access content

as the rest of us in society do.

It's not appropriate
that they can't.

[Luke] So I'll get off my soap box now.
[Narelle] Okay.

[Narelle] No,no, no, don't, because
I've got one more for you.

Hang on. Hang on here, Luke.

Okay, and we
were talking briefly,

One of the things I see as an auditor
is the use of the noscript,

where they inject,
they put JavaScript, basically,

[Luke] Yep.
[Narelle] in a HTML page.

Now that can be possibly
hacked as well, I would assume,

because it's just
adding JavaScript,

and JavaScript is the basis of
what a lot of hackers work with.

[Luke] Yeah. So, JavaScript,
it's a processing language,

so it can do a lot
of really cool stuff.

But if somebody is
going to be putting,

it's possible to put malicious
JavaScript on a page,

but that means they have to
have compromised the page,

-[Narelle] Yeah. Okay.
-[Luke] So,

long as you're, again,

so long as you're
going to reputable sites,

let's just say Telstra
or Optus or AGL,

whoever else it might be,

they're going to have systems

and processes to prevent
those types of attacks.

If somebody is attacking
the website to take it over,

to install malicious code,

then they are dealing with a

different level of
skilled attacker.

And that is a problem for
the business to deal with,

where everybody being at,

with a disability or
without a disability,

now has to deal with.

There was an attack on British
Airways website a few years back

where they did a
similar attack using, um,

I think it was a
Python code repository,

that let them do all sorts of…

from a cyber security
point, pretty cool,

but in reality, pretty evil
things of how they did it.

But that just comes down,

the site got compromised,

because supply chain
wasn't checked correctly.

But that is a problem for
the business to manage,

not the, not the individual.

Because the individuals are
consuming the service.

The business has an obligation…

to make sure that their
systems are secure,

well managed and accessible.

And if they're not doing that,
they need to be held to account.

[Narelle] Yeah.

My minds racing now.

[both laugh]

[Narelle] Okay.

With all that in mind…

[Luke] Yep.

[Narelle] What's a
couple of tips you can give

for the person going
onto the website,

regardless, you know,

disability, without disability,

and you've given some good
tips as you go through it.

What's a couple of other
things that they can do?

Other than the HTTPS
stuff we've talked about,

just to make sure they're safe.

And, particularly, obviously, we
aim at people with disability.

[Luke] Yeah. There's
a couple of things that,

it probably might not
be website specific,

but if your computer is
asking to update itself,

let it.

Same for your phone.

Let it. Your phone saying I need
to restart to apply an update,

don't delay, delay, delay,
for a week, a month, whatever.

Just let it do it.

Do you, like I know you're going
to lose all your browser tabs,

but just let it update.

The same goes for your
browser when it wants to update.

When they're
releasing those updates,

they are addressing
security problems,

they are addressing
performance problems,

and they're addressing
functionality problems.

So by letting it update,
you're removing those risks.

You're letting it do what
it needs to do to fix itself.

That's the first one.
The second one, I'd say,

multi-factor authentication..

If something has
it as an option,

use it.

While it is not the silver bullet
to all prevent impersonations

or account takeover attacks,

it is one of the strongest
tools to prevent that.

If you're dealing with somebody

who can do what's called

a multi-factor bypass attack,

you are dealing with
a very skilled attacker,

and we have a different problem

that we should have a
separate conversation about,

because that's a whole
different barrel of fish.

Multi-factor, if it's
available, use it.

[Narelle] Yeah.

[Luke] The other thing I
could probably think to say is,

if you don't know what it is,
please don't click on it.

And that actually goes
for QR codes as well.

Like QR codes…

[Narelle] Yeah.

[Luke] If they're on
the back of a food packet

or at the 7-eleven
next to the counter,

they're fine.

They are, someone has…

A human or a product
developer in another,

in a warehouse, whatever,

designed a QR code to
go on this food packet.

That's fine. That is safe.

But there's been a tax on

parking meters, on
charging stations,

where bad guys have gone
along and put a QR sticker…

stickers over the QR
codes on those machines.

And when you go and scan them,

it now brings up the attackers
website asking for your details.

So use the app,

i, if you can.

Just use the credit
card tap and pay.

If it's not something that
is in a human's line of sight,

24 by seven,

don't trust it.

I'm not saying put on
your tin foil hat and…

tin foil the windows,
that's my job.

But be aware that people…

will be trying to take
advantage of your good nature,

and your willingness
and want to trust

and the bad guys
take advantage of that

and that is how they
generate revenue.

So just stop,

breathe, think,

then act.

[Narelle] Okay.

Okay, so let's flip
this on its head.

What tips can you
give developers,

designers?

[Luke] Developers and designers,
alt text is your friend.

Use alt text.

Using roll over, drop down,

menu functionality is
not disability friendly.

If you have to hover over a link

to make it pop down the screen,

you've just lost
access to people

who may not have a steady hand,

who do not have perfect vision,

who do not have
the tactile control.

So make it direct
buttons or make it…

things that provide a
function, not a hey, pop down.

Here's 15 things with
sub menu and sub menu,

and if you happen to
move off that menu slightly,

the entire thing collapses

No. If you have to do, pop
down and pop out menus,

give it a two or three
second delay to close,

so the person has the
option to bring it back on.

Make it so that the site
can be navigable via…

tab keys,

arrow keys, things like that,

so there's actually tabination
set up through the site.

Doing that, you're starting
to go on a long way.

Trying to think what else
would be appropriate there.

Those are the big ones.

If you having carousels, don't
make the images move quickly.

-[Narelle] Yep.
-[Luke] Yeah.

[Narelle] I hate carousels.

I really hate carousels now.

[Luke] They're great
from a marketing perspective.

Sure, you got five images,

but don't be image, image,
image, image, image, go.

Image, count to eight.

Image, count to eight.

That's fine. That sort of
pacing, give the person…

the ability to see,

analyse and respond to the
stimuli that's being presented.

Not everybody is able to go,

not everyone's got the
reflexes of a seven year old,

to go push a button, done.

Need to provide the opportunity
and time delays to that.

Or if you really want to push,

if you really want to push
down the accessibility path,

perhaps set up a mirrored
version of your site,

which actually has
accessibility version

as a button that's easy to find.

So then that way,

here's the entire site,

but designed without
all the bells and whistles,

designed to be accessible.

This all provides the
same functionality,

but you don't need to have
those super fast carousels

and the drop down,
roll out menus,

and all of the things that make
it hard for somebody with a,

a form of impairment
to be able to…

use the tools that
everyone else uses.

[Narelle] Luke, thank you.

That's been awesome.

Now, you know, next
time we have a cuppa,

I'm going to say, okay,
Luke, let's keep going.

-[Luke] Happy to.
-[Narelle] Let's discuss this.

[Narelle] Luke, how
can people contact you?

Because, obviously,
for anyone, any developer,

designer, they do need
to know what they're doing.

Digital Accessibility
is so important.

[Luke] Yes.

[Narelle] How can
they get onto you?

[Luke] Yeah, so I
can be reached on…

info@aegiscyber.com.au.

You can look me up on
LinkedIn as Luke Irwin.

I-R-W-I-N.

More than happy to have a
chat around cyber security.

Having to chat around some of
the basics around accessibility,

but for in-depth stuff, I'll
pass you on to an expert I know.

She happens to be the
other person on this chat.

Most of what I've
learned, I've learnt from her.

But yeah, it's, from the
website, from LinkedIn,

happy to have a chat
around cyber security,

what you can do to try
and make things better,

more secure and more accessible.

[Narelle] You know what?

This has really
made me realise how...

digital accessibility
can help cyber security,

because the stuff
we've been talking about,

I mean, there is an actual success
criteria about authentication.

[Luke] Yes.

[Narelle] There's a
success criteria about links,

about…

all types of stuff,
the alt text, it's there.

[Luke] Yeah.

The moment we started
having this conversation,

my brain had already
started processing going,

how can we do MFA
in a secure manner

for somebody who

has a vision impairment?

Okay, what systems and tools,
I can think of a couple,

like, there's one's
called YubiKey,

but they cost $10
per person per month,

and they're generally
aimed at large corporates.

[Narelle] Yeah.

[Luke] So not really suitable or
applicable for the individual.

So I'll be having conversations
with some of my peers to go,

hey guys, how can we do this?

What's a method?

'Cause they're very interesting
and important questions.

[Narelle] Yeah, they are.

I just, look, I really
appreciate your time, Luke.

[Luke] No worries.

[Narelle] Everytime
I sit with you,

I learn and I love learning.

So Luke, have a great week.

And for everyone else
out there, look, please like,

subscribe, review, share.

And please tell people
about digital accessibility.

The benefits are for everyone.

Not just for people like myself.

Luke can see the benefits,

even on cyber security side, SEO
side, it has massive benefits,

And our…

next show will be next week
and talk to you then. Bye, bye.

[music playing]