xpresstex
IT SUPPORT YOU DESERVE

How to Use ZOOM SECURELY

zoom

There's been a barrage of bad press in recent months surrounding the popular virtual meeting software Zoom.

The lockdown saw a massive push for many to start using different software to communicate and collaborate with colleagues.

Zoom was on the receiving end of the majority of this demand. The popularity of the application has outstripped it's development team's ability to keep the app secure.

With several security vulnerabilities discovered the team have been working hard to patch the problems.

In this article, we'll cover the necessary steps you should take when creating a zoom meeting.

URL

First and foremost - never publish a meeting room link publicly. Any time you create a new Zoom meeting to schedule a meeting room URL is generated.

This URL is unique to your account the problem arises when someone finds that URL that's not necessarily invited to the meeting.

This is an easy mistake to make, good examples of accidentally publishing the URL include setting up a meeting on a platform such as Facebook, Meetup or Eventbrite.

All these platforms allow you to publish your Zoom URL; however, these pages are public, and bad actors can easily sniff out Zoom URLs using web scripting tools.

WAITING ROOM

One of the newest features Zoom has created to help combat the issue of unannounced visitors to your meeting is a waiting room.

When creating a new meeting in the Zoom scheduler, the option will now automatically be ticked to enable the waiting room.

This means anyone joining the meeting is automatically placed in the waiting room, and you have to allow them to enter the session manually.

PASSWORDS

Many were initially caught out by not enabling passwords on their Zoom meetings. Hackers had an easy job of just guessing meeting room IDs which are usually just a series of 10 digits.

Zooms response to this issue was to enable passwords on all meetings as default.

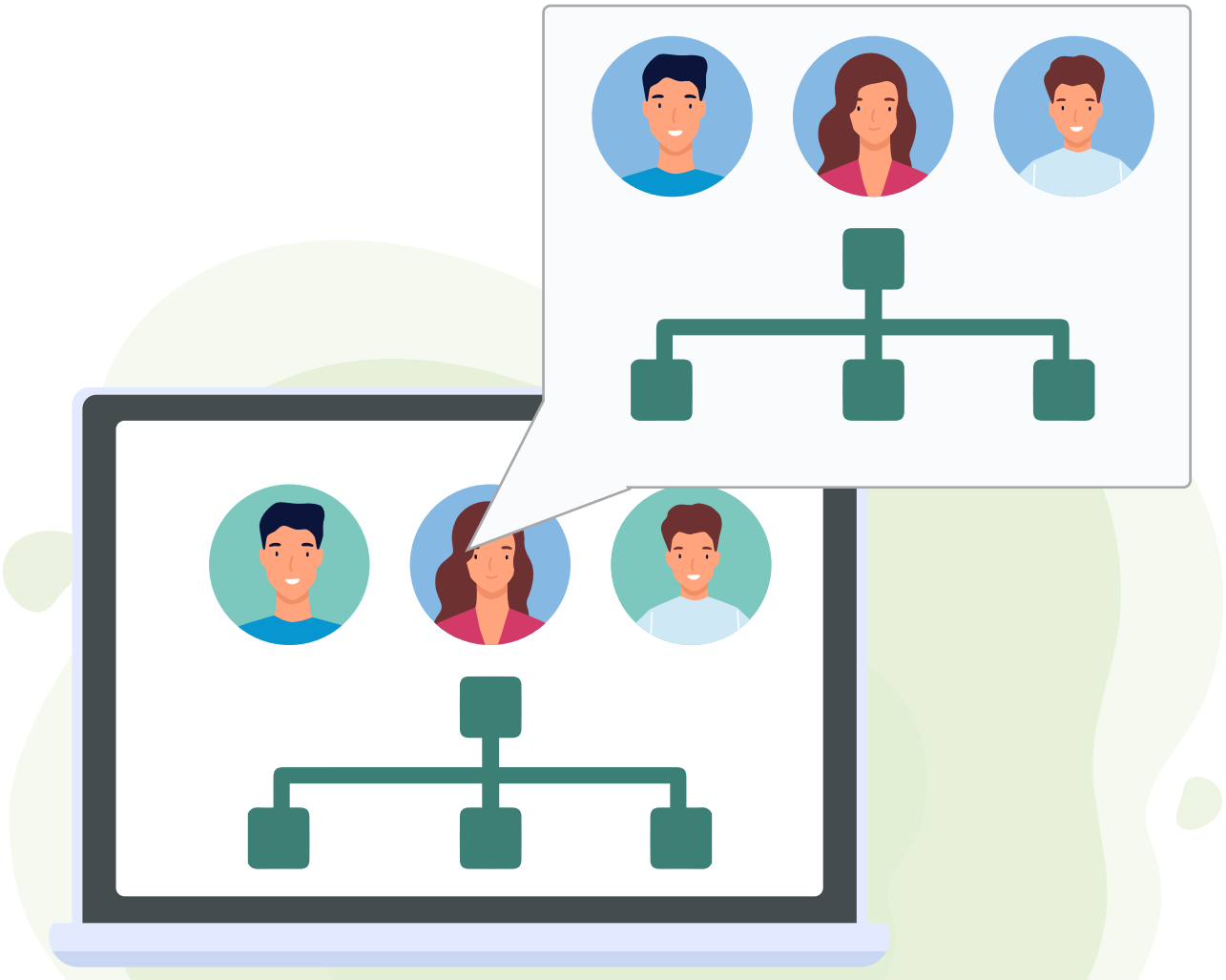
Anytime you create a new meeting now, passwords are enabled. This password is displayed in the meeting invite and is also encoded in the meeting room URL.

Again because it's encoded in the URL anyone with the URL can enter so do not make the URL public.

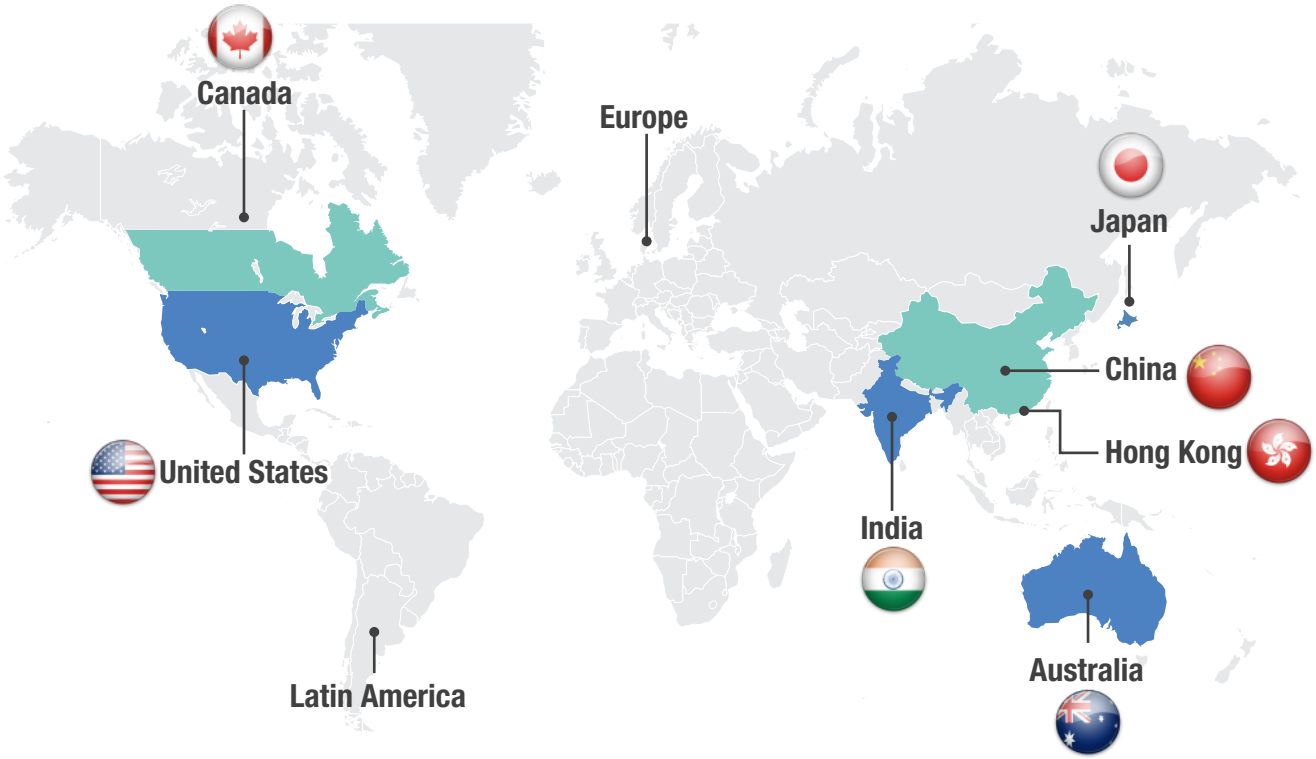
SCREEN SHARING

An easy one to miss but make sure you know who you are sharing your screen within a zoom meeting. Not all companies have a policy in place, but it's worth considering what data you are sharing on the screen and who might see it.

Remember anyone that is in the meeting might be recording the session without your knowledge as such just like you would with any physical data keep in mind what information you have on your screen during a zoom meeting.



DATA CENTRE



One of the latest features zoom now includes as part of their service is the ability to choose which data centre your zoom calls and meetings take place in.

If your company has strict policies about data not leaving the country, then you can now select which data centre to use by default. Here's the available list:

Zoom is actively working on the security of its platform. In this ever-changing environment speaking to a technology expert to make sure your systems are secure is essential.

If you found this article useful and would like further information on how to secure your online meetings no matter what platform you are on, then click here.

CONTACT US

xpresstex
IT SUPPORT YOU DESERVE

enquiries@xpresstex.com.au
1300 991 030