VIDEOCONFERENCING: SKYPING AND ZOOMBOMBING

Kathryn Dalziel

Barrister, Christchurch

Now, more than ever we need video chat to connect. Video chat creates community and communication. It is great for business.

There are plenty of video chat apps from which to choose. For example: Facetime; Google Hangouts Meet; and WhatsApp. The two market leaders are Skype and Zoom.

Skype is Microsoft's well-established video and telephone conferencing tool with instant messaging. Zoom is a product from Zoom Video Communications, Inc California that also provides video and telephone conferencing as well as instant messaging.

With COVID-19 lockdowns happening all over the world, many people are regretting not buying shares in these businesses!

But are Skype and Zoom providing private and secure environments?

- Ironically, both environments carry high risk of spreading online viruses. In any open platform where there is file sharing, people are vulnerable to spam, malware, phishing and other on-line attacks. Never download any attachment from someone you do not know and make sure you have good anti-virus software.
- Invitations to open conference meetings can also be sent to people with criminal intent. Be cautious about joining in an open on-line conference into which anyone can join. Your identity and contact details may not be secure. Don't assume that everyone at the conference is who they say they are.
- Despite claims to the contrary, both environments do not provide secure end to end encryption. What does this mean? It means that Zoom and Skype can technically access the conference or chat. While there is encryption by both platforms to avoid third party eavesdropping, it is decrypted by their servers. You have to rely on their promises not to eavesdrop.
- Both companies use integration tools with other products. For example: both integrate with Outlook, and Zoom integrates with Dropbox. As soon as you have integrations, there is risk other information can be accessed. Again, you have to rely on their promises not to do that.
- As Skype is a Microsoft product, it has the same privacy policy as Microsoft. A Microsoft account is required to use Skype. See privacy policy here: https://privacy.microsoft.com/en-us/privacystatement
- Skype users can access other users' IP addresses which is useful to share a file but also can be used by a hacker to obtain your IP address and match it up with other personal information obtained about a person. You can use a virtual private network (VPN) to work round this.
- There are some privacy benefits with the Microsoft platform including 2-factor authentication: worth exploring to protect your systems. Zoom has brought in optional 2-factor authentication for its conferences. The first authentication is the meeting ID number and the optional authentication is the use of a password.
- Zoom's privacy statement can be found here: https://zoom.us/privacy
- Zoom has been caught out by its sudden popularity during the COVID-19 lockdown (see https://healthitsecurity.com/news/zoom-domains-targeted-by-hackers-as-use-surges-with-covid-19.) It has had to focus on its privacy and security to avoid data breaches including holding

Zoom meeting recordings in an open part of their cloud (now fixed) and "zoombombing" which is the action of an uninvited guest joining a zoom meeting. Key takeaways are:

- Keep your personal meeting ID secure (ie do not give it out to people you do not know). If zooming with a big group meeting: create a random meeting ID
- Use two factor authentication: require a password to join
- Use the waiting room feature so people cannot join the meeting unless authorised
- You can lock the meeting once started
- If meeting is recorded, retain the information in your secure IT environment

There are other tips. See https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/; and https://ftw.usatoday.com/2020/03/zoom-bombing-how-to-prevent-it

Also the NZ Government's National Cyber Security Centre has released good advice on use of Zoom and guidance for working remotely and cloud security: see https://www.ncsc.govt.nz/newsroom/zoom-security-advice-for-public-servants/

In summary, these environments are not secure so always take care. If using any video chat platform: be careful about sharing sensitive information and avoid file sharing where possible.

Happy skyping and zooming everybody!