Eastern Region Special Operations Unit

Regional Organised Crime Unit

COVID-19 CYBER & FRAUD PROTECT MESSAGES

Tuesday 28th April 2020

Today's topic is 'Video Conferencing'.

For many, the sudden adoption of remote working, social distancing and self-isolation has created a demand for simple easy ways to stay in touch with family, friends and co-workers. The demand has popularised many apps and one of the most talked about in Cyber Security circles is Zoom, a video chat platform, available in both free and paid for versions.

Unfortunately, Zoom has received quite a lot of adverse publicity because of a number of important security flaws. Criticism has ranged from uninvited people joining your conversation to deliver racist messages or pornographic images, to poor encryption methods that mean private conversations are not always private. The guidance below has been written for home and business users that may have adopted zoom, for its ease of use, availability and in the absence of a paid for service.

WHAT CAN I DO?
For those of you using Zoom, make sure you have the latest version of their software. Click your user icon and select '**Check for Updates**'. Usually, updates fix known security flaws.
Running anti-virus software or a firewall on your computer and keeping software up-to-date will improve your security.

If you are holding public meetings, where anyone can join the conversation, be sure to configure screen-sharing settings.
Go to '**In Meeting (Basic)**' and select '**host alone can share**' or **turn off screen sharing entirely**. This can also be controlled by the host during a meeting.
Finally, turn of **'Annotation'**, if you are worried about how people might annotate your shared slide show.

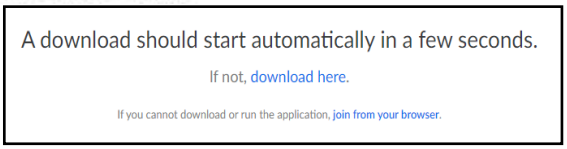
Stop Uninvited Guests
Setting up a Zoom meeting creates a **9 digit ID**. Anyone who has this ID can join the conversation. **Don't advertise it publicly by posting it on your Social media.**
If you use the '**Options Panel**' when setting up a meeting, you can add an **access password** too. Would-be trolls now need an ID and a password to gate crash your meeting.
Use the '**Advanced Options**' to enable a '**Waiting Room**'. This puts people in a holding area before you grant or deny them access to your conversation.
Organisers can lock the meeting once everyone who needs to has joined. Click **Manage Participants** >> **More** >> **Lock Meeting**.

Stay Private
The organiser of a meeting can record audio and video from the meeting. Also, anyone involved in a '**private chat**' can save this as a log file.
Turn off video and mute yourself unless needed. This prevents video recording conversations in your home or exposing information inadvertently. It is possible to encrypt your video calls in the settings panel, which will improve the confidentiality of your conversations. Be aware, however that there is no certainty as to whether this is end-to-end encryption.

Eastern Region Special Operations Unit

Regional Organised Crime Unit

Accessing Zoom through the browser is more secure than downloading the app. The feature is available on the log in screen when invited to a meeting, although hard to spot.



Always Be Aware

Your conversations may not be as private as you would like. Is Siri, Alexa or Google assistant in range? They will ALWAYS be listening and passing info back to their servers to maintain the connection and sampling purposes.

Final Thoughts

Whatever platform is chosen it is vital that all the security settings are reviewed and implemented as appropriate.
In circumstances where sensitive or confidential discussions are being held other providers, such as Google Duo, Skype, Face Time, WhatsApp and Webex might be alternatives.

Hot topics

Reports received of emails purporting to be from Virgin Media, informing recipients that their bill is ready. The emails include information on how Virgin Media are responding to the COVID-19 outbreak. The bill amount commonly equates to £60.78. There are also emails purporting to be from the Virgin Media e-billing team, advising recipient that their account will be frozen because their bank details couldn't be validated.

Recipients are asked to click on a link to re-validate and amend their billing details. The link provides an opportunity for fraudsters to steal email passwords and personal details.
Microsoft Patches for April 2020 were released earlier in the week (Patch Tuesday) and contained over 100 fixes.

Reporting

Reporting to Action Fraud can be done online or by calling 0300 123 2040.
To report offers of financial assistance from HMRC, contact phishing@hmrc.gov.uk.

This advice has been collated by the East Midlands Regional Organised Crime Unit (ROCU) and is intended for wider distribution to raise awareness among businesses and the public.

Advice and information is changing daily as we navigate our way through the COVID-19 pandemic, so please ensure you only take information from reputable sources.

If you require any further information, assistance or guidance please contact the ERSOU Protect Team CyberProtect@ERSOU.pnn.police.uk or your local Force protect team.