ใช้ ZOOM อย่างไรไม่ให้โดนโจมตีแบบ ZOOM-BOMBING

ที่มา:

- https://www.bleepingcomputer.com/news/software/how-to-secure-your-zoom-meetings-from-zoom-bombing-attacks
- https://www.catcyfence.com/it-security/article/secure-zoom-from-zoom-bombing/

Zoom-bombing

คือ คนอื่นสามารถเข้ามาร่วมการประชุม Zoom meeting ได้โดยไม่ได้รับอนุญาต

จุดประสงค์ คือต้องการสร้างการรบกวน เช่น เผยแพร่ภาพอนาจาร ส่งข้อความหยาบคาย หรือ แอบบันทึกการประชุม เพื่อเอาไปเผยแพร่บน Social media ในภายหลัง โดยเมื่อไม่นานมานี้ทาง FBI ได้ออกมาเตือนผู้ใช้งาน Zoom และแนะนำให้มีการตั้งค่าความปลอดภัยบน Zoom อย่างเหมาะสม เพื่อหลีกเลี่ยงจากการโจมตีด้วย Zoom-bombing สามารถทำได้ดังนี้

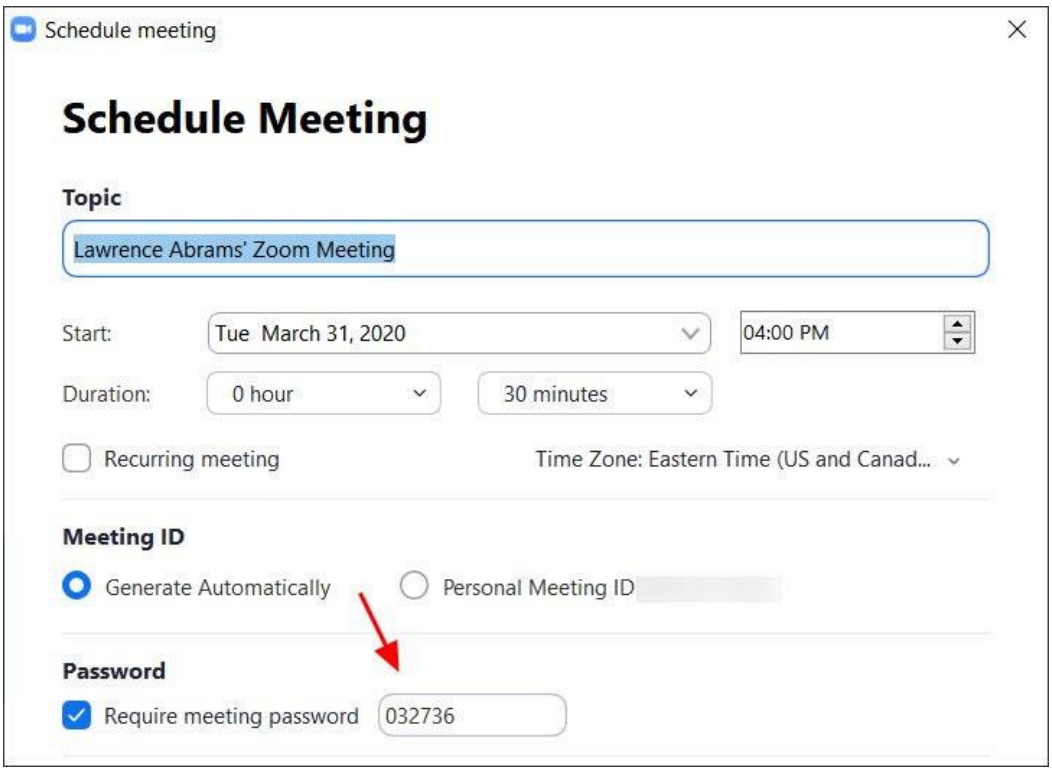
1. หมั่นสังเกตในขณะใช้งาน ZOOM MEETING เพื่อป้องกันตัวเอง

ผู้ตั้งห้องประชุม (Host) ขณะกำลังนำเสนองาน จะสามารถบันทึก Video ในการ Meeting ครั้งนั้น ๆ ได้ แต่เมื่อมีการบันทึก Video โดย Host จะมี Icon ขึ้นมาเตือนมุมซ้ายบนหน้าจอ Meeting ว่า Recording ผู้เข้าร่วมสามารถโต้แย้ง ไม่ให้มีการบันทึก Video ได้ และโปรแกรม Zoom โดยทั่วไปไม่ได้มีการเชื่อมต่อแบบ end-to-end encryption (E2E) หมายความว่า ถึงแม้จะมีการเข้ารหัสการเชื่อมต่อระหว่างผู้เข้าร่วมประชุมกับ Server Zoom ในขณะที่มีการแชร์ข้อมูล หรือ นำเสนองานผ่านเครือข่ายของ Zoom ที่ไม่ได้ถูกเข้ารหัส ก็จะทำให้ทางพนักงานของ Zoom สามารถเข้าถึงข้อมูลเหล่านี้ได้

** ขณะนี้ได้ปรับแก้ไข เพื่อป้องกันและเพิ่มความปลอดภัยให้แก่ผู้ใช้งานแล้ว คนอื่น หรือแม้แต่พนักงาน ZOOM ก็จะไม่สามารถเข้าถึงข้อมูลของผู้ใช้งานได้ แนะนำให้ผู้ใช้งานหมั่นอัปเดตเวอร์ชันสม่ำเสมอ*

2. ตั้งรหัสผ่านห้องประชุม ZOOM MEETING ทุกครั้ง

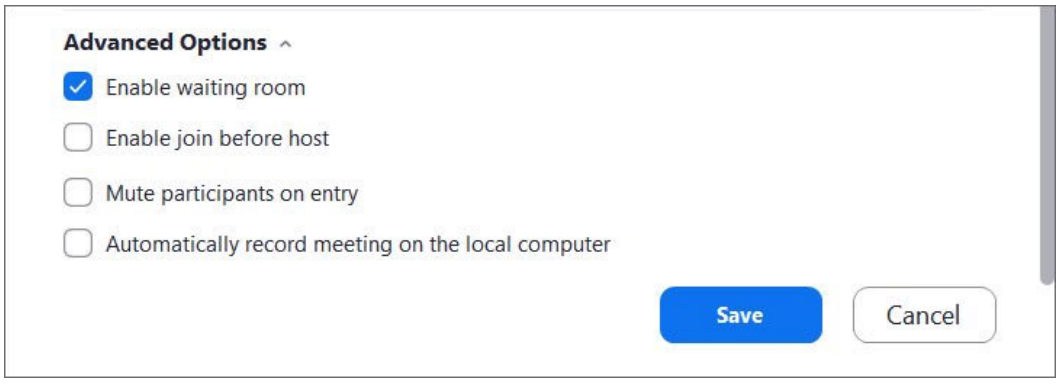
ขณะสร้างห้องประชุม Zoom meeting ให้ Add password ลงไปยังทุก Meeting เพื่อป้องกันไม่ให้คนอื่นเข้าร่วมประชุมได้ ซึ่งโดยปกติแล้ว Zoom จะบังคับให้ใส่ password สำหรับ Meeting โดยถูกสร้างเป็นการตั้งค่าเริ่มต้น



ภาพจาก www.bleepingcomputer.com

3. เปิดฟังก์ชัน “ห้องรอประชุม” ป้องกันผู้เข้าร่วมประชุมก่อนได้รับอนุญาต

เปิดการใช้งาน Enable waiting room เพื่อป้องกันการเข้าถึง Zoom โดยไม่ได้รับอนุญาตจากผู้สร้างห้องประชุม Zoom meeting



ภาพจาก www.bleepingcomputer.com

4. หมั่นอัปเดต ZOOM CLIENT สม่ำเสมอ

ผู้พัฒนาจะพัฒนาโปรแกรมเพื่ออุดรูรั่ว และป้องกันถูกแฮกจากผู้ไม่หวังดี ซึ่งเวอร์ชันล่าสุดได้อัปเดตการบังคับให้ใส่รหัสผ่าน Zoom meeting ดังนั้นจึงจำเป็นต้องอัปเดต Zoom อย่างสม่ำเสมอ

5. ไม่เปิดเผย / แชร์ MEETING ID ให้คนอื่นรับทราบ

ไม่โพส หรือ Share Meeting ID ลง Social media หรือส่งในกรุ๊ปไลน์ ที่มีคนอื่นอยู่ด้วย โดยต้องมั่นใจว่าเราได้ส่ง Meeting ID ให้ถูกคนและผู้ที่ได้รับ Meeting นั้นอยู่ในการประชุมจริง ๆ

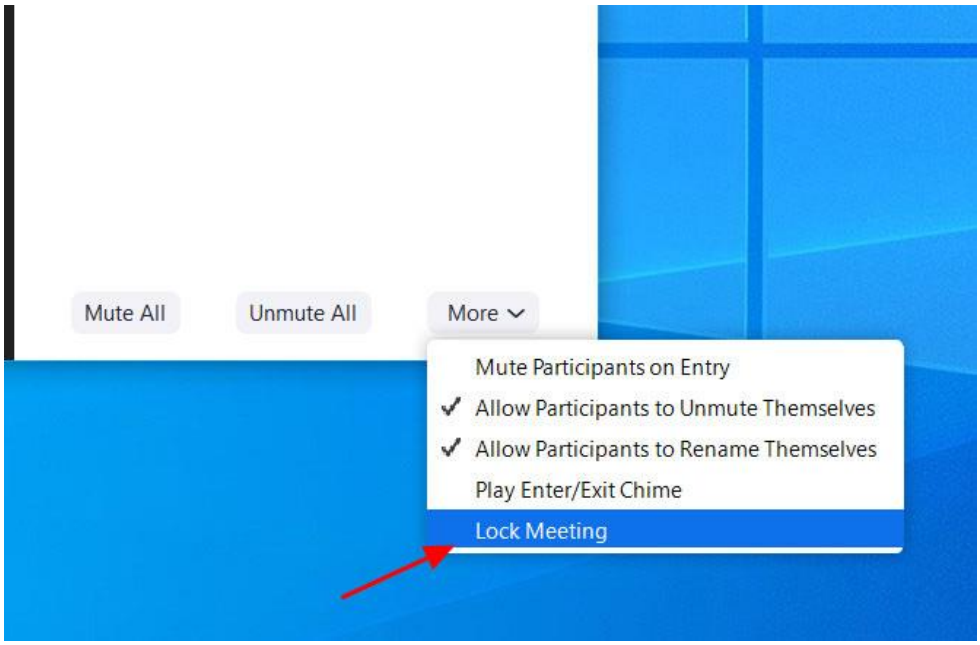
6. ปิดการแชร์หน้าจอ ของผู้เข้าร่วมประชุม

เพื่อป้องกันไม่ให้ผู้เข้าร่วมคนอื่นนอกเหนือจาก Host แชร์หน้าจอของตนไปยังที่อื่น ให้เลือกปุ่ม Share Screen > Advanced Sharing Options > Who Can Share > Only Host.

ภาพจาก www.bleepingcomputer.com

7. ล็อกห้อง ZOOM MEETING ทันที ที่ผู้เข้าร่วมครบ

หลังจากผู้เข้าร่วม Meeting ครบแล้วให้ทำการ Lock Meeting โดยไปที่เมนู Manage Participants > More > Lock Meeting



ภาพจาก www.bleepingcomputer.com

8. ไม่โพสภาพการประชุม ZOOM MEETING ลง SOCIAL MEDIA

ไม่โพสรูปภาพขณะกำลัง Meeting ของ Zoom เนื่องจากจะทำให้ผู้อื่นสามารถเห็น Meeting ID ของเราและทำให้มีผู้ไม่หวังดีอาจพยายามที่จะเข้าร่วม Meeting โดยไม่ได้รับเชิญ