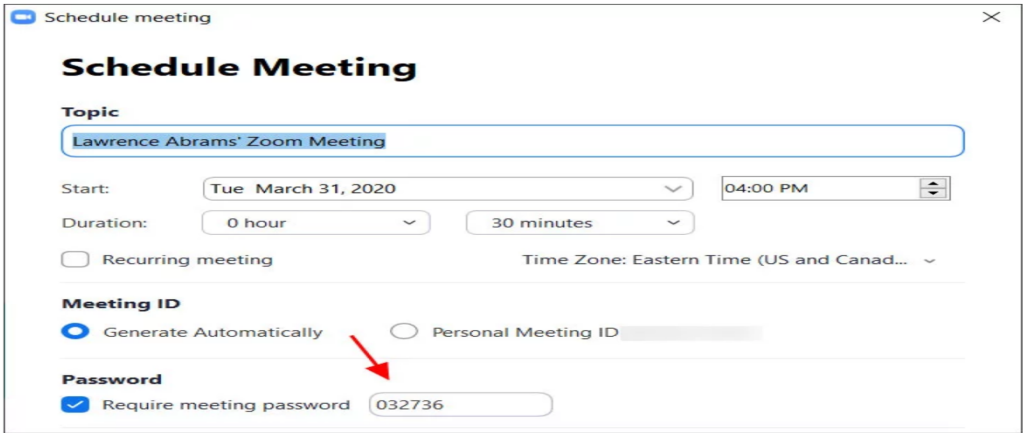
كيفية تأمين الحماية لاجتماعات ومحاضرات منصة زووم من أي هجوم ك "Zoom Bombing Attack"

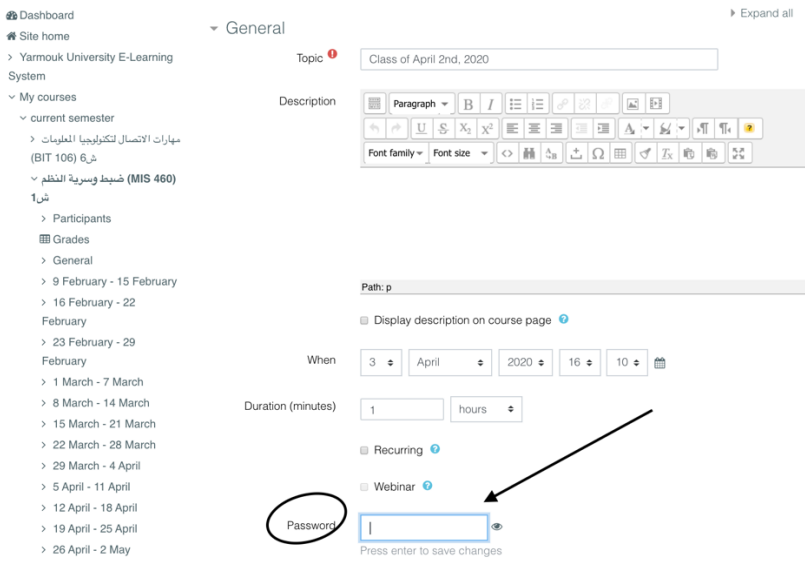
منصة ZOOM هي برنامج يستخدم لعقد الاجتماعات عبر شبكة الانترنت و يقدم خدمة التواصل و مشاركة المعلومات. ومع انتشار فايروس كورونا حول العالم، ازداد استخدام هذا البرنامج بشكل غير مسبوق حيث أن العديد من الشركات والمؤسسات التعليمية بدأت باستخدام هذه البرنامج لتسيير أعمالها. وبرنامج زووم ZOOM كغيره من البرامج والأنظمة المختلفة، فانه عرضة للهجمات الإلكترونية والاختراقات الأمنية والتي من الممكن أن تهدد خصوصية هذه الاجتماعات التي يتم عقدها باستخدام برنامج التواصل زووم ZOOM.

وقد قامت جامعة اليرموك باستخدام برنامج زووم ZOOM في العملية التعليمية وعقد المحاضرات المختلفة ومن أجل زيادة تأمين الحماية أثناء عقد المحاضرات والاجتماعات، تالياً بعض الإجراءات التي يمكن استخدامها من أجل زيادة الحماية أثناء استخدام زووم:

1 - استخدام كلمة المرور "Password": عند البدء بإنشاء اجتماع عبر برنامج زووم ZOOM، بإمكانك تفعيل استخدام كلمة السر للاجتماع بحيث لا يستطيع أي شخص الدخول الى الاجتماع الا من يمتلك كلمة السر الخاصة بالاجتماع.
enable the "Require meeting password" setting and assign a random 6 - 8 digit password.

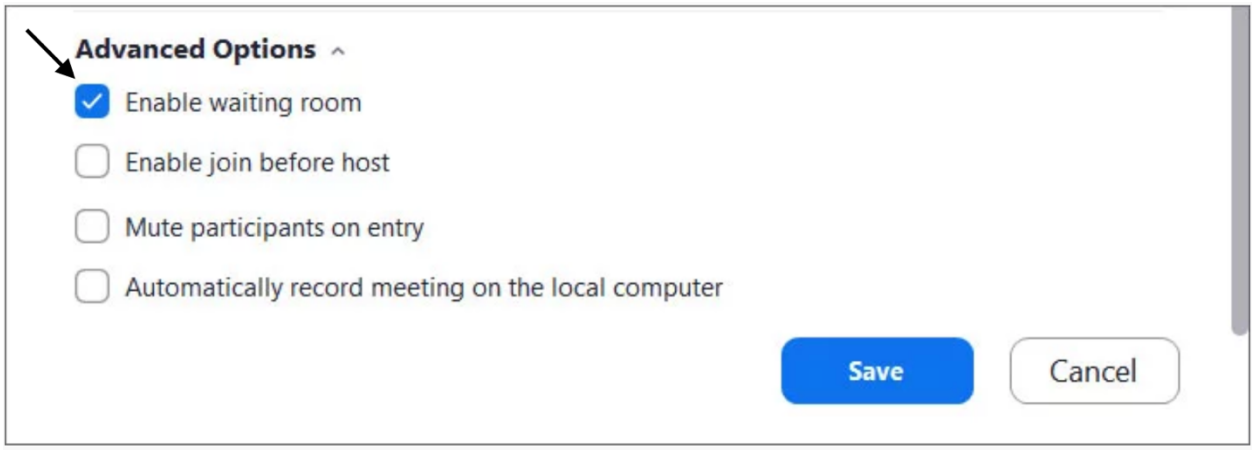
علماً بان الذي تصله الدعوة عبر الايميل او من خلال رابط ال URL تكون كلمة السر متضمنة بالرابط و الذي يقوم بمحاولة الانضمام من خلال ال meeting ID يحتاج الى كلمة المرور. لذا يرجى عدم نشر هذا الرابط على مواقع التواصل الاجتماعي.





2 - استخدام غرف الانتظار (waiting rooms): تمكن هذه الخاصية من منع دخول أي مشارك على الاجتماع الا بعد موافقة من أنشأ هذا الاجتماع (Host).

عندما يدخل المشارك الى الاجتماع، سوف يظهر تنبيه للمستضيف ويستطيع الموافقة على دخول المشترك للاجتماع او رفضه



3 - الحرص على تحديث برنامج الزووم باستمرار (Keep Zoom application updated): احرص على تحديث برنامج الزووم باستمرار (update) حيث ان الشركة المطورة تقوم باستمرار بإصدار تحديثات (updates) بشكل

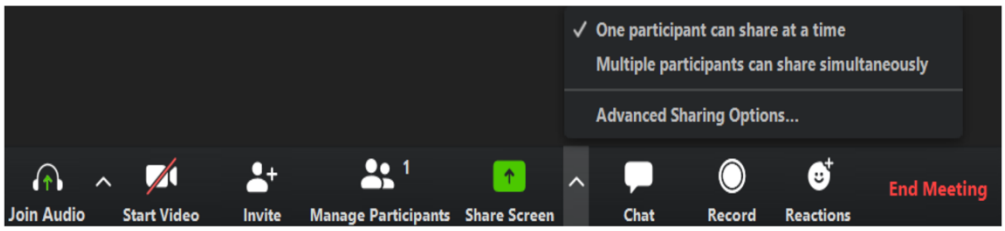
مستمر من اجل اصلاح أي نقاط ضعف في برنامج زووم و اخر هذه التحديثات كانت بتاريخ ٢٠٢٠\٤\٢ سواءً لمستخدمي نظام ال Windows و مستخدمي نظام MAC os.

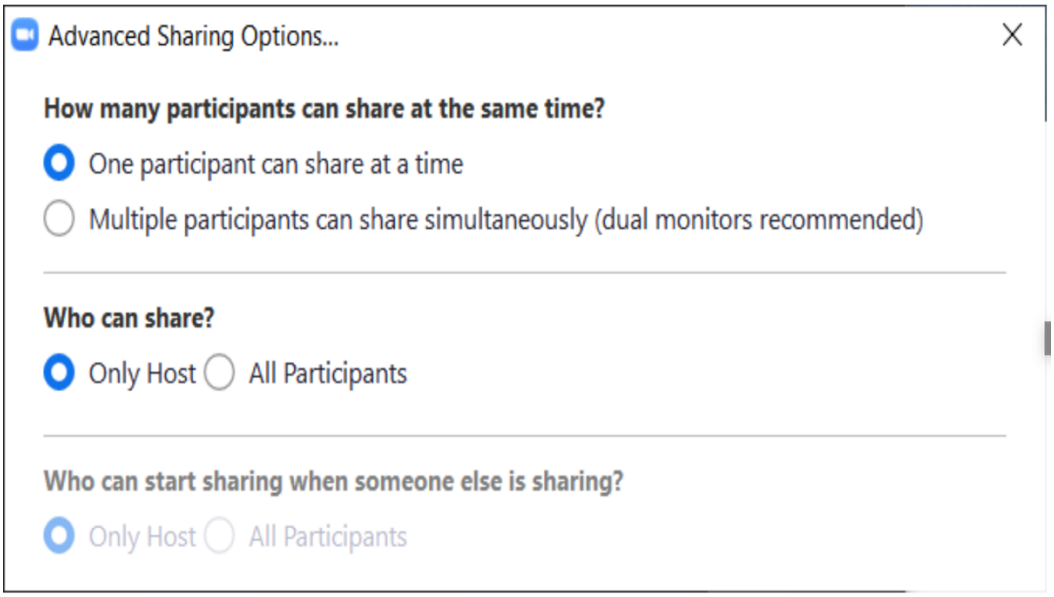
https://support.zoom.us/hc/en-us/articles/201361963-New-Updates-for-macOS

ملاحظة: بسبب سرعة انتشار واستخدام برنامج ZOOM فان العديد من القراصنة يحاولون باستمرار لاستغلال ذلك وإطلاق هجمات الكترونية على مستخدمي هذه البرنامج. لذلك احرص على متابعة اخر الاخبار والتحديثات.

4 - لا تقم بمشاركة او نشر الرقم التعريفي الشخصي الخاص بك "Don't share your Personal meeting ID":
كل شخص يستخدم برنامج الزووم ZOOM يعطى "Personal Meeting ID PMI" و اذا حصل على شخص على PMI فانه يستطيع الدخول في أي وقت و مشاهدة اذا كان هناك اجتماع او محاضرة قائمة.

5 - عدم السماح والتحكم بخاصية مشاركة الشاشة "Disable participant screen sharing": لمنع مشاركة وأي محتوى من قبل المشاركين والتحكم بهذه الخاصية بإمكانك التحكم بمن يستطيع عمل screen sharing وتكون هذه الخاصية فقط للمستضيف "Host"





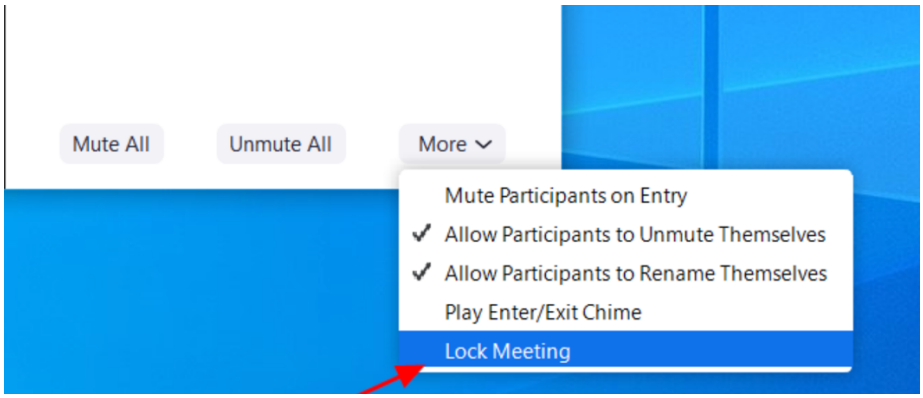
6 - خاصية اغلاق الاجتماع "Lock Meeting": بإمكانك عمل اغلاق للاجتماع عند دخول جميع المشاركين وعدم السماح بالدخول الى الاجتماع بعد الاقفال.

لعمل اغلاق للاجتماع او المحاضرة تستطيع عمل الإجراءات التالية:

1 - النقر على "Manage participants"

2 - النقر على "More"

3 - اختيار خيار "lock meeting"



7 - لا تنشر صور و screen shots للاجتماعات على مواقع التواصل الاجتماعي حيث من الممكن ان تتم سرقة ال PMI.

8 - لا تنشر رابط الاجتماع على مواقع التواصل الاجتماعي المختلفة وجعلها متاحة للجميع Public.

9 - يستخدم برنامج ال ZOOM في جامعة اليرموك من أجل إعطاء المحاضرات، لذا يرجى استخدامه بطريقة مهنية و ضمن نطاق المحاضرة فقط سواءً بمحتوى المحاضرة و المحادثة النصية للحماية من أي أخطاء او إجراءات غير صحيحة.

10 - احرص على تسجيل المحاضرات وتخزينها على جهاز الحاسوب الخاص بك.

11 - يفضل استخدام جهاز الحاسوب بدلا من الهاتف وذلك لان أنظمة الحماية على الحاسوب اعلى منها على الهاتف.

12 - عدم الضغط على عناوين URL مشبوهة أو تثبيت ملفات عشوائية، في بعض الأحيان قد ترى كلمات مثل : Zoomأو Google Hangouts ضمن اسم نطاق أو ملف، وتفترض أنها آمنة، ولكن لا تثق بها بسهولة، خاصةً إذا كانت من مرسِل غير معروف.

المراجع:

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

https://zoom.us/security