



إرشادات التعليم الافتراضي

الاحتياجات التقنية:

- أن يكون لدى الطالب والمعلم جهاز حاسب أو تابلت وفق لمواصفات أدناه أو أعلى
 - Intel Core i3 and faster
 - Memory 4GB or grater
 - Storage 250 SSD or grater
- تحميل برنامج Zoom للحصص الإلكترونية, والعمل على المنصة باستخدام متصفح Google Chrome والتأكد من متابعة التحديثات بشكل مستمر
- الحفاظ على سرية بيانات الحسابات
- تأمين اتصال جيد بالشبكة

الأداء السلوكي:	
1	الإضطلاع على نظام مكافحة جرائم المعلوماتية والتعرف على مخالفات السلوك الرقمي
2	الالتزام بسياسة التسجيل والنشر والتي تحذر دون إذن مسبق
3	الالتزام بأدب الحوار مع الآخرين والتقيد بالإنضباط التام
4	الالتزام بسياسة الحضور في المدارس
5	الالتزام باللباس الرسمي وعدم الظهور بهيئة مخالفة للنظام المدرسي
6	عدم مشاركة أو نشر أية مادة أو رابط يخالف التعليمات المدرسية أو بدون إذن من قبل المدرس
7	تسجيل الحصة الافتراضية للغايات التعليمية فقط ومن قبل المعلم أو الإدارة ويمكن للمعلم نشرها فقط على المنصة الخاصة للمدارس
8	حضور كامل الحصة الافتراضية والتفاعل مع المعلم
9	الالتزام بكافة المهام الأدائية التي نشر للطالب عن طريق المنصة
10	عدم مشاركة الروابط الخاصة بالحصص الإلكترونية والدخول للحصة عن طريق المنصة فقط



السياسات الخاصة ببرنامج (Zoom)

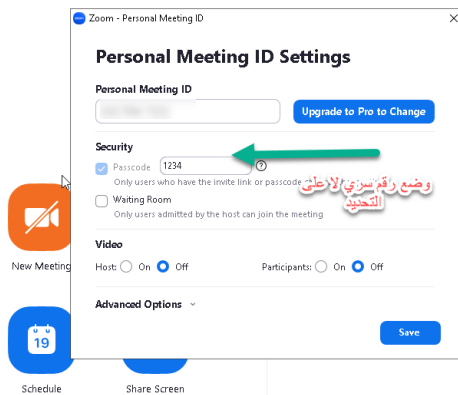
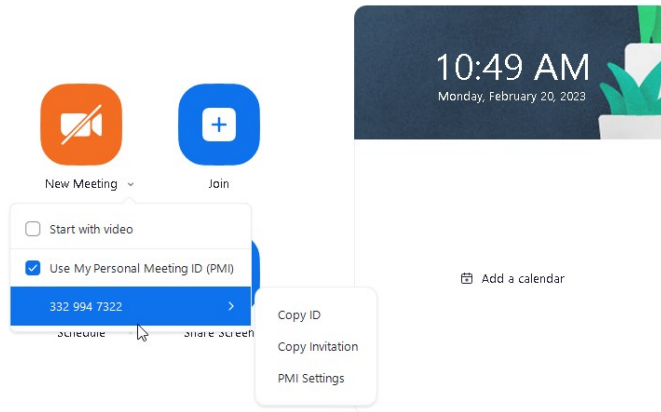
مقدمة:

نظام Zoom هو برنامج الاجتماعات المعتمد حاليا في المدارس لعمل حصة افتراضية ولكن يتم الدخول على الحصة عن طريق المنصة حصرا لتفادي عمليات مشاركة الروابط بين جهات خارجية ولحصار دخول المستخدمين.

إرشادات هامة

1. ضرورة حماية الاجتماع بكلمة مرور

والتي تعتبر أفضل طريقة لمنع دخول أي متسلل أو عابث بالاجتماع ونشر الرقم السري في وصف الحصة





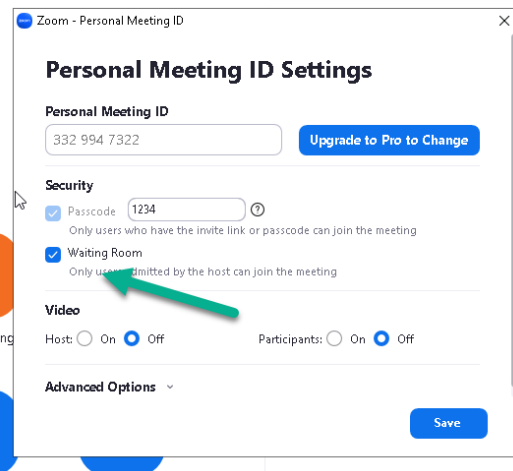
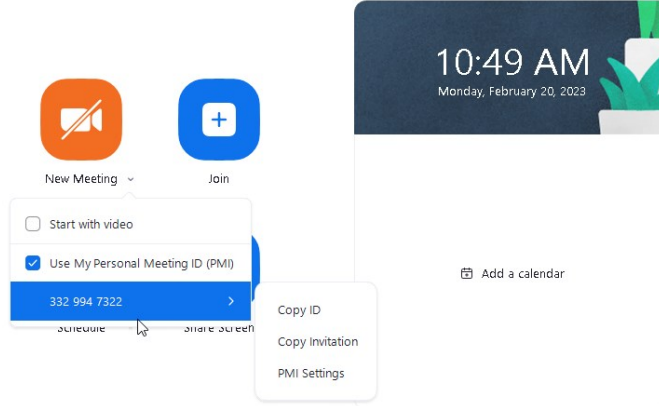
السياسات الخاصة ببرنامج (Zoom)

2. الإبتعاد عن الدخول للتطبيق عن طريق وسائل التواصل الاجتماعي أو حتى مشاركة الرابط الإجتماعات عن طريقهم.



3. تفعيل خاصية الإنتظار

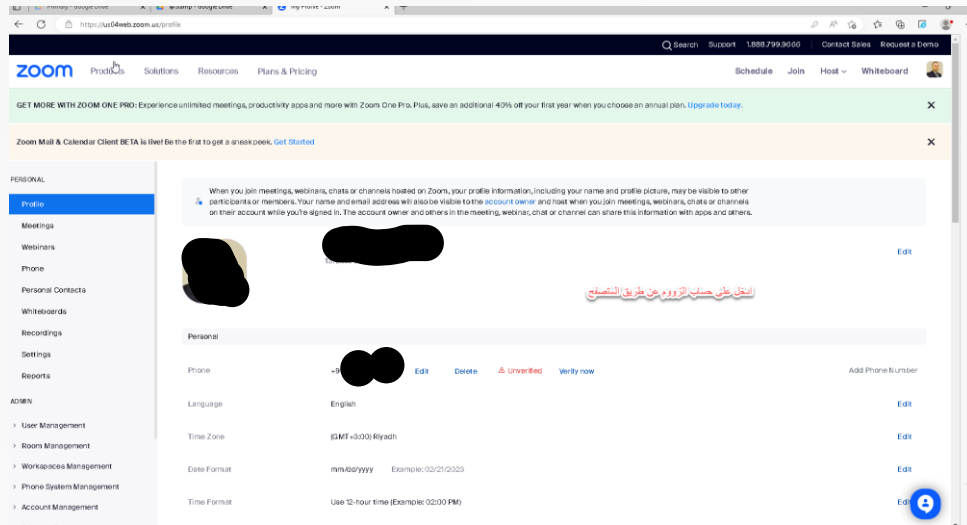
بحيث يظل المشاركون في الاجتماع بالإنتظار لحين موافقة المضيف على كل واحد منهم على حدة, مما يرفع الأمان والحماية من المخترقين.



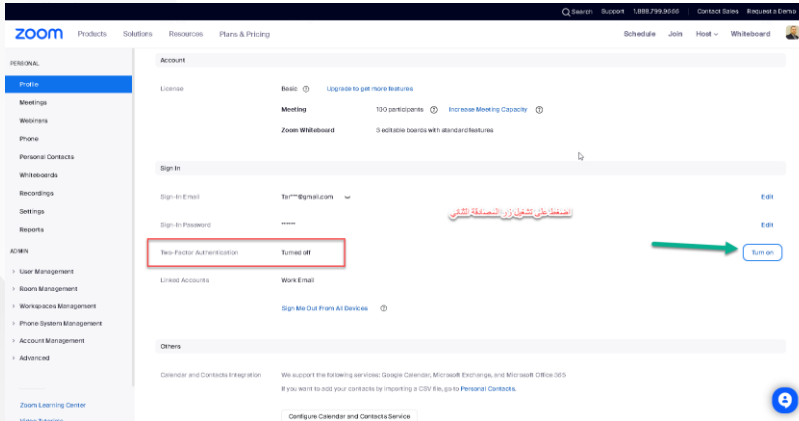


السياسات الخاصة ببرنامج (Zoom)

4. الاهتمام بحماية حسابك على التطبيق بالنسبة للمعلمين من خلال تفعيل ميزات الأمان ووضع كلمة مرور قوية يصعب التنبؤ بها وتفعيل نظام المصادقة الثنائية لزيادة الحماية



1



2

Turn On Two-factor Authentication

You can use any app that supports Time-based One-time Password (TOTP) protocol, including Google Authenticator (Android/iPhone) and Authenticator (Windows Phone 7).

Enter your password to turn on two-factor authentication

Next

Cancel

ضع الرقم السري الخاص بالحساب

3



السياسات الخاصة ببرنامج (Zoom)

Sign-In Password *****

Two-Factor Authentication On

Authentication App	Not configured	Set Up
SMS	Not configured	Set Up
Recovery Codes	Not available	

طريقتان للمصادقة الأولى عن طريق تنزيل تطبيق يسمى Google Authenticator أرىو
الدخول على الرابط لرؤية الشرح عن كيفية عمل المصادقة

4

فيديو لشرح كيف عملية المصادقة الثانية عن طريق رسائل الجوال

<https://www.youtube.com/watch?v=cGJFfdVizZI>

5

5. تحديد ميزات التحكم بالحصة

مثل مشاركة الشاشة فتح الصوت والمايك دون إذن عند البدئ لأي اجتماع

إلغاء صلاحية Chat

إلغاء صلاحية تغيير الاسم

إلغاء صلاحية فتح المايك

إلغاء صلاحية فتح الكاميرا

إلغاء صلاحية الكتابة على السبورة البيضاء

Lock Meeting

- ✓ Enable Waiting Room
- Hide Profile Pictures

Allow participants to:

- Share Screen
- ✓ Chat
- ✓ Rename Themselves
- ✓ Unmute Themselves
- ✓ Start Video
- ✓ Share Whiteboards
- ✓ Collaborate With Zoom Apps

Suspend Participant Activities

Tarek Al Soudani

Mute Start Video Security Participants Chat Share Screen Record Reactions Apps Whiteboards

6. ضرورة متابعة تحديثات تطبيق زووم وتحديثه باستمرار لضمان تحديثات الأمان عليه.