الجامعة العربية الأمريكية
ARAB AMERICAN UNIVERSITY

السياسات التنفيذية والإجراءات الخاصة بكلمات المرور

(باللغة العربية)

أعد بواسطة:
وحدة ضمان الجودة وأمن المعلومات - مكتب مساعد الرئيس لشؤون تكنولوجيا المعلومات

جدول المحتويات

إرشادات عامة حول إنشاء كلمة المرور

**يجب أن يكون جميع المستخدمين في الجامعة العربية الأمريكية على دراية بكيفية اختيار كلمات مرور قوية.

تتميز كلمات المرور القوية بالخصائص التالية:

- **يجب ان تحتوي كلمة المرور القوية على أحرف وأرقام حسب الشروط التالية:**
  1. أحرف صغيرة
  2. أحرف كبيرة
  3. أرقام
  4. أحرف "خاصة" (على سبيل المثال @ # $٪ ^ & * () _ + ~ | - = \ `{}[]:"؛ '<> / etc)
- **تحتوي على 8 أحرف على الأقل.**

تتميز كلمات المرور الضعيفة بالخصائص التالية:

- تحتوي كلمة المرور على أقل من 8 أحرف
- كلمة المرور هي كلمة موجودة في قاموس (إنجليزي أو أجنبي)
- كلمة المرور هي كلمة شائعة الاستخدام مثل:
  - أسماء العائلة والحيوانات الأليفة والأصدقاء وزملاء العمل والشخصيات الخيالية ، إلخ.
  - مصطلحات الكمبيوتر والأسماء والأوامر والمواقع والشركات والأجهزة والبرامج.
  - كلمات "AAUP" أو "sanjose" أو "sanfran" أو أي اشتقاق.
  - أعياد الميلاد وغيرها من المعلومات الشخصية مثل العناوين وأرقام الهواتف.
  - أنماط الكلمات أو الأرقام مثل aaabbb و qwerty و zyxwvuts و 123321 وما إلى ذلك.
  - أي مما ورد أعلاه مكتوب بالمقلوب.
  - أي مما سبق مسبوقًا أو متبوعًا برقم (على سبيل المثال ، secret1، secret1)

حاول إنشاء كلمات مرور يسهل تذكرها. تتمثل إحدى طرق القيام بذلك في إنشاء كلمة مرور بناءً على عنوان أغنية أو تأكيد أو عبارة أخرى. على سبيل المثال ، قد تكون العبارة: "This May Be One Way To Remember" ويمكن أن تكون كلمة المرور: "!TmB1w2R" أو "~ Tmb1W> r" أو بعض الأشكال الأخرى.

(ملاحظة: لا تستخدم أيًا من هذه الأمثلة ككلمات مرور!)

أسلوب المصادقة متعددة العوامل (MULTI FACTOR AUTHENTICATION)

المصادقة الثنائية (two factor authentication) ، التي يشار إليها أحيانًا بالتحقق بخطوتين أو المصادقة ثنائية العامل هي عملية أمان يوفر فيها المستخدمون عاملين مختلفين للتحقق من أنفسهم.

تعتمد أساليب المصادقة الثنائية على قيام المستخدم بتوفير كلمة مرور كعامل أول وعامل ثانٍ مختلف و عادةً ما يكون إما رمز أمان أو بصمة الإصبع أو الوجه.

تضيف المصادقة الثنائية طبقة إضافية من الأمان إلى عملية المصادقة من خلال التصعيب على الأشخاص الآخرين الوصول إلى أجهزة الشخص أو الحسابات عبر الإنترنت لأنه حتى لو تم اختراق كلمة المرور فإن كلمة المرور وحدها لا تكفي للدخول إلى حسابك.

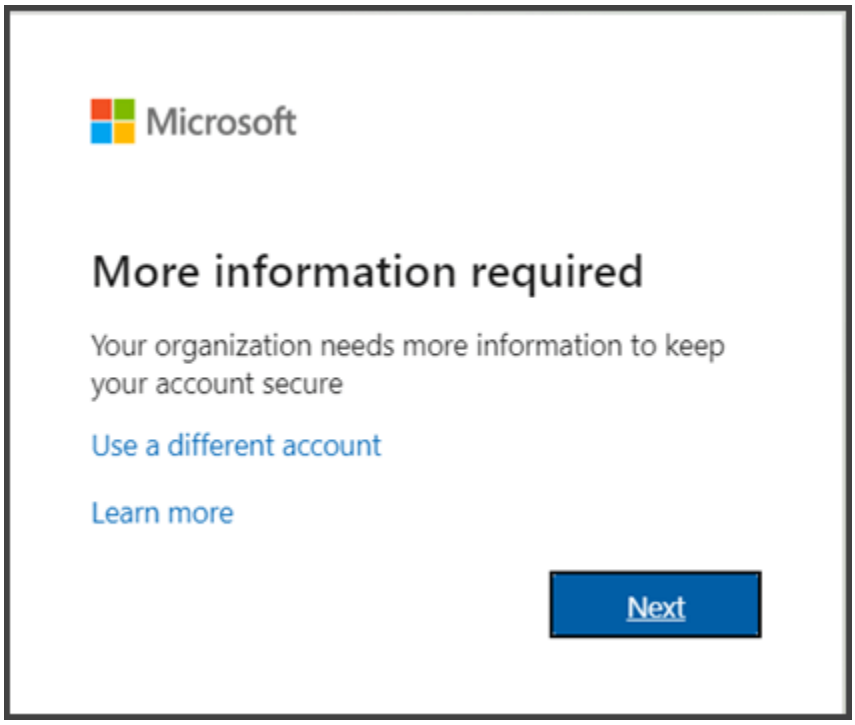
لطالما استخدمت المصادقة الثنائية للتحكم في الوصول إلى الأنظمة و البيانات الحساسة. و يستخدم مقدمو الخدمات عبر الإنترنت المصادقة الثنائية بشكل متزايد لحماية بيانات اعتماد المستخدمين من الهاكرز

تلميح :هل تريد التعرّف على المزيد حول المصادقة متعددة العوامل(MFA) ؟ راجع ما هو: المصادقة متعددة العوامل.

من خلال إعداد المصادقة متعددة العوامل(MFA) ، يمكنك إضافة طبقة أمان إضافية إلى عملية تسجيل الدخول إلى حسابك في Microsoft. على سبيل المثال، أدخل كلمة المرور أولا، وعند مطالبتك بذلك، اكتب أيضا رمز تحقق تم إنشاؤه ديناميكيا تم توفيره بواسطة تطبيق مصدق أو تم إرساله إلى هاتفك.

لتفعيل المصادقة الثنائية يرجى اتباع التعليمات التالية

1. سجّل الدخول إلى Microsoft 365 باستخدام حساب العمل أو المؤسسة التعليمية بكلمة مرورك كما تفعل عادةً.
2. **انقر هنا للدخول الى حسابك في موقع مايكروسوفت**
3. أدخل عنوان بريدك الالكتروني التابع للجامعة (مثال : xxx.xxx@aaup.edu)
4. ادخل كلمة المرور الخاصة بك والتي تستخدمها للدخول عادة.
5. بعد أن تختار **تسجيل الدخول**، ستتم مطالبتك بتوفير المزيد من المعلومات.



6. اختر **التالي**.

7. يجب تحميل تطبيق مايكروسوفت الخاص بالمصادقة الثنائية (Microsoft Authenticator)، لتحميل التطبيق **يرجى اتباع الرابط التالي**:

رابط تحميل تطبيق مايكروسوفت للمصادقة الثنائية (Microsoft Authenticator)

8. أسلوب المصادقة الافتراضي هو استخدام تطبيق Microsoft Authenticator المجاني. إذا كان مثبتاً على جهازك المحمول، فحدد **التالي** واتبع المطالبات لإضافة هذا الحساب. إذا لم يكن مثبتاً عليه، فهناك ارتباط يتم توفيره لتنزيل التطبيق. (**رابط تحميل تطبيق مايكروسوفت للمصادقة الثنائية**)

تلميح :الحصول على تطبيق Microsoft Authenticator المجاني
Microsoft Authenticator يمكن استخدامها ليس فقط في حسابات Microsoft أو العمل أو المدرسة، بل يمكنك أيضا استخدامها لتأمين حسابات Facebook و Twitterو Google و Amazon والعديد من أنواع الحسابات الأخرى. إنه مجاني على نظام التشغيل iOS أو Android.تعرف على المزيد واحصل عليه من هنا.

إذا كنت تفضل استخدام رسائل SMS تُرسل إلى هاتفك بدلاً من ذلك، فحدد **أريد إعداد أسلوب مختلف**. سيطلب Microsoft 365 رقم هاتفك الجوال ثم يرسل إليك رسالة SMS تتضمن رمزاً من 6 أرقام للتحقق من جهازك.

9. بعد إكمال الخطوات الإرشادية لتحديد أسلوب التحقق الإضافي لديك، ستتم مطالبتك في المرة التالية التي تسجّل فيها الدخول إلى Microsoft 365 بتقديم معلومات أو تنفيذ إجراء تحقق إضافي، مثل كتابة رمز التحقق الذي يوفره لك تطبيق المصدق أو الذي يُرسل إليك عبر رسالة نصية.

ملاحظة :بشكل عام، ستحتاج إلى أسلوب التحقق الإضافي فقط في المرة الأولى التي تسجّل الدخول من على جهاز أو تطبيق جديد أو بعد أن تقوم بتغيير كلمة مرورك. **لن يطلب منك على الأرجح رمز التحقق الإضافي بشكل يومي، ما لم تطلب مؤسستك ذلك.**

إضافة رقم هاتفك أو تغييره

يمكنك إضافة أرقام هواتف جديدة أو تحديث الأرقام الموجودة من صفحة التحقق من **الأمان** الإضافي. توصي Microsoft بشدة بإضافة رقم هاتف ثانوي للمساعدة في **منع اختراق** حسابك إذا تم فقدان هاتفك الأساسي أو سرقته، أو إذا حصلت على هاتف جديد ولم يعد لديك رقم هاتفك الأساسي الأصلي.

لتغيير أرقام الهواتف

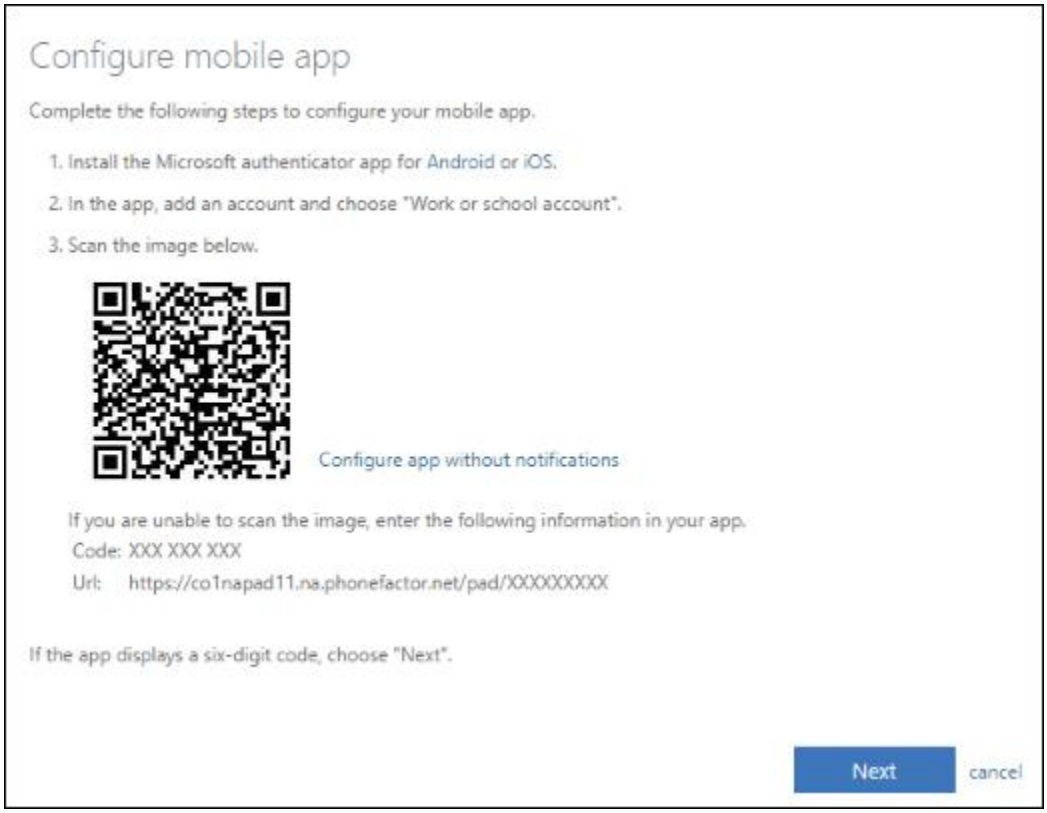
1. من القسم **"كيف تريد الرد؟"** من صفحة التحقق من الأمان الإضافي
2. حدد المربع بجانب خيار هاتف المصادقة البديلة، ثم اكتب رقم هاتف ثانوي حيث يمكنك تلقي المكالمات الهاتفية إذا لم تتمكن من الوصول إلى جهازك الأساسي.
3. حدد **حفظ**.

إضافة حساب جديد إلى تطبيق MICROSOFT AUTHENTICATOR

يمكنك إعداد حساب العمل أو المدرسة على تطبيق Microsoft Authenticator لنظام التشغيلAndroid أو iOS.

إذا قمت بالفعل بإعداد حساب العمل أو المدرسة في تطبيقMicrosoft Authenticator ، فلا تحتاج إلى القيام بذلك مرة أخرى.

1. من المقطع **كيف تريد الرد؟** من صفحة التحقق من الأمان **الإضافي**، حدد إعدادAuthenticator (المصادقة)



2. اتبع الإرشادات التي تظهر على الشاشة، بما في ذلك استخدام جهازك المحمول لمسح رمز الاستجابة السريعة ضوئيا، ثم حدد **التالي** .سيطلب منك الموافقة على إعلام من خلال تطبيقMicrosoft Authenticator ، للتحقق من معلوماتك.
3. حدد **حفظ**.

إدارة كلمات مرور التطبيقات للخدمات المرتبطة

عند استخدام كلمات مرور التطبيق، من المهم تذكر:

- يتم إنشاء كلمات مرور لكل تطبيق على هاتفك المحمول (مثل البريد و الفيسبوك و الانستجرام ، الخ...) **بشكل تلقائي**، ويجب إنشاؤها بإدخالها مرة واحدة لكل تطبيق.
- يوجد حد 40 كلمة مرور لكل مستخدم. إذا حاولت إنشاء كلمة مرور بعد هذا الحد، فسوف يتم مطالبتك بحذف كلمة مرور موجودة قبل السماح لك بإنشاء كلمة مرور جديدة.

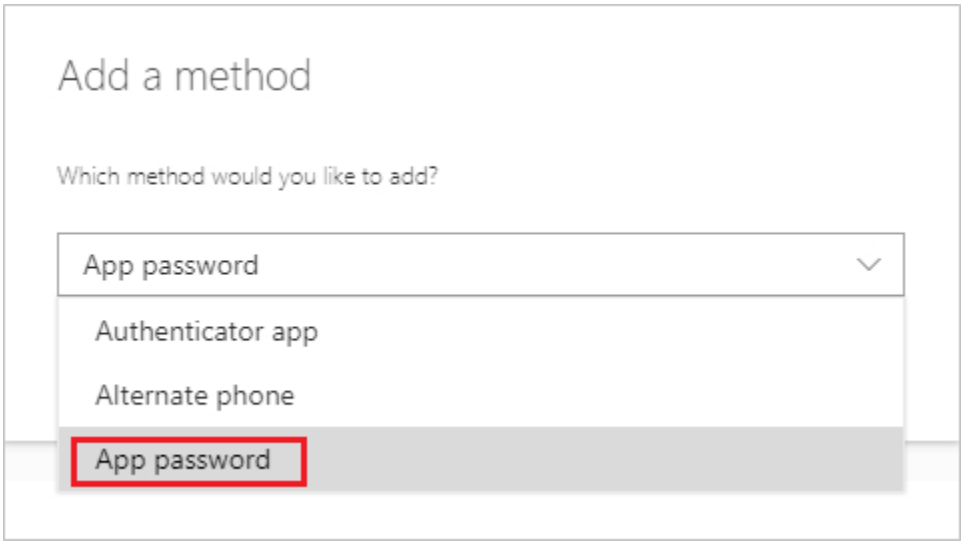
- أثناء عملية التسجيل الأولية ذات العاملين، يتم تزويدك بكلمة مرور واحدة للتطبيقات. إذا كنت بحاجة إلى أكثر من واحد، فسوف تحتاج إلى إنشائها بنفسك. يمكنك إنشاء كلمات مرور للتطبيقات من مناطق متعددة، استنادا إلى كيفية إعداد التحقق من الصحة على أساس عاملين في مؤسستك.

إنشاء كلمات مرور التطبيق وحذفها باستخدام مدخلOFFICE 365

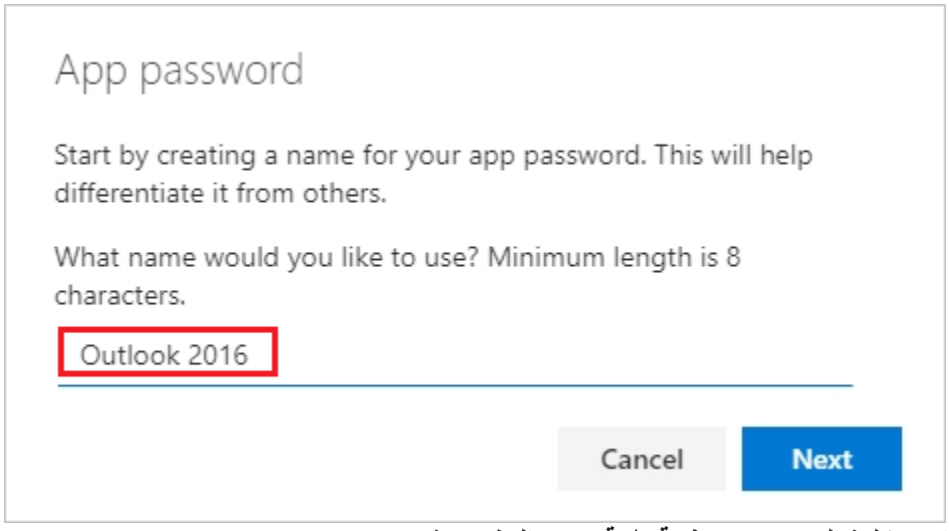
إذا كنت تستخدم التحقق على خطوتين مع حساب العمل أو المدرسة Microsoft 365 لتطبيقاتك، يمكنك إنشاء كلمات مرور التطبيق وحذفها باستخدام.Office 365

لإنشاء كلمات مرور التطبيق باستخدام مدخلOffice 365

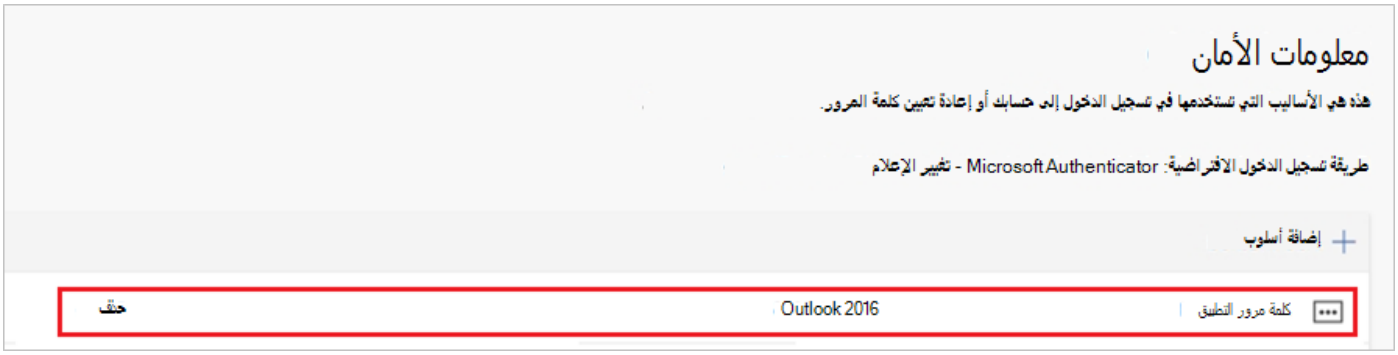
1. سجل الدخول إلى حساب العمل أو المدرسة، واذهب إلى صفحة حسابي وحدد **معلومات الأمان.**
2. حدد **إضافة أسلوب،** واختر كلمة مرور **التطبيق** من القائمة، ثم حدد **إضافة.**



3. أدخل اسما لكلمة مرور التطبيق، ثم حدد **التالي**.



4. انسخ كلمة المرور من **صفحة كلمة مرور** التطبيق، ثم حدد **تم**.
5. في صفحة **معلومات الأمان**، تأكد من إدراج كلمة مرور التطبيق.



6. افتح التطبيق الذي أنشأت كلمة مرور التطبيق له) على سبيل المثال البريد الالكتروني (Outlook 2016)، ثم قم بلصق كلمة مرور التطبيق عند طلبها. يجب أن تحتاج إلى القيام بذلك مرة واحدة فقط لكل تطبيق من تطبيقات الهاتف المحمول.