الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

مبادئ توجيهية
لتأمين حسابات وسائل الإعلام الاجتماعي

عـــام

إخلاء المسؤولية / الحقوق القانونية

قامت الوكالة الوطنية للأمن السيبراني (NCSA) بإعداد ووضع هذا المنشور, بعنوان " المبادئ التوجيهية لتأمين حسابات وسائل الإعلام الاجتماعي " - الإصدار 3.0 لمساعدة المؤسسات على فهم وتخفيف المخاطر السيبرانية على أنظمة المعلومات الخاصة بهم. وهي مسؤولة عن مراجعة هذه الوثيقة والمحافظة عليها.

وعلى الوكالة بصفتها مصدر ومالك, بغض النظر عن طريقة نسخ أي نسخة سواء أكانت كلية أو جزئية من هذه الوثيقة؛ بما يخص « المبادئ التوجيهية لتأمين حسابات وسائل الإعلام الاجتماعي ».

في حالة طلب أي نسخ بخصوص هذه الوثيقة بقصد التسويق التجاري, يلزم الحصول على إذن كتابي من الوكالة الوطنية للأمن السيبراني. ولها أحقية في تقييم مدى فعالية وإمكانية تطبيق جميع النسخ المطورة فيما يخص الأغراض التجارية.

ولا يجوز تفسير الإذن الصادر عن الوكالة الوطنية للأمن السيبراني على أنه تأييد للنسخ المطورة ولا يجوز للمطور بأي حال من الأحوال الإعلان عن ذلك أو إساءة تفسيره بأي شكل من أشكال في وسائل الإعلام أو المناقشات الشخصية / الاجتماعية.

مراقبة الوثائق

تفاصيل الوثيقة	
رقم هوية الوثيقة	IAG-NGE-SSMA
الإصدار	إصدار 3.0
التصنيف والنوع	عام
الخلاصة	التوجيهات الضرورية لمساعدة المؤسسات في إدارة حساباتها على وسائل التواصل الاجتماعي على نحو آمن.

المراجعة / الموافقة

القسم / المهمة	تمت المراجعة / الموافقة	الإصدار	التاريخ
شؤون الحوكمة والضمان السيبرانى الوطني		3.0	

سجل النسخ المنقحة

الإصدار	المؤلف:	وصف المراجعة	التاريخ
اوكتوبر 2015	وزارة الاتصالات و تكنولجيا المعلومات	نشر النسخة الاولى	1.0
نوفمبر 2016	وزارة المواصلات و الاتصالات	تطوير المحتوى + إضافة عدد من التوجيهات	2.0
يونيو 2018	وزارة المواصلات و الاتصالات	تعديل العلامات المؤسسية	2.1
ديسمبر 2022	الوكالة الوطنية للأمن السيبراني	تعديل العلامات المؤسسية + تطوير المحتوى	3.0
ديسمبر 2023	الوكالة الوطنية للأمن السيبراني	تعديلات تصحيحية طفيفة	3.0

التفويض القانوني

يحدد القرار الأميري رقم (1) لسنة 2021 فيما يخص إنشاء الوكالة الوطنية للأمن السيبراني، صلاحياتها. وتتمتع الوكالة الوطنية للأمن السيبراني بسلطة الإشراف على أمن البنية التحتية الوطنية الحيوية وتنظيمها وحمايتها من خلال اقتراح وإصدار السياسات والمعايير وضمان الامتثال.

وقد تم إعداد هذه الوثيقة مع الأخذ في الاعتبار بالقوانين المعمول بها في دولة قطر. وفي حالة نشوء تعارض بين هذه الوثيقة (أحكام أو بنود محددة) وقوانين دولة قطر، تسود قوانين دولة قطر. وبذلك، يعتبر أي مصطلح من هذا القبيل (أحكام أو بنود محددة) محذوفًا من هذه الوثيقة، دون المساس بالأحكام المتبقية من هذه الوثيقة. ويلزم في هذه الحالة إجراء تعديلات لضمان الامتثال للقوانين السارية ذات الصلة بدولة قطر.

جدول المحتويات

1 المقدمة

1.1 السياق

الشبكات الاجتماعية ووسائل التواصل الاجتماعي أصبحت هوية المؤسسة في العالم الافتراضي. وهذه الهوية الاجتماعية مرتبطة إلى حد بعيد بالصورة العامة للمؤسسة لدى الناس، ولذا يجب حمايتها في العالم الافتراضي، تماماً وبنفس القدر الذي نعمل فيه على حمايتها في العالم الحقيقي وعلى أرض الواقع. إن ترك حساب وسائل التواصل الاجتماعي بغير حماية، يفتح الأبواب على مصراعيها لتهديد وتعريض صورة المؤسسة للمخاطر والافتراءات.

وتقدم هذه الوثيقة نصائحاً للحد من المخاطر، وضوابطاً أمنية للمساعدة في الحد من التهديدات مثل الوصول غير المصرح به، وكذلك الخطوات التي يتعين اتباعها لاسترجاع حساب مسروق.

2 الغرض والنطاق والاستخدام والجمهور المستهدف

2.1 الغرض

الغرض من هذه الوثيقة هو تقديم التوجيه اللازم للأفراد والمؤسسات في إدارة حساباتهم على وسائل التواصل الاجتماعي بشكل آمن.

2.2 النطاق

جميع المؤسسات في دولة قطر التي لديها وجود على وسائل التواصل الاجتماعي أو تخطط لذلك.

2.3 الاستخدام

يوصى بهذا التوجيه بشدة للمؤسسات التي تستخدم حسابات وسائل التواصل الاجتماعي للترويج لأعمالها ووجودها وأي أنشطة أخرى عبر أو من خلال استخدام وسائل التواصل الاجتماعي.

2.4 الجمهور المستهدف

الجمهور الذي تستهدفه هذه الوثيقة هو الموظفون المخولون بإدارة واستخدام حسابات الشركات على وسائل التواصل الاجتماعي.

غير أن المستخدمين من الأفراد العاديين ربما يجدون هذه الوثيقة مفيدة لهم أيضاً.

3 التعريفات الرئيسية

المؤسسات/المؤسسة	مؤسسات البنية التحتية الحرجة بدولة قطر.

4 فهم المخاطر

تمثل حسابات الجهات الحكومية وشبه الحكومية والمناسبات الوطنية على وسائل الإعلام الاجتماعي هدفاً مثالياً ومنطقياً لأعداء البلاد، حيث ينظر إلى الإعلام الاجتماعي باعتباره الهوية الافتراضية للجهة الحكومية.

بالإضافة إلى ذلك، فإن تلك الحسابات، وبحكم كونها حسابات حكومية، تحظى بأعداد ضخمة من المتابعين، والذين يولونها ثقة ضمنية.

تتمثل المخاطر المتعلقة بوسائل الإعلام الاجتماعي هذه فيما يلي:

- تسريب معلومات سرية أو غير لائقة
- تخريب المحتوى، ونشر المحتوى الضار
- العواقب القانونية
- الابتزاز

5 التوصيات العامة

5.1 تأسيس نظام حوكمة لوسائل الإعلام الاجتماعي

يجب تحديد سياسة لاستخدام وسائل الإعلام الاجتماعي في مؤسستكم.

ويتعين أن تتضمن هذه السياسة الجوانب التالية، على الأقل:

- أن تحدد الجهات، داخل المؤسسة، المصرح لها بالانخراط في وسائل الإعلام الاجتماعي نيابة عن المؤسسة.
- من يتحكم في ويمتلك المعلومات المدخلة في موقع التواصل لاجتماعي؟
- أي معلومات تقوم الجهات المعنية بتمريرها إلى الجمهور؟
- الحصول على موافقة الجهات المعنية قبل نشر المعلومات المتعلقة بها.
- إجراءات واضحة عن شبكات التواصل الاجتماعي. ما هي الجهة التي يمكن للحساب أن يتابعها أو التي يمكنها أن تؤثر فيه إلخ.؟
- كيف ستتم إذاعة المعلومات التي يتم استلامها من الشبكات المتابعة؟ أي بكلمات أخرى، إعادة التقاسم أو إعادة التغريد إلخ.؟
- تحديد إجراءات التعامل مع الحوادث/خطط التعافي في حالات الاختراق أو الهجمات الخبيثة.
- الأجهزة والبرامج المصرح بالوصول إلى حسابات وسائل الإعلام الاجتماعي من خلالها.

5.2 إنشاء وإدارة الحساب

ومن أجل إنشاء وإدارة ملكية حساب ينصح بالتالي:

- أن يستخدم بريد إلكتروني رسمي من المؤسسة (عادة ما يستخدم كاسم للمستخدم) لإنشاء وصيانة حسابات وسائل الإعلام الاجتماعي. ويجب أن يكون عنوان البريد الإلكتروني المستخدم عاماً وغير محدد من حسابات البريد الإلكتروني للمؤسسة، ليستخدم لتسجيل الدخول إلى شبكات التواصل الاجتماعي. إن عناوين البريد الإلكتروني للأفراد في المؤسسة تكون سهلة التخمين وتقلل من أمن حسابات وسائل الإعلام الاجتماعي.
- يجب أن ترتبط/يرتبط كل قناة/حساب إعلام إجتماعي ببريد إلكتروني مؤسسي فريد منفصل. مثال: اسم المستخدم/عنوان البريد الإكتروني المرتبط باكس مختلف عن اسم المستخدم/عنوان البريد الإكتروني المستخدم على الفيسبوك.
- يجب ألا تستخدم نفس كلمات المرور التي تستخدمها في وسائل الإعلام الاجتماعي للمرور إلى الموارد الحوسبية الموجودة في المؤسسة.
- يجب ألا تستخدم حسابات البريد الإلكتروني الخاصة لإدارة أو الوصول إلى حسابات التواصل الاجتماعي الخاصة بالمؤسسة مثل حساب اكس أو صفحة الفيسبوك.
- يجب أن تظهر وتبرز صفحة حساب التواصل الاجتماعي الشعار الرسمي المعتمد للمؤسسة، كما يجب أن يتضمن النص التعريفي إشارات بأن ذلك الحساب هو "الحساب الرسمي" للمؤسسة.

- يتعين على المؤسسات أن تحدد الجهات أو الوكالات التي يمكن تتبعها، على سبيل المثال يمكن للجهات الحكومية متابعة الجهات الحكومية الأخرى، والحسابات المحققة أو المصادر الموثوق بها.
- من غير المحبذ متابعة المستخدمين الأفراد.
- من غير المحبذ الوصول/إعادة النشر/إعادة التغريد/تقاسم "رسائل غير محققة" بها روابط أو عناوين URL ملحقة.

5.3 تسجيل الدخول إلى الحساب

- يجب تهيئة حسابات التواصل الاجتماعي للتواصل باستخدام بروتوكول نقل النص الآمن (HTTPS) كلما كان ذلك ممكناً. ويدعم الفيسبوك وكذلك اكس ومواقع أخرى هذا الخيار. (ملاحظة: هذا الأمر ضروري جداً عند الاتصال عبر شبكة لاسلكي (واي-فاي) عامة. ويمكن للوكالة الوطنية للأمن السيبراني مساعدتكم في تهيئة حسابكم لتتمكنوا من استخدام (HTTPS) في كل الأوقات.
- يجب أن يكون الدخول فقط من جهاز (كمبيوتر شخصي أو جهاز نقال) معين مملوك أو مدار من قبل المؤسسة مخصص لهذا الغرض فقط.
- يجب أن يكون الدخول من شبكة موثوق بها، ويجب الامتناع عن استخدام الشبكات اللاسلكية (واي-فاي) المفتوحة/العامة مثل تلك الموجودة لدى المقاهي أو في المطارات ..إلخ، ما لم تكن تستخدم شبكة خاصة افتراضية (VPN) لتأمين فترة التواصل.
- إذا تم ربط أي أجهزة نقالة بحساب التواصل الاجتماعي الخاص بالمؤسسة، فيجب التأكد من أن تلك الأجهزة محمية بصورة كافية.
- يجب تعطيل خاصية الموقع الجغرافي خلال النشر أو التغريد.

5.4 إدارة كلمة المرور

- استخدم دائماً كلمات مرور منيعة للوصول إلى شبكات التواصل الاجتماعي. ويجب أن تتفق كلمة المرور مع سياسة المؤسسة المتعلقة بكلمات المرور.
- قم بتغيير كلمات المرور على فترات متقاربة. ويجب أن يكون لديك كلمة مرور مختلفة لكل حساب.
- يجب استخدام المصادقة متعددة العناصر لحسابات التواصل الاجتماعي (إذا كان هذا مدعوماً من قبل المزود).
- لا تشارك كلمة المرور مع اي شخص.

5.5 تقاسم المعلومات/الاستخدام المقبول

- يجب عدم إفشاء اي معلومات رسمية عند تسجيل حسابات التواصل الاجتماعي.
- منع الموظفين من نشر المعلومات أو البيانات الرسمية الحساسة في الشبكات الاجتماعية.

- يجب ألا يسمح إلا للموظفين المخولين فقط بتشغيل حسابات التواصل الاجتماعي الخاصة بالمؤسسة.
- يجب عدم نشر اي مادة قد تتضمن تعليقات تميزية، أو مهينة، أو تشهيرية، أو تعليقات تحرش أو مضايقة بشأن المؤسسة أو أي من موظفيها أو أي طرف ثالث في أي نشرات إلكترونية أو غير ذلك.

5.6 **تهيئة إعدادات الخصوصية:**

- استعرض وراجع، حسب الضرورة، إعدادت الخصوصية الافتراضية التي توفرها مواقع شبكات التواصل الاجتماعي.

5.7 **الرصد**

- تقييد الوصول إلى حساب المؤسسة لوسائل الاعلام الاجتماعية بحيث يكون للموظف المخول فقط، من أجل التحكم في توزيع المحتوى عبر الشبكات الاجتماعية. ويمكن أن يكون هذا الموظف هو ضابط العلاقات العامة، أو الناطق الرسمي، الخ.
- في الحالة توفر حق الوصول إلى حساب وسائل الاعلام الاجتماعية للمؤسسة لأكثر من شخص واحد، ينبغي تحديد الإجراءات الداخلية لتنظيم هذا النشاط، وينبغي أن يشمل هذا تدريب المستخدم على استخدام وسائل الإعلام الاجتماعية، والرصد الفعال، واستخدام حلول إدارة وسائل الإعلام الاجتماعية و/ أو أي ضوابط تعويضية أخرى بحسب ما تقتضيه الضرورة.
- مراقبة الوصول المصرح به لحسابات المستخدمين المخولين بانتظام، وإلغاء تصريحات الموظفين الذين تركوا المنظمة أو الذين لم تعد لديهم حاجة رسمية تقتضيها الوظيفة لاستخدام وسائل الاعلام الاجتماعية.
- يتعين أن يكون لديك شخص من طرف ثالث، غير مسؤول عن المحتوى، يقوم باستمرار برصد حسابات وسائل الاعلام الاجتماعية فيما يتعلق بالنشرات غير المصرح بها أو غير العادية.

5.8 **حلول الطرف الثالث**

- يتعين على المنظمات النظر في إمكانية استخدام أحد حلول إدارة وسائل الإعلام الاجتماعي.

5.9 **الحوادث : في حالة وجود أي نشاط مشبوه**

- يرجى التبليغ للوكالة الوطنية للأمن السيبراني (ncsoc@ncsa.gov.qa) أو الاتصال بهاتف (16555) إذا رايت أياً من الأعراض المشبوهة التالية:
  - إعجابات أتوماتيكية، مجموعات مفضلة، متابعات/عدم متابعة أو طلبات صداقة.
  - رسائل خاصة تنشر لأصدقائك (وقد يصعب التعرف على هذه، ما لم يلفت أحدهم نظرك إليها)
  - رسائل بريد إلكتروني غير متوقعة/وإشعارات من الشبكة الاجتماعية مثل:
  - تحذيرات بأن عنوان بريدك الإلكتروني قد تغير

- تحذيرات بأنه قد تم الوصول لحسابك من موقع مجهول
- تحديثات عن وضعك/تغريدات لم تقم أنت بعملها
- تغييرات على الملف الشخصي أو صور على الحساب

5.10 خطة التعافي

- يرجى التبليغ للوكالة الوطنية للأمن السيبراني (ncsoc@ncsa.gov.qa) أو الاتصال بهاتف (16555)
- جمع كل السجلات، والآثار وأدوات النشاط الضار للتحقيق والمتطلبات القانونية المحتملة.
- فوراً قم بتغيير كلمات المرور الخاصة بالحساب.
- تحقق من وغير كلمة المرور للبريد الإلكتروني المرتبط بالحساب وقم بإعداد نسخة احتياطية من الرسائل.
- قم بالتحقق من خيارات استعادة كلمة المرور المخصصة لحساب التواصل الاجتماعي، وكذلك تحقق من عنوان البريد الإلكتروني البديل الذي تم إنشاؤه.
- تحقق من خيارات إعادة الإرسال أتوماتيكياً، إذا وجدت، للحساب والبريد الإلكتروني المرتبط.
- قم بزيارة صفحة التطبيقات للشبكة الاجتماعية وإزالة أي تطبيقات لا تتعرف عليها. وإذا ما استمر الحساب في التصرف بطريقة غير منطقية، فإننا ننصح بإلغاء الوصول لجميع التطبيقات.

5.11 التوعية الأمنية

- يجب توعية الموظفين الذين يقومون بإدارة أو صيانة حسابات وسائل الاعلام الاجتماعي الخاصة بالمؤسسة، وتثقيفهم في أمن المعلومات. وينبغي أن يكونوا على علم بالتهديدات السائدة مثل الإنتحال والهندسة الاجتماعية.

6 تأمين مواقع التواصل الاجتماعي الأكثر شعبية

6.1 الفيسبوك:

إدارة الحساب:

تأمين صفحة فيسبوك يعتمد على أمان حساب مدير الصفحة, لذا يجب الحرص على ما يلي:

- تأكد من أنك تستخدم اتصالاً آمنًا متى كان متاحً, انقر على زر الأمن في الجزء الأيمن من إعدادات حساب فيسبوك وتأكد من تفعيل "التصفح الآمن".
- تتيح لك إعدادات الأمان أيضًا تمكين إشعارات تسجيل الدخول والموافقات ، وعرض وتعديل أجهزتك المعترف بها والجلسات النشطة.
- قراءة و فهم سياسة بيانات فيسبوك لمعرفة البيانات التي يجمعها فريق فيسبوك عنك https://www.facebook.com/policy.php

سياسة كلمة المرور:

- يجب أن يكون أطول من 6 أحرف ، ويكون فريدًا بالنسبة لك ، ويصعب على الآخرين تخمينه.

كيفية تفعيل المصادقة الثنائية:

- يوفر فيسبوك ثلاثة خيارات للتحصل على المصادقة الثانية. يمكن للمستخدم إستعمال إما الرسائل القصيرة أو المفتاح الأمن أو تطبيقات المصادقة التابعة لجهات خارجية, إذهب إلى https://www.facebook.com/help/148233965247823 للحصول على تفاصيل إضافية حول كيفية تفعيل المصادقة الثنائية على فيسبوك.

نصائح أمنية:

- استخدم كلمة مرور قوية.
- استخدم ميزات الأمان الإضافية في فيسبوك.
- تأكد من أن حساب (حسابات) بريدك الإلكتروني آمن.
- قم بتسجيل الخروج من فيسبوك بعد الانتهاء من عملك.
- قم بتشغيل برنامج مكافحة الفيروسات على جهاز الكمبيوتر الخاص بك.
- فكر قبل النقر فوق أو تنزيل أي شيء.
- قم بتمكين "موافقات تسجيل الدخول" من قسم "أمن الحساب" في صفحة إعدادات الحساب. اتبع الرابط https://www.facebook.com/notes/facebook-engineering/introducing-login-approvals/10150172618258920[1]
- قم بتحديث حساباتك وفقًا لنصائح الأمان وإرشادات فيسبوك. يمكنك العثور عليها في https://www.facebook.com/help/379220725465972[2]

[1] قد يتم تغيير هذا الرابط من قبل فيسبوك, يرجى مراجعة قسم "المساعدة" على فيسبوك إذا لم يؤدي هذا الرابط وظيفته
[2] قد يتم تغيير هذا الرابط من قبل فيسبوك, يرجى مراجعة قسم "المساعدة" على فيسبوك إذا لم يؤدي هذا الرابط وظيفته

نصائح الخصوصية:

- قم بتعطيل الآخرين من النشر في الملف الشخصي, ويمكن القيام بذلك من (الملف الشخصي والإشارات) في الإعدادات.
- لا تسمح للحسابات الأخرى بوضع إشارة لحسابك الشخصي على صورة قبل مراجعتها. يمكن القيام بذلك من (الملف الشخصي والإشارات) في الإعدادات.

استرجاع الحساب:

- توفر الروابط التالية تفاصيل وخطوات لاستعادة الحساب

https://www.facebook.com/help/231208473756221,
https://www.facebook.com/help/105487009541643,
https://www.facebook.com/help/132243923516844

- إذا كنت تعتقد أن الحساب قد تم اختراقه, فانتقل إلى https://www.facebook.com/help/1216349518398524/ للحصول على تفاصيل لاسترجاع الحساب.

6.2 اكس (تويتر سابقاً):

إدارة الحساب:

- قراءة وفهم سياسة خصوصية اكس لفهم البيانات التي يجمعها اكس منك والمعلومات التي يشاركونها أو يفصحون عنها https://twitter.com/en/privacy
- انتقل إلى https://help.twitter.com/en/safety-and-security/account-security-tips للحصول على نصائح حول كيفية تأمين حساب اكس الخاص بك.

سياسة كلمة المرور:

يجب ألا يقل طول كلمة المرور عن 8 أحرف.

كيفية تفعيل المصادقة الثنائية:

- يوفر اكس ثلاثة خيارات للتحصل على المصادقة الثانية. يمكن للمستخدم إستعمال إما الرسائل القصيرة أو المفتاح الأمن أو تطبيقات المصادقة التابعة لجهات خارجية, إذهب إلى https://help.twitter.com/en/managing-your-account/two-factor-authentication للحصول على تفاصيل إضافية حول كيفية تفعيل المصادقة الثنائية على اكس.

نصائح أمنية:

- استخدم كلمة مرور قوية.
- يجب على المؤسسات الحكومية التحقق من صحة حساباتها وتفعيل العلامة الزرقاء. يمكنك التحقق من حساب اكس الخاص بك باتباع التعليمات وملء نموذج على اكس https://support.twitter.com/articles/20174631
- احترس من الروابط المشبوهة ، وتأكد دائمًا من أنك على twitter.com قبل إدخال معلومات تسجيل الدخول الخاصة بك.
- لا تقم أبدًا بإعطاء / مشاركة اسم المستخدم وكلمة المرور الخاصين بك مع أي شخص.
- استخدم حماية إعادة تعيين كلمة المرور لضمان عدم تمكن أي شخص من التسلل ، ثم أحكِم حسابك على اكس (account lock). سيتطلب منك تحديد هذا الخيار تقديم عنوان بريد إلكتروني أو رقم هاتف كلما حاولت تغيير كلمة مرورك.

نصائح الخصوصية:

- عند التسجيل في اكس, لديك خيار الاحتفاظ بتغريداتك عامة (إعداد الحساب الافتراضي) أو حماية تغريداتك.
- الحسابات ذات التغريدات المحمية تتطلب موافقة لكل شخص يمكنه مشاهدة تغريدات هذا الحساب.
- تعطيل بيانات الموقع والإشارات من الظهور مع تغريداتك. للقيام بذلك, إذهب إلى **الإعدادات والخصوصية ← الخصوصية والأمان ← معلومات الموقع** وقم بإلغاء **تحديد إضافة معلومات الموقع إلى تغريداتي**.

- امنع إمكانية قيام حسابات أخرى بوضع إشارة إلى حساب اكس الخاص بك على الصور من **الإعدادات والخصوصية ← الخصوصية والأمان ← وضع علامات على الصور**.

استرجاع الحساب:

- في حالة كشف حسابك أو اختراقه، يجب اتباع عدة خطوات لاسترداد الحساب: انتقل إلى https://help.twitter.com/en/safety-and-security/twitter-account-compromised للحصول على التعليمات والتفاصيل.
- إذا كنت تعتقد أن الحساب قد تم اختراقه، فانتقل إلى https://help.twitter.com/en/safety-and-security/twitter-account-hacked للحصول على تفاصيل لاسترجاع الحساب.

6.3 إنستغرام:

إدارة الحساب:

- قراءة وفهم سياسة بيانات إنستغرام لفهم البيانات التي يجمعها إنستجاجرام منك والمعلومات التي يشاركونها أو يفصحون عنها (بشكل عام أو مع Facebook) https://help.instagram.com/519522125107875/?helpref=hc_fnav&bc[0]=Instagram%20Help&bc[1]=Policies%20and%20Reporting
- اقرأ سياسة النظام الأساسي للفيسبوك على https://developers.facebook.com/terms?helpref=hc_fnav .

سياسة كلمة المرور:

يجب أن تتكون كلمة المرور من ستة أحرف أو أكثر , ولم يتم استخدامها من قبل.

كيفية تفعيل المصادقة الثنائية:

- يوفر إنستغرام خياران للتحصل على المصادقة الثانية. يمكن للمستخدم استعمال إما الرسائل القصيرة أو تطبيقات المصادقة التابعة لجهات خارجية, لتفعيل المصادقة عن طريق الرسائل القصيرة إذهب إلى https://help.instagram.com/843785199163974 و التعليمات اللازمة. لتفعيل المصادقة عن طريق تطبيقات المصادقة التابعة لجهات خارجية إذهب إلى https://help.instagram.com/1582474155197965

نصائح أمنية:

- استخدم كلمة مرور قوية.
- تأكد من أن حساب (حسابات) بريدك الإلكتروني آمن. قم بتغيير كلمات المرور لجميع حسابات البريد الإلكتروني الخاصة بك وتأكد من عدم وجود كلمتي مرور متماثلتين.
- قم بتسجيل الخروج من إنستغرام بعد الإنتهاء من عملك. لا تقم بتفعيل خيار "تذكرني" عند تسجيل الدخول.
- فكر جيداً قبل السماح لأي تطبيق تابع لجهة خارجية.
- قم بتحديث حساباتك وفقًا لإرشادات وإرشادات الأمان الجديدة الخاصة بإنستغرام. يمكنك العثور عليها في https://help.instagram.com/369001149843369[3]
- لا تقم أبدًا بإعطاء / مشاركة اسم المستخدم وكلمة المرور الخاصين بك مع أي شخص.
- يجب على المؤسسات الحكومية التحقق من صحة حساباتها وتفعيل العلامة الزرقاء. يمكنك التحقق من حساب إنستغرام الخاص بك باتباع التعليمات وملء النموذج التالي https://help.instagram.com/854227311295302[4]

[3] قد يتم تغيير هذا الرابط من قبل إنستغرام، يرجى مراجعة قسم "المساعدة" على إنستغرام أو فيسبوك اذا لم يؤدي هذا الرابط وظيفته.
[4] قد يتم تغيير هذا الرابط من قبل إنستغرام، يرجى مراجعة قسم "المساعدة" على إنستغرام أو فيسبوك اذا لم يؤدي هذا الرابط وظيفته..

نصائح الخصوصية:

- راجع الصور التي تم الإشارة لحسابك عليها قبل نشرها في ملفك الشخصي. للقيام بذلك ، انتقل إلى **الإعدادات** ← **الخصوصية** ← **المنشورات** ثم قم بتمكين **الموافقة على الإشارات يدويًا**.
- لا تقم بإظهار حالة نشاطك حتى لا يتمكن الأشخاص من رؤيتك عندما تكون متصلاً بالإنترنت. للقيام بذلك ، انتقل إلى **الإعدادات** ←**الخصوصية** ← **حالة النشاط** ثم قم بتعطيل **عرض حالة النشاط**.

إسترجاع الحساب:

- إذا كان حساب إنستغرام الخاص بك مرتبطًا بحسابك على فيسبوك، فارجع إلى تفاصيل استرداد حساب فيسبوك أعلاه.
- إذا لم يكن حساب إنستغرام الخاص بك مرتبطًا بحسابك على فيسبوك، فراجع الرابط التالي: https://help.instagram.com/149494825257596 للحصول على تفاصيل لإسترجاع الحساب.

6.4 لينكدإن:

إدارة الحساب:

- قم بتحديث حساباتك وفقًا لإرشادات وإرشادات الأمان الخاصة بـ لينكدإن https://www.linkedin.com/help/linkedin/answer/267/account-security-and-privacy-best-practices?lang=en.
- اقرأ واستوعب سياسة خصوصية لينكدإن https://www.linkedin.com/legal/privacy-policy, اتفاقية المستخدم على لينكدإن https://www.linkedin.com/legal/user-agreement, وإذا كنت مشتركًا في لينكدإن بريميوم , فتأكد من قراءة اتفاقية اشتراك لينكدإن https://www.linkedin.com/legal/l/lsa.

سياسة كلمة المرور:

يجب أن تتكون كلمة المرور من ستة أحرف أو أكثر.

كيفية تفعيل المصادقة الثنائية:

- يوفر لينكدإن خيارين لتمكين المصادقة الثنائية وتطبيق المصادقة التابع لجهة خارجية ورمز الرسائل القصيرة, إذهب إلى https://www.linkedin.com/help/linkedin/answer/544 لتفعيل المصادقة الثنائية على لينكدإن.

نصائح أمنية:

- استخدم كلمة مرور قوية.
- تأكد من أن حساب (حسابات) بريدك الإلكتروني آمن.
- قم بتسجيل الخروج من لينكدإن بعد الإنتهاء من عملك.
- قم بتشغيل برنامج مكافحة الفيروسات على جهاز الكمبيوتر الخاص بك.
- تحقق من الأجهزة التي يمكنها الوصول إلى حساب لينكدإن الخاص بك , وللقيام بذلك , انتقل إلى **الحساب** ← **الإعدادات والخصوصية** ← **تسجيل الدخول و الأمان** ← **الأجهزة التي تتذكر كلمة مرورك**.
- تحقق من الخدمات التي قمت بربطها بحسابك على لينكدإن, وللقيام بذلك, انتقل إلى **الحساب** ← **الإعدادات والخصوصية** ← **تفضيلات الحساب** ← **الشركاء و الخدمات**.
- كن حذرًا من عمليات التصيد الاحتيالي الإلكترونية (شائعة جدًا على لينكدإن). تم تصميم رسائل التصيد الاحتيالي لتبدو وكأنها واردة من أشخاص أو شركات تبدو حقيقية. غالبًا سيطلبون منك (أو يخيفونك) للنقر على الروابط أو إرسال معلوماتك الشخصية أو إرسال الأموال.

نصائح الخصوصية:

- إقتصر قائمة جهات الإتصال على الاشخاص المعروفين بالنسبة لك.
- اسمح فقط لجهات اتصالك بمتابعة تحديثاتك العامة ورؤيتها. للقيام بذلك , انتقل إلى **الحساب** ← **الإعدادات والخصوصية** ← **العرض** ← **ظهور نشاطك على لينكدإن** ← **المتابعون**.

- لا تسمح للينكدإن بعرض معلومات من ملفك الشخصي لمستخدمي الخدمات الأخرى. للقيام بذلك , انتقل إلى **الحساب ← الإعدادات والخصوصية ← العرض ← ظهور ملفك الشخصي على لينكدإن ← اكتشاف الملف الشخصي وعرضه خارج لينكدإن**.

- لا تسمح للحسابات الأخرى بالإشارة إلى حسابك أو وضع علامة مرجعية إليه، حيث يمكن القيام بذلك من خلاله. للقيام بذلك , انتقل إلى **الحساب ← الإعدادات والخصوصية ← العرض ← ظهور نشاطك على لينكدإن ← الإشارات**.

- لا ترسل أي بيانات عن راتبك على لينكدإن.

إسترجاع الحساب:

- تواصل مع مركز المساعدة لاستعادة الوصول إلى حسابك. سيُطلب منك تحميل صورة من بطاقة الهوية الحكومية السارية أو رخصة القيادة أو جواز السفر. مزيد من التفاصيل يمكن العثور عليها هنا https://www.linkedin.com/help/linkedin/answer/127580/verify-identity-to-recover-account-access?lang=ar.

- يوفر الرابط التالي تفاصيل وخطوات للإبلاغ عن الحسابات المكشوفة أو المخترقة: https://www.linkedin.com/help/linkedin/answer/56363/reporting-a-compromised-account?lang=ar.

6.5 واتساب :

إدارة الحساب:

- اقرأ شروط خدمة واتساب https://www.whatsapp.com/legal/updates/terms-of-service/?lang=ar, سياسة خصوصية واتساب https://www.whatsapp.com/legal/updates/privacy-policy/?lang=ar, و سياسة الملكية الفكرية: حقوق النشر الخاصة بك وعلامتك التجارية https://www.whatsapp.com/legal/ip-policy.
- إذهب إلى https://www.whatsapp.com/security للحصول على نصائح حول كيفية تأمين حساب واتساب الخاص بك.
- **الرسائل الخادعة على واتساب**: لن يتصل بك واتساب نفسه أبدًا من خلال التطبيق. أيضًا ، لا يرسل واتساب رسائل بريد إلكتروني حول الدردشات أو الرسائل الصوتية أو الدفع أو التغييرات أو الصور أو مقاطع الفيديو ، ما لم ترسل بريدًا إلكترونيًا للمساعدة والدعم. أي شيء يقدم اشتراكًا مجانيًا ، أو يدعي أنه من واتساب أو يشجعك على متابعة الروابط من أجل حماية حسابك هو بالتأكيد عملية احتيال ولا يمكن الوثوق بها.
- واتس اب ويب:

1. على الرغم من أن واتساب ويب قد تم تصميمه لتسهيل الحياة من خلال الوصول إلى واتساب على سطح المكتب ، إلا أن الخدمة عرضة لسوء الاستخدام. يمكن فقط لأي شخص لديه حق الوصول إلى هاتفك وتطبيق واتساب بدء جلسة ويب ، ومسح رمز الإستجابة السريعةQR code الخاص بأمان واتساب والوصول الكامل إلى محادثات واتساب الخاصة بك. يمكن تجنب ذلك من خلال التأكد من عدم السماح لأي شخص آخر بالوصول الفعلي إلى هاتفك. في حالة احتياجك للمشاركة ، تأكد من قفل التطبيق برقم التعريف الشخصي PIN.
2. تذكر تسجيل الخروج من واتساب ويب: تعمل خدمة النسخ المتطابق على تسهيل الحياة أثناء العمل على جهاز الكمبيوتر. ومع ذلك ، لا يدرك معظم المستخدمين أنه يجب عليهم بشكل كامل تسجيل الخروج من واتساب ويب على متصفح جوجل كروم إما من هاتفهم المحمول أو المتصفح.
3. يجب الوصول إلى واتساب ويب فقط من جهاز الشركة مخصص.

سياسة كلمة المرور:

لا توجد كلمة مرور.

كيفية تفعيل المصادقة الثنائية:

لتمكين التحقق من خطوتين عن طريق إدخال رمز PIN عند فتح واتساب ، قم بما يلي:

1. افتح إعدادات واتساب
2. انقر على **الحساب** ← **التحقق على خطوتين** ← **تفعيل**.
3. أدخل رقم التعريف الشخصي المكون من ستة أرقام من اختيارك وقم بتأكيده.
4. أدخل عنوان بريد إلكتروني يمكنك الوصول إليه أو انقر على "تخطي" إذا كنت لا تريد إضافة عنوان بريد إلكتروني. يوصى بإضافة عنوان بريد إلكتروني لأن هذا يسمح لك بإعادة تعيين التحقق من خطوتين ويساعد في حماية حسابك.
5. اضغط على التالي.

6. قم بتأكيد عنوان البريد الإلكتروني وانقر فوق حفظ أو تم.

نصائح أمنية:

- تأكد من أن حساب بريدك الإلكتروني آمن. قم بتغيير كلمات المرور لجميع حسابات البريد الإلكتروني الخاصة بك وتأكد من عدم وجود كلمتين متماثلتين.
- لا تقم بمشاركة رمز تحقق واتساب عبر الرسائل النصية القصيرة مع الآخرين ، ولا حتى مع الأصدقاء أو العائلة.
- **التشفير**:

1. تأكد من أن واتساب لديه حق الوصول إلى الكاميرا الخاصة بك. ربما تكون قد سمحت بذلك بالفعل عند تثبيت واتساب ، ولكن إذا لم تقم بذلك ، فمن السهل تعديل ذلك في منطقة التطبيقات بهاتفك.
2. بعد ذلك ، افتح محادثة مع جهة الإتصال في واتساب ثم إنقرعلى اسم الشخص أعلى المحادثة. سيؤدي هذا إلى فتح نافذة الاتصال لهذا الشخص. بالقرب من الجزء السفلي من تلك الشاشة ، سترى إعدادًا للتشفير.
3. انقر فوق حقل التشفير ، وستظهر لك شاشة تعرض رمز للإستجابة السريعة QR بالإضافة إلى رمز عشري مكون من 60 رقمًا يمثل محتويات رمز الاستجابة السريعة.
4. في الجزء السفلي من شاشة رمز الاستجابة السريعة ، يوجد رابط سيمكنك من مسح رمز جهة الإتصال ضوئيًا ، ويمكنهم فعل الشيء نفسه مع رمزك. لهذا السبب تحتاج إلى السماح بالوصول إلى الكاميرا في واتساب ، حتى ولو مؤقتًا فقط.
5. قم بإلغاء إمكانية وصول إلى الكاميرا عند الانتهاء.

نصائح الخصوصية:

- حظر ظهور صور واتساب في قائمة الصور: يمكنك تقييد ظهور صور واتساب في قائمة الصور.

iPhone: انتقل إلى قائمة الإعدادات بهاتفك ، ثم "الخصوصية" ، و "الصور" ، وقم بإلغاء تحديد واتساب من قائمة التطبيقات التي يتم إدخال صورها في تدفق الصور.

Android: باستخدام تطبيق مستكشف الملفات مثل ES File Explorer ، ابحث عن مجلدات "الصور" و "مقاطع الفيديو" في واتساب. أنشئ ملفًا داخل كل ملف يسمى ".nomedia". سيؤدي ذلك إلى منع معرض Android من فحص المجلد.

- إخفاء الطابع الزمني "آخر ظهور": يمكنك تعطيل أو تقييد من يرى وقت "آخر ظهور لك" في "الملف الشخصي" في واتساب ؛ قائمة "الخصوصية" في Android أو iOS أو Windows أو Blackberry. ومع ذلك ، كن على علم ، إذا قمت بإيقاف تشغيله ، فلن تكون قادرًا على رؤية مرات "آخر ظهور" للمستخدمين الآخرين أيضًا.

- تقييد الوصول إلى صورة الملف الشخصي: إذا كانت مشاركة واتساب الخاصة بك عامة ، فيمكن لأي شخص تحدثت إليه - حتى لو قمت بالرد للتو على رسالة غير مرغوب فيها - تنزيل صورتك من ملف تعريف واتساب الخاص بك ، وباستخدام البحث عن الصور من Google ، يستطيع اكتشف المزيد عنك بسرعة. قم بتعيين مشاركة صورة الملف الشخصي على "جهات الاتصال فقط" في قائمة الخصوصية. بالنسبة لحسابات الشركات ، يجب أن تكون صورة الملف الشخصي هي شعار الشركة.

- كن حذرًا فيما تتحدث عنه: لا ترسل معلومات شخصية إذا كان بإمكانك تجنبها - العناوين وأرقام الهواتف وعناوين البريد الإلكتروني - ولا ترسل مطلقًا بيانات البنك أو البطاقة الشخصية أو بطاقة الائتمان أو جواز سفرك أو تفاصيل التعريف الأخرى كما هي حيث ان ذلك يمكن أن يكون خطيرًا جدًا في حالة فقد / سرقة الهاتف المحمول أو اختراق الحساب.
- يمكنك ضبط عداد الوقت لإختيار متى ستبدأ الرسائل في الاختفاء بعد أن يقرأها المستلم.

إسترجاع الحساب:

- قم بإلغاء تنشيط واتساب إذا فقدت هاتفك. يوصي واتساب بأن تقوم على الفور بتنشيط التطبيق بنفس رقم الهاتف على هاتف مختلف ، باستخدام بطاقة SIM بديلة. يمكن لرقم واحد فقط على جهاز واحد استخدام التطبيق في كل مرة ، لذلك من خلال القيام بذلك ، يمكنك على الفور حظر استخدامه على هاتفك القديم. إذا لم يكن ذلك ممكنًا ، فيمكن لـ واتساب إلغاء تنشيط حسابك.
- يمكنك الحصول على مزيد من التفاصيل والإرشادات هنا: https://faq.whatsapp.com/general/account-and-profile/lost-and-stolen-phones/?lang=en

6.6 سناب شات :

إدارة الحساب:

- اقرأ واستوعب سياسة خصوصية سناب شات https://snap.com/en-US/privacy/privacy-policy.
- للحصول على نصائح حول كيفية تأمين حساب سناب شات الخاص بك إذهب إلى https://support.snapchat.com/en-US/article/safety-tips-resources.

سياسة كلمة المرور:

ما لا يقل عن 8 أحرف ، ولا تتضمن معلومات شخصية ، مثل الاسم أو اسم المستخدم أو رقم الهاتف أو تاريخ الميلاد. قم بتضمين مزيج من الأرقام والرموز والأحرف الكبيرة والصغيرة في كلمة مرورك.

كيفية تفعيل المصادقة الثنائية:

لتفعيل المصادقة الثنائية ، اتبع الخطوات أدناه:

1. افتح سناب شات على جهازك.
2. اضغط على أيقونة الشبح في الجزء العلوي من الشاشة.
3. اضغط على أيقونة الترس لفتح قائمة الإعدادات.
4. قم بالتمرير لأسفل وحدد التحقق من تسجيل الدخول.
5. انقر على "متابعة."
6. اختر للتحقق عبر النص أو تطبيق المصادقة.
7. أدخل رمز التحقق المقدم عبر النص أو من خلال تطبيق المصادقة.

نصائح أمنية:

- استخدم كلمة مرور قوية.
- قم بتفعيل التسجيل عن طريق المصادقة الثنائية.
- تأكد من أن حساب (حسابات) بريدك الإلكتروني آمن.
- قم بتسجيل الخروج من سناب شات بعد الإنتهاء من عملك.
- قم بتشغيل برنامج مكافحة الفيروسات على جهاز الكمبيوتر الخاص بك.

نصائح الخصوصية:

- إحتفظ بإمكانية الوصول لمنشوراتك و قصصك إلى اصدقائك فقط: يضبط سناب شات خيارات حسابك على الأصدقاء فقط افتراضيًا. هذا يعني أن الأشخاص الذين قمت بإضافتهم كصديق والذين قاموا بإضافتك مرة أخرى فقط يمكنهم إرسال Snaps إليك أو عرض Snaps الخاصة بك. نوصي بشدة بالحفاظ عليها على هذا النحو ، حتى تعرف دائمًا من يشاهد ما تقوم بإنشائه. لا تغير إعداداتك إلى "الجميع" ، لأن هذا يعني حرفيًا أن أي شخص لديه حساب سناب شات يمكنه إرسال رسائل إليك أو مشاهدة قصصك.

- تأكد من أنك تعرف تماماً من هم على قائمة أصدقائك. إذا حاول مستخدم آخر إضافتك كصديق ، فتحقق مما إذا كنت تعرف هويته قبل قبول طلب الصداقة. إذا كان اسم المستخدم الخاص بالشخص الذي أضافك لا يبدو أنه أي شخص تعرفه ، فقد يكون تطبيق إحتيالي ، أو غريبًا فضوليًا وليس لديه سبب لمعرفة المزيد عن حياتك عبر سناب شات. من الأفضل تجاهل هذه الطلبات.

- إذا كنت لا تريده أن يكون دائمًا ، فلا تنشره على ال سناب شات: ينتهي محتوى سناب شات بعد وقت محدد ، ويجب أن يخطرك سناب شات أيضًا إذا قام شخص ما بالتقاط لقطة شاشة لأحد الـ Snaps أو الدردشات الخاصة بك. لكن لا تدع هذا يخدعك بالثقة في ذلك - فمن المؤكد أنه يمكن حفظ الـ Snaps الخاصة بك (ومشاركتها) دون علمك.

- سناب شات مباشر: إذا حاولت إرسال شيء ما إلى قصة "Snapchat Live" - مجموعة القصص التي ينشئها سناب شات للأحداث أو العطلات أو المواقع أو لأسباب أخرى مختلفة - ضع في اعتبارك أنه من الممكن أن يشاهدها الجميع إذا تم تحديده. لذلك ، قبل محاولة إرسال شيء ما ، تأكد من أنك مرتاح لذلك.

- إذا كان هناك شخص ما يجعلك تشعر بعدم الارتياح ، يمكنك حظر هذا الشخص وترك أي محادثة جماعية تجمعك به/بهم . انقر هنا للتعرف على الإبلاغ عن إساءة استخدام سناب شات. https://support.snapchat.com/en-GB/a/report-abuse-in-app

- اختر من يمكنه الاتصال بك مباشرة من خلال Snaps والدردشات والمكالمات وما إلى ذلك.

- قم بتخصيص من يمكنه عرض موقعك أو يفضل تشغيل وضع الشبح لإخفاء تفاصيل عنك.

- اختر من يمكنه استخدام صورة النقش "Cameos selfie" في النقش "Cameos" لشخصين.

- اختر من يمكنه رؤيتك في الإضافة السريعة "Quick Add" ، وهي ميزة تظهر حول سناب شات تسهل إضافة الأصدقاء.

إسترجاع الحساب:

- إذا كنت تعتقد أن الحساب قد تم اختراقه , فانتقل إلى:
https://support.snapchat.com/en-GB/i-need-help?start=5145405817880576 and https://support.snapchat.com/en-GB/a/hacked-howto for recovery details للحصول على تفاصيل استرجاع الحساب.

6.7 تمبلر:

إدارة الحساب:

- اقرأ واستوعب سياسة خصوصية تمبلر https://www.tumblr.com/privacy/ar و شروط خدمة تمبلر https://www.tumblr.com/policy/en/terms-of-service.

سياسة كلمة المرور:

يجب أن تتكون من 8 أحرف على الأقل ، وألا تصنف على أنها كلمة مرور ضعيفة.

كيفية تفعيل المصادقة الثنائية:

لتفعيل المصادقة الثنائية ، اتبع الخطوات أدناه:

1. انقر على "إعدادات" ضمن قائمة الحساب أعلى لوحة التحكم.
2. في قسم الأمان ، قم بتمكين "المصادقة الثنائية".
3. أدخل رقم هاتفك.
4. حدد الآن ما إذا كنت ترغب في تلقي الرمز عبر رسالة نصية أو من خلال تطبيق المصادقة.
5. اتبع الخطوات الموضحة في صفحة الإعدادات. مزيد من التفاصيل يمكن العثور عليها هنا: https://tumblr.zendesk.com/hc/en-us/articles/226270148-Two-factor-authentication

نصائح أمنية:

- استخدم كلمة مرور قوية.
- قم بتفعيل التسجيل عن طريق المصادقة الثنائية.
- لا تشارك كلمات مرورك حتى مع من تثق بهم.
- تأكد من أن حساب (حسابات) بريدك الإلكتروني آمن.
- قم دائماً بتسجيل الخروج بعد الإنتهاء من عملك.
- تحقق من التطبيقات المتصلة بحسابك من **الحساب** ← **التطبيقات**.
- الإبلاغ عن الرسائل الاقتحامية:

1. من المنشورات على الويب: من لوحة التحكم أو صفحة نتائج البحث ، انقر على قائمة المشاركة (طائرة ورقية) أسفل المنشور ، وانقر على "إبلاغ."
2. من المدونات على الويب: أبلغ عن مدونة كاملة عن طريق تمرير مؤشر الماوس فوق الصورة الرمزية للمدونة ، والنقر على الصورة الظلية للشخص الصغير ، والنقر على "وضع علامة على هذه المدونة".
3. من الرسائل في التطبيق أو على الويب: المس أو انقر على "وضع علامة كرسالة غير مرغوب فيها" أسفل الرسالة الأولى لمرسل البريد العشوائي. لاحظ أن "علامة الرسالة غير مرغوب فيها " لن يظهر إذا كنت تتابع شخصًا ما ، أو كنت قد أجريت محادثة معه بالفعل.
4. من بريد المعجبين على الويب: من البريد الوارد ، انقر على النقاط الثلاث أسفل رسالة البريد العشوائي واختر "إبلاغ".
5. إذا لم يكن لديك حق الوصول إلى جهاز كمبيوتر الآن ، فيمكنك استخدام عرض سطح المكتب لمتصفح الجوال للإبلاغ عن الرسائل غير المرغوب فيها باتباع الخطوات المذكورة أعلاه. للوصول إلى عرض سطح المكتب في iOS ، افتح Safari وقم بزيارة tumblr.com ،

وقم بتسجيل الدخول ، وانقر فوق رمز المشاركة (مربع صغير به سهم) في الجزء السفلي من الشاشة ، ثم انقر فوق الزر الرمادي "طلب موقع سطح المكتب". على نظام Android ، افتح الإنترنت أو Chrome وقم بزيارة tumblr.com ، وقم بتسجيل الدخول ، وانقر على أيقونة النقاط الثلاث في الزاوية العلوية اليمنى من الشاشة ، وحدد مربع "عرض سطح المكتب".

- أنشئ رموزًا احتياطية للرجوع إلى حسابك في تمبلر في حالة عدم قدرتك على الوصول إلى هاتفك لسبب ما. إليك كيفية الحصول عليها:
  1. انتقل إلى إعدادات حسابك على الويب.
  2. في قسم الأمان ، انقر فوق الزر "إنشاء رموز احتياطية" (لاحظ أنك ستحتاج إلى تمكين المصادقة الثنائية لرؤية هذا الخيار).
  3. أدخل كلمة مرور حسابك عندما يُطلب منك ذلك وستحصل على 10 رموز احتياطية.

نصائح الخصوصية:

- لا يسمح تمبلر بالمدونات الخاصة. لكن تمبلر يعرض عليك إنشاء مدونة ثانوية يمكنك تقييد الوصول إليها. لإنشاء مدونة ثانوية ، انتقل إلى: https://tumblr.zendesk.com/hc/en-us/articles/226340308-Secondary-blogs للمزيد من التفاصيل.

إسترجاع الحساب:

- إذا كنت تعتقد أن الحساب قد تم اختراقه ، فانتقل إلى: https://tumblr.zendesk.com/hc/en-us/articles/226176987-Compromised-accounts للحصول على تفاصيل استرجاع الحساب.

6.8 يوتيوب/ جوجل:

إدارة الحساب:

- يتحكم حساب جوجل في الوصول إلى منصة الوسائط الاجتماعية على يوتيوب بالإضافة إلى جي مايل GMail والعديد من المواقع والتطبيقات التي تزورها / تستخدمها ؛ لذلك ، يجب أن تكون التكوينات الأمنية الخاصة بها في مكانها الصحيح. اقرأ واستوعب سياسات جوجل https://policies.google.com/privacy?hl=en-US, شروط خدمة اليوتيوب https://www.youtube.com/static?template=terms و إرشادات المنتدى https://www.youtube.com/intl/ar/howyoutubeworks/policies/community-/guidelines
- تأكد من أنك تستخدم أحدث إصدار من متصفحك. تعرف على كيفية تحديث جوجل كروم من هنا: https://support.google.com/chrome/answer/95414?hl=ar

سياسة كلمة المرور:

- يجب أن تتكون كلمة المرور من 8 أحرف على الأقل. يمكن أن يكون أي مجموعة من الأحرف والأرقام والرموز (أحرف ASCII القياسية فقط). لا يمكن إستخدام العلامات والأحرف المُعلَّمة.
- لا يمكنك استخدام كلمة مرور
  - ضعيفة بصوة واضحة. مثال"password123".
  - تم استخدامه من قبل على الحساب.
  - يبدأ أو ينتهي بمساحة فارغة.

كيفية تفعيل المصادقة الثنائية:

تتيح Google عدة خيارات لتمكين المصادقة الثنائية من خلال أحد الإجراءات التالية:

1. رسائل المطالبة من جوجل.
2. رمز التحقق من رسالة نصية أو مكالمة
3. تطبيق مصادقة جوجل او تطبيقات المصادقة الاخرى
4. رموز النسخ الاحتياطي
5. مفاتيح الأمان

لتمكين المصادقة الثنائية مع أي مما سبق ، انتقل إلى:
https://myaccount.google.com/signinoptions/two-step-verification/enroll-welcome

نصائح أمنية:

- استخدم كلمة مرور قوية.
- قم بتفعيل التسجيل عن طريق المصادقة الثنائية.
- قم دائماً بتسجيل الخروج بعد الإنتهاء من عملك.
- قم بتشغيل برنامج مكافحة الفيروسات على جهاز الكمبيوتر الخاص بك.
- قم بإجراء فحص أمان جوجل. تمنحك هذه الأداة خطوة بخطوة توصيات مخصصة وقابلة للتنفيذ للمساعدة في تعزيز أمان حساب جوجل الخاص بك.

- قم بتثبيت التطبيقات الأساسية وملحقات المستعرض فقط على الأجهزة التي يمكنها الوصول إلى المعلومات الحساسة. تجنب تثبيت تطبيقات غير معروفة أو تطبيقات من مصادر غير معروفة لحماية جهازك ومعلوماتك الشخصية. ها هو الرابط لمعرفة الكيفية: https://support.google.com/chromebook/answer/2589434
- تحقق بشكل متكرر من طرق الاتصال الاحتياطية. هذا هو ما ستستخدمه جوجل في حالة حظر دخولك إلى حسابك للتحقق من أنك مالك الحساب.
- تحقق من الأجهزة التي تم استخدامها للوصول إلى حسابك وراجعها. للقيام بذلك ، انتقل إلى: https://myaccount.google.com/security وسترى قائمة بأجهزتك.

نصائح الخصوصية:

- قم بإزالة الوصول إلى الحساب لأي تطبيقات غير ضرورية لحماية المعلومات الحساسة بشكل أفضل.
  1. إدارة التطبيقات مع الوصول إلى حسابك ومعرفة المزيد عن المخاطر.
  2. قم بإيقاف تشغيل الوصول للتطبيقات التي تستخدم تقنية تسجيل دخول أقل أمانًا.
- للتحقق مما إذا كان شخص آخر لديه حق الوصول إلى حسابك ، قم بتسجيل الدخول إلى حساب جيميل الخاص بك وانتقل إلى أسفل الصفحة ، وانقر فوق آخر نشاط للحساب في نهاية هذا السطر ، وانقر فوق التفاصيل لمعرفة متى وكيف وأين تم إستخدام حسابك. إذا كنت تشك في أي نشاط مشبوه ، فانقر فوق الزر المسمى تسجيل الخروج من جميع جلسات ويب جيميل الأخرى وقم بتغيير كلمة مرورك على الفور.
- تعيين الأذونات والتحقق منها على قناتك على يوتيوب ، يمكنك دعوة شخص آخر لإدارة قناتك على يوتيوب دون منح حق الوصول إلى حساب Google الخاص بك. ادعُ شخصًا ما للوصول إلى القناة بصفة:
  1. المدير: يمكنه إضافة أو إزالة الآخرين وتحرير تفاصيل القناة.
  2. المحرر: يمكنه تحرير جميع تفاصيل القناة.
  3. المشاهد: يمكنه عرض (ولكن ليس التعديل) جميع تفاصيل القناة.
  4. مشاهد مع صلاحيات محدودة: يمكنه عرض (لكن ليس تعديل) جميع تفاصيل القناة باستثناء معلومات الإيرادات.

للقيام بذلك ، قم بزيارة: https://support.google.com/youtube/answer/9481328

إسترجاع الحساب:

- إذا كنت تعتقد أن الحساب قد تم اختراقه ، فانتقل إلى: https://support.google.com/accounts/answer/7299973 و https://support.google.com/accounts/answer/6294825 للحصول على تفاصيل استرجاع الحساب.

6.9 تيليجرام:

إدارة الحساب:

- اقرأ واستوعب سياسة خصوصية تيليجرام https://telegram.org/privacy و شروط خدمة تيليجرام https://telegram.org/tos.
- تيليجرام - *في الوقت الحاضر* - يعتبر وجهة المحتالون بالعملات المشفرة لذا يتوجب التعامل معه بحذر.

سياسة كلمة المرور:

لا توجد كلمة مرور.

كيفية تفعيل المصادقة الثنائية:

لتفعيل المصادقة الثنائية ، اتبع الخطوات أدناه:

1. افتح تطبيق تيليجرام.
2. اضغط على "**الإعدادات**" في الركن الأيمن السفلي من الشاشة.
3. حدد "**الخصوصية والأمان**".
4. بالقرب من أعلى الشاشة ، انقر على "**التحقق بخطوتين**".
5. قم بإختيار "**تعيين كلمة مرور إضافية**".
6. أدخل كلمة المرور وقم بتأكيدها عن طريق إعادة إدخالها.
7. الآن اضغط على "**إنشاء كلمة مرور**".
8. في الصفحة التالية ، أدخل تلميحًا لمساعدتك على تذكر كلمة المرور ثم إضغط على "**متابعة**".
9. أدخل عنوان البريد الإلكتروني الذي تريد استخدامه لاستعادة كلمة المرور, ثم إضغط على "**متابعة**".
10. ستتلقى رمز التحقق على عنوان بريدك الإلكتروني. أدخل الرمز لمصادقة بريدك الإلكتروني.

نصائح أمنية:

- قم بتفعيل التسجيل عن طريق المصادقة الثنائية.
- لا تشارك رمز التحقق من رسائل تيليجرام القصيرة الخاص بك مع الآخرين ، ولا حتى الأصدقاء أو العائلة.
- التشفير من طرف إلى طرف ليس هو الوضع الافتراضي في محادثات تيليجرام. لإجراء محادثة مشفرة من طرف إلى طرف ، ستحتاج إلى تشغيل "**محادثة سرية**" والتي يمكن تفعيلها من خلال الانتقال إلى ملف تعريف جهة الاتصال التي تريد بدء الدردشة المشفرة معها ، والنقر على الخيارات ، ثم اختيار وتأكيد خيار "**بدء محادثة سرية**".

نصائح الخصوصية:

- حاول عدم مشاركة معلوماتك مع جميع مستخدمي تيليجرام, فإليك بعض النصائح حول تكوينات الخصوصية والتي يمكنك تعديلها من **الإعدادات** ← **الخصوصية والأمان**:

1. قم بتعيين "**من يمكنه رؤية رقم هاتفي**" على لا أحد.
2. قم بتعيين "**من يمكنه العثور علي برقمي**" على جهات الاتصال.
3. عيّن "**من يمكنه رؤية الطابع الزمني الخاص بي**" على لا أحد.

4. قم بتعيين "**من يمكنه رؤية صورة ملفي الشخصي**" على جهات الاتصال الخاصة بي.
5. قم بتعيين "**من يمكنه الاتصال بي**" على جهات الاتصال الخاصة بي.
6. اضبط "**مكالمات نظير إلى نظير**" على لا أحد.
7. قم بتعيين "**من يمكنه إضافة رابط إلى حسابي عند إعادة توجيه رسائلي**" إلى جهات الاتصال الخاصة بي.
8. اضبط "**المجموعات والقنوات ← من يمكنه إضافتي**" إلى جهات الاتصال الخاصة بي.

إسترجاع الحساب:

- قم بإلغاء تنشيط تيليجرام إذا فقدت هاتفك. توصي تيليجرام بأن تقوم على الفور بتنشيط Telegram بنفس رقم الهاتف على هاتف مختلف، باستخدام شريحة إتصالات بديلة. يمكن لرقم واحد فقط على جهاز واحد استخدام التطبيق في كل مرة ، لذلك من خلال القيام بذلك ، يمكنك على الفور حظر استخدامه على هاتفك القديم.
- إذا لم يكن ذلك ممكنًا ، فيمكنك الاتصال بدعم تيليجرام أو استخدام تطبيق تابع لجهة خارجية ، وسوف تحتاج إلى تقديم بعض المعلومات الشخصية مثل الاسم والبريد الإلكتروني.

6.10 سيجنال:

إدارة الحساب:

- يتم تشفير محادثات الرسائل الخاصة لتطبيق سيجنال من طرف إلى طرف افتراضيًا ، وقد تم تصميم التطبيق ليلائم ارسال و استقبال الرسائل والمعلومات الحساسة والشخصية.
- تطبيق المراسلة الخاصة سيجنال هو برنامج مفتوح المصدر يحاول تقليل كمية البيانات المخزنة على خوادم سيجنال. https://signal.org/blog/signal-profiles-beta/, https://signal.org/bigbrother/eastern-virginia-grand-jury/
- اقرأ سياسة خصوصية سيجنال https://signal.org/legal/#terms-of-service واكتشاف الاتصال بهم https://signal.org/blog/contact-discovery/.

سياسة كلمة المرور:

لا توجد كلمة مرور.

كيفية تفعيل المصادقة الثنائية:

لتفعيل المصادقة الثنائية عن طريق إدخال رقم تعريف شخصي أو كلمة مرور عند فتح تطبيق سيجنال ، قم بما يلي:

1. اضغط على أيقونة ملفك الشخصي في الزاوية العلوية اليسرى ثم قم بإختيار **الخصوصية**.
2. قم بالتمرير إلى أسفل وقم بتمكين **قفل التسجيل**.
3. إذا كنت لا تتذكر رقم التعريف الشخصي ، فيمكنك ببساطة النقر فوق تغيير رقم التعريف الشخصي وإنشاء رقم جديد. يمكنك إنشاء رقم تعريف شخصي مكون من 4 أرقام أو 20 رقمًا كحد أقصى
4. لا يدعم سيجنال تطبيقات المصادقة ولا يقدم أي رموز احتياطية.
5. إذا نسيت رقم التعريف الشخصي ولم تتمكن من الوصول إلى جهازك القديم ، فسيتعين عليك الانتظار 7 أيام حتى تنتهي صلاحية قفل التسجيل. بعد ذلك فقط ، ستتمكن من تسجيل الدخول إلى Signal وإنشاء رقم تعريف شخصي جديد.

نصائح أمنية:

- قم بتفعيل التسجيل عن طريق المصادقة الثنائية.
- لا تشارك رمز التحقق من رسائل تيليجرام القصيرة الخاص بك مع الآخرين ، ولا حتى الأصدقاء أو العائلة.
- تفعيل قفل الشاشة لحماية رسائلك من الوصول غير المصرح به.
- قم بتعيين رقم التعريف الشخصي لإعادة التثبيت واستعادة النسخة الاحتياطية والتحقق من الهوية.

نصائح الخصوصية:

- تعطيل إشعار الانضمام إلى جهات اتصال سيجنال.
- قم بتعديل إعدادات الإشعارات للحصول على إشعار باسم المرسل دون أي رسالة.

- يمكنك تعتيم الوجوه على سيجنال قبل مشاركة الصور.
- يمكنك ضبط عداد الوقت لتحديد متى ستبدأ الرسائل في الاختفاء بعد أن يقرأها المستلم.
- إحظر صور إلتقاط الشاشة.
- ترحيل المكالمات بحيث لا يتم الكشف عن عنوان IP الخاص بك لجهات الاتصال الخاصة بك.
- إنشاء نسخة احتياطية محلية.
- تحقق من جهات الاتصال لتجنب احتمال هجوم رجل في المنتصف ، وللقيام بذلك اتبع الخطوات التالية:

1. افتح الملف الشخصي لجهة الاتصال الذي تريد التحقق منه.
2. مرر لأسفل وافتح "عرض رقم الأمان".
3. اضغط على رمز الاستجابة السريعة وقم بمسح رمز الاستجابة السريعة ضوئيًا من جهاز جهة الاتصال الأخرى.

أو بدلاً من ذلك:

1. افتح الملف الشخصي لجهة الاتصال الذي تريد التحقق منه.
2. مرر لأسفل وافتح "عرض رقم الأمان".
3. اضغط على زر "مشاركة" لإرسال رقم الأمان الخاص بك إلى مستخدم آخر.
4. قارن وتحقق من أرقام الأمان.

إسترجاع الحساب:

- إذا فقدت رقم هاتفك ، فلا يوجد شيء يمكن فعله باستخدام تطبيق سيجنال.
- قامت سيجنال بتطوير استعادة القيمة الآمنة Secure Value Recovery الذي يبقي الرسم البياني الاجتماعي الخاص بك غير معروف لخوادم سيجنال. إذا فقدت جهازك المحمول أو قمت بتبديله ، فيمكن لرقم التعريف الشخصي استرداد ملفك الشخصي ، والإعدادات ، وجهات الاتصال ، والحسابات التي حظرتها ، لكن رقم التعريف الشخصي ليس نسخة احتياطية للدردشة. سجل رسائلك غير مرتبط برقم التعريف الشخصي ولا يمكن استخدام رقم التعريف الشخصي لاستعادة سجل الدردشة المفقود. مزيد من التفاصيل هنا: https://signal.org/blog/secure-value-recovery/.

6.11 تيك توك:

إدارة الحساب:

- تتركز مخاوف تيك توك الأمنية إلى حد كبير على حقيقة أن تيك توك هي شركة صينية وأن القوانين الصينية تفرض على الشركات في الصين مشاركة المعلومات مع حكومة الصين.
- اقرأ واستوعب سياسة خصوصية تيك توك لفهم البيانات التي يجمعها تيك توك منك وأي المعلومات يشاركونها أو يفصحون عنها https://www.tiktok.com/legal/privacy-policy?lang=en و شروط الخدمة https://www.tiktok.com/legal/terms-of-service?lang=en.
- انتقل إلى https://www.tiktok.com/safety/en/privacy-and-security-on-tiktok لمعرفة المزيد حول ميزات الخصوصية والأمان في تيك توك.

سياسة كلمة المرور:

يجب أن تكون كلمة المرور بين 8 و 20 حرفًا من حروف وأرقام ورموز خاصة.

كيفية تفعيل المصادقة الثنائية:

1. لتفعيل المصادقة الثنائية ، اتبع الخطوات أدناه:
2. اذهب إلى ملف التعريف الخاص بك.
3. اضغط على زر الثلاثة خطوط لفتح الإعدادات الخاصة بك.
4. انقر فوق الأمن وتسجيل الدخول.
5. قم بتغيير التحقق بخطوتين من إيقاف تشغيل إلى تشغيل.
6. قم إما بإختيار الرسائل النصية القيرة أو البريد الإلكتروني لإرسال رمز التحقق.

نصائح أمنية:

- تأكد من أن حساب تيك توك الخاص بك خاص. للقيام بذلك ، انتقل إلى **الإعدادات** في ملف التعريف الخاص بك ← **الخصوصية والأمان** وابحث عن **عنوان الاكتشاف**، ثم قم بتفعيل خيار الحساب الخاص.
- يمكنك إيقاف تشغيل خيار اقتراح حسابك للآخرين من الاكتشاف كما هو مذكور أعلاه. سيؤدي إيقاف تشغيل هذا الإعداد إلى إيقاف التوصية بحسابك للمستخدمين الآخرين وسيمنع الأشخاص الآخرين من العثور على حسابك عبر محركات البحث.
- تجنب فتح روابط تيك توك خارج التطبيق.
- قم بتسجيل الخروج من تيك توك عند الانتهاء من عملك.
- تحقق من الأجهزة المحمولة التي تستخدم حاليًا أو وصلت مؤخرًا إلى حساب تيك توك الخاص بك. للقيام بذلك ، انتقل إلى **الخصوصية والأمان** ← **إدارة حسابي** ← **الأمان** ← **أجهزتك**.
- كن حذرًا مما تختار نشره. وأن مقاطع الفيديو الخاصة بك لا تحتوي على معلومات شخصية مثل علامات العنوان أو الهوية الوطنية.
- قم بتمكين التنبيهات الأمنية لضمان تنبيهك عندما يتعرض حسابك إلى إجراء مشبوه. للقيام بذلك ، انتقل إلى ملف التعريف الخاص بك ثم انقر فوق قائمة الخطوط الثلاثة ثم اختر **الأمن** حيث يمكنك العثور على **تنبيهات الأمن** وتفعيلها.

نصائح الخصوصية:

- اقرأ نصائح الأمان الخاصة بتيك توك: https://www.tiktok.com/creators/creator-/portal/en-us/community-guidelines-and-safety/safety-tips
- التقليل قدر الإمكان من كمية المعلومات التي تشاركها على التطبيق.
- الحد من تفاعل المستخدمين الآخرين مع مقاطع الفيديو الخاصة بك. للقيام بذلك ، انتقل إلى **الخصوصية** ← **الأمن** ثم اضبط **السماح بتنزيل مقاطع الفيديو الخاصة بك** على إيقاف التشغيل ، وقم بتعيين **من يمكنه إرسال رسالة مباشرة إليك** على **الأصدقاء فقط** وتعيين **من يمكنه الإشتراك مع مقاطع الفيديو الخاصة بك** على **أنا فقط**.
- قم بإيقاف تشغيل "**السماحية للإعلانات**". للقيام بذلك ، انتقل إلى **الإعدادات** في ملف التعريف الخاص بك ← **الخصوصية** وابحث عن **عنوان التخصيص والبيانات** ، ثم قم بإيقاف **تشغيل ترخيص الإعلان**.

إسترجاع الحساب:

قم بزيارة هذا الرابط للحصول على تفاصيل حول الحسابات المخترقة:
https://support.tiktok.com/en/log-in-troubleshoot/log-in/my-account-has-been-hacked ، اتصل بدعم تيك توك إذا كنت تعتقد أن حسابك تم اختراقه.

7 الامتثال والإنفاذ

7.1 الامتثال والإنفاذ

تم نشر هذه المبادئ التوجيهية لمساعدة المؤسسات في إدارة حساباتها على وسائل التواصل الاجتماعي على نحو آمن

هذه المبادئ التوجيهية تكمل سياسة تصنيف البيانات الوطنية ومعيار تأمين المعلومات الوطنية.

8 المرفقات

8.1 الاختصارات

NCSA	الوكالة الوطنية للأمن السيبراني
2FA	المصادقة الثنائية.
QR Code	رمز الاستجابة السريعة.
PIN	رقم التعريف الشخصي
ASCII	الشفرة الأمريكية القياسية لتبادل المعلومات.
SMS	خدمة الرسائل القصيرة.
IP	بروتوكول الإنترنت

8.2 المراجع

القرار الأميري رقم 1 للعام 2021

قرار رئيس الوكالة الوطنية للأمن السيبراني رقم 3 للعام 2022.

8.3 قائمة الأشكال

لا توجد

8.4 الإبلاغ عن الحوادث إلى الوكالة الوطنية للأمن السيبراني

يمكن للمؤسسات التي تواجه هجوم حجب الخدمة الموزعة إبلاغ الوكالة الوطنية للأمن السيبراني عن الحادث بإحدى الطرق التالية:

الاتصال بالخط الساخن الخاص بالوكالة الوطنية للأمن السيبراني على رقم 16555 (خدمة على مدار الساعة طوال أيام الأسبوع)

إرسال بريد الإلكتروني على البريد الالكتروني الخاص بالوكالة الوطنية للأمن السيبراني ncsoc@ncsa.gov.qa

قد تجد المؤسسات أيضًا الإرشادات التالية مفيدة في الاستعداد لمواجهة أي هجوم / حادث.

إرشادات لإدارة الحوادث - الإجراءات المطلوبة مسبقًا