

دليل السلامة الرقمية للمدافعين والمدافعات عن حقوق الإنسان

حماية وتأمين حساباتك

5 تفعيل المصادقة الثنائية من خلال
"الإعدادات والخصوصية".
استخدام مفاتيح الحماية أو برامج المصادقة
الثنائية الموثقة



6 التحقق من تسجيل الدخول
قم بتسجيل الخروج من أي جهاز غير معروف.



7 تجنب النقر على روابط أو ملفات غير
معروفة، وتحقق من مصدرها.



افحص الروابط والملفات على:
<https://www.virustotal.com>



8 تحديث الأجهزة والتطبيقات بشكل
دوري.



1 استخدام كلمة مرور قوية
يفضل استخدام مزيج طويل من الحروف،
الأرقام، والرموز، مع التحلي بتنوع يشمل
جملة كلمات تستخدم ككلمة مرور.



تأكد من قوة كلمة المرور لديك على الرابط:
www.security.org/how-secure-is-my-password/



2 استخدام برامج حفظ كلمات المرور



3 تحديث بريدك الإلكتروني ورقم
الهاتف



4 تفعيل تنبيهات تسجيل الدخول



حماية الخصوصية على الإنترنت

1



تحكّم في مرئية معلوماتك الشخصية لدى الآخرين.

- تحديد خاصية خدمات الموقع إلى "أبدًا" في جميع التطبيقات، أو "أثناء استخدام التطبيق فقط".
- أجر فحوصات السلامة بانتظام.

آيفون: الانتقال إلى الإعدادات والبحث عن فحص السلامة، ثم النقر على "إدارة للمشاركة والوصول".

2



إدارة الوصول العام على حساباتك للمحتوى والوسوم والتعليقات.

فيسبوك

استكشف "الملف القفل"، إذا كان متاحًا.

<https://www.facebook.com/help/196419427651178>



4



فعل نمط المنع (Lockdown Mode)

متوفر على أجهزة آيفون وأندرويد.

للحماية القصوى ضد الهجمات السيبرانية النادرة والمتطورة للغاية.

3



احذف أي أفعال المشبوهة عبر تقرير خصوصية التطبيقات

تواصل بأمان

1

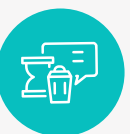


استخدم رسائل مشفرة بين الطرفين.

فعل خاصية التشفير بين الطرفين يدويًا:

ماسنجر: شفر محادثاتك عبر اختيار 'اذهب الى المحادثة السرية' في قائمة المعلومات الموجودة في أعلى يمين المحادثة.
انستغرام: قم بتبديل أيقونة القفل في الجزء العلوي الأيمن من صفحة الرسائل الخاصة بانستغرام.

2



حذف سجل المحادثات باستمرار.

4



استخدام الرسائل المخفية.

واتساب: "التخزين والبيانات" في إعدادات واتساب أو في محادثة معينة باستخدام "معلومات المحادثة".

ماسنجر: داخل المحادثة اذهب إلى "الخصوصية والدعم".

انستغرام: اسحب المحادثة للأعلى لتفعيل وضعية الاختفاء.

3



فعل قفل المحادثة على واتساب

الإبلاغ عن انتهاك الخصوصية

يمكنك الإبلاغ عن أي انتهاك للخصوصية عبر الروابط التالية:

فيسبوك  
<https://bit.ly/fb-privacyreport>

انستغرام  
<https://bit.ly/ig-privacyreport>

القواعد الست لأي عنف رقمي

إذا وجدت نفسك في موقف تتعرض فيه للتنمر عليك أو مضايقتك، أو تهديدك، أو مشاركة الصور دون موافقتك، أو التعامل معك بعنف، تذكر القواعد الست الأساسية:

1 عدم الرد

لا ترد بنفس الطريقة؛ الجاني ينتظر أي تفاعل من قبل الضحية.

2 حفظ الأدلة

حافظ على دليل لديك، مثل لقطات الشاشة، لاستخدامها في التحقيق.

3 الإبلاغ

قم بالإبلاغ الفوري عن حساب الجاني عبر المنصة المستخدمة.

4 حذف الحساب

احذف الحساب من قائمة أصدقائك ومتابعيك.

5 الحظر

قم بحظر حساب الجاني، لكي لا يتمكن من التواصل معك.

6 اتصل بمؤسسة مختصة



في حالة وجود خطر، شارك الموقف مع شخص تثق به أو تواصل مع الجهات الرسمية فورًا.

الإبلاغ عن مشكلة في الحساب

الحسابات المعطلة أو الملقاة

وصول اشعارات أو تحذيرات حول حسابك الخاص، وبالغالب بسبب اختراق المعايير المجتمعية لمتنا. يمكنك تقديم اعتراض لاسترجاع الحساب من خلال:

فيسبوك  
<https://www.facebook.com/help>

انستغرام  
<https://help.instagram.com/>

الحسابات المخترقة

يمكنك التبليغ عن اختراق حسابك من خلال الروابط التالية:

فيسبوك  
<https://www.facebook.com/hacked>

انستغرام  
<http://www.instagram.com/hacked>

واتساب

● قم بتسجيل دخول الى حساب واتساب باستخدام رقمك.

● قم بتوثيق رقمك من خلال ادخال رمز التحقق (6 أرقام) التي استلمتها عبر رسالة نصية. وبذلك سوف يتم تسجيل خروج تلقائي من قبل جهاز الشخص المخترق للحساب.

● قم بادخال رمز المصادقة الثنائية.

أمان جهازك أثناء المظاهرات

استخدم خاصية التشفير بين الطرفين،
وتجنب الرسائل القصيرة والمكالمات
الهاتفية.



تأكد من تحميل مقاطع الفيديو
والصور على مساحة آمنة ومشفرة.



فعل وضعيّة الطيران على جهازك من
أجل وقف مشاركة البيانات والمعلومات
الجغرافية.



فعل وضعيّة الطيران على جهازك من
أجل وقف مشاركة البيانات والمعلومات
الجغرافية.



انقطاع الوصول إلى الإنترنت أو الحجب

استخدم شبكات افتراضية آمنة
(VPN) للوصول للمواقع والتطبيقات
الخاضعة للرقابة أو المحجوبة



استخدم متصفحات الإنترنت الآمنة
والسرية.



قم بزيارة منصة "أمان رقمي" للتعرف أكثر على
هذه التطبيقات

<https://amanraqami.org>



احمي نفسك خلال الأزمات

خطوط المساعدة للأمن الرقمي في الشرق الأوسط وشمال أفريقيا

يمكنك طلب المساعدة والتبليغ عن أي انتهاكات
رقمية

الجمعية الأردنية للمصدر المفتوح
<https://er.josa.ngo>



مركز حملة
<https://7or.7amleh.org>



سمكس
<https://smex.org/helpdesk>



فروننت لاين ديفنדרز
<http://frontlinedefenders.org/emergency-contact>



Access Now
<https://www.accessnow.org/help-ar/>



مساعدة إضافية؟

البقاء بأمان على منصات ميتا

قم بالتسجيل في دورة ميتا
المجانية للأمن الرقمي باللغة
الإنجليزية، العربية أو
الفرنسية عن طريق مسح
الرمز هذا.



استخدم الرمز 909215