الدليل الارشادي حول الاستخدام الأمن لشبكات التواصل الاجتماعي للأفراد

نحو بيئة سيبرانية آمنة

مقدمة

تعتبر قضايا الابتزاز الالكتروني من أكثر التحديات التي تهدد أمن وسلامة المجتمعات من أفراد وأسر، وهي نوع من أنواع الجرائم السيبرانية الحديثة، التي قد تقوم باستغلال عدم وعي الأفراد بمخاطر وتهديدات مواقع التواصل الاجتماعي، وبالتالي محاولة الايقاع بهم في فخ الابتزاز.

وقد جاءت هذه المبادرة؛ إيمانا بأهمية رفع مستوى الوعي لدى الأفراد بأهم المخاطر والتهديدات لمواقع ومنصات التواصل الاجتماعي، وهي جزء من عدة مبادرات مرتبطة بالاستعداد لمتطلبات الثورة الصناعية الرابعة، وكما هو معلوم فإن الأمن السيبراني من أهم عناصر ومكونات الثورة الصناعية الرابعة، وتأتي هذه المبادرة نتيجة تعاون مشترك، ونتاج مشاركة في عدة مؤتمرات اقليمية ودولية ناقشت هذا التهديد، منها المؤتمر الدولي: الثورة الصناعية الرابعة، وأثرها على التعليم، ومؤتمر البيانات الشخصية، الذي أوصى بضرورة بحث الأساليب الأمنية لحماية شبكات التواصل الاجتماعي وتأثيرها على أمن الدول والمجتمعات.

ونرجو أن يضيف هذا الدليل الارشادي قيمة لدى الأفراد والمجتمع، وأن ينشر الوعي بين أفراد المجتمع حول استخدام وسائل التواصل الاجتماعي الاستخدام الآمن، كما نأمل بأن يسهم في تقليل حالات الابتزاز المتزايدة في الوطن العربي.

صالح الهيملي، أ.هانية فطاني

المحتوى

تمهيد

في ظل التطورات المستمرة، والخدمات التي تتيحها منصات وبرامج التواصل الاجتماعي على الانترنت، طورت شبكات التواصل الاجتماعي اليوم إمكانات التفاعل مع الآخرين، بتمكين المستخدمين من تشارك الرسائل والصور والملفات، وحتى أحدث المعلومات عن أماكنهم وأنشطتهم.

وأدى هذا التطور السريع إلى تزايد الأخطار المحيطة والحوادث الأمنية، وتنامي الهجمات والتهديدات ضد مواقع ومنصات التواصل الاجتماعي، وباتت هذه المنصات والبرامج سلاح ذو حدين قد يقع بالضرر على مستخدميها في حال عدم استخدامها الاستخدام الامثل.

ويهدف هذا الدليل برفع مستوى التوعية لدى الأفراد عن طرق تأمين واستخدام منصات وبرامج التواصل الاجتماعي الاستخدام الآمن، كما يوفر الدليل الخطوات الأساسية والاجراءات الاحترازية لتأمين مختلف حسابات منصات التواصل الاجتماعي، وطرق الحماية من الوقوع ضحية للاختراق أو الابتزاز الالكتروني، بالاضافة الى الاجراءات الضرورية التي يجب اتخاذها في حال اختراق هذه الحسابات، وطرق استرجاعها.

الفئة المستهدفة

يستهدف هذا الدليل الإرشادي الأفراد وجميع مستخدمي حسابات مواقع التواصل الاجتماعي وبرامجه، من مختلف شرائح المجتمع.

الابتزاز الالكتروني

الابتزاز الإلكتروني هو عملية تهديد وترهيب للضحية، وذلك بنشر صور أو مواد مصورة أو تسريب معلومات سرية تخص الضحية، مقابل دفع مبالغ مالية أو استغلال الضحية للقيام بأعمال غير مشروعة لصالح)المبتزين(كالإفصاح عن معلومات سرية خاصة بجهة العمل أو غيرها من الأعمال غير القانونية .

إن الابتزاز الإلكتروني ينطوي على تهديدات تستخدم لإجبار شخص ما على التخلي عن المال أو الخدمات أو الممتلكات الشخصية رغما عن إرادته. في كثير من الأحيان، تتعلق هذه التهديدات بالعنف الجسدي، أوالتعرض لمعلومات حسّاسة، أو إساءة معاملة أحد افراد العائلة أو المقرّبين. يمكن أن يكون التعامل مع الابتزاز الإلكتروني من الأمور المرهقة ولكنها ليست مستحيلة ابداً. من هنا إن معرفة أفضل طريقة للتعامل مع هذه المشكلة وكيفية الوقاية منها في المستقبل يمكن أن يساعد في السيطرة على الوضع وعدم الوقوع فيفخّ مخاطرها.

وبالحديث عن المجال الذي يرمي به المبتزون مصائدهم فعادة ما يتم تصيد الضحايا عن طريق البريدالإلكتروني أو وسائل التواصل الاجتماعي المختلفة ك"الفيس بوك، وتويتر، وإنستغرام، وهنجأوت" وغيرها من وسائل التواصل الاجتماعي نظراً لانتشارها الواسع واستخدامها الكبير من قبل جميع فئات المجتمع

كيفية الوقاية من الابتزاز الالكتروني

1. تجنب طلب صداقات أو قبول طلب صداقات من قبل أشخاص غير معروفين
2. عدم الرد والتجاوب على أي محادثة ترد من مصدر غير معروف .
3. تجنب مشاركة معلوماتك الشخصية حتى مع أصدقائك في فضاء الإنترنت "أصدقاء المراسلات
4. ارفض طلبات إقامة محادثات الفيديو مع أي شخص، ما لم تكن تربطك به صلة وثيقة
5. لا تنجذب للصور الجميلة والمغرية، و تأكد من شخصية المرسل
6. قم بتزويد جهازك الإلكتروني ببرامج مكافحة الفيروسات، وغيرها من برامج الحماية، فضلاً عن المواظبةعلى التحديث الدوري للبرنامج، والحرص على اقتناء النسخ الأصلية من هذه البرامج والمتوفرة في المحلات المخصصة بالبيع لها
7. لا تقم بالموافقة على طلبات التحميل لأي مادة ترد إليك من مصدر غير معروف، أو لم تقم بنفسك بطلب تحميلها إلى جهازك الإلكتروني مع التأكد من الصيغة الإلكترونية للمادة التي تقوم بتحميلها من الشبكة المعلوماتية فيما إذا كانت مطابقة لصيغة الوصف الذي طلبت تحميله من عدمه
8. تجنب فتح أي روابط مجهولة قبل التأكد من سلامتها، وعدم احتوائها على محتويات خبيثة.

إرشادات مستخدمي حسابات التواصل الاجتماعي

تبدأ معظم عمليات الابتزاز الإلكتروني بالقرصنة، إما على أحد حساباتك الاجتماعية أو بريدك الخاص والتي قد تكون طريقاً أيضاً نحو التعرّض إلى كامل معلوماتك الخاصة الموجودة على هاتفك الذكي أو الكومبيوتر. هناك عدد من خطوات حماية الخصوصية التي يمكنك اتخاذها لتقلل من احتمال تعرضك للاختراق والابتزاز الإلكتروني.

أولًا: ضبط الاعدادات العامة لبرامج التواصل الاجتماعي

1. تأمين الحماية للجهاز المستخدم في الدخول لبرامج التواصل الاجتماعي عن طريق كلمة مرور قوية
2. تفعيل قفل الجهاز/الشاشة تلقائيًا بعد ثوانٍ معدودة من عدم الاستخدام
3. تفادي تثبيت أي تطبيقات أو برمجيات غير معروفة وينصح بتحميل التطبيقات من المتاجر الرسمية للتطبيقات (مثل Apply Store أو Google Play)؛ وذلك لتقليل احتمالية اختراق الجهاز أو إصابته بالبرمجيات الضارة
4. التأكد من تفعيل خاصية تعقب الجهاز والإقفال التلقائي في حالة الفقدان أو السرقة؛ لحماية الجهاز وتسهيل العثور عليه.
5. الامتناع عن الدخول إلى الوظائف والتطبيقات غير الضرورية بالأجهزة أو تنزيل وتثبيت الألعاب وغيرها من التطبيقات المنتشرة في بعض برامج التواصل.
6. عدم تحميل أي تطبيق طرف ثالث (مثل التطبيقات التي تحتوي على مزايا إضافية عن التطبيقات الرسمية)، أو التطبيقات غير الرسمية أو المشبوهة.
7. عدم السماح لأي تطبيق آخر بالتزامن مع برامج التواصل الاجتماعي أو السماح لها باستخدام صلاحيات البرامج الرسمية.
8. التأكد من عدم تفعيل خاصية معرفة المكان في التطبيق.
9. استخدام شبكة موثوق بها للإتصال بالإنترنت وتجنب شبكات الواي فاي العامة والمجانية.
10. التأكد من تحديث نظام التشغيل والمتصفح وتطبيقات التواصل الاجتماعي بأحدث الإصدارات وبشكل مستمر ودوري لتجنب التهديدات الأمنية.
11. التأكد من تحديث برامج مكافح الفيروسات والبرمجيات الضارة بشكل دوري.
12. تجنب الدخول إلى الروابط المجهولة التي تظهر على صفحات الإنترنت أو ترسل عبر البريد الإلكتروني.
13. عدم فتح ملفات أو فتح روابط من مصادر مجهولة أو مشبوهة.

ثانيًا: خصائص كلمة المرور

تعتبر حماية البريد الإلكتروني وكلمات المرور جزءًا أساسيًّا لحماية حسابات مواقع التواصل الاجتماعي، وينصح مراعاة التالي:

1 استخدام كلمات مرور قوية ومختلفة لكلٍّ من البريد الإلكتروني -المتسخدم لفتح الحساب -وحسابات مواقع التواصل الاجتماعي، ويمنع إعادة استخدام كلمة المرور الواحدة على أي مواقع أو حسابات إلكترونية أخرى، ويجب أن تكون كلمات المرور كالتالي:

1. إنشاء كلمة مرور لا تقل عن ١٢ حرفًا.
2. استخدام مزيج من الأحرف الكبيرة والصغيرة والأرقام والرموز مثل (٨٢yN%gtul$Da)، مع مراعاة عدم تكرار أي منها في كلمة المرور.
3. استخدام كلمة مرور مختلفة لكل موقع إلكتروني أو حساب إلكتروني.
4. الالتزام بتغيير كلمة مرور بشكل دوري (كل شهر).

2 تجنب الاخطاء التالية عند بناء كلمة مرور:

1. عدم استخدام المعلومات الشخصية في كلمة المرور الخاصة بالحساب مثل أرقام الهواتف، وأعياد الميلاد، واسم المؤسسة، وأسماء الموظفين، ..إلخ.
2. عدم استخدام حروف متسلسلة مثل "abcd١٢٣٤"، أو متتاليات لوحة المفاتيح مثل "asdfghjkl".
3. يجب أن لا تحتوي كلمة المرور على أي كلمة موجودة في القاموس (حتى لا يسهل اختراقها).

ملاحظة مهمة جدًا:

إذا لم تملك ما يثبت صلتك بالحساب؛ قد لا تتمكن من استرجاعه للأبد عند تعذر الدخول إليه أو اختراقه؛ لذلك من الضروري إدخال بريد إلكتروني إضافي وأرقام الهاتف، ومعرفة بعض التفاصيل كتاريخ إنشاء الحساب، وتاريخ آخر تسجيل دخول، وآخر كلمة مرور مستخدمة، وإجابات الأسئلة الأمنية التي تم وضعها عند إنشاء الحساب؛ حيث سيتم لاحقًا استخدام هذه التفاصيل لاسترجاع الحساب في حالة عدم تمكنك من تسجيل الدخول إليه.

ثالثًا: تفعيل خصائص التأمين الإضافية في بعض مواقع التواصل الاجتماعي

هناك مجموعة واسعة من برامج التواصل الاجتماعي التي توفر خصائص حماية إضافية للمستخدم، ويعتبر تفعيلها ذا أهمية قصوى من أجل زيادة مستوى الحماية المتعلقة بالحسابات، وفيما يلي نستعرض أهم هذه الخصائص:

1 تفعيل المصادقة الثنائية (Two Factor Authentication):

الواتساب (WHATSAPP)

1. في تطبيق الواتساب، انقر على الاعدادات "Settings"
2. اذهب الى ملف الحساب الخاص بك "Account"
3. انقر على التحقق باستخدام خطوتين "Two-Step Verification"
4. انقر على زر التفعيل "Enable"
5. أكمل الخطوات وتأكد من تفعيل خاصية التحقق

الهوتميل (HOTMAIL)

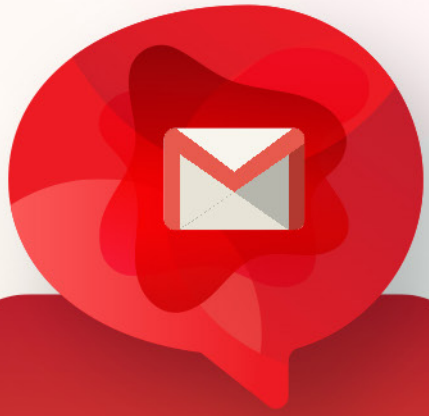
1. انتقل إلى إعدادات الأمان وسجّل دخولك باستخدام حساب Microsoft
2. حدد المزيد من خيارات الأمان.
3. ضمن المقطع التحقق على خطوتين، اختر إعداد التحقق على خطوتين لتشغيله
4. اتبع باقي الخطوات للتأكد من تفعيل الخاصية

ملاحظة*: يمكنك إيجاد الخطوات في رابط أيقونة الهوتميل أعلاه

الفيسبوك
(FACEBOOK)

1. انتقل الى اعدادات الامان وتسجيل الدخول
2. مرر لأسفل إلى استخدام المصادقة الثنائية ثم انقر على تعديل.
3. إذا لم تقم بإعداد المصادقة الثنائية من قبل، يجب عليك النقر على بدء الاستخدام. قد تتم مطالبتك بإدخال كلمة السر الخاصة بفيسبوك مرة أخرى عند هذه النقطة.
4. انقر على رسالة نصية عندما يُطلب منك اختيار طريقة الأمان، واتبع التعليمات الظاهرة على الشاشة.
5. بمجرد تشغيل رموز الرسالة النصية (SMS)، يجب عليك أيضا إعداد ميزة أمان ثانية، مثل جهات الاتصال الموثوقة أو رموز الاسترداد. يساعدك ذلك في حمايتك في حالة فقدان هاتفك المحمول أو سرقته أو اختراقه.

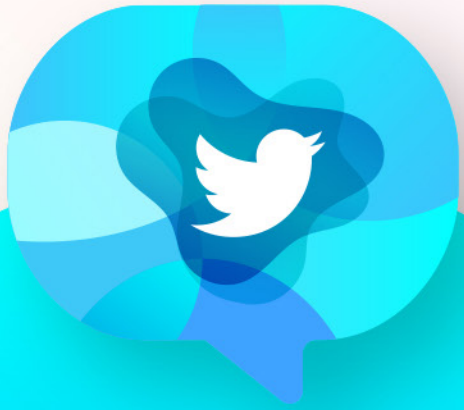
***ملاحظة:** يمكنك إيجاد الخطوات في رابط أيقونة الهوتميل أعلاه



الجيميل
(GMAIL)

1. افتح التطبيق الجيميل، اذهب الى الاعدادات "Settings"
2. في أعلى الصفحة، انقر على الأمان "Security"
3. ضمن "تسجيل الدخول إلى Google"، انقر على التحقُّق بخطوتين "Two Factor Verification"
4. انقر على البدء.
5. اكمل الخطوات المبينة في الشاشة في التطبيق

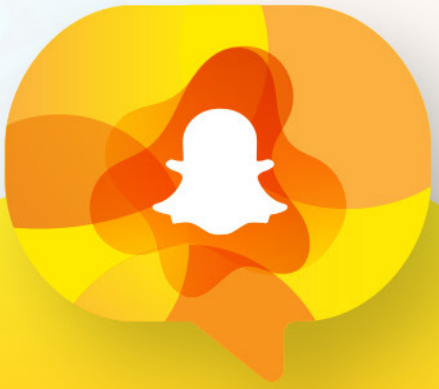
***ملاحظة:** يمكنك إيجاد الخطوات في رابط أيقونة الجيميل أعلاه



التويتر
(TWITTER)

1. في أعلى القائمة، انقر على الملف الخاص بك "Profile"
2. اضغط على الاعدادات والخصوصية "Settings and Privacy"
3. اضغط على اعدادات الحساب، ثم التحقق من الدخول "Set up login verification"
4. واتبع باقي الخطوات في تطبيق التويتر واضغط زر البدء "Start"
5. ادخل الرقم السري الخاص بحسابك "Password" وانقر "Verify"
6. اضغط على ارسال الرمز "Send code" لاضافة رقم الهاتف الخاص بك
7. ستصلك رسالة قصيرة برمز الامان الخاص بك، ثم اضغط "Submit"
8. اضغط على استعادة الرمز الخاص "Get Backup Code"

ملاحظة:* يمكنك إيجاد الخطوات في رابط أيقونة التويتر أعلاه.

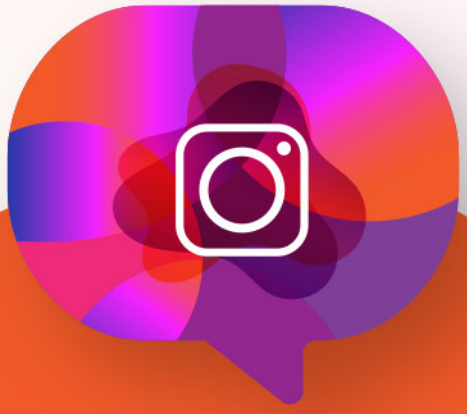


سناب شات
(SNAPCHAT)

1. في شاشة الكاميرا، انقر على الملف الخاص بك "Profile"
2. اضغط على الاعدادات "Settings"
3. اضغط على المصادقة الثنائية "Two-Factor Authentication"
4. واتبع باقي الخطوات في تطبيق السناب شات

- ينصح بشدة إذا قمت بتمكين مصادقة Two-Factor أن تقوم أيضًا بإنشاء رمز الاسترداد وحفظه في مكان آمن للوصول اليه مثل السحابة بدلاً من الجهاز الفعلي الخاص بك
- بهذه الطريقة، في حالة فقدانك لجهازك، أو تغيير رقم هاتفك، أو استعادة هاتفك إلى إعدادات المصنع الأصلية، فستتمكن من تسجيل الدخول!

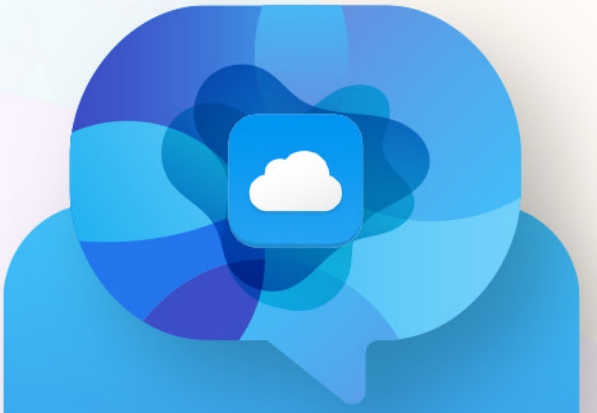
ملاحظة:* يمكنك إيجاد الخطوات في رابط أيقونة السناب شات أعلاه.



انستجرام
(INSTAGRAM)

1. انتقل إلى ملفك الشخصي، ثم اضغط على الضبط
2. اضغط على الاعدادات
3. اضغط على الخصوصية والامان
4. اضغط على المصادقة الثنائية
5. اضغط على زر التفعيل بجانب رسالة نصية
6. إذا لم يكن بحسابك رقم هاتف تم تأكيده، فستتم مطالبتك بإدخال رقم هاتف. بعد إدخال رقم الهاتف، اضغط على التالي (iPhone) أو (Android).

- يرجى العلم أنه يجب أن يتوفر لحسابك على Instagram رقم هاتف مؤكد لاستخدام المصادقة الثنائية عبر الرسائل النصية. عند إدخال رقم الهاتف لتشغيل المصادقة الثنائية، سيتم اعتبار هذا الرقم هو الرقم المؤكد لحسابك.



آيكلاود
(ICLOUD)

1. انتقل الى حساب "iCloud" الخاص بك
2. اضغط على اعدادات الامان وكلمة المرور "Password & Security"
3. اضغط على المصادقة الثنائية "Two-Factor Authentication"
4. قم باضافة رقم الهاتف الخاص بك
5. اضغط على الحصول على رمز التحقق "Get Verification Code"
6. قم باكمال الخطوات للتحقق من تفعيل الخاصية

***ملاحظة:** يمكنك إيجاد الخطوات في رابط أيقونة الانستجرام أعلاه.

رابعـــاً: توثيـــق الحسابـــــات

تتيح خدمة توثيق الحسابات معرفة الحسابات الأصلية التي تمثل الشخصيات المعنية ذات الاعتبار.

توصيات عامة لتوثيق الحساب:

هناك شروط يجب الأخذ بها لزيادة فرص توثيق الحساب سريعًا، تتمثل في ما يأتي:

1. يجب أن يعكس الملف الشخصي دور الشخصية ومجال عملها.
2. يجب أن يكون هناك محتوى وتفاعل بين الحساب والمتابعين (الصفحات والحسابات الجديدة لا يتم توثيقها مباشرة).
3. يجب أن تعبّر صورة الملف الشخصي عن شخصية الحساب.
4. عدم استخدام برامج زيادة المتابعين إطلاقًا؛ لأنها تتعارض مع معايير التوثيق.
5. أي تغييرات على صورة الملف الشخصي والمعلومات العامة والموقع وتفاصيل الاتصال؛ قد يلغي توثيق الحساب دون ذكر أي سبب واضح! لذلك يجب التحقق و تحديث الملف الشخصي للحساب جيدًا قبل طلب التوثيق؛ لأن تغيير هذه المعلومات لاحقًا قد يؤدي إلى إلغاء التوثيق.

طريقة توثيق الحسابات:

كيفية توثيق حساب تويتر (Twitter)

1. ادخل إلى حسابك على موقع تويتر عن طريق كتابة عنوان البريد الإلكتروني وكلمة المرور.
2. أدخل إلى الرابط الآتي: https://verification.twitter.com/welcome، حيث ستظهر لك نافذة جديدة.
3. اضغط على كلمة التالي، ثمّ أدخل اسمك الموجود على تويتر، واضغط على كلمة التالي.
4. أدخل عنوان موقعك، ثمّ اضغط على كلمة التالي.

ملاحظة: سيتم الرد عليك عبر رسالة بريد إلكتروني في حال القبول، أو في حال الرفض، حيث سيتم توضيح أسبابه، ومن الممكن إعادة إرسال الطلب مرة أخرى بعد ٣٠ يوماً، مع الحرص على إكمال كافة الشروط والمعلومات المطلوبة، كما يمكنك الحصول على تفاصيل التوثيق عبر النقر على أيقونة التويتر الموثقة أعلاه.

قبل طلب توثيق الحساب، يجب التأكد من توافر التالي:

01 رقم هاتف موثق

02 عنوان بريد الكتروني مؤكد

03 النبذة التعريفية

04 صورة الملف الشخصي

05 تاريخ الميلاد

06 موقع الكتروني

07 تعيين التغريدات على أنها عامة في إعدادات الخصوصية للتغريدة

كيفية توثيق حساب الانستجرام (INSTAGRAM)

1. من خلال حسابك الشخصي اضغط على قائمة الخيارات التي تظهر في أقصى الزاوية اليمين
2. اضغط على الإعدادات (Settings)
3. اضغط على طلب توثيق (Request Verification)

قبل طلب توثيق الحساب، يجب التأكد من التالي:

01 تحتاج إلى التأكد من أن حسابك يتوافق مع بنود شروط الخدمة وإرشادات المجتمع.

02 إرفاق صورة لمستند يثبت هويتك كإرفاق صورة بطاقة الهوية أو رخصة قيادة أو جواز سفر.

03 إدخال اسمك بالكامل.

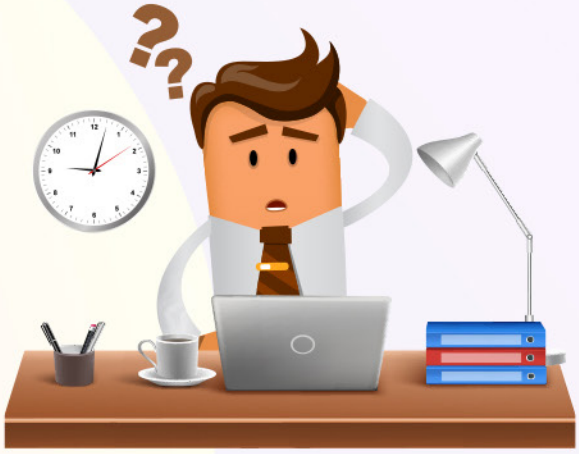
04 إرسال الطلب والانتظار، لحين قيام إنستغرام بمراجعة طلبك.

خامسا: آداب النشر والتفاعل

ينصح مستخدمي مواقع التواصل الاجتماعي بتجنب النشر أو التفاعل أو التعليق سواءً تصريحًا أو ضمنًا بكل ما يحتوي على:

1. الاستهانة بالمعتقدات الدينية أو الطائفية أو الإساءة إليها.
2. التشهير أو القذف أو التمييز.
3. النشر أو التعامل مع معلومات كاذبة وغير موثوقة.
4. التعليق أو المشاركة في كل ما يدعم أو يحرض على القيام بأنشطة غير قانونية.
5. التعليقات والمشاركات التي تخالف أي حقوق قانونية أو حقوق الملكية الفكرية.

على الرغم من عدم وجود ضمانات مطلقة ضد الابتزاز الإلكتروني، إذا اتبعت هذه الخطوات، ستكون أقل عرضة للوقوع ضحية لهذه المؤامرات الخطيرة. ومع ذلك ، إذا وجدت نفسك متورطًا في عملية احتيال للابتزاز ، فاتصل بالشرطة او بالجهة المتخصصة في ملاحقة تلك الجريمة الإلكترونية على الفور!



ماذا أفعل اذا وقعت ضحية للابتزاز ؟

1. عدم التواصل مع الشخص المبتز، حتى عند التعرض للضغوطات الشديدة.
2. عدم تحويل أي مبالغ مالية، أو الإفصاح عن رقم بطاقة البنك، أو تلبية أي طلب للمبتز إذ قد ينطوي ذلك زيادة الضغوط على الضحية لتلبية طلبات المبتز.
3. تجنب المشادات مع المبتز وعدم تهديده بالشرطة، وقم بالإبلاغ عند وقوع الحادثة مباشرة لدى الجهات المختصة دون أن توجه إلى المبتز أي تلميح أو تخبره برغبتك في إبلاغ الجهات المختصة.
4. في حالة التعرض للابتزاز قم بالتواصل مباشرة مع وحدة الجرائم الاقتصادية بشرطة عمان السلطانية على الرقم ٢٤٥٦٩٧٠١ أو اطلب المساعدة من المركز الوطني للسلامة المعلوماتية بهيئة تقنية المعلومات على الرقم ٢٤١٦٦٨٢٨.

طرق التعامل مع الحسابات المخترقة لمختلف مواقع التواصل الاجتماعي

الواتساب
(WHATSAPP)

1. إذا تم اختراق حساب الواتساب الخاص بك، قم بحذف تطبيق الواتساب من جهازك، وأعد تنصيبه من جديد.
2. سيتم تعطيل الحساب من جهاز المخترق، ويتفعل الحساب في جهازك من جديد.
3. قم بتفعيل التحقق بخطوتين فورا، أما اذا قام المخترق بتفعيل التحقق بخطوتين، فلن تتمكن من استعادة الحساب بهذه الطريقة، ويجب عليك التواصل مع فريق الواتساب عن طريق الاتي:

١. اذهب الى تطبيق الواتساب، وانتقل الى الاعدادات "Settings"
٢. انقر زر المساعدة "Help"
٣. اضغط على اتصل بنا "Contact Us"
٤. بامكانك الابلاغ وشرح المشكلة بالتفصيل
٥. كما يمكنك التواصل مع فريق الدعم الخاص بتطبيق واتساب عبر ارسال رسالة الى العنوان support@whatsapp.com وعنوان الرسالة "مفقود او مسروق"، وتطلب من الفريق تعطيل الحساب الخاص بك، مع ذكر رقم الهاتف بشكل كامل (+٩٦٨ ٩XXXXXXX)

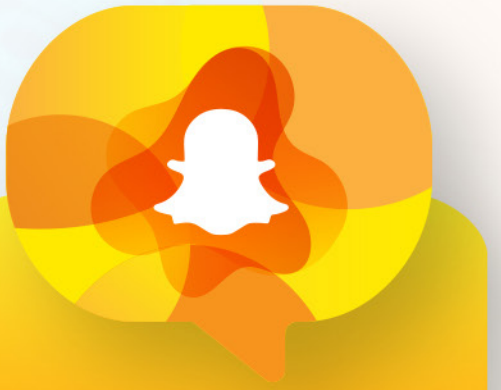
ملاحظة*: توجد تفاصيل الخطوات في رابط أيقونة الواتساب أعلاه

الجيميل
(GMAIL)

1. إذا تم اختراق أي حساب من حسابات جوجل حاول استرجاع الحساب عبر رابط أيقونة الجيميل أعلاه

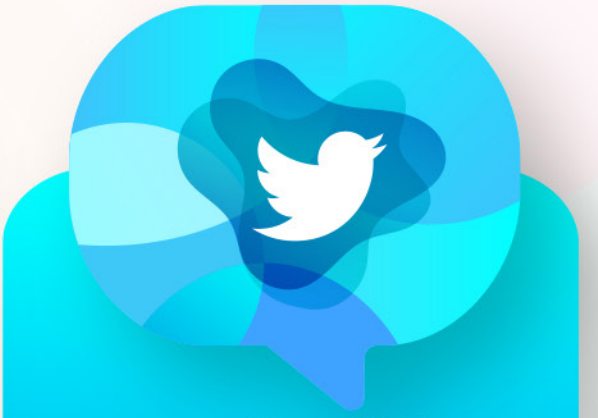
الفيسبوك
(FACEBOOK)

1. إذا تم استهداف أو اختراق الحساب عن طريق هجوم التصيد الإلكتروني؛ أرسل بلاغًا إلى ممثل فيس بوك مع شرح القضية Katie.Harbath@fb.com
2. ولاسترجاع الحساب، اتبع الرجاء الضغط على أيقونة الفيسبوك أعلاه.



سناب شات
(SNAPCHAT)

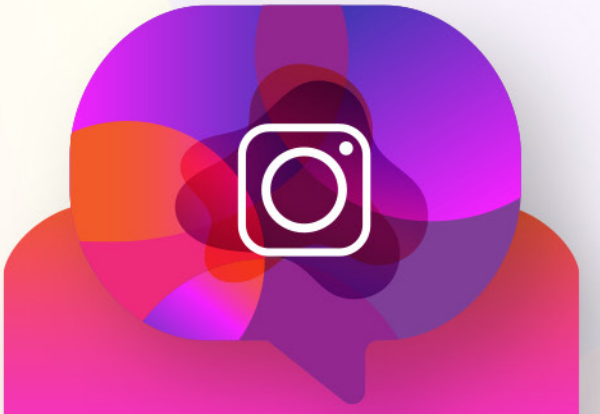
1. في حالة اختراق الحساب؛ اطلب المساعدة عبر الموقع الرسمي وذلك بالنقر على الايقونة أعلاه.
2. ولاسترجاع الحساب، اتبع الخطوات في أيقونة الاسترجاع أدناه.



التويتر
(TWITTER)

1. إذا تم استهداف أو اختراق الحساب؛ تواصل على الفور مع تويتر عن طريق إرسال إيميل يتضمن اسم الموضوع "Hacking" ويحوي نسخا من رسائل البريد الإلكترونية المشتبه بها على hacked*twitter.com
2. اضغط على الاعدادات والخصوصية "Settings and Privacy"

لاسترجاع الحساب، اتبع الخطوات في رابط أيقونة التويتر أعلاه.



انستجرام
(INSTAGRAM)

1. اطلع على خطوات استرجاع حساب إنستجرام المخترق عبر الرابط في الأيقونة أعلاه.