الدوكسينج.. نصائح للوقاية ومراقبة الأضرار

نصائح للوقاية

1

ابحث عن نفسك عبر الإنترنت وانظر ما تجده.

اعمل على عزل أو مراقبة حساباتك على وسائل التواصل الاجتماعي.

استخدم مولِد ومدير كلمات المرور للتأكد من أن لديك كلمات مرور.

إن كان ممكنا استخدم تطبيق المصادقة متعددة العوامل (MFA).

لا تستخدم اسمك الكامل أو الحقيقي كاسم مستخدم.

استخدم أسماء مختلفة للحسابات التي ترغب في الاحتفاظ بها منفصلة.

- قد ترغب في تجنب استخدام أسماء مستخدم تحمل تمييزًا جنسيًا ("girlygirl10001") أو استخدام صور وجهك لملفك الشخصي.
- تجنب "ربط الحسابات". قد تتيح عدة مواقع تسجيل الدخول باستخدام حسابك على فيسبوك مثلاً. الأفضل أن تنشىء حسابًا منفصلًا حيث يمكنك القيام بذلك.

إعدادات الخصوصية

2

لا تسمح للتطبيقات بتتبع موقعك أو جمع بياناتك إلا إذا كان ذلك ضروريًا بشكل ملح.

لا تقدم وسائل أخرى للاتصال في ملفك الشخصي (مثل هاتفك الشخصي أو بريدك الالكتروني).

تحقق من إعدادات الخصوصية لحساباتك وقم بتقييد من يمكنه رؤية معلومات معينة عنك وعن ما تنشره.

إذا كان هناك إعداد لـ "الأصدقاء المقترحين"، قم بإيقافه. اخفي من يعجب بمنشوراتك. لا تسمح لأي شخص أن يقوم بوسمك دون إذن.

3

نصائح للوقاية المتقدمة

إذا لم تعتقد أنك تمثل هدفًا،
ولكن لديك سبب للاشتباه

1- قد يكون من الأفضل، بدلاً من متابعة حسابات لجهات سياسية راديكالية، متابعة شخصٍ مرتبط بها يعيد نشرها باستمرار، وذلك لتجنب الربط المباشر بينك وبين هذه الجهات عبر الإنترنت.

2- بدلاً من إظهار اعجابك (like) بالمنشورات السياسية الراديكالية، قم بالاحتفاظ بها (save) لأن خيار الحفظ يدعم المنشور أكثر من الإعجاب كما أنه غير علني.

4

إذا اكتسب منشورٌ لك شيئًا من الشهرة عبر الإنترنت، قم بتتبع الإشارات mentions إلى أسمائك (اسم المستخدم الخاص بك أو اسمك الكامل) المستخدمة على منصات وسائل التواصل الاجتماعي عبر:

- استخدام تطبيق أو موقع فحص التسرب ("haveibeenpwned.com") واحصل على تطبيق يطلب إزالة البيانات (Incogni, EasyOptOuts)

- التحقق مِن مَن يشاهد قصصك (Stories) بانتظام ومن يتابعك، حتى لو كان يظهر كـ "بوت". كثير من الـ "بوتات" إما مستخدمون متنكرون، أو تمثل برنامجًا يُستخدم للتحقق منك.

- استخدام تطبيق المراسلة المشفرة (مثل Signal) بقدر الإمكان وقم بتعيين وقت محدد لرسائلك لتختفي (Disappearing Messages)

- استخدام بريدًا إلكترونيًا مشفرًا، مثل بروتونميل. واستخدام TOR وVPN قدر الإمكان.

5

إجراءات الحماية

إذا كنت تعرضت أو ستتعرض للكشف عن هويتك وتحتاج إلى تقليل التهديد:

سجّل جميع الحوادث المتعلقة بالكشف عن الهوية. ما هي الصور التي تم تسريبها؟ ما هي المعلومات؟ ما هو اسم المستخدم للشخص/المنظمة التي نشرتها؟

بالنسبة لجميع الحوادث التي تحدث عبر الإنترنت، استخدم وظيفة "التبليغ" على منصة التواصل الاجتماعي عند الإمكان وشجع الآخرين على الإبلاغ عن المنشور المسيء أيضًا.

لا تتفاعل مع التهديدات العدائية. قم بإيقاف وقفل الحسابات ذات الصلة وقم بتدوين قائمة بها.

إذا كنت تعلم أن شخصًا أو مجموعة قد اعترضت على منشورك، قد يكون من الجيد متابعتهم عبر حساب بديل.

عندما تتجه إلى مكان لا ترغب في أن يتم تتبعك إليه قم بتحويل هاتفك إلى وضع الطيران أو أطفئه . ولا تستخدم المكالمات الهاتفية للمحادثات الحساسة!

إجراءات الحماية

إذا كنت طالبًا أو موظفًا في شركة

- لا تقوم بتحديد انتمائك إلى مدرستك/شركتك على حساباتك. ولا تذكرها بأي شكل من الأشكال.

- إذا طُلِبَ منك تقديم حسابات وسائل التواصل الاجتماعي، ارفض إذا كان ذلك ممكنًا. وإذا لم يكن ،قل إنك لا تمتلك حسابًا!

- إذا لزم الأمر، قم بإنشاء حساب لا تستخدمه للأنشطة العادية وقدمه لهذا الغرض.

- لا تسجل في حسابات باستخدام عنوان بريدك الإلكتروني الخاص بالمدرسة/العمل.

- لا تتصفح الإنترنت وأنت مسجل في حساب Google للمدرسة أو العمل الخاص بك.

- قم بإزالة اسمك من أي دلائل عامة على الإنترنت.

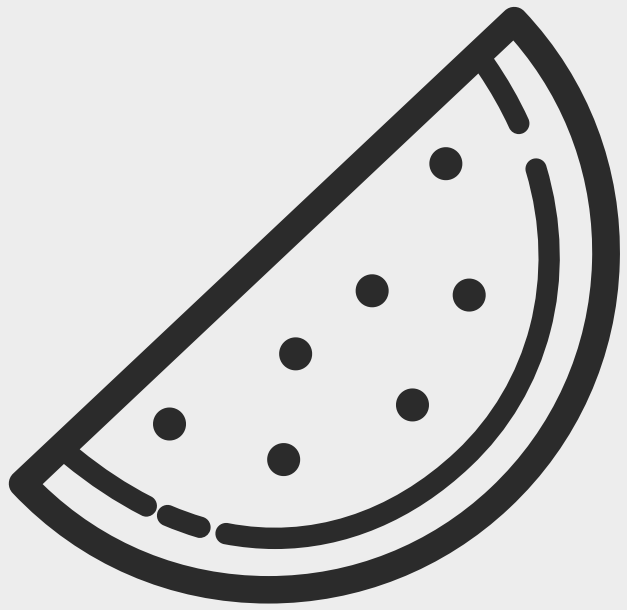
10

- لا تتابع حسابات مرتبطة بالمدرسة أو العمل.

- إذا كان اسمك غير شائع، تجنب استخدام النسخة الكاملة في ملفاتك الشخصية على وسائل التواصل الاجتماعي الخاصة.

- لا تضع علامات المواقع أو تعليقات تتعلق بالمدرسة أو العمل على وسائل التواصل الاجتماعي.

الأشكال المختلفة للمراقبة



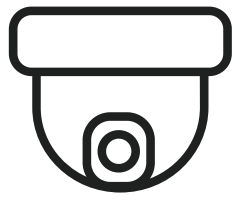
إذا كنت ناشطًا فلسطينيًا أو جزءًا من
مجموعة نشطة من أجل فلسطين

مراقبة منشورات على الحسابات الاجتماعية

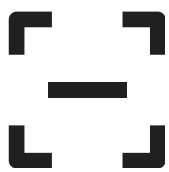
عمليات تفتيش

استجواب من قبل السلطات

كاميرات المراقبة



كاميرات التعرف على الوجوه



قواعد البيانات الفوتوغرافية (Blue Wolf)

- مراقبة المكالمات الهاتفية
- تتبع مواقع أو برامج اختراق البيانات (Pegasus)

حملة - المركز العربي لتطوير الاعلام الاجتماعي
Partners Global

تم إنشاء موارد الاستجابة لحرب غزة بالتعاون مع عدد من المنظمات
وهي متاحة للاستخدام والنشر من دون أي شرط.