HUMAN RIGHTS WATCH

secure our SOCIALS
نحو منصّات آمنة

يجب أن يشعر أفراد مجتمع الميم-عين بالأمان على الإنترنت
نصائح للتوعية

يستهدف العناصر الحكوميون في منطقة الشرق الأوسط وشمال أفريقيا المثليين/ات، ومزدوجي/ات التوجه الجنسي، وعابري/ات النوع الاجتماعي (مجتمع الميم-عين) بناء على نشاطهم على مواقع التواصل الاجتماعي. تستخدم قوات الأمن وأفراد عاديون منشورات مواقع التواصل الاجتماعي لتحديد أفراد وناشطي مجتمع الميم-عين واستهدافهم بالمضايقات، والابتزاز، والتهديدات، والرقابة. تصيّدت قوات الأمن أفراد مجتمع الميم-عين على مواقع التواصل الاجتماعي، وابتزتهم وضايقتهم على الإنترنت، وكشفت توجههم الجنسي أو هويتهم الجندرية بدون موافقتهم، واطّلعت عنوة على هواتفهم وحساباتهم على مواقع التواصل الاجتماعي، واعتمدت في المحاكمات على صور رقمية، ومحادثات، ومعلومات مماثلة حصلت عليها بطرق غير مشروعة.

لمعرفة المزيد حول الاستهداف عبر الإنترنت وعواقبه في الحياة الفعلية، اقرأوا التقرير الكامل وشاهدوا الفيديوهات التي أعدّتها "هيومن رايتس ووتش".

ينبغي لشركات التواصل الاجتماعي بذل المزيد من الجهود لحماية المستخدمين من هجمات الإنترنت، بمن فيهم أفراد مجتمع الميم-عين في الشرق الأوسط وشمال أفريقيا. في حين تقع مسؤولية تحسين الأمن الرقمي على عاتق الشركات، هناك بعض الخطوات التي يمكنكم اتخاذها لحماية أنفسكم بشكل أفضل على الإنترنت. تجدر الإشارة إلى أن نماذج تهديد الأشخاص تختلف بناء على عوامل عدة، منها العمر، والموقع الجغرافي، والعرق، والنوع الاجتماعي، والخلفية الاجتماعية-الاقتصادية، فضلا عن التوجه الجنسي والهوية الجندرية.

رغم أن ما يلي ليس الغرض منه أن يكون قائمة شاملة، إليكم بعض الخطوات لاتخاذها من أجل خصوصيتكم وسلامتكم بناء على نتائج تحقيقات «هيومن رايتس ووتش» وتوصياتها. تتكون نصائح التوعية هذه من ثلاثة أجزاء:

1. مؤشرات على وجود حساب أو نشاط يحتمل أن يكون ضار
2. التخفيف من عواقب الاستهداف الرقمي
3. الموارد

1. علامات وجود حساب أو نشاط يحتمل أن يكون ضارا **هل أنا مستهدف رقميا؟**

نعرض أدناه بعض المؤشرات ونصائح التوعية التي قد تسمح لكم بتحديد حد أدنى يسمح لكم بتقييم ما إذا كنتم مستهدفين رقميا. رغم أن السلوك الموضح أدناه قد لا يكون ضارا ولا يشير دائما إلى أنكم مستهدفون، يحدد بحثنا المتعلق بتجارب أفراد مجتمع الميم-عين على الإنترنت في الشرق الأوسط وشمال أفريقيا بعض الأنماط التالية كممارسات شائعة تسبق الاستهداف الرقمي:

البروفايل

- حسابهم حديث جدا، وتفاصيله غامضة أو قليلة. تسمح لكم بعض المنصات مثل فيسبوك وإنستغرام بمعرفة وقت إنشاء الحساب.
- حساب يدّعي أنه صديقكم ويطرح عليكم أسئلة ينبغي للصديق أن يكون يعرفها مسبقا، مثل معلومات التعريف، ومكان السكن، والتوجه الجنسي أو الهوية الجندرية.

الصور والفيديوهات

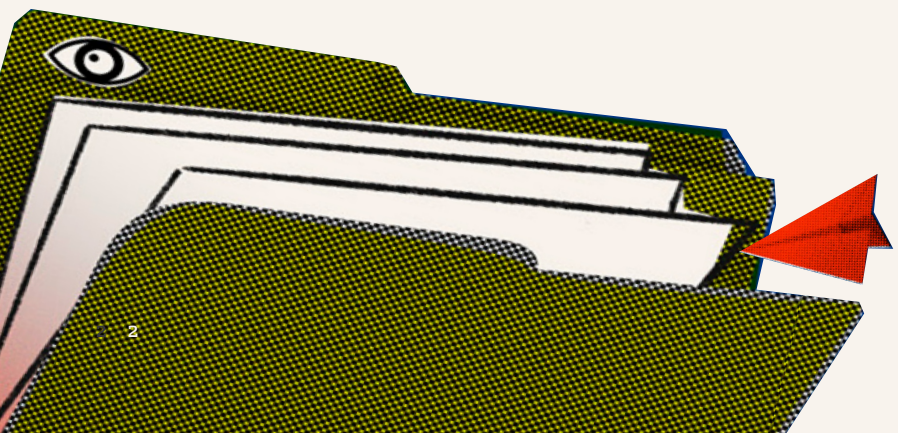
- يُطلب منكم فورا إرسال صور، منها صور عارية لكم أو لغيركم.
- يُطلب منك فورا ممارسة "السايبرسكس".

المعلومات الشخصية

- يُخبرونكم فورا بمعلومات شخصية للغاية ويطلبون منكم مشاركة معلوماتكم.
- يسألونكم عن المبلغ الذي تتقاضونه مقابل ممارسة الجنس رغم أنكم لا تعملون حاليا في الجنس.
- يسألونكم إذا كنتم تتعاطون المخدرات أو لديكم مخدرات رغم أنك لا تتعاطون المخدرات حاليا.
- يطلبون رقم هاتفكم قبل أن تتأكدوا من هويتهم.

مكان اللقاء

- يطلبون منكم اللقاء في مكان جديد أو غير مألوف، مثل مسكن خاص.
- تلتقون في مكان عام، ويُصرّون على التصرف بشكل حميم علنا، مثل اللمس أو التقبيل، بعد أن تعربوا عن عدم ارتياحكم.
- يأتي أشخاص آخرون غير متوقعين إلى اللقاء.



2. تخفيف عواقب الاستهداف الرقمي: ماذا يمكنني أن أفعل؟

إليكم بعض الخطوات التي يمكنكم اتخاذها لحماية حسابكم على الإنترنت وتقليل المخاطر وتأثير الاستهداف الرقمي:

الصور والفيديوهات

- اطلبوا منهم مشاركة صورة ثم تحقّقوا منها عبر البحث باستخدام الصور.
- اطلبوا منهم أن يرسلوا فيديو مدته خمس ثوان أو أجروا معهم مكالمة فيديو لتتمكنوا من رؤية وجوههم.
- تجنّبوا إرسال صور تُظهر وجهكم أو ميزات أخرى يمكن التعرف عليها، مثل أي معالم مرئية في الخلفية تسمح بتحديد الهوية، في حسابات شخصية ذات أسماء مستعارة أو من خلالها إلى حسابات لا تعرفونها أو تثقون بها.
- احذفوا الصور والفيديوهات من هواتفكم الشخصية بعد مشاركتها.
- إذا كنتم تستخدمون "واتساب" لإرسال الصور، فاستخدموا خيار العرض مرة واحدة. سيمنع ذلك الآخرين من التقاط لقطة شاشة لصورتكم.

البروفايل

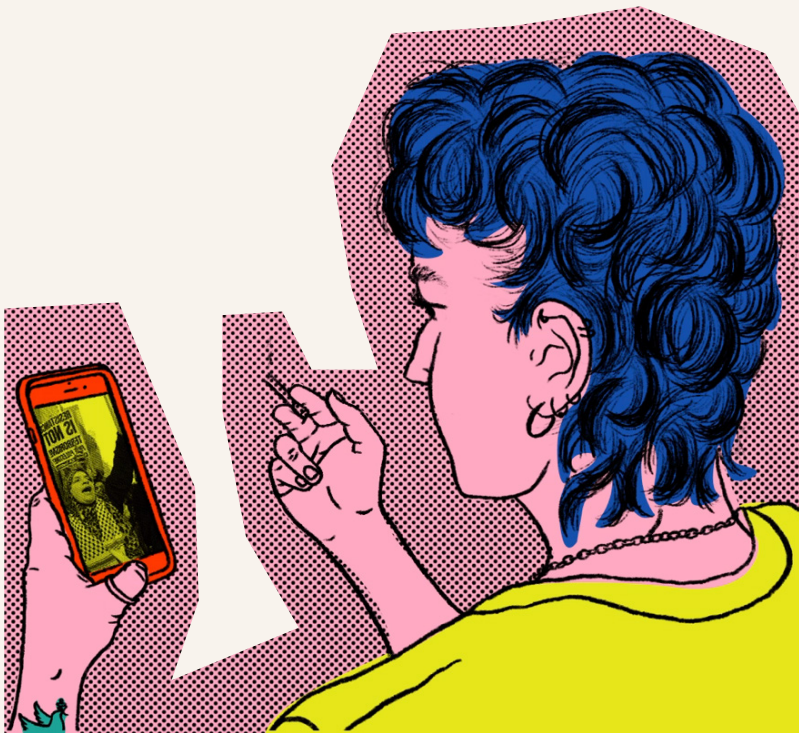
- تحققوا من حساباتهم الشخصية على منصات التواصل الاجتماعي الأخرى للتأكد من هويتهم.
- يُفضّل إنشاء حساب منفصل لتطبيق المواعدة غير مربوط بحساباتكم على تطبيقات التواصل الاجتماعي ولا يستخدم اسمكم الحقيقي لمشاركة توجهكم الجنسي أو هويتكم الجندرية.
- راجعوا إعدادات الخصوصية لحسابكم لكي تكون ملفاتكم الشخصية، ومنشوراتكم، وموقعكم الجغرافي على وسائل التواصل الاجتماعي مرئية فقط لمن ترغبون في مشاركتها معهم.

مكان اللقاء

- قابلوهم في مكان عام محايد.

المعلومات الشخصية

- تجنّبوا إرسال معلومات شخصية حول موقعكم، أو مكان عملكم، أو عائلتكم.



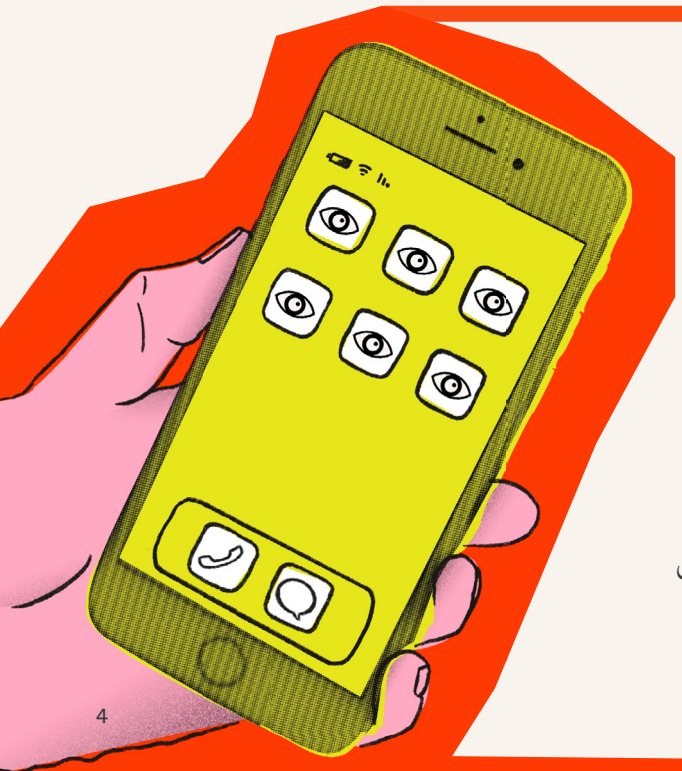
2. تخفيف عواقب الاستهداف الرقمي: ماذا يمكنني أن أفعل؟

أمن البيانات والأجهزة

- شغّلوا المصادقة الثنائية في كل حساباتكم.
- استخدموا كلمات مرور أو عبارات مرور قوية وبرنامجا آمنا لإدارة كلمات المرور.
- عطلوا تسجيل الدخول بالوجه وبصمة الإصبع.
- عطلوا إشعارات الشاشة للتطبيقات التي قد تحتوي على معلومات حساسة (تطبيقات المواعدة، تطبيقات المحادثة، الخ)
- استخدموا الميزات التي تسمح بتمويه تطبيقات معينة على هاتفكم أو إخفائها، مثل هذه الميزة من "غرايندر" التي تجعل أيقونات تطبيقاتكم سرية.
- استخدموا تطبيقات المراسلة ذات التشفير الشامل مثل "سيغنال" و "واتساب".
- استخدموا الرسائل المختفية، خيار العرض مرة واحدة أو اضبطوا رسائلكم على الحذف التلقائي.
- استخدم شبكة «في بي إن» موثوقة، خاصة عند استخدام شبكة «واي فاي» عامة كتلك التي في المقاهي أو المطارات.

الاستجابات الأولى للاستهداف الرقمي

- إذا تعرّضتم للتصيّد، والذي يشمل قيام أجهزة أمنية بانتحال هوية أفراد مجتمع الميم-عين على وسائل التواصل الاجتماعي وتطبيقات المواعدة لخداع أفراد من مجتمع الميم-عين ولقائهم ثم اعتقالهم، من قبل شخص قابلتموه على الإنترنت، التقطوا لقطة شاشة للاحتفاظ بدليل، ثم احظروا الحساب وبلّغوا عن الحادثة مباشرة إلى المنصة ذات الصلة.
- اطلبوا الدعم النفسي الفوري، إذا توفر، من خلال أفراد أو مجموعات موثوقين.
- بعد التقاط لقطة الشاشة للاحتفاظ بالدليل، خزّنوها في مكان آخر، واحذفوا جميع سجلات التفاعل مع الشخص، منها الصور والمحادثات الموجودة على جهازكم.
- إذا تم استهدافكم على وسائل التواصل الاجتماعي، عطّلوا جميع حساباتكم.
- إذا كنتم معرضين لخطر الاعتقال نتيجة للاستهداف الرقمي، اتركوا هاتفكم في مكان آمن إذا كان ذلك ممكنا.
- بلّغوا خط المساعدة ذي الصلة (انظروا الموارد).



ماذا يمكنني أن أطلب من شركات التواصل الاجتماعي للمساعدة في تأمين الحسابات على الإنترنت؟

تدعو حملة #نحو_منصات_آمنة منصتَيْ «ميتا»، فيسبوك وإنستغرام، إلى التحلي بقدر أكبر من المسؤولية والشفافية بشأن سلامة المستخدمين عبر نشر بيانات مفيدة حول استثمارها في سلامة المستخدمين، منها الإشراف على المحتوى. يمكنكم المشاركة في الدعوة بتوجيه رسالة إلكترونية إلى مديري ميتا التنفيذيين مباشرة على www.hrw.org/ar/SecureOurSocials

3. الموارد
تريدون معرفة المزيد؟

هناك بعض التوجيهات الممتازة التي تُقدم نصائح شاملة للخطوات التي يمكنكم اتخاذها لحماية خصوصيتكم وأمنكم عبر الإنترنت. هناك أيضا خطوط مساعدة تديرها مجموعات المجتمع المدني باللغات العربية، والإنغليزية، والفرنسية، والتي يمكنكم التواصل معها إذا كنتم بحاجة إلى المزيد من الدعم الموجه. أنظروا:

توجيهات

- منظمة الجبهة الإلكترونية
- https://ssd.eff.org/ar/
- داتا ديتوكس كيت
- واير كاتر،
- دليل غرايندر للأمان الشامل
- دليل غليتش تشاريتي دوكيومينتيشين
- دليل غلاد للأمان الرقمي
- دليل ميداني للحماية من للمضايقات الإلكترونية

خطوط المساعدة

- أكسيس ناو
- سميكس
- حلم