ما هو التحرش الإلكتروني؟!

يُعد التحرش الإلكتروني إحدى أسرع الجرائم نموًا في العالم، فهو جريمة خطيرة يمكن أن تدمر حياة الناس عبر استخدام الإنترنت لاستهداف الضحية وتخويفها.

لا شك أن التكنولوجيا قد غيرت حياتنا، فالآن يمكننا بسهولة البقاء على تواصل مع الأصدقاء حتى لو كانوا في قارات مختلفة، ومشاركة صور رحلات العطلات الرائعة، وإدارة حياتنا باستخدام مجموعة من التطبيقات المفيدة؛ ولكن للأسف، يوجد جانب سلبي لكل ذلك! فبعض الناس يستخدمون هذه التكنولوجيا لأغراض المضايقة والترهيب.

ما هو التحرش الإلكتروني؟

يُعرف التحرش الإلكتروني بكل بساطة بأنه "استخدام الإنترنت أو الوسائل الإلكترونية الأخرى لمضايقة ضحية بعينها وترهيبها".

تشمل الخصائص الشائعة -على سبيل المثال لا الحصر- سلوك "التحرش" الكلاسيكي، أي تتبع موقع شخص معين ومراقبة أنشطته على الإنترنت. في الواقع، من المعروف أن المتحرشين الإلكترونيين يستغلون أجهزة GPS الموجودة في سيارات ضحاياهم ويستفيدون من برامج التجسس لتحديد الموقع الجغرافي على هواتفهم، ومن ثم يتتبعون مواقع الضحايا بهوس من خلال مواقع التواصل الاجتماعي.

ويمكن أن يتضمن التحرش الإلكتروني سلوكًا آخر يهدف إلى تخويف الضحايا أو جعل حياتهم لا تُطاق! فمثلًا قد يستهدف المتحرشون الإلكترونيون ضحاياهم على مواقع التواصل الاجتماعي ويتصيدونهم ويرسلون إليهم رسائل تهديد، كما قد يخترقون رسائل البريد الإلكتروني للتواصل مع جهات اتصال الضحية، بما في ذلك الأصدقاء وحتى أصحاب العمل. التحرش عبر مواقع التواصل الاجتماعي يمكن أن يتضمن تزييف الصور أو إرسال رسائل تهديد خاصة، بل حتى ينشر المتحرشون الإلكترونيون في كثير من الأحيان شائعات خبيثة ويوجهون اتهامات كاذبة أو يفبركون مواد إباحية انتقامية وينشرونها، كما قد يتورطون أيضًا في سرقة الهوية وإنشاء ملفات تعريف وهمية على مواقع التواصل الاجتماعي أو مدونات حول ضحيتهم.

الآن نحن نعرف تعريف التحرش الإلكتروني. ولكن من هم ضحاياه؟ قد تفاجئك الإجابة! في حين أن معظم ضحايا التحرش الإلكتروني من النساء، إلا أن الرجال يمثلون نسبة تتراوح من ٢٠ إلى ٤٠ بالمائة من الضحايا.

يتعدى التحرش الإلكتروني أكثر من مجرد متابعة شخصٍ ما على إحدى مواقع التواصل الاجتماعي، بل قد يصل إلى الترهيب المتعمد، وهي السمة المميزة للتحرشٍ الإلكتروني.

كيفية حماية نفسك من المتحرشين الإلكترونيين

كيفية تجنب التعرض للتحرش الإلكتروني

أحد الإجراءات الجيدة التي يجب عليك القيام بها الآن هي البحث عن نفسك على جوجل -أو أي محرك بحث آخر- واكتشاف المعلومات التي يمكن أن يجدها المتحرش الإلكتروني المحتمل عبر الإنترنت. قد يصدمك مدى سهولة تعقبك، ناهيك عن العثور على عنوان منزلك ورقم هاتفك وتفاصيل شخصية أخرى!

إذا شعرت أن هذا أمرًا سيئًا، فقد ترغب في التحقق كذلك من مقدار البيانات التي يمكن لشخص ما تجميعها إذا كان بإمكانه الوصول إلى مواقع التواصل الاجتماعي الخاصة بأصدقائك وعائلتك أيضًا، فبهذا قد يكتشف مثلًا الكافية الذي كنت موجودًا فيه أول أمس، والأصدقاء الذين كانوا بصحبتك، أو وجهتك في عطلتك القادمة وموعدها.

قد تجد حتى أشياء منسوبة لك ولكن قام بتحميلها شخص آخر: مدونة مزيفة أو حساب على موقع يعرض يضع رقم هاتفك وعنوان منزلك به!

هذه هي الطريقة التي يبدأ بها المتحرشون الإلكترونيون لإجراء بحث عن ضحاياهم ومعرفة كل ما يمكنهم معرفته، وهذا يعني أنك ستحتاج بالتأكيد إلى زيادة صعوبة الحصول على هذه المعلومات قدر الإمكان.

نصائح لحماية نفسك من المتحرشين الإلكترونيين

زيادة إعدادات خصوصيتك

ابدأ ببياناتك الخاصة. تفقّد حساباتك على مواقع التواصل الاجتماعي جيدًا واعمل على تفعيل إعدادات خصوصية قوية إذا لم تكن قد فعلت ذلك بالفعل.

حدد رؤية منشوراتك على "الأصدقاء فقط" حتى يتمكن الأشخاص الذين تعرفهم فقط من رؤيتها.

لا تسمح لمواقع التواصل الاجتماعي بنشر عنوانك أو رقم هاتفك علنًا (قد يكون عليك أيضًا تخصيص عنوان بريد إلكتروني منفصل لمواقع التواصل الاجتماعي).

إذا كنت بحاجة إلى مشاركة رقم هاتفك أو معلومات خاصة أخرى مع أحد الأصدقاء، فافعل ذلك في رسالةٍ خاصة وليس في منشورٍ عام.

استخدم لقب لا يحدد جنسك (ذكرًا أم أنثى) أو اسمًا مستعارًا لحساباتك على مواقع التواصل الاجتماعي، وليس اسمك الحقيقي

اترك الحقول الاختيارية في ملفات تعريف مواقع التواصل الاجتماعي فارغة (مثل تاريخ ميلادك).

لا تقبل سوى طلبات الصداقة الواردة من الأشخاص الذين قابلتهم شخصيًا بالفعل. قم بتعيين حساباتك على مواقع التواصل الاجتماعي بحيث لا تقبل سوى طلبات الصداقة القادمة من أصدقاء الأصدقاء فقط.

عطّل إعدادات تحديد الموقع الجغرافي. قد يكون عليك أيضًا تعطيل خاصية GPS على هاتفك.

إذا كانت هناك بيانات شخصية أخرى متاحة على الإنترنت خارج حساباتك على مواقع التواصل الاجتماعي، فابدأ بإزالتها؛ في حال عرض رقم ضمانك الاجتماعي مثلًا، سيساعدك جوجل في إزالته. قد تحتاج إلى الاتصال بمواقع خارجية لإزالة بعض البيانات. إذا كنت بحاجة إلى عنوان بريدي للأعمال أو لتسجيل نطاق الويب الخاص بك، فاستخدم عنوان منطقتك أو عنوان مكتب (مثل عنوان محاسبك) وليس عنوان منزلك.

إذا كنت تستخدم موقع للمواعدة عبر الإنترنت، فلا تقدم هويتك الكاملة على الموقع أو عبر البريد الإلكتروني. لا تعط رقم هاتفك إلا للأشخاص الذين قابلتهم بالفعل ولا تمانع في رؤيتهم مرة أخرى؛ إن أفضل نصيحة أمنية هي عدم ذكر اسمك بالكامل على الإنترنت أبدًا، بل اسمك الأول فقط.

كيفية الدفاع عن نفسك في مواجهة المتحرشين الإلكترونيين

احذر من أي مكالمات هاتفية ورسائل بريد إلكتروني واردة تطلب منك ذِكر معلومات شخصية، مهما كان الطلب المزعوم معقولًا! إذا اتصل بك البنك أو شركة البطاقات الائتمانية هاتفيًا، فاترك الهاتف واستخدم هاتفًا آخر (على سبيل المثال: إذا كان الاتصال على خطك الأرضي، فاستخدم هاتفك المحمول) للاتصال مرة أخرى والتحقق من صحة المكالمة. بالمثل، عند الاتصال بهم استخدم رقم هاتف المقر الرئيسي أو رقم الفرع الموجود في أوراق تعاقدك معهم وليس الرقم الذي تم إعطاؤه لك للتو. أيضًا لا تفصح عن رقم ضمانك الاجتماعي مطلقًا.

قم بتأمين جهاز الكمبيوتر والهاتف

لن يساعدك تأمين بياناتك إذا تم اختراق هاتفك الذكي أو جهاز الكمبيوتر الخاص بك. لمنع التحرش الإلكتروني، يجب عليك توفير مستوى أساسي من الأمان في حياتك عبر الإنترنت.

احذر من شبكات الإنترنت العامة التي يمكن اختراقها بسهولة. إذا كنت بحاجة إلى تسجيل الدخول في على شبكة مقهى أو فندق، فمن الأفضل أن تستخدم شبكة افتراضية خاصة (VPN) لمنع أي شخص من التنصت على اتصالاتك.

ستعمل شبكة VPN كذلك على إخفاء عنوان IP الخاص بك، والذي يمكن استخدامه لتتبع حساب شركة الإنترنت التي تزودك بالخدمة، ومن خلالها يمكن الوصول إلى عنوانك ورقم بطاقتك الائتمانية والمزيد!

انتبه للأماكن التي تترك فيها هاتفك الذكي. ليس من الصعب تثبيت برامج التجسس دون ترك أي أثر، فمجرد ترك هاتفك على مكتبك لبضع دقائق يكفي لفعل ذلك.

تأكد من حماية هاتفك وأجهزة الكمبيوتر بكلمة مرور. استخدم كلمة مرور قوية وليس كلمة يسهل تخمينها، وأعد تعيين كلمات المرور بانتظام.

استخدم برنامجًا لمكافحة برامج التجسس لاكتشاف أي برامج ضارة مثبتة ومن ثم حذفها؛ أو كحل أفضل من ذلك، انسخ بياناتك احتياطيًا ثم أعد تعيين إعدادات المصنع للجهاز لضمان القضاء التام على برامج التجسس. تذكر دائمًا تسجيل الخروج من حساباتك عند الانتهاء، ولا تترك حساباتك على مواقع التواصل الاجتماعي مفتوحة.

احذر من تثبيت التطبيقات التي تريد الوصول إلى جهات اتصال فيس بوك أو قوائم جهات الاتصال الأخرى، فأنت لا تعلم ما الذي يخططون لاستخدامها فيه.

ما هو الانتحال الإلكتروني؟

الانتحال الإلكتروني هو شكل من أشكال الاحتيال أو إساءة استخدام البيانات، ويقوم فيه شخصٌ ما بإنشاء هوية مزيفة عبر الإنترنت لاستهداف ضحية معينة. قد يستدرج المنتحلون الإلكترونيون ضحاياهم لإرسال صور أو مقاطع فيديو حميمة ثم يبتزونهم، أو قد يبدؤون علاقة ثم يطلبون المال لحالات طوارئ مفاجئة.

يمكن أن يكون المنتحلون الإلكترونيون مقنعين للغاية، ولكن يمكنك اكتشاف خداعهم بعدة طرق:

إذا كانت جميع صورهم على الإنترنت صورًا ذاتية (سيلفي) أو لقطات احترافية لهم مع عدم وجود أي أصدقاء آخرين ولا أفراد من العائلة ولا سياق، فهذا مصدر شك كبير.

أجر بحث عكسي في جوجل عن الصورة الموجودة على موقع المواعدة. قد تجد أن الشخص لديه العديد من الملفات الشخصية على الإنترنت بنفس الصورة ولكن بأسماء مختلفة.

اسأل عما إذا كان يمكنك إجراء مكالمة فيديو ، فعادة ما يختلق المنتحلون الإلكترونيون الأعذار، ولن يتصلوا بك مرة أخرى!

ما الذي يجب عليك فعله إذا تعرضت للتحرش الإلكتروني

إذا تعرضت للتحرش عبر الإنترنت، فلا تنتظر مع عدم فعل شيء إلا الدعاء بأن تختفي المشكلة من تلقاء نفسها، بل تصرف فورًا.

وضِّح للمتحرش الإلكتروني أنك لا ترغب في التواصل معه أبدًا. افعل ذلك كتابيًا وحذره من أنه إذا استمر فأنك ستتوجه إلى الشرطة. لا تتعامل معه على الإطلاق بعد توجيه هذا التحذير.

توجه إلى الشرطة إذا استمر. يوجد لدى العديد من أقسام الشرطة فريق مختص بالتحرش الإلكتروني وجرائم الإنترنت، لكنهم سيحتاجون إلى بعض التفاصيل. إذا تعرضت للتهديد أو تعرضت للتحرش والترهيب، فسيتعاملون مع الأمر، سواء كان ذلك على فيس بوك أو البريد الإلكتروني أو من خلال برامج التجسس على هاتفك.

إذا كنت تعتقد أن شخصًا ما يتتبعك عبر برنامج تجسس، فلا تستخدم الكمبيوتر أو الهاتف الخاصين بك لطلب المساعدة، بل عليك استعارة هاتف أحد الأقارب أو الأصدقاء.

اجعل أحد المتخصصين يفحص الكمبيوتر والهاتف بحثًا عن برامج التجسس أو غيرها من علامات اختراق الحسابات.

قم بتغيير جميع كلمات مرورك.

في حال التحرش عبر مواقع التواصل الاجتماعي، استخدم إعدادات الخصوصية لحظر الشخص ثم أبلغ الشبكة عن إساءة الاستخدام. يمكنك بسهولة معرفة كيفية الإبلاغ عن التحرش الإلكتروني في معظم صفحات المساعدة والدعم الخاصة بمواقع التواصل الاجتماعي.

يمكنك تصفية رسائل البريد الإلكتروني المسيئة في مجلد منفصل حتى لا تضطر لقراءتها.

إذا كنت تعتقد أن المتحرش الإلكتروني قد يضايقك في مكان العمل، فأبلغ صاحب العمل بذلك.

احفظ نسخًا من أي اتصالات مُضمنة، بما في ذلك اتصالاتك الخاصة مثل تقارير الشرطة ورسائل البريد الإلكتروني الواردة من الشبكات. أنشئ نسخة احتياطية من الأدلة الموجودة على وحدة تخزين USB أو محرك أقراص خارجي.

ويستطيع المواطن تقديم البلاغات الخاصة بجرائم الانترنت بالمكان المخصص لتقديم البلاغات فى وحدة تلقى بلاغات المنطقة المركزية بميدان العباسية بمعهد التنمية البشرية، فضلاً عن تقديم البلاغات بكافة مديريات الأمن على مستوى الجمهورية.
ويمكن للمواطن التواصل مع مباحث الانترنت عن طريق الاتصال بـ" الإدارة العامة لتكنولوجيا المعلومات" على الرقم "٠٢٢٤٠٦٥٠٥٢ -٠٢٢٤٠٦٥٠٥١" أو الخط الساخن "١٠٨" بإدارة مكافحة جرائم الحاسبات.
من الجيد تعريف التحرش الإلكتروني الآن على أنه جريمة خطيرة، فهو قادر على تدمير حياة الناس، ولكن لا تسمح له بأن يدمر حياتك أنت!