التحرش الإلكتروني وأساليب الحماية والتعامل للحد منه

م. باهرة محمود جعفر

ورقة عمل مقدمة الى وحدة الارشاد النفسي والتوجيه التربوي

في الندوة العلمية الموسومة

ظاهرة التحرش في المجتمع العراقي

يوم الاثنين الموافق 4/4/2022

المقدمـــة:

لا شك أن التكنولوجيا قد غيرت اشياء كثيرة في 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.

فقد نتعرض للإساءة عبر الإنترنت، اذا لم يتم استخدام تطبيقات المراسلة ووسائل التواصل الإجتماعي وغيرها من وسائل الاتصال الإلكتروني بشكل مسؤول، يمكن أن يكون مصدراً للضرر، مثل: الملاحقة عبر الإنترنت والتنمر عبر الإنترنت وانتهاك الخصوصية والمعلومات غير الصحيحة ومشاركة الصور التي من شأنها ان تضر شعور الناجين بالأمان والصورة الذاتية واحترام الذات.

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

نوع المضايقات الإلكترونية

يقع الترهيب والمضايقات الإلكترونية ضمن فئة أو أكثر من الفئات التالية:

1. **المضايقة والمطاردة:** إرسال تهديدات متكررة أو رسائل مؤذية عبر منصات الرسائل أو المكالمات الهاتفية.

2. **الفَضح والخداع:** إشراك شخص ما في المراسلة الفورية وخداعه أو خداعها للكشف عن معلومات شخصية وحساسة. و قد ينطوي ذلك في السياق المحدد للمجتمعات التي وقعت ضحية لتنظيم داعش على "انتحال الهوية" وهي خدعة لإختبار ولاء "العائدين من الأسر" والتأكد مما إذا كانوا لا يزالون يتلقون العقيدة.

3. **تشويه السمعة:** إرسال أو نشر ثرثرة أو إشاعات عن شخص ما للإضرار بسمعته أو صداقاته أو الإضرار بإندماجه الإجتماعي.

الاجراءات الواجب القيام بها عند التعرض للتحرش الالكتروني

قد يكون اختبار المكالمات والرسائل المزعجة أمراً صعباً للغاية من الناحية العاطفية، ولذلك فأنه من المهم أن تعرف أنه يمكنك حماية نفسك من مثل هذه التهديدات ولا تدع المتنمرين يسكتونك! إذا كنت تعتقد أنك تتعرض للتهديد عبر الإنترنت، فإن أهم شيء هو ضمان سلامتك. يُعَد التحدث إلى شخص موثوق به - أي شخص تشعر بالأمان عند التحدث إليه - أحد أهم الخطوات الأولى التي يمكنك اتخاذها، ثم قُم باتخاذ الإجراءات التالية لحماية نفسك

1 - جمع المعلومات

حاول ان توثق المضايقات الإلكترونية قدر الإمكان وبغض النظر عن مدى عدم الأهمية التي تعطيها لها، وقد يشمل جمع المعلومات هذا حفظ الرسائل ومواد التهديد وعمل لقطات شاشة وتسجيل المكالمات وتتبع الأوقات والأماكن والأشخاص المتورطين في الفعل.

2- التوقف عن التفاعل

* إذا كانت مكالمة هاتفية، أخبر الشخص الذي يقوم بالتهديد بهدوء أن يوقف سلوك التحرش ثم انهي المكالمة وأوقف جميع أنواع التفاعل مع المتحرش.
* إذا كان منشوراً أو رسالة نصية، فلا ترد.
* تحديد وتسجيل الرقم (الأرقام) التي يستخدمها المتحرش للإتصال بك.

3- تجاهل أو حظر الإتصالات:

يمكن أن تكون إحدى الإستراتيجيات هي منع الشخص المسيء من الإتصال بك، إذ تعمل خاصية الحظر بشكل مختلف اعتماداً على النظام الأساسي التكنولوجي أو جهاز الهاتف الذكي وقد يكون من المفيد اختبار ميزة الحظر مع شخص تثق به لمعرفة كيفية عملها.

4- ضبط إعدادات الخصوصية

بالإضافة إلى حظر جهة الاتصال، يمكنك عبر تطبيق واتس آب (WhatsApp) والشبكات الإجتماعية الأخرى: إيقاف تشغيل "آخر ظهور" ومنع الأشخاص غير المعروفين من إضافتك إلى المجموعات.

إخفاء صورة ملفك الشخصي، سيحد هذا من ظهور نشاطك على الشبكات الإجتماعية المختلفة.

5- الأبلاغ عن الحادث

من الضروري الإبلاغ عن الحوادث لمكافحة الإفلات من العقاب ووقف الظلم.

الإبلاغ بالتفصيل عن التهديد لضباط الأمن المحليين ولا سيما جهاز الأمن الوطني والشرطة المجتمعية, فضلا عن القيام بعمل ابلاغات على حسابات المتحرش للحد من تواصله مع الآخرين أيضاً.

أساليب الحماية والتعامل لتجنب التحرش الالكتروني

نظراً لزيادة حالات التحرش الالكتروني، والاعداد الكبيرة التي تتعرض لهذه الجريمة الالكترونية، كان لابد من التحذير لتجنب والحماية من التحرش الالكتروني بكافة انواعه واشكاله، ولا ننسى أن " درهم وقاية خيرٌ من قنطار علاج"، وتتمثل طريقة تجنب التحرش الالكتروني فيما يلي:

1. تجنب النقر على أي روابط إعادة توجيه redirect linksمن أي شخص لا تعرفه او غير موثوق، لأنها قد تكون فخ من المتطفلين لكي يوقعوك فيه لمحاولة اختراق جهازك والسيطرة عليه.
2. الحذر من اي شخص غريب او مجهول بالنسبة لك، وعدم إعطائه أي معلومات شخصية مهمة عنك، لأنه قد يستخدمها ضدك.
3. فكر ملياً قبل نشر أو مشاركة أي شيء عبر الإنترنت، فإنه سيبقى داخل الإنترنت إلى الأبد ويمكن استخدامه لإيذائك لاحقاً.

4. قم بالحد من المعلومات التي تنشرها على حسابك وخاصة التفاصيل الشخصية مثل عنوانك ورقم هاتفك واسم ومدينة وموقعك.

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

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

7. اجعل رقم هاتفك خاصاً. ضع في اعتبارك جعل رقم هاتفك "سرياً" حتى يرى المتلقي "الرقم الخاص" أو "معرف المتصل غير متاح" على هاتفه عند الرنين حيثُ يمكن أن يساعد ذلك في الحد من نشر البيانات الشخصية.

8. عطّل إعدادات تحديد الموقع الجغرافي. قد يكون عليك أيضًا تعطيل خاصية GPSعلى هاتفك

9. ضع في اعتبارك فتح حساب على تطبيق واتس آب ((WhatsApp، بدلاً من تطبيق الفايبر(Viber)حيثُ يضمن التطبيق الاول خصوصية أفضل.

10. لا تقبل على الشبكات الإجتماعية الشخصية إلا الأشخاص الذين تعرفهم ولا تقبل طلبات الصداقة من الغرباء.

11. حذر أصدقائك ومعارفك من نشر معلومات شخصية عنك.

12. لا تنشر صوراً لمنزلك قد تشير إلى موقعه.

13. تعرف على إعدادات الخصوصية لتطبيقات الوسائط الإجتماعية الخاصة بك، بما في ذلك من يمكنه رؤية معلوماتك وخيارات حظر وإخفاء المحتويات.

14. تحقق بشكل منهجي من خلفية مقاطع الفيديو/الصور الخاصة بك قبل نشرها.

15

15. الإبلاغ عن الحسابات المشبوهة أو المُهدِدة.

16. حافظ على فصل الحسابات الخاصة والتجارية بشكل قطعي.

17. أخذ لقطة شاشة لجميع التهديدات وطباعتها على ورق بما فيها رابط حساب المعتدي... وتجنبي استخدام الفوتوشوب على الأدلة الرقمية كي لا يُدمر تصرفك الدليل ويعتبر مزورًا.

18. وتذكر إذا كنت ضحية للمضايقة، فأنت لست مسؤولاً عن سلوك المتحرش ولا يجب إلقاء اللوم عليك بأي شكل من الأشكال.

وكل ماذكرناه اعلاه لايساعدك على تأمين بياناتك إذا تم اختراق هاتفك الذكي أو جهاز الكمبيوتر الخاص بك. ،لذا يجب عليك توفير مستوى أساسي من الأمان في حياتك عبر الإنترنت لمنع التحرش الإلكتروني.

- 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 ((VPNتقوم بتشفير حركة البيانات الخاصة بك على الإنترنت وإخفاء هويتك الإلكترونية، مما يجعل تتبع أنشطتك عبر الإنترنت وسرقة بياناتك أمرًا في غاية الصعوبة بالنسبة للغير لمنع أي شخص من التنصت على اتصالاتك. يمكن التمتع باتصال آمن في أي مكان توجد فيه من خلال .Kaspersky's VPN

- ستعمل شبكة VPNكذلك على إخفاء عنوان IPالخاص 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. يأتي برنامج مكافحة الفيروسات Kasperskyبإصدارين لكل من أجهزة الكمبيوتر وأجهزة Androidللحفاظ على أمان جميع أجهزتك.
- 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.

التوصيات :

1. التوسع في اعداد البحوث والدراسات حول ظاهرة التحرش عبر الإنترنت ،
2. استخدام وسائل التواصل الاجتماعي وتكنولوجيا المعلومات في نشر الوعي حول التحرش عبر الإنترنت،
3. ضرورة إدخال خطة التثقيف التكنولوجي للآباء ضمن مجموعات الوالدية واتجاهات التربية ومجموعات تمكين المرأة ،
4. إدخال رجال الدين والإعلام في الخطة الشاملة لمواجهة التحرش عبر الإنترنت عن طريق خطب الجمعة والدروس الدينية ووسائل الإعلام ،
5. وضرورة إعادة النظر في الخطط المتبعة في التعامل مع التحرش بشكل عام ،والتحرش عبر الإنترنت بشكل خاص من الخطط العلاجية الى الخطط الوقائية .
6. وضرورة التركيز على المحيط المدرسي ،وتقييم تفشي الظاهرة في المدارس والمؤسسات التعليمية الأخرى.

شكراً لحسن إستماعكم