



BritishRedCross



Home Office

مشروع التمكين التقني والتواصل للاجئين

دليل ورش العمل المرافقة 3



السلامة التقنية

تم إعداد هذا الدليل ليكون بمثابة أداة لدعم النساء المشاركات في ورش عمل مشروع التمكين التقني والتواصل للاجئات. هذا الدليل موجه للنساء ممن يندرجن ضمن فئة "لاجئ" أو يحظين بالحماية الإنسانية أو لم شمل الأسرة للاجئين ويعيشون في المملكة المتحدة. يُموّل هذا المشروع بواسطة صندوق مكتب دعم اللجوء والانماج للاجئين (Home Office Resettlement Asylum Support and Integration) (directorate).

نرغب في توصيل الشكر إلى أعضاء شبكة فويسز (VOICES) وسفرائها ممن ساعدوا في إعداد هذه المستندات المهمة. تتوفر مواد هذا المشروع باللغة الإنجليزية والأمهرية والعربية والفارسية والكردية (السورانية الكردية) والصومالية والتغرينية والأردية. ومن المرجو أن تستفيد اللاجئات اللواتي لم يشاركن في ورش العمل من العمل من خلال المعلومات الواردة هنا ودراساتها بالوتيرة التي يختارونها.

المحتويات

3	تمهيد.....
3	المصطلحات الأساسية.....
4	ما هي السلامة التقنية؟.....
4	التوصيات الأساسية للسلامة التقنية.....
4	امتلاك كلمات مرور قوية.....
5	استخدم مدير كلمة المرور.....
5	تمكين المصادقة الثنائية.....
5	حماية أجهزتك من الفيروسات.....
6	الحفاظ على نسخة احتياطية لبياناتك.....
6	الملخص.....
6	ما الذي يجب فعله إذا ساءت الأمور.....
7	أنواع التهديدات الشائعة عبر الإنترنت.....
7	عمليات الاختتيال والخداع.....
7	التصيد الاحتيالي.....
9	مواقع الويب الآمنة وغير الآمنة.....
10	ما الإجراءات المتبعة في حال تعرضت لعملية اختيال.....
10	العلاقات الإلكترونية.....
11	الاختيال الرومانسي.....
11	التنمر الإلكتروني.....
12	الاستدراج.....
12	المراسلات الجنسية والانتقام الإباحي.....
13	المطاردة والمراقبة عبر الإنترنت.....
13	العنف المنزلي والتحرش والمراقبة.....
15	الملخص.....

تمهيد

لا يمكن لهذه الأداة أن تتناول بالكامل وتوضح كافة المخاطر والإجراءات المعنية بالحماية المتاحة لمستخدمي شبكة الإنترنت وإنما تسعى للفت انتباهكم إلى عدد من النقاط الرئيسية ومن أين يمكنكم الحصول على المزيد من المعلومات.

نحن على دراية أنه بالحديث عن السلامة التقنية، فإننا نتطرق بذلك إلى موضوعات تدور حول العنف القائم على التمييز بين الجنسين والاعتداء والأفعال الإجرامية، ويمكن لتلك الموضوعات أن تكون حساسة أو محرمة في كثير من الأحيان. إن رسالتنا الإنسانية ومبدأ عدم إلحاق الضرر يعنينا أننا مطالبون ببذل ما بوسعنا للتصدي للعنف القائم على أساس التمييز بين الجنسين، بما في ذلك تقديم المعلومات اللازمة لدعم الأفراد على اتخاذ خيارات تعمل على تمكينهم والقرارات اللازمة لحمايتهم.

ترد في هذا الدليل مجموعة من الروابط المدرجة في النص، والتي عند النقر عليها ستقودك إلى الموقع المذكور. على سبيل المثال، عند النقر [هنا](#)، سيفتح الموقع الإلكتروني للصليب الأحمر البريطاني (British Red Cross). حاولنا قدر الإمكان إدراج روابط لموارد مترجمة، ولكن العديد من الروابط في هذا الدليل تحتوي على معلومات باللغة الإنجليزية. وعلى الرغم من اعترافنا بوجود قيود لعملية الترجمة الآلية، إلا أننا نوفر معلومات حول كيفية استخدام تلك الخاصة في الدليل الثاني. يمكن الاطلاع على نصائح شاملة حول السلامة التقنية بما يشمل كيفية حماية أجهزتك والخطوات اللازمة لحماية نفسك والآخرين من التهديدات الموجودة عبر الإنترنت على الموقع الإلكتروني www.getsafeonline.org.uk وفي المركز القومي للأمن السيبراني (National Cyber Security Centre) على الموقع www.ncsc.gov.uk. كما يمكن الاطلاع على مزيد من المعلومات حول ضحايا الانتهاكات الإلكترونية ودعمهم من خلال موقع أوقفوا الانتهاكات الإلكترونية (Stop Online Abuse) - www.stoponlineabuse.org.uk. للحصول على مزيد من المعلومات أو تقديم الدعم للتصدي لأي نوع من العنف القائم على التمييز بين الجنسين أو العنف المنزلي أو التحرش أو الإبلاغ عن أي منهم، يُرجى التواصل مع خط مساعدة اللاجئين (Refuge Helpline) أو خط المساعدة الوطني لمكافحة العنف المنزلي (National Domestic Abuse Helpline) من خلال الموقع الإلكتروني www.refuge.org.uk/www.nationaldahelpline.org.uk أو الاتصال بالرقم 0808 2000 247.

إذا كان لديك أي مخاوف عاجلة أو أردت الإبلاغ عن جريمة، يُرجى الاتصال بالشرطة على الرقم 999 (الطوارئ) - 101 (الحالات غير الطارئة).

المصطلحات الأساسية

السلامة التقنية – الممارسات والعادات التي تحافظ على أمنك وأمن الآخرين وسلامة معلوماتك الشخصية عند استخدام شبكة الإنترنت.

بين الأفراد - ما يتعلق بالتعاملات بين الأشخاص.

التهديدات عبر الإنترنت - مخاطر أو مشاكل تتسبب في وقوع أحداث أو أفعال غير مرغوب فيها عبر الإنترنت.

كلمة المرور - مجموعة سرية من الحروف التي تسمح بالدخول إلى نظام الحاسوب أو الوصول إلى خدمة ما.

أمن - البقاء آمناً ودون تهديد، مع عدم التعرض للخطر أو الأذى.

ما هي السلامة التقنية؟

يُقصد بالسلامة التقنية الإحاطة بالمخاطر الموجودة على الإنترنت ومعرفة كيفية حماية نفسك (وبياناتك) منها. عادةً ما يقصد بالسلامة التقنية التحلي ببعض العادات الجيدة التي تجعلك أقل عرضة لمخاطر الجرائم السيبرانية أو الاحتيال أو التهديدات. يشمل ذلك معرفة بعض الحيل التي قد يستخدمها المجرمون في محاولتهم لإجبار الأشخاص على مشاركة معلوماتهم أو ابتزازهم للحصول على أموالهم أو التدخل في شؤون حياتك الخاصة.

تتمثل أكثر التهديدات الشائعة عبر الإنترنت فيما يلي:

- الفيروسات أو البرامج الضارة التي تحاول سرقة ("اختراق") معلوماتك الشخصية أو تفاصيل حسابك أو تثبيت البرامج التي يمكنها التجسس عليك.
- الاحتيال عبر الإنترنت، حيث يمكن للمجرمين محاولة إقناعك بتسليم معلوماتك الخاصة إليهم.
- المتعمرون والملاحقون والمعتدون الذين يستغلون هويتهم المجهولة في التحرش أو الاعتداء عليك أو التحكم بك.

التهديدات الموجودة عبر الإنترنت التي من شأنها التأثير على رفاية الشخص المادية والعاطفية والشخصية. ومع أخذ هذه الفكرة في عين الاعتبار، تجدر الإشارة إلى أن الوعي بالسلامة التقنية يساعد الأشخاص على زيادة ثقتهم على الإنترنت.

التوصيات الأساسية للسلامة التقنية

امتلاك كلمات مرور قوية

تُغلق حسابات البريد الإلكتروني وجميع الحسابات الأخرى باستخدام كلمة مرور، تكون بمثابة المفتاح الذي يمنع الآخرين من الوصول إلى حسابك. يُعد استخدام كلمة مرور معقدة أو "قوية" هو أفضل طريقة لمنع الآخرين من الوصول إلى معلوماتك الشخصية.

يلزم امتلاك كلمة مرور قوية للبريد الإلكتروني. في حال تمكّن أحد المخترقين من الدخول إلى بريدك الإلكتروني، قد يمكنهم إعادة تعيين جميع كلمات المرور الأخرى الخاصة بالحساب باستخدام خاصية "نسيت كلمة المرور" (Forgot Password) والوصول إلى معلومات شخصية حساسة في جميع حساباتك.

يعلم المخترقون أن الكثير منا يستخدم كلمات مرور مثل 123456 أو تاريخ لحدث مهم في حياتنا أو اسم طفل - لا تستخدم أي شيء يسهل تخمينه. يمكن اختراق كلمات المرور السهلة بسرعة، ولكن كلمات المرور الجيدة تحبط محاولات المجرمين من دخول حسابك. الأمر يستحق قضاء مزيد من الوقت لابتكار كلمة مرور.

اتبعي هذه الخطوات لإنشاء كلمة مرور جديدة وقوية:

1. ادجي ثلاث كلمات عشوائية: مثل rug و fire و fork لتكون كلمة rugfirefork.
2. أضيفي حروفًا كبيرة، مثال: RugFireFork
3. أضيفي أرقامًا، مثال: 19RugFireFork90.
4. أضيفي رمزًا لجعل كلمة المرور أكثر تعقيدًا: !19RugFireFork90!

يتبادل المخترقون قوائم تحتوي على الملايين من كلمات المرور المخترقة، وسيكون استخدام ثلاث كلمات عشوائية هو الطريقة الأسهل لإنشاء كلمات مرور جديدة والتي من المرجح أن تكون فريدة بالنسبة لك وأقل عرضة لأن يتم تخمينها. يوصى بشدة بتغيير كلمات المرور بشكل دوري وعدم استخدام كلمة المرور ذاتها لجميع حساباتك. قد تكون مولدات كلمة المرور خيارًا جيدًا في حال واجهتك صعوبة في ابتكار كلمات مرور جديدة.

استخدم مدير كلمة المرور

إذا كنت قلقاً حول نسيانك لكلمة مرور "قوية"، يمكنك استخدام مدير كلمة المرور. تهدف برامج إدارة كلمات المرور إلى حفظ كلمات المرور الخاصة بك في متصفح الويب (مثل جوجل كروم) (Google Chrome) أو مايكروسوفت إيدج (Microsoft Edge) حتى يتمكن المتصفح من تذكر كلمة المرور من أجلك. تُعد طريقة مدير كلمات المرور أكثر أماناً من استخدام كلمات مرور سيئة أو ضعيفة، ولكن تأكد من حماية كلمات المرور في حال فقدت جهازك. تقوم بعض الشركات المتخصصة في برامج مكافحة الفيروسات والأمان على شبكة الإنترنت بتقديم مدير لكلمات المرور بشكل أساسي عند شراء أدوات مكافحة الفيروسات الخاصة بها، في حين تقدم الشركات الأخرى برامج إدارة كلمات المرور بشكل منفصل.

تمكين المصادقة الثنائية

تضيف المصادقة الثنائية طبقة حماية أخرى إلى حسابك من خلال طلب معلومة إضافية بالإضافة إلى كلمة المرور الخاصة بك. يساعد ذلك على منع الآخرين من الدخول إلى حساباتك، حتى وإن كان لديهم كلمة المرور خاصتك. يمكن الاطلاع على التوجيهات الخاصة بكيفية تمكين المصادقة الثنائية للبريد الإلكتروني ووسائل التواصل الاجتماعي الشائعة من خلال موقع المركز القومي للأمن السيبراني [هنا](#).

حماية أجهزتك من الفيروسات

تمثل الفيروسات برامج مخفية تُنقل عن طريق المواقع أو روابط البريد الإلكتروني أو المرفقات أو الوسائط القابلة للإزالة (مثل وحدات التخزين النقالة). يمكن لتلك الفيروسات التسبب في أعطال بالغة، كما يمكنها منعك من الدخول إلى الحاسوب الخاص بك أو حساباتك وسرقة المعلومات أو البيانات الشخصية لبيعها أو استخدامها والاستيلاء على أموالك أو حتى مشاهدتك في منزلك. إنه أمر مثير للقلق ألا يكون الجميع على دراية بكيفية حماية أجهزتهم، كما أنهم لا يتخذون الإجراءات اللازمة لذلك. سجل مكتب الإحصاءات الوطنية (ONS) عام 2020 أن 17% من البالغين الذين يمتلكون هواتف ذكية لا يمتلكون برامج لتأمينها، في حين أن 32% منهم لم يكونوا على علم بامتلاكهم لبرامج تأمين من الأساس.

تُعد برامج مكافحة الفيروسات أداة مثبتة على أجهزة الحاسوب المحمولة أو الأجهزة اللوحية أو الهواتف، وتعمل عمل حارس الأمن، فتقوم بوقف البرامج المسببة للمشاكل التي تفسد أجهزتك. يلزم توفير برامج الحماية من الفيروسات على الحاسوب أو الحاسوب المحمول أو الأجهزة اللوحية أو الهواتف الذكية للمساعدة في منع التهديدات الشائعة، مثل:

- **فيروس حصان طروادة (Trojans)** هو فيروس يتظاهر أنه برنامج تودين تنزيله (مثل برنامج مكافحة الفيروسات أو صورة أو فيلم مجاني) لكنه يمثل برامج ضارة (malware) أو يحتوي عليها، والتي تنشط عند تثبيتها على الحاسوب أو الهاتف.
- **برامج التجسس (Spyware)** هي برامج تقوم بتتبع المعلومات وتراقب ما تفعليه على حاسوبك لأغراض إجرامية.
- **برامج الإعلانات المتسللة (Adware)** هي برامج تقوم بفتح نوافذ منبثقة لمحاولة بيع بعض المنتجات لك.
- **برامج الفدية الضارة (Ransomware)** هي برامج تمنعك من دخول جهازك وتطالبك بدفع المال.
- **البريد العشوائي (Spam)** هو بريد يقوم بإنشاء برامج تُدعى بالفيروسات المتنقلة والتي تدخل إلى نظامك من خلال الاتصال بشبكة الويب ونسخ الكثير رسائل البريد الإلكتروني العشوائية من جهات الاتصال لديك لإرسالها. يُشار إلى اتصالات البريد الإلكتروني غير المرغوب فيها باسم البريد العشوائي أو البريد الإلكتروني غير المهم (junk email). يمكن للبريد العشوائي أن يكون ببساطة مصدر إزعاج، ولكن يمكن استخدامه أيضاً للاحتيال على الأشخاص ونشر المعلومات المضللة.

تحتوي معظم الأنظمة على برامج مثبتة بالفعل للحماية من الفيروسات وبرامج التجسس، على سبيل المثال، تحتوي الحواسيب المحمولة التي تعمل على نظام ويندوز 10 (Windows10) على برنامج ويندوز ديفيندر (Windows Defender) مثبتاً بها.

يمكنك الحصول على المزيد من الحماية من الفيروسات: في بعض الأحيان يكون هذا مجانيًا، ولكن هناك أيضًا شركات تقدم برامج مدفوعة.

قد تحتوي البرامج القديمة على ثغرات تتسلل من خلالها الفيروسات. **التحديثات** تسمح بتصحيح تلك الثغرات. يمكنك الترتيب لإجراء تحديثات تلقائية على البرامج والبرمجيات لتصحيح أي ثغرات في نظامك الأمني. ما يعني أنه ليس عليك تذكر القيام بذلك. قد يكون عليك في بعض الأحيان تحديث الجهاز يدويًا وستتلقين في تلك الحالة تذكيرًا. لا تتجاهلهم!

الحفاظ على نسخة احتياطية لبياناتك

يمكن للفيروسات حذف البيانات والمعلومات الخاصة بك أو سرقتها. يجب عليك الاحتفاظ بنسخة احتياطية من بياناتك قبل تحديث جهازك حتى تقومي بحماية صورك الشخصية والملفات والمعلومات الخاصة بك. يُقصد بعمل نسخة احتياطية إنشاء نسخة، يمكن أن تكون نسخة مادية باستخدام قرص صلب محمول، ولكنها عادة ما تُخزن في جهاز آخر أو في "سحابة" (cloud) (عبر الإنترنت). يرجع سبب ذلك إلى حدوث تغييرات في الملفات نتيجة لإجراء تحديثات، ولكن في حال إجراء نسخ احتياطية لبياناتك، يمكنك استعادتها بسرعة ولا يمكن ابتزازك من قبل هجمات برامج الفدية الضارة. يمكنك تشغيل النسخ الاحتياطي التلقائي، وهذا يعني أنك لا تحتاجين إلى تذكر عمل نسخة احتياطية لبياناتك.

يمكنك العثور على المزيد من التوجيهات حول عمل نسخة احتياطية لبياناتك في الموقع التالي:

www.getsafeonline.org/protecting-your-computer/Backups

الملخص

- احتفظي بكلمة مرور منفصلة لبريدك الإلكتروني.
- تحقق من أن لديك كلمة مرور قوية لبريدك الإلكتروني وحساباتك الأخرى.
- تأكدي من معرفتك بكيفية تغيير كلمة المرور وقومي بذلك بانتظام.
- لا تستخدمي كلمة المرور ذاتها لعدة حسابات وفكري في استخدام مدير كلمة المرور إذا شعرت بالقلق حول نسيان كلمات المرور.
- استخدمي المصادقة الثنائية
- تحقق من امتلاكك لبرنامج مكافحة الفيروسات وأنه مُفعّل (واحصلي على واحد من هذه البرامج إن لم تكوني متأكدة من امتلاكه).
- استخدمي برنامج مكافحة البيانات وقومي بتحديثه - قومي بإجراء فحص كامل للنظام بانتظام وحدثي برنامج مكافحة الفيروسات لحمايتك من الفيروسات المطورة حديثًا أو الأخطاء.
- كوني حذرة بشأن ما تقومين بتنزيله - حيث قد تصل برامج الإعلانات المتسللة وبرامج التجسس إلى حاسوبك من خلال ربط أنفسهم بالأشياء التي تقومين بتنزيلها، لذا تحقق من مكان حصولك على تلك الملفات.

ما الذي يجب فعله إذا ساءت الأمور

في حال قمتي بفتح رابط على حاسوبك المحمول أو اتبعتي تعليمات لتنصيب شيء ما ولكنك قلقة بشأنه، قومي بفتح برنامج مكافحة الفيروسات وإجراء فحص كامل. اسمحي لبرنامج مكافحة الفيروسات بمحاولة إصلاح المشكلة وإعادة ضبط الجهاز عن طريق اتباع النصيحة التي يقدمها. إن لم يكن بالإمكان إصلاح الأمر يمكنك الحصول على المساعدة من شخص خبير.

اتصلت بك صديقتك المقربة وتبدو مستاءة للغاية. لقد قاموا بفتح ملف مرفق ببريد إلكتروني ظنًا منهم بأنه صورة. ولكنه في الواقع كان فيروس حصان طروادة وقد أخفى برنامج الفدية الضارة لذا تم منعهم من الدخول إلى الحاسوب الخاص بهم. ما الذي ستفعلينه، وما الذي ستخبرينهم بفعله؟

إذا تم إصابة جهازك ببرامج الفدية الضارة، اعلمي أنه في حال قبولك لدفع الفدية فإنها ستستخدم في تمويل الأنشطة الإجرامية، ولا يوجد ضمان أنك ستكونين قادرة على الدخول إلى جهازك، ومع الأسف، قد يعطي ذلك انطباعًا أنك على استعداد للدفع مرة أخرى في المستقبل والتعرض للمزيد من هجمات الاختراق المستقبلية.

أنواع التهديدات الشائعة عبر الإنترنت

عمليات الاحتيال والخداع

يُعد الاحتيال طريقة لخداع شخص ما من أجل الحصول على المال أو على معلوماته الشخصية، حتى يتمكن المجرم من سرقة حسابه أو هويته. وقد يتضمن الأمر استخدام الفيروسات لسرقة البيانات من على الحاسوب الخاص به أو حسابه عبر الإنترنت أو جعل شخص يقدم الأموال بإرادته من خلال تضليله أو خداعه.

عادةً ما تتم عملية الاحتيال باستخدام رسائل البريد الإلكتروني الوهمية (**التصيد الاحتيالي**) أو الرسائل النصية (**التصيد الاحتيالي عبر الرسائل النصية**) أو الاتصال الهاتفي (**التصيد الاحتيالي الصوتي**). قد تحتوي رسائل البريد الإلكتروني أو الرسائل النصية على رابط لموقع مزيف يحاول استدراجك لإدخال بياناتك الشخصية أو يكون بمثابة ممر يسمح للفيروسات بالدخول إلى حاسوبك. أو قد تحتوي رسالة البريد الإلكتروني على مرفق يحتوي على فيروس يقوم بسرقة معلوماتك البنكية أو الشخصية أو الصور.

تقوم فكرة عملية الاحتيال على اعتقادك بأن هناك منظمة تعرفينها تتواصل معك أو شخصًا بحاجة إلى المساعدة. تهدف هذه العمليات لجعلك تشعرين بأنك مجبرة على التصرف بسرعة، وأن عليك "فعل" شيء ما - فتح رابط أو إعطاء تفاصيل أو النقر على المرفق. لا تصدقي مثل هذه الأشياء!

ليس لدينا متسع من الوقت لسرد جميع أنواع عمليات الاحتيال والخداع في هذا الدليل. لمزيد من المعلومات حول أنواع عمليات الاحتيال التي يلجأ لها المجرمون، وكذلك للحصول على نصائح حول كيفية الإبلاغ عن عمليات الاحتيال والجرائم السيبرانية، يُرجى زيارة الموقع التالي: www.actionfraud.police.uk

التصيد الاحتيالي

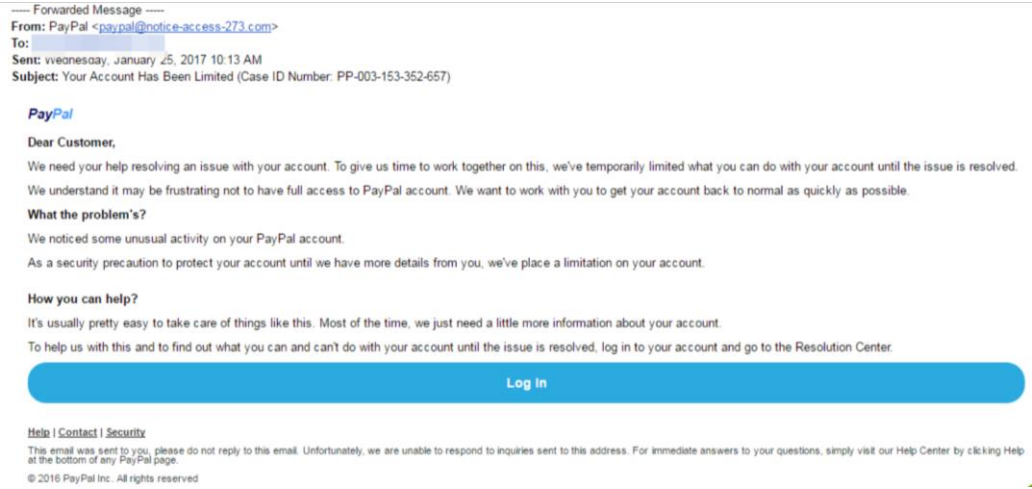
يُعد التصيد الاحتيالي أحد أنواع عمليات الاحتيال، حيث يستخدم المجرم السيبراني "خطافًا" لاستدراج الأشخاص لتقديم معلوماتهم الشخصية أو البنكية أو تفاصيل البطاقة البنكية أو الحساب البنكي وكلمات المرور. ويستخدم المجرمون عندها تلك المعلومات للدخول إلى حساباتك وسرقة الأموال أو جهات الاتصال بالبريد الإلكتروني لسرقة هويتك. يُرسل المجرمون رسائل البريد الإلكتروني الاحتيالية إلى الآلاف من الناس، أملين أن يتمكنوا من خداع القليل منهم للحصول على المال أو المعلومات.

إن المخترقين والمخادعين بارعين للغاية في التظاهر بأنهم أشخاص أو منظمات يمكنك الوثوق بها، ويمكنهم حتى استخدام اسمك وغيرها من المعلومات الشخصية لمحاولة اقناعك بذلك. سيحاولون استدراجك باستخدام العروض أو يوقعون بك بأحد التهديدات. على سبيل المثال، قد يتظاهرون بأنهم جهة حكومية، مثل مكتب الضرائب ويتواصلون معك ليعرضوا عليك إعادة بعض الأموال ولكنهم بحاجة للحصول على معلوماتك البنكية حتى يتمكنوا من سداد المبلغ لك. كما يمكنهم التظاهر أنهم من المجلس المحلي الذي تتبعين له، قائلين أنك معرضة لغرامة يجب دفعها وإلا سيتم محاكمتك، أو التظاهر بأنهم من البنك الخاص بك أو وسيط مصرفي مثل باي بال (PayPal) وسيختلقون أضرارًا مثل كونك محظورة من استخدام حسابك البنكي.

شاهدي الفيديو التالي عما قالته شرطة العاصمة (Metropolitan police) حول التصيد الاحتيالي.

يوجد طريقة سريعة للتحقق من الهوية الحقيقية لمرسل البريد الإلكتروني وإذا ما كانت إحدى محاولات التصيد الاحتيالي، وذلك من خلال التحقق من عنوان البريد الإلكتروني للمرسل، وليس فقط العنوان الظاهر في خانة "المُرسل" (From). عادةً ما تُرسل الرسائل لحقيقية من عناوين مؤسسية يمكن التعرف عليها (مثل: noreply@yourbank.com) في حين لا يمكن للمخادعين والمجرمين استخدام اسم النطاق الحقيقي للبنك أو المنظمة الخاصة بك، لذا عادةً ما يكون عنوان البريد الإلكتروني ملتبسًا بالحروف والأرقام العشوائية (مثل: noreply@1234bank12.com). في حال كانت الرسالة مُرسلة من عنوان خاص (مثل: person@gmail.com) فإنه من غير المرجح أن تكون من منظمة رسمية - حتى أن شركة جوجل (Google) لا تستخدم اسم النطاق (@gmail) المخصص للبريد الإلكتروني لجوجل (GoogleMail) لترسل الرسائل الإلكترونية الخاصة بالمنظمة.

وبالنظر لهذا المثال، يمكننا أن نستنتج أنه على الرغم من أن البريد الإلكتروني يبدو بريداً حقيقياً من باي بال، إلا أنه يحتوي على اسم مختلف للنطاق: Paypal@notice-accessxxx.com



يجدر الحذر من رسائل البريد الإلكتروني التي تبدو أفضل من أن تكون حقيقية أو التي تدفعك إلى اتخاذ قرارات سريعة، حتى وإن كانت تحمل الشعارات الأصلية للمنظمات وتبدو شرعية. حافظي على هذوك وتحققي من الرسائل المستلمة. لا تستجبي أو تنقري على أي روابط. بمجرد فتحك للرابط، قد يتم تثبيت الفيروسات على حاسوبك لسرقة المعلومات أو قد يتم إعادة توجيهك إلى موقع مزيف أو ضار يطلب منك إدخال تفاصيل حسابك أو تفاصيلك البنكية والتي ستسرق منك عندها.

التعرف على أساليب التصيد الاحتيالي والرسائل البريدية المخادعة

- هل تعرفين المرسل؟ هل يخاطبوك في رسائلهم بتحية عامة؟
- هل هناك أي أخطاء إملائية أم أنها ركيكة الصياغة؟
- هل يطلب منك فعل شيء أو يلح عليك في أمر ما أو يهددك؟
- قومي بفتح عنوان البريد الإلكتروني الذي تم إرسال الرسالة منه. هل لديه اسم نطاق صحيح؟
- هل هو غير متوقع أو من شركة ليس هناك تعاون فيما بينكم؟
- في حال وجهك إلى موقع ويب، هل يوجد رمز قفل أو <https://> في بداية عنوان الويب؟

لمزيد من الإرشادات حول التعرف على رسائل التصيد الاحتيالي عبر البريد الإلكتروني، يُرجى زيارة الرابط التالي: www.ncsc.gov.uk

تلقت زهرة بريداً إلكترونياً معتقدة أنه من البنك التابع لها- وحينما فتحتة وجدت أنهم يبلغونها بتعليق حسابها البنكي بشكل مؤقت. وفي أجواء مفعمة بالفرح تكتشف زهرة أن البنك التابع لها اكتشف نشاطاً مريباً في حسابها البنكي وسرعان ما بادرت بإغلاقه لحمايتها. صرحت بأنه لا يمكنها استخدام الحساب البنكي إلا بعد تسجيل الدخول وإعادة تنشيط الحساب أولاً ومن ثم يُطلب منها النقر على رابط. لدى زهرة التزام بموعد دفع الإيجار غذاً ولذا عليها الوصول إلى حسابها البنكي على الفور، لكنها قلقة حيال هذه الخطوة.

تطلب زهرة إسداء المشورة في هذا الصدد: ما النصيحة التي ستوجهينها إلي ها؟

مع العلم أن هذا الرابط ربما يكون خطيرًا. ربما يحاول المخترقون تثبيت شيء ما على حاسوبها لدوافع غير قانونية، مثل سرقة المعلومات أو اختراق بريدها الإلكتروني أو حساباتها المصرفية أو حسابات وسائل التواصل الاجتماعي. قد يوجهها الرابط إلى موقع ويب آخر (موقع وهمي للبنك) ومن ثم يطلب منها رقم الهوية وكلمة المرور أو أي تفاصيل بنكية أخرى. فور تقديمها مثل هذه المعلومات إلى موقع الويب، تصبح فريسة لأولئك المخادعين، فبذلك قد تكون سلمتهم حسابها البنكي ومالها الخاص.

ولذا كوني على حذر، فلن يتواصل معك البنك الذي تتبعين له عن طريق البريد الإلكتروني أو الهاتف أو الرسائل النصية ويطلب منك مثل هذه البيانات الشخصية. في حال راودتك شكوك حول ما إذا كان هذا البنك الذي يتواصل معك هو البنك الذي تتبعين له أم لا، وليست عملية تصيد عبر الهاتف، قومي على الفور بإنهاء المكالمة وابعثي عن رقم خدمة العملاء عبر الإنترنت. تمهلي لخمس دقائق قبل معاودة الاتصال أو استخدمي هاتف مختلف نظرًا لأنه بإمكان المخادعين سرقة خطوط الهاتف.


عقب المناقشة التي أجريت معك:

بحثت زهرة عن رقم هاتف خدمة عملاء البنك الذي تتبعين له عبر الإنترنت. أكدت البنك من جانبه أن هذا بريد إلكتروني وهمي وأن حسابها البنكي يعمل بشكل جيد. وأخبروها أن الرابط المرفق في البريد الإلكتروني يوجهك إلى موقع ويب وهمي للبنك الذي تتبعين له. وقد يتعثر على ضحايا هذا النوع من الاحتيال استرداد أموالهم في حال أثبت البنك أنهم لم يتخذوا سبل الأمان الكافية.

يمكنك العثور على المزيد من المعلومات حول أساليب التصيد الاحتيالي والخداع لدى المركز القومي للأمن السيبراني عبر الرابط التالي www.ncsc.gov.uk/guidance/phishing

مواقع الويب الآمنة وغير الآمنة

يرجى التحقق جيدًا من أمن المواقع الإلكترونية التي تزورينها. أي موقع تقومين بتصفحه ربما يكون غير آمن، أو قد يقوم المخترقون ممن يرسلون رسائل بريدية وهمية بإعادة توجيهك إلى موقع ويب وهمي قد يبدو موثوقًا تمامًا.

عليك بالبحث عن رمز القفل هذا  أو هذه الأحرف <https://> في شريط المتصفح، مما يوضح ما إذا كان موقع الويب آمن أم لا.

    <https://www.redcross.org.uk>

في بعض الأحيان سيظهر لك كل من رمز القفل و **https**، أو رمز القفل فقط، فهذا يعتمد على الحاسوب أو المتصفح. موقع الويب الذي يحتوي على **http** فقط قد لا يكون آمنًا حيث يشير حرف **"s"** لكونه آمن.

في حال طلب منك تسجيل الدخول إلى حساب يُقدم تفاصيل معنية بالدفع أو معلومات أخرى، عليك التأكد مما إذا كان الموقع يحتوي على رمز **"https"** في بداية العنوان في شريط المتصفح أم لا. أدخل بيانات تسجيل الدخول فقط بعد التأكد من صحة عنوان موقع الويب وأمنه.

اكتب دائماً عنوان موقع الويب بالكامل عند زيارتك لموقع الويب الخاص بالبنك الذي تتابعه له، خاصة إذا كنت تقوم بتسجيل الدخول إلى الحساب البنكي عبر الإنترنت. تجنب استخدام محرك بحث للوصول إلى موقع الويب الخاص بالبنك الذي تتابعه له، حيث يمكن للمخترقين استخدام هذه الخطوة للسيطرة على سبل الأمان وسرقة بياناتك.

اتخاذ الإجراءات اللازمة ضد مواقع التصيد الاحتيالي والمواقع المخادعة

يرجى اتباع النصائح الآتية لمحاولة تأمين نفسك:

- حدثي برامج المتصفح وبرامج مكافحة الفيروسات والتجسس بشكل مستمر.
- تجنب تصفح مواقع الويب غير الآمنة أو التي لا تحتوي على رمز القفل
- لا تنقري على أي رابط مرفق في رسالة بريدية من مصدر مجهول أو مريب.
- لا تفصح عن بياناتك الشخصية أو كلمات المرور أو رموز الأمان عبر البريد الإلكتروني أو الهاتف.

ما الإجراءات المتبعة في حال تعرضت لعملية احتيال

قومي بالإبلاغ عن البريد الإلكتروني أو المكالمات أو الرسالة أو موقع الويب.

في حال تلقيت بريداً إلكترونياً ولست متأكدة من مصدره، يمكنك إعادة توجيهه إلى خدمة الإبلاغ عن رسائل البريد الإلكتروني المشبوهة (SERS) عبر الرابط التالي report@phishing.gov.uk. سوف يبلغونك إذا كان هذا البريد بريداً إلكترونياً للتصيد الاحتيالي أو كان مشتبهاً فيه.

في حال تلقيت رسالة نصية مشبوهة، يمكنك إعادة توجيهها مجاناً على رقم 7726. حيث يسمح لمزود خدمة هاتفك بالتحقيق في الرسالة واتخاذ الإجراءات اللازمة في حال كانت عملية احتيال.

لا تشاركي بياناتك قبل التحقق من المصدر. لا تحاولي الاتصال بالرقم الموجود في البريد الإلكتروني أو النقر على الروابط، فربما توجهك إلى حساب وهمي. تصفحي مواقع الإنترنت وقومي بالبحث عن الرقم الموثق واتصلي به بدلاً من الرقم المرفق في البريد.

لا تتبعي الروابط دون الاستفسار عن الموقع الذي سيوجهوك إليه. افتحي متصفح الويب الخاص بك وانتقلي مباشرة عن طريق كتابة الاسم في شريط الروابط، للتأكد من أن موقع الويب آمن.

لا تشاركي كلمة المرور الخاصة بك أو رمز الحماية. لا تفصح عن كلمة المرور الخاصة بك لأي شخص حتى لو كانت والدتك أو صديقتك المقربة.

في حال تعرضت لعملية خداع لتقديم بياناتك البنكية، توجهي لإخبار البنك الذي تتابعين له على الفور.

في حال تعرضت لخسارة أموال، فعليك إخبار البنك، ومن ثم قومي بإبلاغ مركز الإبلاغ عن حالات الاحتيال (Action Fraud) (في إنجلترا وويلز وأيرلندا الشمالية)، أو إبلاغ شرطة اسكتلندا (Police Scotland) (في اسكتلندا). باتخاذ هذه الإجراءات، سوف تساهم بذلك في منع وقوع المزيد من الضحايا.

مركز الإبلاغ عن حالات الاحتيال www.actionfraud.police.uk

العلاقات الإلكترونية

نتحدث في هذا القسم عن تأثير الإنترنت على العلاقات الشخصية. تتأثر حياتنا الشخصية بشكل مباشر بكل ما نقوم به على الإنترنت. لذا من الضروري توخي الحذر بشأن أي معلومات تشاركينها مع أي شخص عبر الإنترنت.

جميعنا يرغب في التواصل مع الأشخاص، وربما تلك من أفضل مزايا الإنترنت حيث يسهل التواصل مع الأصدقاء والعائلة ومن نتشارك معهم اهتماماتنا من شتى أنحاء العالم. وبينما نتمتع بتلك المزايا، علينا أن نكون حريصين في التواصل مع الأشخاص عبر الإنترنت كما هو الحال عند مقابلة شخص ما في الشارع، فمن المؤسف قد يرغب البعض في التواصل مع الأشخاص بنية سيئة مما يؤدي إلى قد يفضي إلى سوء التصرف وغيرها الانتهاكات.

يمكن أن تكون الانتهاكات الإلكترونية من غرباء أو أشخاص نعرفهم بالفعل، وسنعرض أدناه أمثلة على الانتهاكات الإلكترونية.

الاحتيال الرومانسي

يُعرف الاحتيال الرومانسي بأنه عملية يقوم فيها شخص ما بترتيب مواعيد عبر موقع أو تطبيق ما، محاولاً الدخول في علاقة مع شخص ما للحصول على ثقته، ثم بعدها يبدأ في طلب المال أو البيانات الشخصية. ومن المحتمل أن يقوموا بهذه العملية من خلال حسابات وهمية، وربما يبدو أشخاص صادقين ومهتمين. ومن سمات هذا الشخص أنه يسأل عن الكثير من التفاصيل الشخصية دون أن يخبر الكثير عن نفسه. كما يتمهل هذا الشخص إلى أن ينال ثقة الطرف الآخر ويأخذ من التعلق العاطفي سبيلاً في طلب المساعدة، والتي عادة ما تكون مال، وربما تكون الحصول على طرد أو تزويدهم بعنوان ما. وقد يرسل رسومات أو صور مزيفة له، عادة ما يأخذها من أي مواقع على الإنترنت.

لا ترسلي أو تتلقي أي أموال أو تفصحي عن أي بيانات بنكية لأي شخص، مهما بلغت ثقتك أو تصديقك لقصته عبر الإنترنت.

نعلم أنه من المحزن أو المخجل التعرض للخداع بعد ظنك بأنك كونت صداقة أو علاقة عبر الإنترنت، ولكن يمكنك الإبلاغ عن ذلك إلى [مركز الإبلاغ عن حالات الاحتيال](https://www.03001232040.gov.uk) أو الاتصال بالرقم **0300 123 2040**

حتى يتسنى لك التحقق من مصدر الصورة، يمكنك إجراء بحث عكسي عن الصورة كما هو واضح من الاسم، فهو يتيح لك البحث في الصور المتاحة على الإنترنت للعثور على صور مشابهة. يمكنك إجراء بحث عكسي للصورة [هنا](#)

التنمر الإلكتروني

التنمر الإلكتروني هو مصطلح عام يستخدم للتعبير عن التنمر والتحرش عبر الإنترنت أو باستخدام التكنولوجيا. يُعد من ضمن الانتهاكات الإلكترونية التي تستهدف إلحاق الأذى بالأشخاص أو مضايقتهم أو التسبب في خسائر شخصية. غالباً ما يلجأ المتنمرون لاستخدام مواقع شبكات التواصل الاجتماعي مثل فيسبوك (Facebook) أو تويتر (Twitter) أو خدمات المراسلة أو المنتديات التفاعلية. يمكن للتنمر للإلكتروني أن يكون من أشد أساليب الانتهاكات إزعاجاً، إذ يسهل الوصول للأشخاص في أي وقت عبر الإنترنت والهواتف المحمولة، وليس موقفاً معيناً في المدرسة أو العمل.

وفي حال نشر شخص ما على الإنترنت أو على وسائل التواصل الاجتماعي إشاعات مضللة أو مغرضة عنك، فيُعد ذلك من أساليب التحرش الذي هو جريمة في حد ذاته. وعلى غرار ذلك، في حال تلقيت مكالمات تهددك أو تخيفك، فقد تُعد تلك الفعل جريمة جنائية.

لا ريب في تأثير التنمر على أي شخص سواء الأطفال أو البالغين، ولكن ما يهم هو أن تكوني على دراية بكيفية التعامل مع هذه الحالة سواء بصفتك ولي أمر أم من مقدمي الرعاية للأطفال. في حال تعرضت أنت أو طفلك أو أي شخص تعرفيه للتنمر، بما في ذلك التنمر الإلكتروني، يمكنك الاتصال [بخط المساعدة الوطني لمكافحة التنمر \(national bullying helpline\)](https://www.nationalbullyinghelpline.org.uk)، وطلب المشورة في هذا الصدد، يمكنك الاتصال على رقم **0300 323 0169**.

الاستدراج

يتمثل الاستدراج في كون شخص ما يحاول توطيد علاقته وتواصله مع شخص آخر حتى يتسنى له استغلاله والتحكم فيه. تُثير عملية استدراج الأطفال والشباب عبر الإنترنت قلقًا خاصًا، حيث يمكن استدراج القاصرات لأغراض الاعتداء الجنسي سواء (عبر الإنترنت أو في الواقع) أو استدراجهم للاتجار بالمخدرات أو غيرها من أساليب الاستغلال.

ربما تتم عملية الاستدراج هذه على مدار فترة زمنية قصيرة أو طويلة، بل وقد يشرع أولئك المخادعين في إقامة علاقة مع عائلة الطفل حتى يظهرون بهيئة أشخاص أهل للثقة وموثوق بهم ومعاونين. يمكن لأي شخص أن يكون مخادع بغض النظر عن عرقه أو جنسه أو عمره أو علاقته بالطفل.

يمكن أن تتم عملية الاستدراج عبر الإنترنت حيث يمكن لأولئك المخادعين أن يقدموا أنفسهم على أنهم زملاء لهذا الطفل ويرسلون صور أو مقاطع فيديو تدعم ادعاءاتهم. قد يلعبون معهم ويقدمون النصائح ويظهرون تفهمهم ويشترطون الهدايا لهم من أجل توطيد علاقتهم بصفتهم أصدقاء موثوق بهم، أو يحاولون جعل الطفل في عزلة بعيدًا عن العائلة أو الأصدقاء، ومن ثم يبتزونهم لمحاولة جعل الطفل يستجيب لأوامرهم، أو يعملون على ترسيخ فكرة "الأسرار" فيما بينهم حتى يتسنى لهم السيطرة على الطفل.

لمزيد من المعلومات حول الاستدراج، يُرجى زيارة موقع الجمعية الوطنية لمنع القسوة ضد الأطفال (NSPCC) فضلاً عن مصادر أخرى حول كيفية التحدث مع الأطفال حول الانتهاكات والتهديدات الإلكترونية. www.nspcc.org.uk

لا تتردي في التواصل مع الشرطة وإبلاغهم في حال كانت هناك شكوك أن الطفل يتعرض لخطر. يمكنك أيضًا التواصل مع [الجمعية الوطنية لمنع القسوة ضد الأطفال](http://www.nspcc.org.uk) للحصول على المشورة والدعم والإبلاغ عن الانتهاكات الإلكترونية

المراسلات الجنسية والانتقام الإباحي

تتمثل المراسلات الجنسية في إرسال رسالة أو صورة أو مقطع فيديو جنسية مرسله لشخص آخر. قد يرسل الشخص صورة لنفسه أو لشخص آخر. يمكن أن تكون الرسائل الجنسية موجهة إلى صديق أو شريك أو شخص آخر عبر الإنترنت، وقد تتضمن عري جزئي أو كلي أو الظهور بأوضاع مخلة صريحة أو الحديث عن أفعال جنسية.

في حين أنه يمكن إرسال رسالة جنسية بين طرفين باتفاقهم، إلا أن الصور قد تتم مشاركتها سريعًا عبر الإنترنت دون موافقة صاحبها. حيث أنه بمجرد حيازة أي شخص لصورة أو فيديو عبر الإنترنت، قد يقوم بمشاركة هذه الصورة أو الفيديو لأي شخص آخر.

يتمثل الانتقام الإباحي حينما يقوم شخص ما بعرض أو نشر صورة أو فيديو لمحتوى جنسي دون موافقة الشخص الظاهر في الصورة أو الفيديو وهو عازم على إلحاق الأذى به.

ومن ضمن أساليب الابتزاز والتي تُعد جرمًا جنائيًا هو تهديد شخص ما بالإفصاح عن بياناته الشخصية وصوره. يتوفر المزيد من المعلومات حول الانتقام الإباحي من هنا

خط المساعدة لمكافحة الانتقام الإباحي (Revenge Porn Helpline) - 0845 6000 459

www.revengepornhelpline.org.uk/

ليس من الجيد مطلقًا إجبار أي شخص على إرسال صور عارية.

وعليك معرفة أن الصور المرسله باستخدام تطبيقات مثل سناب شات (Snapchat)، لا يزال من الممكن التقاطها وحفظها. في حال أرسلت صورة عارية أو جنسية وكنّت قلقة حيال ما قد يحدث، فيمكنك اتباع النصائح التالية:

- اطلبي حذف الرسالة.
- لا تردي على التهديدات.
- تحدثي إلى شخص ما واطلبي منه الدعم. يمكنك التواصل مع [خط المساعدة لمكافحة الانتقام الجنسي](http://www.revengepornhelpline.org.uk/).

– **قومي بالإبلاغ عما حدث.** يمكنك الإبلاغ عن محتوى موقع الويب الذي تُنشر عليه هذه الصور. تتضمن معظم منصات وسائل التواصل الاجتماعي أدوات للإبلاغ عن المحتوى المسيء. يجب عليك أيضًا إبلاغ الشرطة بهذا النوع من أساليب المضايقات: إن لم تكن حالة طارئة، يمكنك الاتصال على رقم 101.

كما يتعين عليك معرفة أن تبادل صور عارية لشخص أقل من 18 عامًا يعد من أساليب الاعتداء على الطفل، وهي جريمة يعاقب عليها قانون مكافحة الجرائم الجنسية لعام 2003 (Sexual Offences Act 2003). فقد تفضي مشاركة أي "محتوى جنسي" لشخص أقل من 18 عامًا إلى الاستدعاء للتحقيق من قبل الشرطة.

في حال كنت قلقة بشأن مشاركة صور الأطفال أو كانت لديك مخاوف أخرى بشأن حماية الطفل على الإنترنت، يمكنك التواصل مع مركز أمان لمكافحة استغلال الأطفال وحمايتهم على الإنترنت (Child Exploitation and Online Protection safety centre) www.ceop.police.uk

المطاردة والمراقبة عبر الإنترنت

تتمثل المطاردة في سلوك شخص آخر اتجاهك حيث يثير بداخلك الفزع من استخدام العنف ضدك أو يتسبب لك في قلق أو ضيق فضلاً عن تأثيرها الخطير على أنشطتك اليومية المعتادة. ويطلق عليها اسم المطاردة الإلكترونية حينما تتم عبر الإنترنت. وربما تتمثل في جمع معلومات عنك أو انتحال شخصيتك أو إرسال رسائل غير مرغوب فيها أو تهديدك أو مراقبتك أو الوصول إلى حسابك عبر الإنترنت ونشر معلومات مضللة عنك. يمكن أن يكون المطارد شخصًا تعرفه أو غريب. تؤثر المطاردة الإلكترونية بصورة خطيرة على ضحيتها كما أنها تُعد جريمة جنائية.

خط المساعدة الوطني لمكافحة المطاردة (National Stalking Helpline) - 0808 802 0300

www.stalkinghelpline.org/faq/about-the-law/

في حال كانت لديك أية مخاوف من كون المسيء يطارذك أو يراقبك:

- تجنب التعامل مع المطارد، فغالبًا سيرغب في التحدث معك وبناء علاقة. لا توافق أبدًا على مقابلتهم أو مواجهتهم.
- خذي الأمر على محمل الجد وأبلغ الشرطة بما حدث. يمكنك الاتصال على رقم 101 للتحدث مباشرة إلى الشرطة، وفي حال كان تهديدًا مباشرًا، عليك بالاتصال على رقم 999.
- تحققي من إعدادات الخصوصية الخاصة بك وتأكدي من توافر الحد الأدنى من بياناتك عبر الإنترنت، ومن ثم أوقفي أيقونة تحديد الموقع من على جهازك.
- قومي بتحذير الأشخاص من حولك. قد يحتاجون إلى التحقق مما يشاركونه عنك وقد يحتاجون إلى التحقق من إعدادات الخصوصية الخاصة بهم أيضًا.
- احتفظي بتسجيل لما يحدث وربما عليك أخذ لقطة شاشة للمكالمات أو الرسائل أو منشورات وسائل التواصل الاجتماعي، وبالتالي يكون لديك نسخة من الأدلة حتى لو حذف الشخص المسيء رسائله ومنشوراته في وقت لاحق.

العنف المنزلي والتحرش والمراقبة

يُحتمل أن يسيء المعتدي استخدام خصائص جهاز متصل بالإنترنت حتى يتسنى له مشاهدة الضحية ومراقبتها والتحكم فيها. يمكن أن يشمل ذلك مراقبة اتصالاتك مع الآخرين أو تتبع موقعك من خلال جهازك أو التحقق من نفقاتك المالية. بموجب القوانين المعمول بها في المملكة المتحدة، تُعد تلك السلوكيات من أساليب العنف المنزلي في حال قام بها شريك حالي أو سابق أو أحد أفراد الأسرة أو مقدم الرعاية.

في حال كنت قلقة من أن يراقب شخص ما جوالك أو أي جهاز آخر، فإن خط المساعدة الوطني للعنف يتيح لك **أداة شاملة** لمساعدتك في تغيير إعداداتك حتى يجعله -جهازك- آمنًا.

خط المساعدة الوطني للعنف (24 ساعة) 0808 220 0247

www.nationaldomesticviolencehelpline.org.uk

هل توافق على البيانات التالية؟

لا تشكل التهديدات عبر الإنترنت خطرًا حقيقيًا، لأنها ليست على "أرض الواقع"

لا، الانتهاكات الإلكترونية جادة، ولها تأثير حقيقي على حياة الناس، ويجب على الهيئات التعامل الدائم معها بحزم. إن الملاحقة والمراقبة والمضايقات كلها سلوكيات عالية الخطورة، وهي ليست خطأ تلام عليه. ولك الحق في الإبلاغ عن مثل هذه السلوكيات، والبحث عن مشورة، وأن يتم دعمك للتعامل مع هذه المسألة.

جريمة التحرش تعني التهديد مع استخدام العنف على أرض الواقع.

ينص القانون على أن "التحرش" هو عندما يتصرف أحد ما بطريقة تتسبب في مضايقتك أو ترويعك، ويحدث هذا السلوك في أكثر من موقف. وقد يكون لذلك أوجه سلوكية مختلفة، وفي مناسبات أو حالات منفصلة. على سبيل المثال: لا تعتبر رسالة الابتزاز المرسلة لمرة واحدة من أساليب المضايقات. إلا أن رسالتين قد يعتبران إزعاجًا، أو مكالمات هاتفية بعد رسالة تهديد عبر البريد الإلكتروني، قد تُعتبر إزعاجًا أيضًا. ومن الأنشطة الأخرى التي قد تُعد من المضايقات، أن يتم ملاحقتك، أو مراقبة محل إقامتك أو عملك، أو تلف ممتلكاتك، أو أن يتم الإبلاغ عنك لدى الشرطة زورًا وبهتانًا دون أن تفعل شيئًا.

لدى زهرة ابنة عم/خال مقربة منها جدًا. وفي الأونة الأخيرة، كانت تتصرف بشيء من الغرابة، فتظهر منزعة ومضطربة وتفحص هاتفها بشكل انفعالي طوال الوقت الذي يقضيه معًا. وأخيرًا، قامت ابنة عم/خال زهرة بإخبارها أنها لا تنعم بنوم هادئ وهي في قمة التوتر والضغط بسبب التهديدات التي يرسلها إليها زوجها السابق، والذي انفصلت عنه. إذ يرسل لها رسائل بريدية بشكل دائم ليخبرها أنها زوجة وأم فظيعة، وقد جلبت العار لكلا عائلتيهما، ولذلك عليها أن تعود للعيش معه. وتشعر ابنة عم/خال زهرة أنها مستاءة للغاية بسرد هذا الأمر.

وقد سربت أيضًا أن زوجها السابق يحوز صورًا عارية لها، عندما كانا مستمرين في علاقتهما. وقد هدهدها بارسال هذه الصور لأهلها إن لم ترجع له مجددًا.

هل ابنة عم/خال زهرة ضحية في جريمة؟

نعم. فابنة عم/خال زهرة ضحية **للتحرش والسيطرة القسرية**. فهذه التهديدات وقعت ضدها بغرض محاولة فرض السيطرة عليها. وينص القانون على اعتبار هذه جريمة عندما يتصرف أحدهم بطريقة يهدف بها مضايقتك أو ترويعك. ويتعين أن يكون هذا السلوك في أكثر من مناسبة.

وبما أن مرتكب هذا الفعل هو زوجها السابق، فيُعد هذا الإزعاج أحد أشكال **السيطرة القسرية** (أحد أنواع **العنف المنزلي**). فهو فعل إجرامي. وبإمكانها الإبلاغ عن ذلك إلى الشرطة.

كما أنه أحد أشكال الانتقام الإباضي، حيث يهددها بنشر صور حميمية خاصة بها بدون موافقتها، بغرض مضايقتها وإذلالها. لا يُعد هذا التهديد في حد ذاته جريمة، ولكن إذا شارك هذه الصورة على الإنترنت، عن طريق البريد الإلكتروني أو وسائل التواصل الاجتماعية، بما في ذلك واتساب (WhatsApp) أو غيرها من خدمات المراسلة، فإن ذلك يصبح جريمة.

كما يتحدث زوج زهرة عن كرامة العائلة، وأن انفصالهم يُعد "عارًا" في عرف العائلة. فما تُسمى بجريمة الشرف هي إحدى أشكال الاعتداء، وقد تود زهرة في الحصول على دعم من إحدى المنظمات المتخصصة في العمل مع ضحايا العنف والتهديدات باسم الشرف. تخصص كارما نرفانا (Karma Nirvana) خط مساعدى، من الاثنين إلى الجمعة، 0800 5999 247، www.karmanirvana.org.uk

الملخص

- فكري قبل النشر. لا تُحملي أو تشاركي أي شيء دون التفكير فيما قد يحدث إن وقعت هذه المعلومات في اليد الخطأ. فبمجرد أن تنشري شيئاً، فإنك تفقدين السيطرة عليه، خاصة لو أخذ أحدهم لها لقطة شاشة.
- احمي هويتك ولا تشاركي كل شيء على شبكات التواصل الاجتماعي. فوسائل التواصل الاجتماعي رائعة، لأنها تتيح على تواصل مع الأصدقاء والعائلة، لكن فكري في الأمر كأنك تخبرين العالم كله عن حياتك الخاصة أكثر مما قصدت. فضعي في اعتبارك، وبعناية، من يمكنهم أن يروا ما تشاركيه عبر الإنترنت، وتأكدي من ضبط إعدادات الخصوصية على أعلى مستوى، وفكري فيمن تتكلمين معه.
- وكوني على دراية بأنواع الاحتمالات وكيف تبحثين عن الرسائل والمواقع الإلكترونية الاحتمالية.
- ولا تفصحي أبداً عن أي معلومات شخصية، كعنوانك أو رقم هاتفك أو اسمك كاملاً أو تاريخ ميلادك.
- ولا تعطي أحداً تفاصيل تسجيل دخولك وكلمة المرور الخاصة بك.
- ولا تفتحي رسالة بريدية أو ملفات أو مرفقات من مجهول، وكوني على دراية بالتصيد والاحتمالات.

