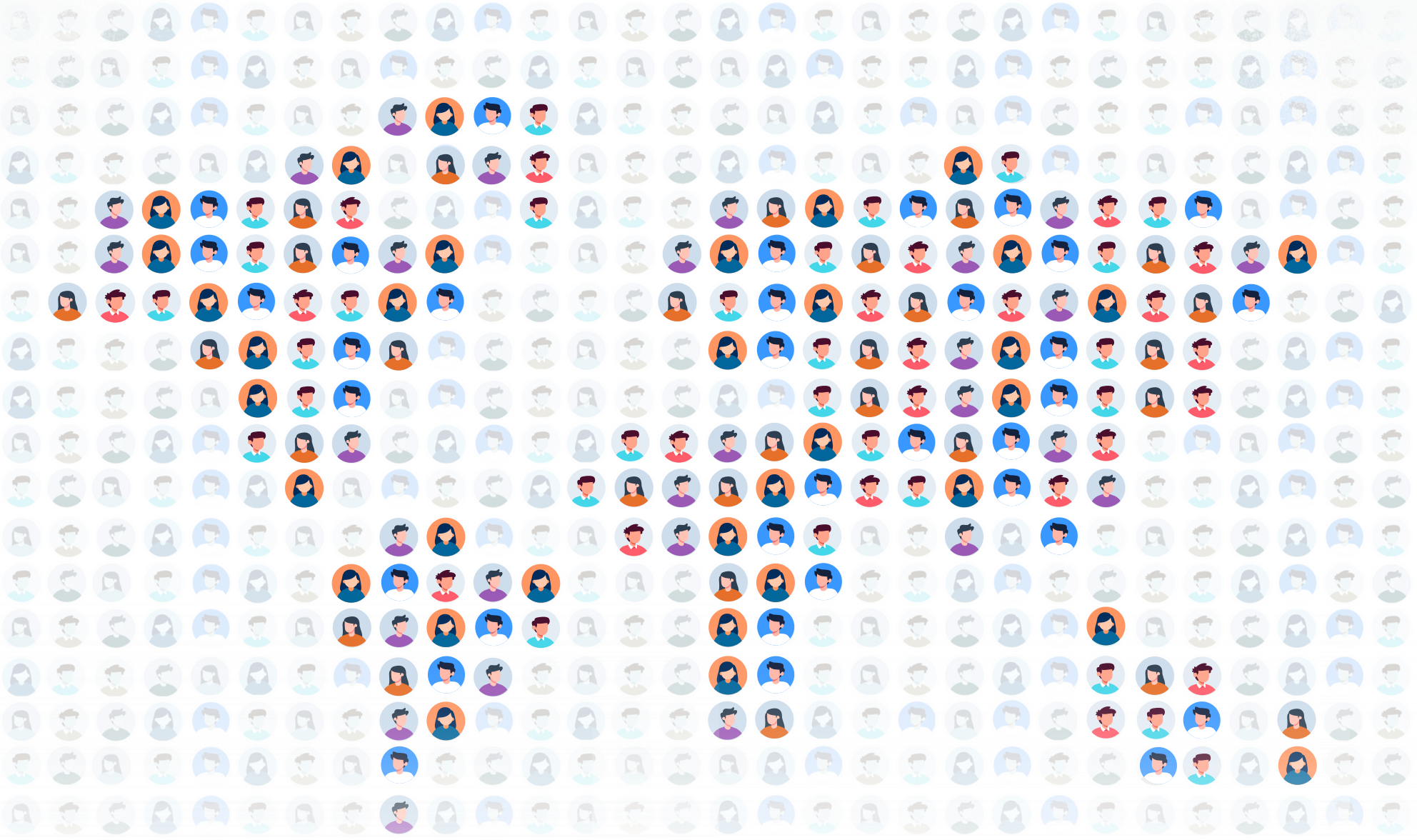


دليل الأمن الرقمي

خارطة الطريق للحماية عبر الإنترنت

مهارات
Maharat

دليل الأمن الرقمي

خارطة الطريق للحماية عبر الإنترنت

تم إعداد هذا الدليل من قبل مؤسسة مهارات، بدعم من هيئة الأمم المتحدة للمرأة والسفارة الفرنسية في بيروت.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

مهارات
Maharat

UN WOMEN

الجزء

الصحة النفسية والسلامة الرقمية:
التعامل مع التأثير النفسي للتهديدات الرقمية وكيفية طلب المساعدة.

إعداد:
خبير في الأمن الرقمي بهاء نصر

ان التأثير النفسي للتهديدات الرقمية مثل التنمر الإلكتروني، المراقبة، التحرش، الاختراق، والتعرض للمحتوى الضار، يمكن ان يكون خطيرا وغالبًا ما يتم تجاهله. فهذه التهديدات باي من اشكالها يمكن أن تعرض الصحة النفسية، والثقة بالنفس، والرفاهية العامة للخطر. وقد تؤدي إلى التوتر، والقلق، والاكتئاب، والصدمة النفسية، وأحيانًا إلى أفكار انتحارية، خاصة عندما يشعر الأفراد بأن خصوصيتهم وسلامتهم الشخصية قد تم انتهاكها.

نعرض بعض المعلومات التي تساعد على فهم آثار التهديدات الرقمية على الصحة النفسية واستراتيجيات لمواجهتها او لطلب المساعدة.

ما هي التهديدات الرقمية التي يمكن أن تؤثر على الصحة النفسية؟

التنمر الإلكتروني والتحرش عبر الإنترنت

يعد التنمر الإلكتروني والتحرش عبر الإنترنت شكلين من أشكال الإساءة الرقمية، حيث يتم استخدام التقنيات الرقمية لإلحاق الأذى أو التخويف أو الإحراج الآخرين بشكل متعمد ومتكرر. وغالبًا ما تحدث هذه السلوكيات عبر منصات التواصل الاجتماعي، وتطبيقات المراسلة، والبريد الإلكتروني، ومنصات الألعاب على الإنترنت.

التصيد الاحتيالي والاحتيال الإلكتروني

التصيد الاحتيالي والاحتيال الإلكتروني هما ممارسات خداعية يستخدمها مجرمو الإنترنت لخداع الأفراد من أجل الحصول على معلومات حساسة أو دفعهم للقيام بأفعال ضارة. يشمل التصيد الاحتيالي رسائل البريد الإلكتروني أو الرسائل النصية أو المواقع الإلكترونية المزيفة التي تحاول سرقة البيانات الشخصية. أما الاحتيال الإلكتروني، فيشمل مجموعة أوسع من الأنشطة الاحتيالية التي تهدف إلى تحقيق مكاسب مالية، وكلاهما يعتمدان على أساليب الهندسة الاجتماعية لخداع الضحايا.

اختراق البيانات وسرقة الهوية

يحدث اختراق البيانات عندما يتمكن أشخاص غير مصرح لهم من الوصول إلى بيانات حساسة، مثل المعلومات الشخصية أو المالية، من أنظمة أو شركات معينة. أما سرقة الهوية، فتحدث عندما تُستخدم هذه البيانات المسروقة لإنتحال هوية شخص ما، وغالبًا لأغراض احتيالية مثل سرقة الأموال أو تنفيذ أنشطة غير قانونية باسمه.

برامج الفدية والابتزاز الإلكتروني

برامج الفدية هي نوع من البرمجيات الخبيثة التي تقوم بتشفير بيانات الضحية أو أجهزتهم، مع طلب فدية مالية لإعادة الوصول إليها. أما الابتزاز الإلكتروني، فيتضمن التهديد بنشر معلومات حساسة ما لم يتم دفع الفدية. كلا النوعين يسببان الخوف، والضغط المالي، وقد يشكلان خطرًا جسديًا، مثل تعطيل ملفات طبية مهمة في المستشفيات، مما يمنع الأطباء من تقديم الرعاية المناسبة للمرضى.

المراقبة والملاحقة الإلكترونية (التجسس الرقمي)

المراقبة والملاحقة الإلكترونية تشمل تتبع أنشطة الأشخاص عبر الإنترنت دون موافقتهم بهدف التخويف أو التحكم أو التحرش بهم. وقد تشمل هذه الأنشطة التجسس على وسائل التواصل الاجتماعي أو الرسائل أو بيانات الموقع الجغرافي، مما يهدد خصوصية الأفراد وسلامتهم.

المعلومات الخاطئة والتضليل الإعلامي

المعلومات الخاطئة تشير إلى نشر معلومات خاطئة دون قصد، في حين أن التضليل الإعلامي يتمثل في نشر محتوى كاذب عمدًا لخداع الآخرين أو تشويه السمعة أو التلاعب بالرأي العام. كلاهما يمكن أن يشوه الواقع، ويثير القلق، ويؤدي إلى فقدان الثقة في وسائل الإعلام والمؤسسات، بل وحتى في الإرشادات الصحية العامة.

الإدمان الرقمي والتعرض المفرط للمحتوى الرقمي

الإدمان الرقمي هو الاستخدام المفرط للمنصات الرقمية، وغالبًا ما يكون مدفوعًا بوسائل التواصل الاجتماعي أو الألعاب الإلكترونية.
التعرض المفرط يشير إلى قضاء فترات طويلة أمام الشاشات، مما قد يؤدي إلى اضطرابات في الصحة النفسية، واضطرابات النوم، وضعف التواصل الحقيقي مع الآخرين.

التزييف العميق والتلاعب الإعلامي

التزييف العميق (Deepfakes) هو تقنية تعتمد على الذكاء الاصطناعي لإنشاء صور أو مقاطع فيديو أو تسجيلات صوتية مزيفة ولكنها تبدو حقيقية، حيث يمكنها محاكاة شخصيات حقيقية.
التلاعب الإعلامي يشمل تعديل المحتوى لإيهام الجمهور أو تضليله، مما يؤدي إلى زعزعة الثقة، والإضرار بالسمعة، ونشر الخوف والارتباك حول حقيقة ما يحدث.

1- فهم التأثير النفسي للتهديدات الرقمية

يجب التعامل بجدية مع التأثير النفسي للتهديدات الرقمية، خاصة في مناطقنا حيث يمكن أن يؤدي الوصم الثقافي المتعلق بالفضائح العلنية إلى تفاقم التأثير العاطفي لهذه التهديدات. على سبيل المثال، التحرش عبر الإنترنت، لا سيما التحرش القائم على النوع الاجتماعي، يستهدف النساء والمجموعات المهمشة بشكل غير متناسب، مما يؤدي إلى مشاعر العزلة والخوف والقلق والاكتئاب، وقد يدفع البعض إلى الانسحاب من المجالات العامة، مثل الانتخابات أو الحياة السياسية.

الخوف المستمر، الاكتئاب والقلق

يمكن أن تؤدي التهديدات الرقمية إلى الشعور بعدم الأمان، والعجز، وفقدان السيطرة، مما يساهم في زيادة معدلات القلق والاكتئاب وحتى نوبات الهلع. على سبيل المثال، يمكن أن تجعل الملاحقة الإلكترونية (Cyberstalking) أو التنمر الإلكتروني أو التحرش الأشخاص يشعرون بأنهم مراقبون باستمرار أو غير آمنين حتى داخل منازلهم. قد تؤدي هذه الهجمات إلى أفكار انتحارية، خاصة بين المراهقين.

انخفاض الثقة بالنفس والاكتئاب

يمكن أن تؤثر التعليقات المؤذية، والسخرية من المظهر الجسدي (Body Shaming)، والتحرش الموجه عبر الإنترنت بشكل سلبي على الصحة النفسية والثقة بالنفس. يؤدي التنمر الإلكتروني، خاصة عبر وسائل التواصل الاجتماعي، إلى شعور الضحايا بعدم القيمة والعزلة الاجتماعية. قد يتجنب الأشخاص المستهدفون التفاعل الاجتماعي، سواء عبر الإنترنت أو في الواقع، مما يزيد من مشاعر الوحدة والاكتئاب. وهذا ما دفع بعض الدول، مثل أستراليا، إلى فرض قيود على استخدام وسائل التواصل الاجتماعي لمن هم دون سن 16 عامًا.

فقدان السيطرة والخصوصية

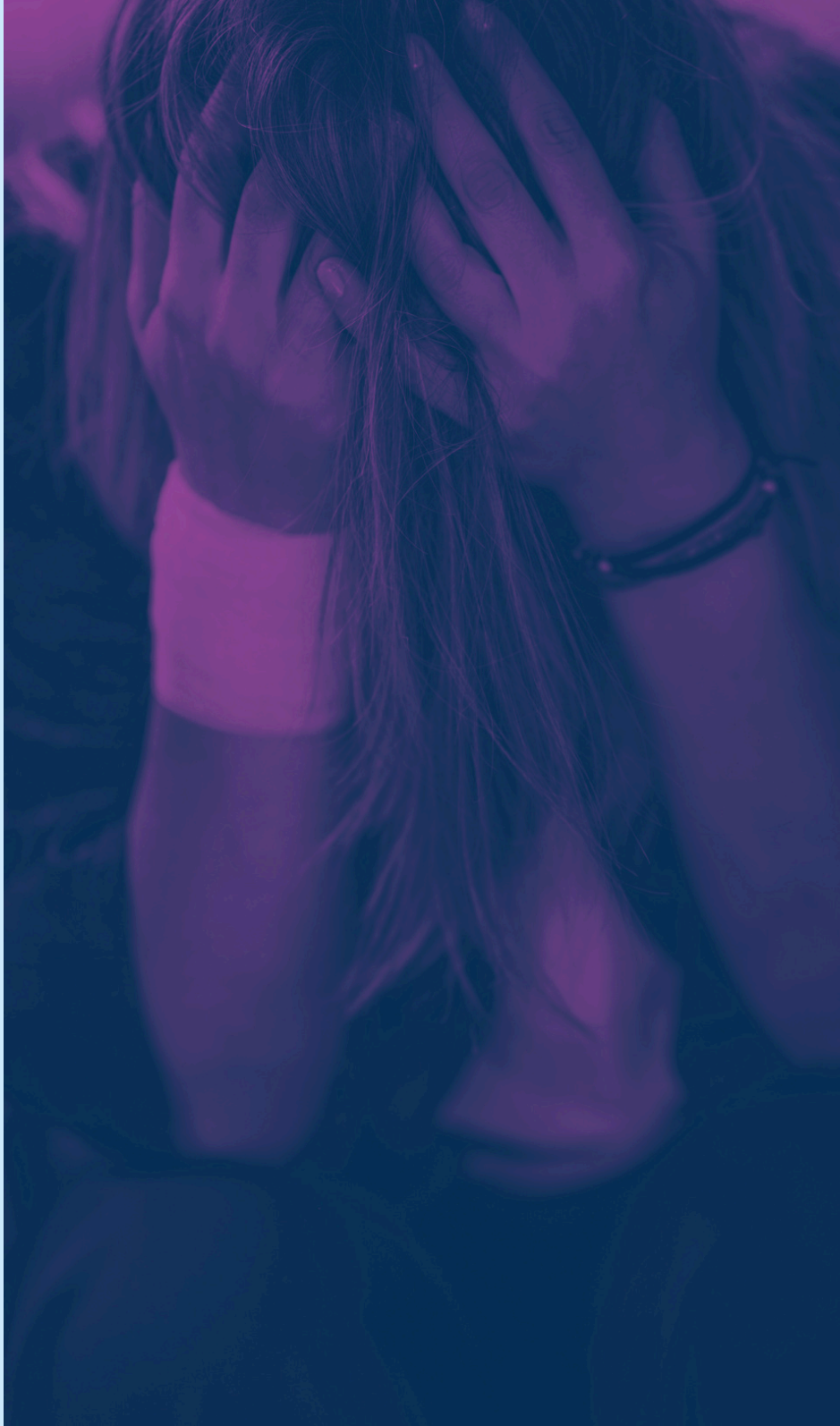
يمكن تشبيه التعرض للاختراق الإلكتروني، أو انتحال الهوية، أو النشر غير القانوني للمعلومات الشخصية (Doxxing) باقتحام منزل شخص دون إذنه. يشعر الضحايا بانعدام السيطرة، والضعف، وانتهاك خصوصيتهم، مما يولد لديهم خوفًا مستمرًا من وقوع هجمات مستقبلية. هذه التجارب قد تؤدي إلى فقدان الثقة بالتكنولوجيا، وإحساس دائم بعدم الأمان.

اضطرابات النوم

يمكن أن يؤدي التعرض للتحرش عبر الإنترنت أو الاختراقات الأمنية إلى الأرق وضعف جودة النوم. فالتوتر والخوف المستمر وزيادة اليقظة تجعل من الصعب الاسترخاء، مما يساهم بمرور الوقت في زيادة القلق والاكتئاب وضعف القدرة الإدراكية.

اضطراب ما بعد الصدمة (PTSD) والتفكير الانتحاري

في الحالات الشديدة، قد تؤدي الهجمات الرقمية، مثل التنمر الإلكتروني أو التحرش، إلى اضطراب ما بعد الصدمة (PTSD) وأفكار انتحارية. قد يشعر الضحايا بالإرهاق الشديد بسبب العنف الرقمي والضغوط النفسية، مما يدفعهم أحيانًا إلى فقدان الأمل والنظر إلى إيذاء النفس كحل أخير، خاصة بين المراهقين.



2- استراتيجيات للتعامل مع التأثير النفسي للتهديدات الرقمية

تخصيص أوقات "للابتعاد عن الإنترنت"
حاولوا تحديد فترات زمنية للبقاء بعيدًا عن الإنترنت لمنح أنفسكم مساحة ذهنية لاستعادة طاقتكم. تقليل الوقت الذي تقضونه على وسائل التواصل الاجتماعي يحد من التعرض للمحتوى الضار ويعزز صحتكم النفسية.

تقليل التفاعل مع التهديدات الرقمية
تجنبوا الرد المباشر على التهديدات أو التحرش عبر الإنترنت، حيث يمكن أن يؤدي ذلك إلى تصعيد الموقف. استخدموا خاصية الحظر (Block) والإبلاغ (Report) على المنصات الرقمية لإدارة وتقليل التفاعلات السلبية.

ممارسة تقنيات اليقظة والاسترخاء
يمكن أن تساعد تقنيات مثل التأمل، وتمارين التنفس العميق، وتمارين اليقظة الذهنية على تقليل القلق والتوتر. يمكن لهذه الأساليب مساعدتكم في الحفاظ على توازنكم العاطفي، خاصة بعد التعرض لمواقف مزعجة عبر الإنترنت.

التركيز على المساحات الرقمية الإيجابية
اقضوا وقتًا على منصات تدعم بيئة آمنة وإيجابية. ابحثوا عن مجموعات أو مجتمعات تشعرون فيها بالدعم والتقدير، وابتعدوا عن المنصات التي قد تعرضكم للمحتوى السلبي أو التهديدات.

3. ممارسات الأمان الرقمي لتقليل الأثر النفسي

التحكم في الأمان الرقمي: إدارة الأمان الرقمي بشكل استباقي، مثل استخدام كلمات مرور قوية، وتفعيل التحقق بخطوتين، وتأمين إعدادات الخصوصية، يمكن أن يساعدكم على الشعور بمزيد من التحكم ويقلل من القلق بشأن التهديدات المحتملة.

- **تعزيز إعدادات الخصوصية:** حددوا من يمكنه رؤية محتوى ما تنشروه، إرسال الرسائل إليكم، أو رؤية حالتكم على الإنترنت.
- **تحديد المعلومات التي تشاركونها عبر الإنترنت:** قوموا بتعيين ملفاتكم الشخصية على خاص أو للأصدقاء فقط. تجنبوا مشاركة المعلومات الشخصية علنًا التي قد تُستخدم ضدكم، مثل الموقع الجغرافي، الروتين اليومي، أو التفاصيل التعريفية. فكروا في استخدام الأسماء المستعارة حيثما كان ذلك ممكنًا للحفاظ على الخصوصية.
- **مراقبة تسريبات البيانات الشخصية بانتظام:** استخدموا أدوات مثل Google Alerts أو خدمات مراقبة تسريبات البيانات للحصول على إشعارات إذا ظهرت معلوماتكم في أماكن غير متوقعة. يمكن أن يساعدكم تنبهكم لمخاطر اختراق البيانات في اتخاذ إجراءات سريعة إذا لزم الأمر قبل أن تنتشر المعلومات على نطاق واسع.
- **اعداد خطوات لمواجهة تصعيد التهديدات الرقمية:** وضع خطة مسبقة يمكن أن يعطيكم إحساسًا بالتحكم في حال تصاعد التهديد الرقمي. قد تشمل هذه الخطة تحديد من يمكنكم الاتصال بهم للحصول على الدعم، الاحتفاظ بنسخ احتياطية من الملفات، معرفة كيفية الإبلاغ عن المشكلات، وإعداد جهات الاتصال للطوارئ.

4- طلب الدعم النفسي لمواجهة القلق الناتج عن التهديدات الرقمية

الاعتراف بالمشكلة هو الخطوة الأولى نحو التعافي

إدراك تأثير التهديدات الرقمية على الصحة النفسية هو خطوة أساسية نحو التعامل معها. تذكروا دائمًا: طلب المساعدة هو قوة وليس ضعفًا. لا تترددوا في التواصل مع الأصدقاء، العائلة، أو مجموعات الدعم التي يمكنها تقديم المساندة والاستماع إليكم. مشاركة تجاربكم مع أشخاص تثقون بهم تخفف الضغط النفسي، وقد توفر حلولًا عملية، وتذكّركم بأنكم لستم وحدكم.

يمكن أن يكون التواصل مع معالج نفسي متخصص في القلق أو الصدمات المرتبطة بالإنترنت خطوة فعالة لمعالجة المشاعر السلبية وتطوير استراتيجيات تكيّف صحية. يمكن أن يساعدكم العلاج النفسي على التعامل مع مشاعر القلق، الخوف، أو الصدمة الناتجة عن التنمر أو التهديدات الرقمية.

إجراء تغييرات بسيطة، مثل تقليل وقت الشاشة أو خلق بيئة رقمية آمنة، يمكن أن يحسن الصحة النفسية بشكل كبير على المدى الطويل. لا تضغطوا على أنفسكم لتغيير كل شيء دفعة واحدة، خذوا الأمور خطوة بخطوة.

لا ينبغي أن يكون طلب المساعدة النفسية أمرًا مخجلًا. خدمات الصحة النفسية سرية وفعالة ومتاحة، واللجوء إلى مختصين عند الشعور بالإرهاق العاطفي أمر ضروري لا يستوجب الخجل أو التردد.

الانضمام إلى مجموعات الدعم أو المنتديات التي تجمع الأشخاص الذين مروا بتجارب مشابهة قد يكون علاجًا نفسيًا بحد ذاته. مشاركة التجارب مع الآخرين تعزز الشعور بالتضامن وتساعد في بناء المرونة النفسية للتعامل مع الأزمات.

5- الإبلاغ عن التهديدات الرقمية

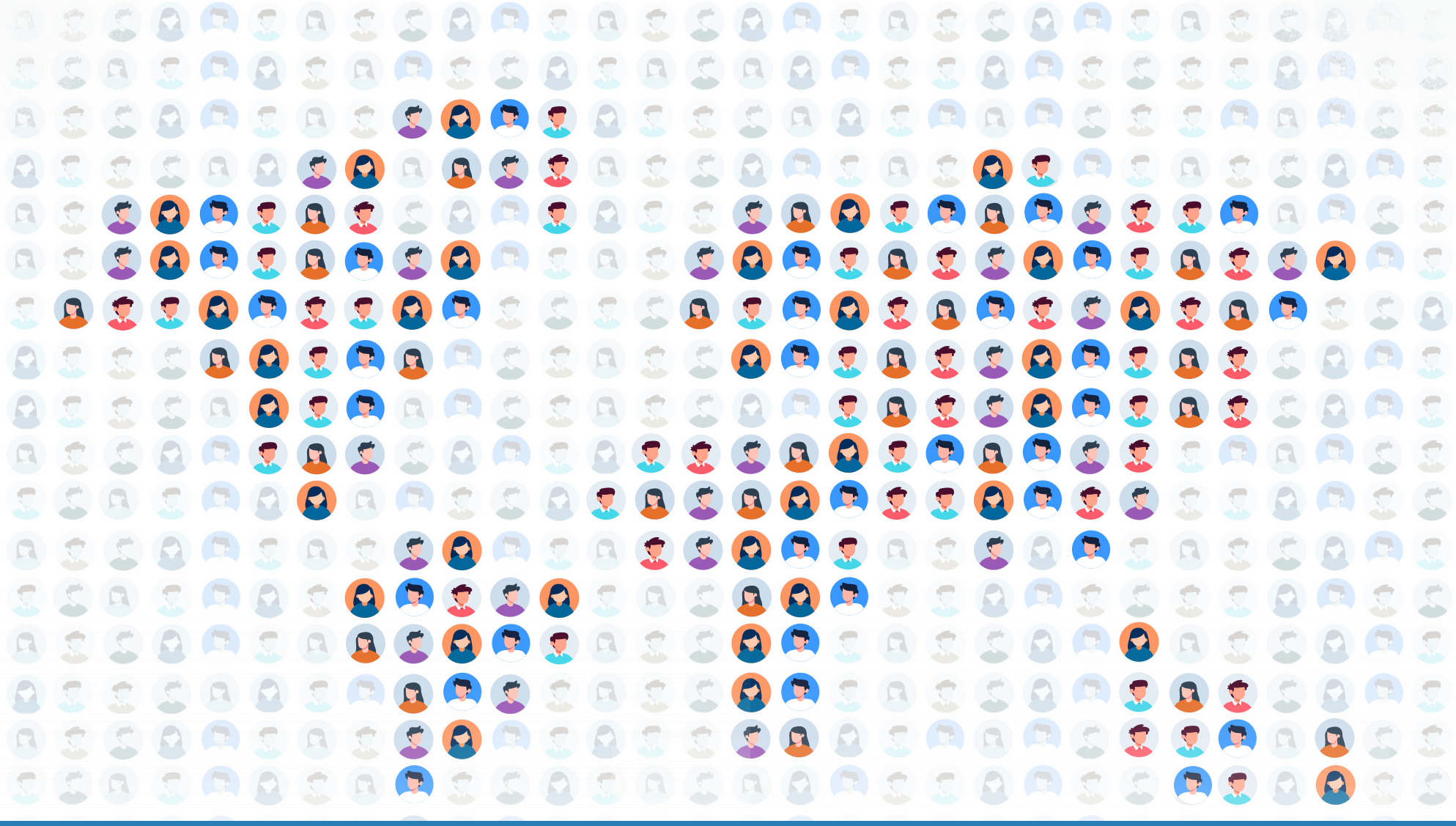
الاحتفاظ بالأدلة: احتفظوا بكل الأدلة المتعلقة بالحوادث، مثل لقطات الشاشة، رسائل البريد الإلكتروني، والمحادثات، لتكونوا قادرين على تقديمها عندما تحتاجون.

- الإبلاغ عن الإساءة والتحرش عبر المنصات: تقدم مواقع التواصل الاجتماعي، مزودو البريد الإلكتروني، وتطبيقات المراسلة عادةً آليات للإبلاغ عن السلوك المسيء. يمكن أن يؤدي الإبلاغ إلى تعليق حساب المعتدي ويقلل من تعرضكم للتهديدات المستقبلية. من المهم تقديم الإبلاغ من حساب الضحية نفسه، والإبلاغات من الأصدقاء ستدعم التقرير الأصلي.
- إبلاغ السلطات القانونية في حالات التهديدات الجسدية: إذا تصاعدت التهديدات إلى مستوى يشكل تهديدًا للسلامة الشخصية، مثل التهديدات الجسدية أو الملاحقة الإلكترونية، من المهم إشراك السلطات القانونية.

- التعرف على قوانين الملاحقة الإلكترونية والموارد المتاحة في بلدكم: تمتلك معظم الدول اليوم قوانين تغطي الملاحقة الإلكترونية، والتحرش، والتهديدات عبر الإنترنت. تحققوا من الموارد القانونية أو منظمات الأمان الرقمي في بلدكم لفهم حقوقكم القانونية والخيارات المتاحة لكم.
- التواصل مع منظمات الحقوق الرقمية والمناصرة في بلدكم ومنطقتكم: قد يكون لهذه المنظمات خبرة في التعامل مع حالات مشابهة، ويمكنها توفير الموارد والدعم، خاصة مساعدتكم على فهم قوانين الخصوصية والحقوق الأساسية.

المساعدة متاحة، وطلبها خطوة جيدة نحو استعادة السيطرة والسلام النفسي

لا يجب مواجهة التهديدات الرقمية وحدكم. اتخاذ الخطوات الصحيحة، مثل الإبلاغ عن التهديدات وطلب الدعم النفسي والقانوني، يساعد في تعزيز الأمن الرقمي والصحة النفسية. يمكنكم التعافي بسرعة، بناء مرونتكم النفسية، وزيادة إحساسكم بالأمان من خلال طلب المساعدة المناسبة والمضي قدمًا بخطوات ثابتة نحو بيئة رقمية أكثر أمانًا.



مؤسسة مهارات

العنوان:
جديدة، المتن
لبنان

معلومات التواصل:
الموقع الإلكتروني: maharatfoundation.org
البريد الإلكتروني: info@maharatfoundation.org

مهارات
Maharat