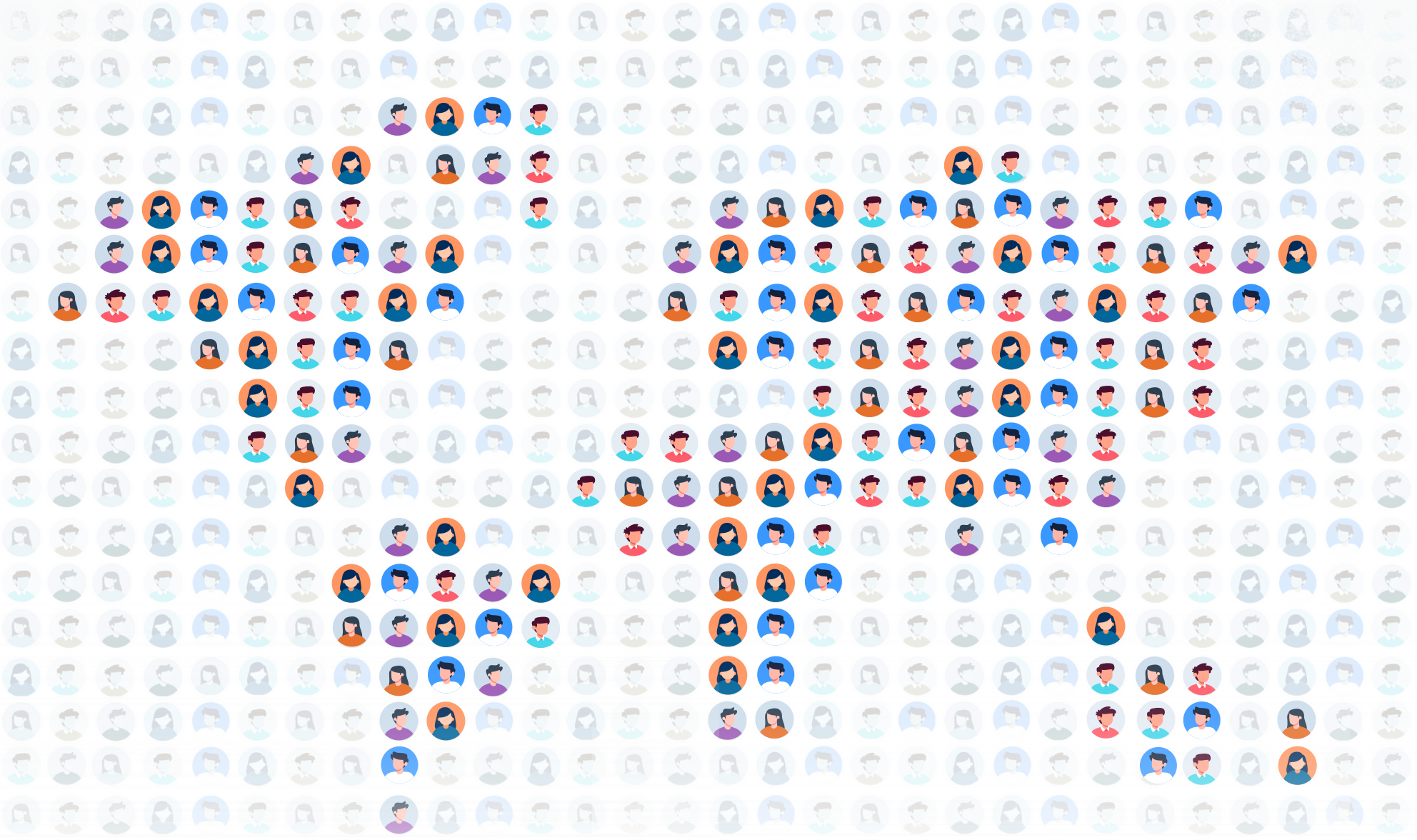


دليل الأمن الرقمي

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 ٩

أفضل الممارسات:
التحديثات المنتظمة، كلمات المرور القوية، استخدام البرمجيات المرخصة والتحقق بخطوتين.

إعداد:
خبير في الأمن الرقمي بهاء نصر

أخذ السلامة الجسدية والأمن الرقمي في الاعتبار أمر أساسي للصحافيين/ت والناشطين/ات وأي شخص يعمل في بيئات حيث تكون السلامة الشخصية وأمن المعلومات في خطر.
يمكن للتهديدات والهجمات الإلكترونية أن يكون لها تأثير كبير على حياتنا. كما يمكن للهجمات الجسدية ان تعرض أمننا الرقمي للخطر، مثلما يحدث عند سرقة، مصادرة أو تفتيش الأجهزة. لذلك، من المهم اتباع نهج شامل لتعزيز الرفاهية العامة والأمن الشخصي.

النقاط التالية ستساعدكم على تحسين سلامتكم الجسدية والرقمية:

1. ابدأوا بتقييم شامل للمخاطر

تحديد التهديدات المحتملة

فكروا في المخاطر الجسدية (مثل المراقبة، الاحتجاز، أو الهجوم الجسدي) والمخاطر الرقمية (مثل الاختراق، مصادرة الأجهزة، أو تتبع الموقع). ضعوا قائمة بالتهديدات المحددة الشائعة في مناطقكم والمرتبطة بأوضاعكم الشخصية، وطبيعة عملكم.

محلية خططكم الأمنية

تختلف المخاطر من مكان إلى آخر، لذا قوموا بتقييم احتياجات الأمن الجسدي والرقمي وفقاً لكل موقع ستعملون فيه أو تسافرون إليه.

تقييم مصادر التهديد

حددوا الجهات التي قد تمثل خطراً عليكم: هل هم جهات حكومية؟ شركات؟ أفراد؟ أطراف مسلحة؟ تختلف الاحتياطات المطلوبة لأمنكم الجسدي والرقمي بناءً على ما إذا كنتم قلقين من صديق ابتعد عنكم أو حكومة قوية. تعتمد شدة تدابير الأمان التي تحتاجون إلى اتخاذها على مدى الموارد والاصرار الذي تمتلكه الجهات المهددة.

RISK ASSESSMENT

2. استخدموا أجهزة آمنة ومنفصلة

أجهزة مخصصة للعمل الحساس

احتفظوا بالأعمال الحساسة على أجهزة منفصلة مخصصة فقط للاتصالات أو البيانات الآمنة. يساعد هذا التقسيم على تقليل مخاطر الخلط بين البيانات الشخصية والمهنية أو تسريب المعلومات عن طريق الخطأ.

تهيئة إعدادات أمان الأجهزة

قوموا بتفعيل تشفير القرص الصلب الكامل، واستخدموا كلمات مرور قوية على جميع الأجهزة، وفعلوا التحقق بخطوتين عند توفرها. تأكدوا من إيقاف خدمات الموقع ما لم تكن ضرورية، وحددوا أذونات التطبيقات لمنع تسرب البيانات في الخلفية.

استخدام أجهزة مؤقتة أو احتياطية

استخدموا هواتف احتياطية وحسابات بريد إلكتروني مؤقتة للمهام عالية المخاطر. تخلصوا من هذه الأجهزة بشكل آمن بعد الانتهاء أو احتفظوا بها مغلقة عند عدم الحاجة إليها.

3. اضمنوا اتصالات آمنة ومجهولة

استخدام قنوات مشفرة للاتصالات الرقمية

استخدموا تطبيقات مشفرة من طرف إلى طرف مثل "Signal" للتواصل في الأمور الحساسة، وقوموا بتغيير الإعدادات لاستخدام اسم مستخدم بدلاً من رقم الهاتف، وفعّلوا الرسائل ذاتية الاختفاء. تجنبوا استخدام وسائل التواصل الاجتماعي أو الحسابات الشخصية للتواصل الحساس.

تجنب شبكات Wi-Fi المفتوحة

تعد الشبكات العامة عرضة لهجمات "الرجل في الوسط" (MitM). استخدموا شبكة خاصة أو شبكة افتراضية خاصة (VPN) عند الإمكان.

حذف سجلات الاتصالات بانتظام

احذفوا الرسائل وسجلات المكالمات من أجهزتكم لتقليل التعرض في حال فقدان الجهاز أو سرقته أو مصادرته. فعّلوا ميزة الرسائل ذاتية الاختفاء كلما كان ذلك ممكنًا.

4. نسقوا الحركة الجسدية وخصوصية الموقع

الحد من إمكانية تتبع موقعكم

قوموا بتعطيل تتبع الموقع على أجهزتكم وتجنبوا تسجيل الدخول على وسائل التواصل الاجتماعي التي تكشف عن مواقعكم. ابحثوا عن وظائف تتبع مخفية في التطبيقات التي قد لا تتوقعوا أن يتم تتبعكم فيها.

اختيار أماكن اجتماعات آمنة

خططوا لاجتماعاتكم في أماكن آمنة وخاصة تقل فيها احتمالية وجود مراقبة. إذا كنتم قلقين، فكروا في تغيير المكان في اللحظة الأخيرة، وتجنبوا الإعلان عن أماكن الاجتماعات بشكل علني. تجنبوا استخدام الفنادق أو الأماكن العامة لعقد الاجتماعات الحساسة، حيث يمكن أن يكون الموظفون معرضين لضغوط للإبلاغ عنكم. استخدموا طرقًا وأماكن تساعدكم في تجنب التتبع أو المراقبة.

وضع خطة طوارئ

أبلغوا جهات اتصال موثوقة بمكانكم ووقت عودتكم المتوقع، واتفقوا على أوقات للتحقق في الحالات التي قد تكونون فيها في خطر. استخدموا كلمات سرية أو رموز خاصة لتعزيز الأمان إذا كنتم قلقين بشأن الاحتجاز أو المراقبة.

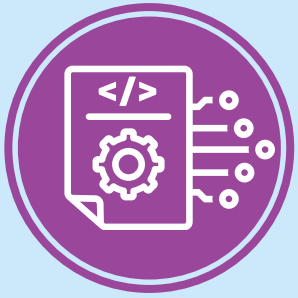
5. اتبعوا ممارسات قوية للأمان

اتباع مبدأ "محدودية الحاجة إلى المعرفة"

شاركوا المعلومات الأساسية فقط مع أعضاء الفريق أو المصادر. كلما قل عدد الأشخاص الذين يعرفون التفاصيل الحساسة، قلت فرص الكشف العرضي أو القسري عنها.

تأمين أماكن العمل المادية

إذا كنتم تعملون في مكتب أو موقع يمكن أن يتعرض للاختراق، قللوا من الوصول المادي إلى المواد الحساسة، وضعوا الشاشات بعيدة عن أنظار العامة، واستخدموا فلاتر الخصوصية للشاشات.



6. انتبهوا إلى البيانات الوصفية (Metadata)

إزالة البيانات الوصفية من الملفات

قبل مشاركة الملفات أو الصور، قوموا بإزالة البيانات الوصفية التي يمكن أن تكشف عن معلومات حساسة مثل أسماء المصادر، الأوقات، المواقع، وبيانات الأجهزة.

7. شفروا جميع البيانات على الأجهزة والنسخ الاحتياطية

تشفير الأقراص الصلبة والتخزين الخارجي

قوموا بتفعيل تشفير كامل للقرص الصلب على جميع أجهزتكم (مثل الحواسيب المحمولة، الهواتف، وحدات التخزين USB). يضمن ذلك بقاء بياناتكم غير قابلة للوصول حتى في حالة فقدان الأجهزة أو مصادرتها. احرصوا دائمًا على قفل أجهزتكم عندما لا تستخدمونها، وقوموا بإيقاف تشغيلها قبل تسليمها للآخرين لتوفير حماية إضافية.

تأمين النسخ الاحتياطية بالتشفير

تأكدوا من أن النسخ الاحتياطية المحلية والسحابية مشفرة ومخزنة بشكل آمن لحمايتها من الوصول غير المصرح به. في أوقات الحرب أو التدمير المادي، قد تكون النسخ الاحتياطية السحابية الخيار الأكثر أمانًا، حيث يمكن أن تتعرض التخزينات المحلية للتلف أو الفقدان أو السرقة. عند اختيار خدمة تخزين سحابي، اختاروا خدمة توفر التشفير من طرف إلى طرف مثل Tresorit أو Proton Drive.

استخدام كلمات مرور قوية وفريدة

قوموا باستخدام كلمات مرور قوية لجميع الأجهزة والحسابات. تجنبوا استخدام نفس كلمة المرور لأكثر من حساب. هل تجدون صعوبة في تذكرها جميعًا؟ استخدموا مدير كلمات مرور لإنشاء كلمات مرور فريدة وتخزينها بشكل آمن.

8. خططوا لنقل البيانات بشكل آمن

استخدام روابط تخزين سحابي مؤقتة

عند إرسال الملفات عبر الإنترنت، استخدموا خدمات تخزين آمنة مثل Tresorit أو Proton Drive. تجنبوا تخزين البيانات الحساسة بشكل دائم على منصات السحابة الشائعة التي تفتقر إلى أمان قوي.

استخدام طرق نقل ملفات آمنة

اعتمدوا أدوات مشاركة الملفات المشفرة مثل OnionShare أو SecureDrop.

التحقق من أمان الشبكة للبيانات الحساسة

عند تحميل أو تنزيل بيانات حساسة، تجنبوا استخدام الشبكات غير الآمنة. استخدموا شبكات VPN، أو متصفح Tor لمزيد من الخصوصية.

تقييد أذونات الوصول للملفات

امنحوا حق الوصول إلى الملفات للأشخاص الضروريين فقط، وحددوا تواريخ انتهاء صلاحية الروابط أو الملفات المشتركة عند استخدام منصات التخزين عبر الإنترنت.

9. راقبوا التهديدات واتخذوا الخطوات المناسبة

تفعيل تنبيهات التهديدات

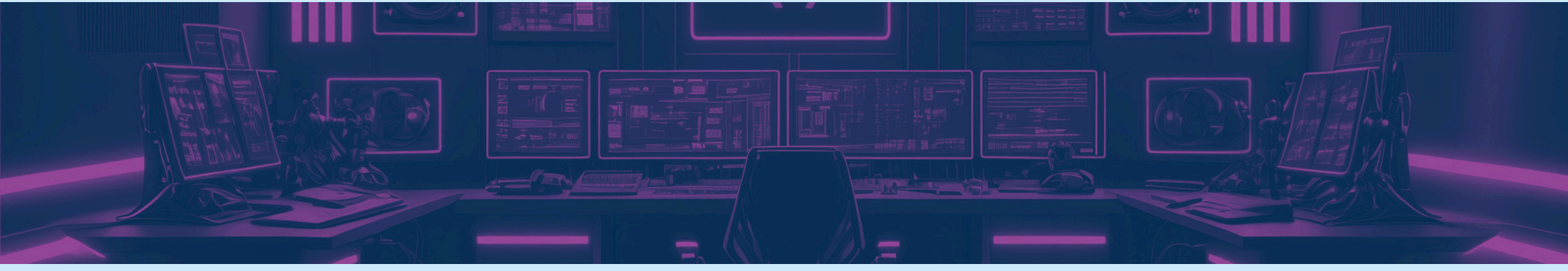
راقبوا الأخبار المتعلقة باختراق البيانات، العيوب الأمنية، أو التهديدات الجديدة التي قد تؤثر عليكم. يمكن لأدوات مثل "Have I Been Pwned" تنبيهكم إذا تم اختراق إحدى كلمات المرور الخاصة بكم.

إجراء فحص أمني دوري

راجعوا بانتظام البروتوكولات الأمنية المطبقة لحمايتكم الجسدية والرقمية، خاصةً عند العمل في بيئات عالية الخطورة. قوموا بتحديث كلمات المرور، مراجعة أذونات الوصول، والتحقق من قنوات الاتصال.

الاستعداد لأسوأ السيناريوهات

خططوا لحالات الطوارئ المحتملة (مثل مصادرة الأجهزة، المخاطر القانونية، أو التهديدات الجسدية). على سبيل المثال، تعلموا كيفية إجراء مسح بيانات الأجهزة عن بُعد لحماية البيانات الحساسة في حالة فقدانها أو مصادرتها أو سرقتها.



10. أمنوا الدعم القانوني وخطة للاستجابة للحوادث

استشارة قانونية بشأن حقوق الخصوصية الرقمية

اطلعوا على الحماية القانونية والقواعد المرتبط بتفتيش الأجهزة، المراقبة، والاحتفاظ بالبيانات في بلدكم أو أي بلد ستعملون فيه.

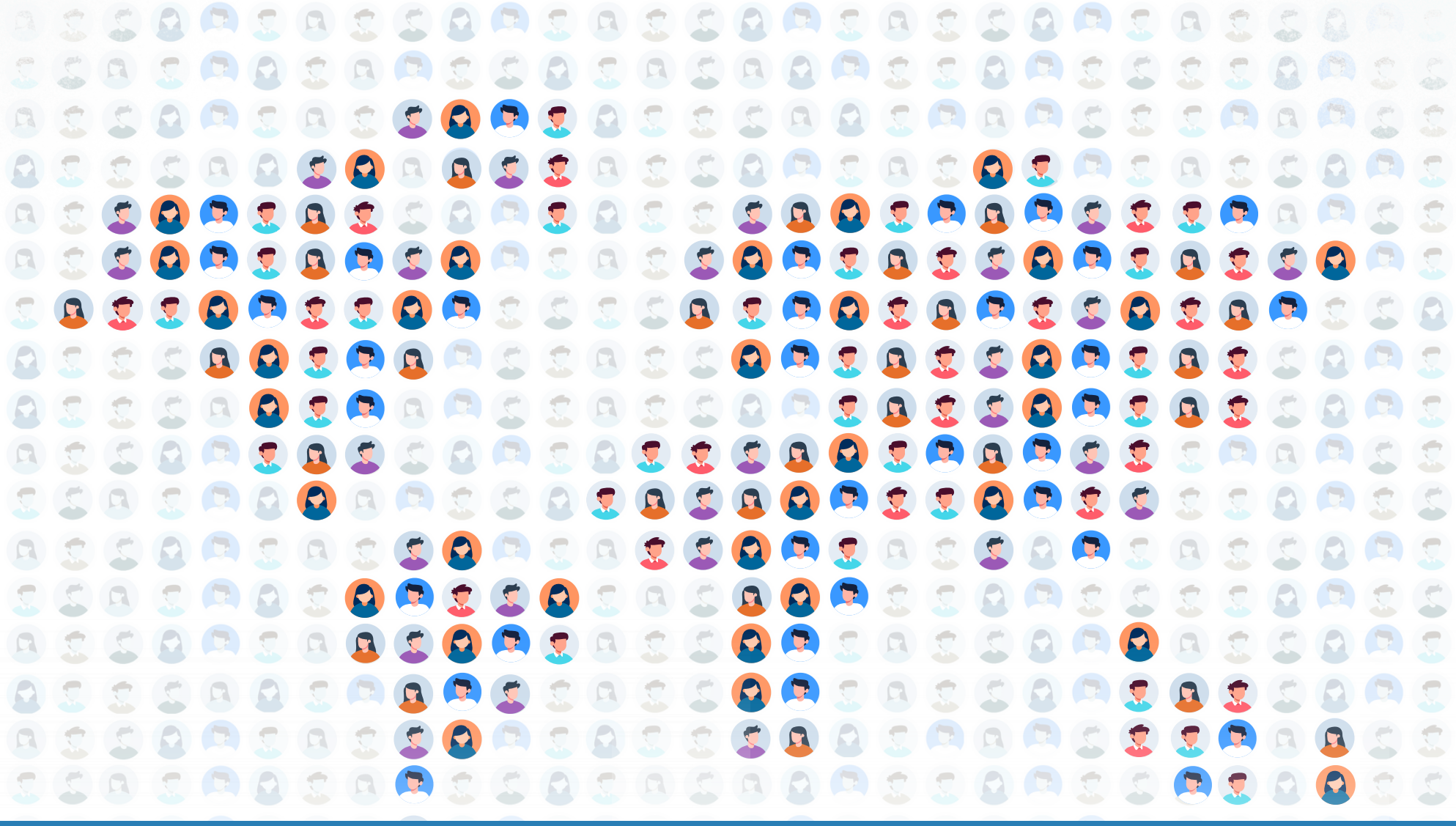
تطوير خطة استجابة للمصادرات أو الاحتجاز

حددوا الخطوات التي ستتخذونها إذا تمت مصادرة الأجهزة أو إذا تم احتجازكم أنتم أو أحد أفراد فريقكم. كونوا مستعدين من خلال إنشاء نسخ احتياطية مشفرة، وتأكدوا أنه لديكم إمكانية مسح البيانات عن بُعد على أجهزة الهاتف المحمول، وقائمة بجهات الاتصال الطارئة التي يمكنها اتخاذ الإجراءات نيابةً عنكم عند الضرورة.

استخدام أدوات مادية ورقمية مموهة

في الحالات القصوى، فكروا في إستخدام أجهزة أو حسابات مموهة يمكن إظهارها في حالات الطوارئ مع الاحتفاظ بالأجهزة أو الحسابات الرئيسية الآمنة مخفية.

سلامتكم مهمة. كونوا استباقيين، فاتباع هذه الاستراتيجيات سيساعدكم أنتم والمقربين منكم على العمل بأمان أكبر في البيئات العالية الخطورة. رفع مستوى الأمان الخاص بكم يجعل من الصعب على المهاجم المحتمل استهدافكم، ويجنبكم أن تكونوا هدفًا سهلاً.



مؤسسة مهارات

العنوان:
جديدة، المتن
لبنان

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

مهارات
Maharat