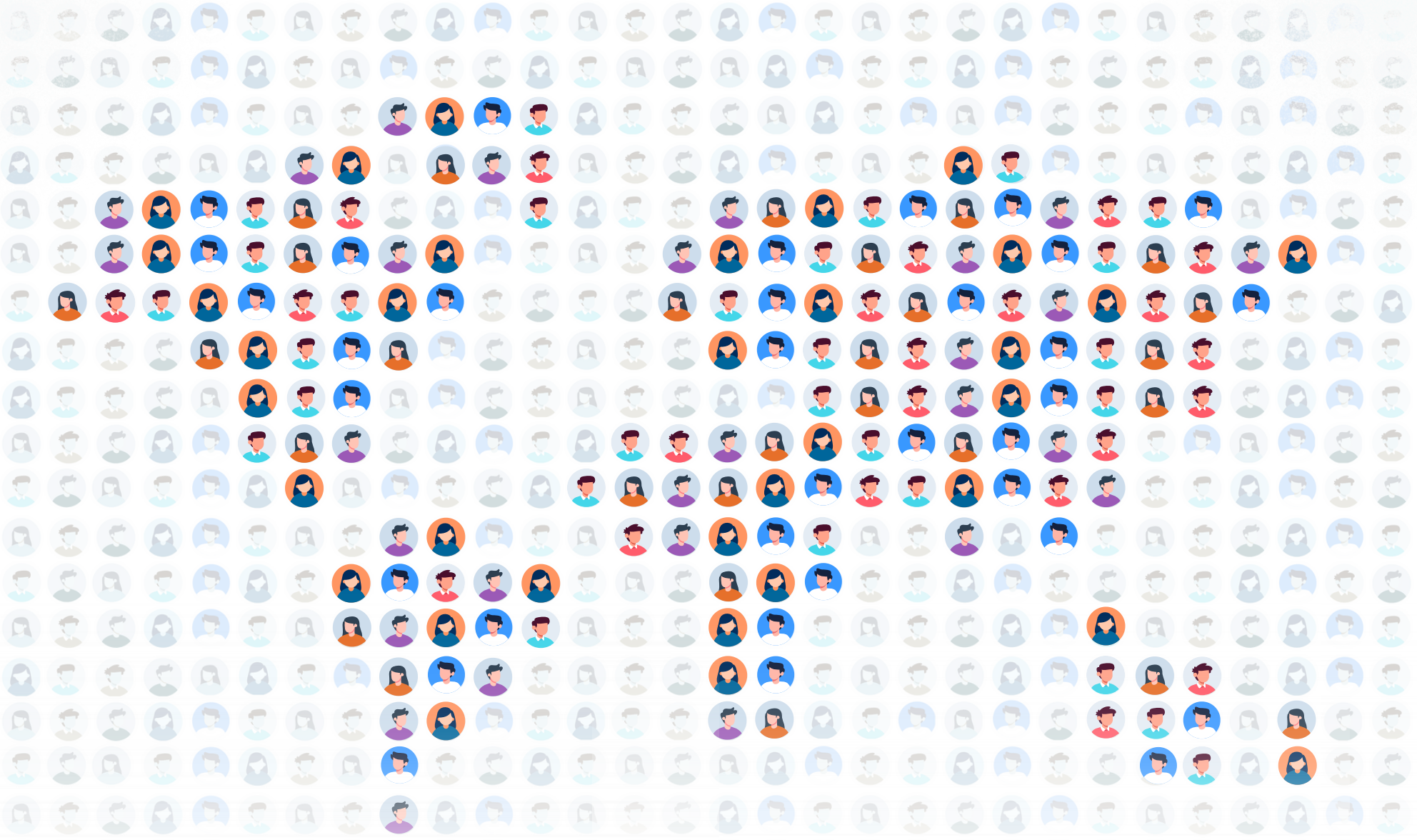


دليل الأمن الرقمي

خارطة الطريق للحماية عبر الإنترنت

مهارات
Maharat

دليل الأمن الرقمي

خارطة الطريق للحماية عبر الإنترنت

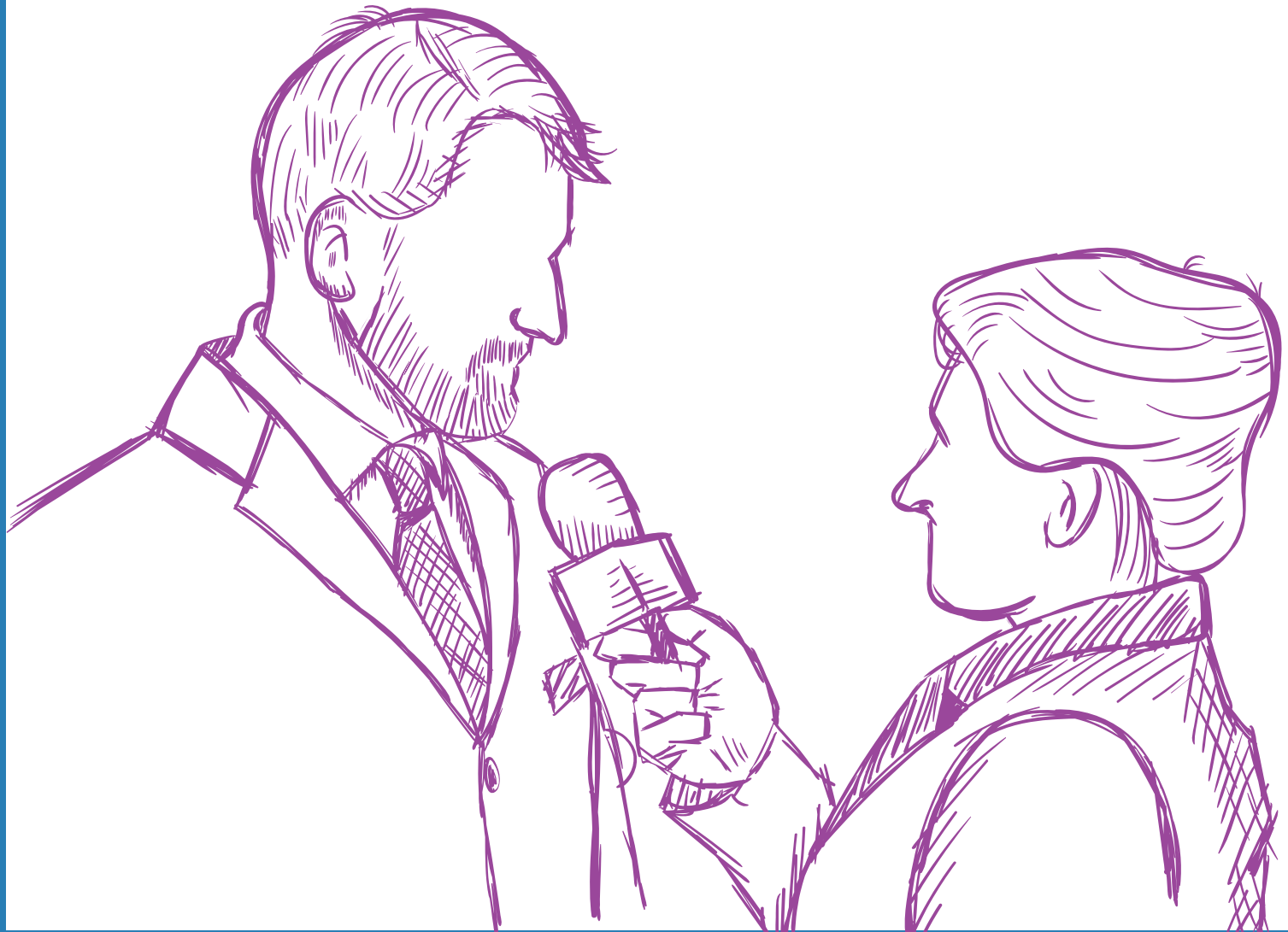
تم إعداد هذا الدليل من قبل مؤسسة مهارات، بدعم من هيئة الأمم المتحدة للمرأة والسفارة الفرنسية في بيروت.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

مهارات
Maharat

UN WOMEN

الجزء V



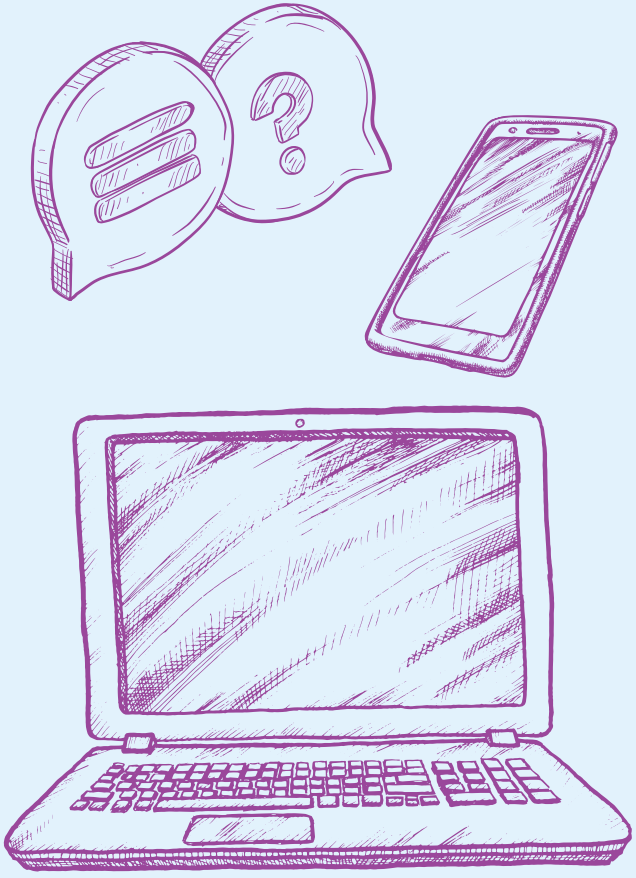
حماية المصادر والمبلغين:
استراتيجيات للحفاظ على سرية وأمان المصادر.

مخصص للصحافيين/ات

إعداد:
خبير في الأمن الرقمي بهاء نصر

غالبًا ما يعتمد الصحافيون/ات على المعلومات السرية والمبلغين لكشف المخالفات. **إن حماية المصادر والمبلغين عن المخالفات بالغ الأهمية للحفاظ على الثقة**، وبالتالي يجب على الصحافيين/ات التأكد من عدم الكشف عن مصدر المعلومات عن غير قصد والحفاظ على سرية وأمن مصادرهم.

كيفية حماية الصحافيين، المصادر والمبلغين عن المخالفات:



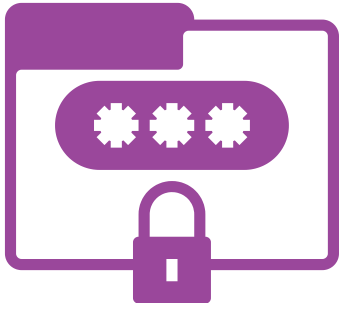
يرجى الملاحظة: ان النصائح المذكورة أدناه هي بنفس الأهمية لكل من الصحافيين والمبلغين.

إنشاء قنوات اتصال آمنة

استخدموا تطبيقات مراسلة مشفرة:

- استخدموا تطبيقات المراسلة المشفرة مثل "سيغنال" للتواصل مع المصادر، للحفاظ على خصوصية المحادثات. يوصى باستخدام سيغنال بشكل خاص بسبب ممارساته الأمنية القوية وقلة حفظ البيانات الوصفية.
- فعلوا الرسائل التي تختفي تلقائيًا لحذف المحادثات بعد فترة زمنية محددة.
- تجنبوا استخدام البريد الإلكتروني أو الهواتف الثابتة أو المكالمات الهاتفية أو الرسائل النصية للمراسلات الحساسة، حيث إنها أقل أمانًا ويمكن مراقبتها وتتبعها بسهولة.

- قوموا بإنشاء طريقة آمنة لإجراء التواصل الأول مع المصادر وذلك عبر البريد الإلكتروني المشفر أو حساب سيغنال. هناك أيضًا تطبيقات متخصصة للمبلغين توفر "صناديق بريد آمنة".
- يجب أن يتمكن المبلغون من تقديم المعلومات بشكل مجهول دون الخوف من التتبع أو من امكانية التعرف عليهم. أدوات مثل "SecureDrop" أو "GlobaLeaks" هي أدوات ممتازة لهذا الغرض. يجب على الصحافيين الاستقصائيين تثبيت هذه الأدوات على مواقعهم الإلكترونية مع دليل سهل الفهم حول كيفية استخدامها، وتحذير واضح للمبلغين لعدم إرسال المعلومات عبر قنوات اخرى غير آمنة.
- يجب على المبلغين تجنب استخدام الأجهزة أو الإنترنت في مكان العمل لتسريب المعلومات، اذ قد تكون هذه الأجهزة والشبكات مراقبة. بل عليهم استخدام الأجهزة الشخصية والشبكات الخاصة الآمنة كلما أمكن ذلك.



استخدموا خدمات البريد الإلكتروني المشفرة

إذا كانت المراسلة عبر البريد الإلكتروني ضرورية، استخدموا خدمات مشفرة مثل "ProtonMail"، التي تقدم تشفيرًا من طرف إلى طرف. من أجل أمان أفضل، يجب أن يكون الطرفان يستخدمان "ProtonMail".

ممارسات الأمن الرقمي

تعلموا وطبقوا ممارسات قوية للأمن الرقمي لحماية أجهزتكم وبياناتكم وتتضمن هذه الممارسات

استخدام كلمات مرور قوية ومعقدة ومميزة لجميع حساباتكم، وتحديث الأجهزة والبرامج بانتظام لسد أي ثغرات أمنية، وتفعيل التحقق بخطوتين لتعزيز الحماية. يجب تشفير الملفات الحساسة على اجهزتكم.

احفظوا البيانات بشكل آمن

استخدموا التشفير لحفظ ملفاتكم ومستنداتكم عندما تكون المعلومات حساسة. يمكنكم استخدام تطبيقات مثل Veracrypt لإنشاء حاوية مشفرة لحفظ جميع البيانات الحساسة داخلها، مما يجعلها مثل خزنة آمنة للملفات.

من المهم ايضا حذف البيانات التي زودتكم بها المصادر بشكل دائم وآمن عند الطلب أو عندما تنتفي الحاجة منها. يمكن استخدام أدوات مثل BleachBit لحذف الملفات بشكل دائم وجعلها غير قابلة للاسترجاع، حيث إن الحذف عبر سلة مهملات الكومبيوتر لن يزيل الملفات بشكل دائم ويمكن استعادتها باستخدام أدوات رقمية.

قللوا من الآثار الرقمية

تجنبوا استخدام الأجهزة الخاصة بالعمل لأي أمور متعلقة بموضوع التبليغ، وقوموا بمسح سجل التصفح وتعطيل تتبع الموقع على أجهزتكم لتقليل إمكانية ترك أثر لكم.

استخدموا اسماء مستعارة

تجنبوا استخدام الأسماء الحقيقية في المراسلات، ويفضل استخدام أسماء مستعارة أو ألقاب لابقاء الهويات بأمان اكبر.

استخدموا الشبكات الافتراضية الخاصة (VPNs)

تخفي شبكات الـ VPN عناوين البوتوكولات IP وتشفّر الإنترنت، مما يصعّب على المخترقين أو الجهات الحكومية مراقبة أنشطتكم على الإنترنت أو تتبع مواقعكم. استخدموا VPN خاصة عند الاتصال بالإنترنت في الأماكن العامة، ولكن من المهم معرفة سياسات حفظ البيانات وسياسات المشاركة للشبكات الافتراضية المستخدمة، حيث قد تقوم بعض الشركات بتخزين بيانات حساسة وتسليمها للجهات المختصة عند الطلب.

استخدموا متصفح Tor لابقاء هويتكم مغفلة

يوفر Tor درجة عالية من اخفاء الهوية عن طريق توجيه حركة المرور عبر خوادم متعددة. ويمكن للصحافيين والمصادر على حد سواء استخدامه للوصول إلى الإنترنت بشكل مغفل.

حماية الهوية المغفلة

دافعوا عن الهوية المغفلة عند طلبها من المصادر. اتخذوا احتياطات إضافية عند مشاركة أي معلومات أو التعامل مع الاتصالات أو الاجتماعات مع المبلغين لتجنب الكشف عن هويتهم عن طريق الخطأ. تأكدوا من أن القصة التي يتم نشرها بناءً على المعلومات المقدمة من المبلغين لا تحتوي على أي معلومات شخصية يمكن أن تكشف عن مصدر المعلومات.

مارسوا مبدأ "الحاجة إلى المعرفة فقط"، أي اجعلوا النقاشات المتعلقة بالمعلومات الحساسة مقتصرة على الأشخاص الضروريين فقط لإنجاز القصة، حتى داخل منظمتكم أو مع أقرب الأشخاص لكم.

تجنبوا استخدام معلومات تعريفية في مساحات العمل المشتركة، وقوموا بإزالة جميع المؤشرات الشخصية مثل الأسماء والعناوين أو تفاصيل العمل المحددة التي قد تكشف هوية المصدر من المستندات المشتركة بين المصادر والصحافيين. إذا كنتم تعملون ضمن فريق، تجنبوا تخزين تفاصيل المصادر في مساحات العمل الرقمية المشتركة أو قواعد البيانات غير الآمنة.

ممارسات صحية للتعامل مع البيانات الوصفية

قوموا بإزالة البيانات الوصفية من الملفات:

غالبًا ما تحتوي الصور والمستندات ومقاطع الفيديو على بيانات وصفية يمكن أن تكشف عن اسم الشخص الذي أنشأ الملف، أو آخر من قام بتحريره أو حفظه، أو العلامة التجارية ورقم أو نوع الجهاز المستخدم، أو الموقع، أو وقت وتاريخ الإنشاء، بالإضافة إلى معلومات تعريفية أخرى قد توفر أدلة تؤدي إلى كشف هوية المُبلِّغ. احذفوا البيانات الوصفية من خصائص الملفات قبل مشاركتها أو نشرها.

قللوا الآثار الرقمية وحفظ السجلات

تجنبوا استخدام التخزين السحابي للملفات الحساسة:
احفظوا الملفات الحساسة على أجهزة محلية أو في مواقع تخزين آمنة ومشفرة بدلًا من الخدمات السحابية العامة التي قد يمكن الوصول اليها من قبل أطراف ثالثة.

احذفوا سجلات الاتصالات:
احذفوا بانتظام الرسائل وسجلات المكالمات وتاريخ التواصل لتقليل خطر الكشف في حالة مصادرة الأجهزة أو اختراقها.

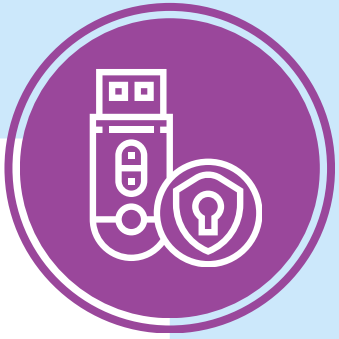
استخدموا أجهزة منفصلة للعمل الحساس:
إذا كان ذلك ممكنًا، استخدموا أجهزة مخصصة فقط للتواصل مع المصادر لإبقاء العمل الحساس منفصلًا عن الأنشطة الشخصية أو الأقل حساسية.

استخدموا هواتف مؤقتة:
يمكن للهواتف المؤقتة تقليل إمكانية التتبع والحماية من التنصت.

حماية السلامة الشخصية وخصوصية الموقع

أوقفوا خدمات تحديد الموقع:
تأكدوا من إيقاف تتبع الموقع على الأجهزة المحمولة.

اجتمعوا في مواقع آمنة وخاصة:
بالنسبة للمحادثات شديدة الحساسية، يُفضل الاجتماع شخصيًا بدلاً من التواصل إلكترونيًا. اختاروا مواقع خاصة وغير مرتبطة بالصحافي/ة أو المصدر، وتجنبوا الأماكن التي تحتوي على كاميرات مراقبة أو مراقبة عامة قد تلتقط التفاعلات. استخدموا قنوات اتصال آمنة للاتفاق على مكان الاجتماع.



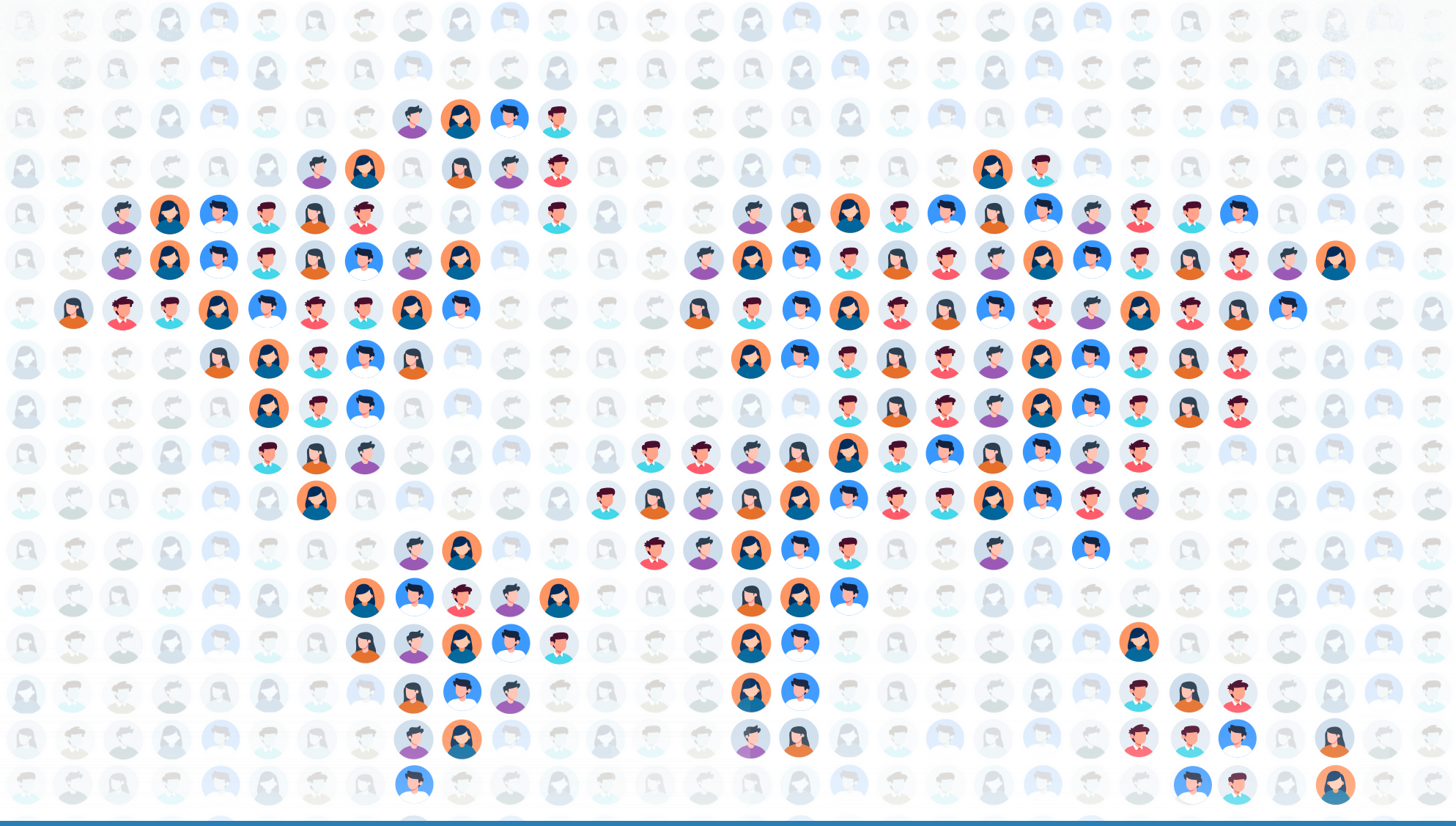
إنشاء نسخ احتياطية وخطط طوارئ

احفظوا النسخ الاحتياطية في مواقع آمنة:
قوموا دائمًا بإنشاء نسخ احتياطية من الملفات والمستندات والتسجيلات الهامة واحفظوها في جهاز خارجي مشفر وآمن. هذا يضمن وجود نسخة من المعلومات الهامة في حال تعرض المصادر الأساسية للتلف أو المصادرة أو السرقة.

ضعوا خطط طوارئ:
خططوا للتعامل مع المواقف التي قد يواجه فيها الصحافي أو المصدر مخاطر قانونية أو يُعتقل. اتفقوا على إجراءات محددة، مثل حذف البيانات الحساسة أو التواصل مع جهات قانونية موثوقة، إذا كان أي من الطرفين عرضة للخطر.

فهم الحماية القانونية والمخاطر

تعرفوا على قوانين حماية المبلغين ذات الصلة، حيث تختلف هذه القوانين حسب القطاع والاختصاص القضائي.
اعلموا أنه لا توجد قوانين دولية شاملة لحماية المبلغين، وأن الحماية قد تختلف بين موظفي القطاع الخاص والعام وكذلك حسب الدولة.



مؤسسة مهارات

العنوان:
جديدة، المتن
لبنان

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

مهارات
Maharat