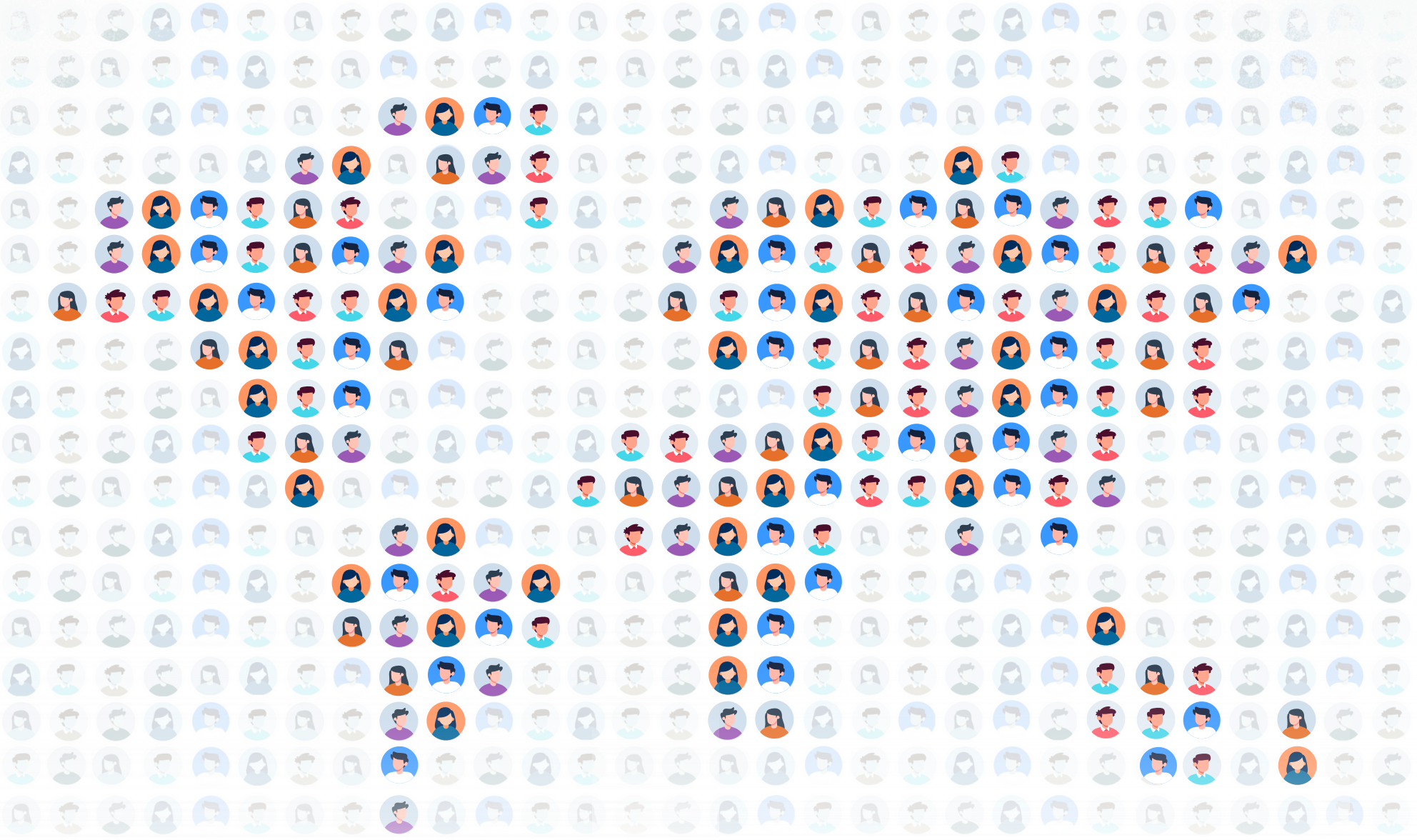


دليل الأمن الرقمي

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

٨

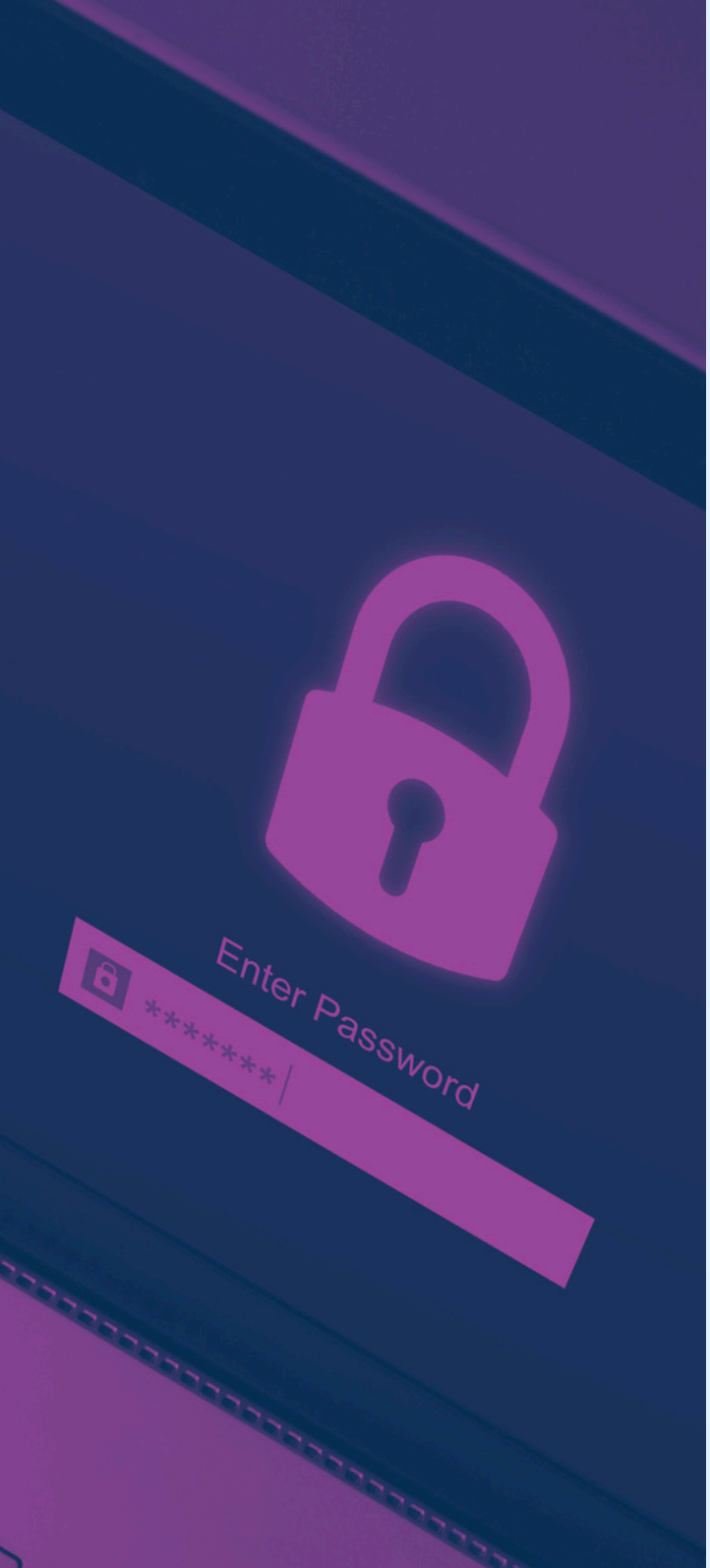
التخطيط للاستجابة للحوادث: تطوير خطة الاستجابة للحوادث الأمنية الرقمية

إعداد:
خبير في الأمن الرقمي بهاء نصر

أفضل ممارسات الأمن الرقمي

في العصر الرقمي الحالي، نقوم بمعظم أعمالنا على أجهزة الكمبيوتر، وعندما لا نعمل، تكون أجهزتنا المحمولة غالبًا في متناول أيدينا. **من الأنشطة المهنية إلى الشخصية، نعتمد بشكل كبير على المنصات الرقمية.** ونتيجة لذلك، تضاعفت المخاطر الرقمية التي نتعرض لها، **وأصبح الالتزام بأفضل ممارسات الأمن الرقمي أكثر أهمية من أي وقت مضى لحماية معلوماتنا الشخصية، وأعمالنا، ورفاهيتنا.**

اتباع هذه النصائح سيُحسن بشكل كبير من أمانكم الرقمي ويقلل من مخاطر الوقوع ضحية للقوى الخبيثة أثناء وجودكم على الإنترنت:



1. استخدام كلمات مرور قوية وإدارتها بشكل آمن

- إنشاء كلمات مرور قوية: استخدموا ما لا يقل عن 15 حرفًا مزيجًا من الأحرف الكبيرة والصغيرة والأرقام والرموز. يمكنكم استخدام عبارة مرور سهلة التذكر مثل:
- Ne5na we zou7al jiran!
- الالتزام بكلمة مرور فريدة لكل حساب: لا تعيدوا استخدام كلمات المرور.
- استخدام برامج إدارة كلمات مرور: لتخزين وإنشاء كلمات مرور معقدة بشكل آمن، استخدموا أدوات مثل KeepassXC أو Bitwarden. ستساعدكم هذه الأدوات على استخدام كلمات مرور معقدة وفريدة لكل حساب مع الحاجة لتذكر كلمة مرور رئيسية واحدة فقط.
- تفعيل المصادقة متعددة العوامل (MFA): إعداد طريقة مصادقة ثانية مثل التطبيقات على الهواتف المحمولة أو المصادقة البيومترية (بصمة الإصبع / التعرف على الوجه) يُضيف طبقة إضافية من الأمان إلى حساباتكم وأجهزتكم. أمثلة على ذلك: Google Authenticator أو Twilio Authy Authenticator.

2. حماية أجهزتكم:

- تحديث اجهزتكم بانتظام: قوموا بتحديث أنظمة التشغيل (OS)، والتطبيقات، والبرامج على جميع أجهزتكم بانتظام. تُصدر هذه التحديثات لمعالجة الثغرات الأمنية المعروفة التي يستغلها القراصنة عادة.
- تفعيل التحديثات التلقائية كلما كان ذلك ممكنًا لضمان أن أجهزتكم تعمل دائمًا بأحدث التصحيحات والإصلاحات الأمنية.
- تنزيل البرامج الأصلية فقط من المواقع الرسمية: حتى بالنسبة للبرامج المجانية. ابتعدوا عن البرامج المقرصنة – فقد تدفعون ثمنًا باهظًا لمحاولتكم توفير المال. البرامج المقرصنة عادة لا تُحدّث وقد تحتوي أيضًا على برامج ضارة.
- استخدام برامج مكافحة الفيروسات للحماية من الهجمات الخبيثة. وتأكدوا من وقت لآخر أن برامج مكافحة الفيروسات محدثة وتعمل بشكل صحيح لضمان اكتشاف وإزالة أحدث التهديدات. يمكنكم استخدام Windows Defender أو تثبيت برنامج مكافحة فيروسات معروف وموثوق.
- اقفال الأجهزة بكلمات مرور قوية أو بمصادقة بيومترية لمنع الوصول غير المصرح به، حتى عند ترك الجهاز دون مراقبة لدقيقة واحدة فقط.
- تشفير أجهزتكم: تأكدوا من أن بياناتكم مشفرة لمنع الوصول غير المصرح به في حالة السرقة. قوموا بتشفير الملفات الحساسة باستخدام أدوات مثل BitLocker أو VeraCrypt.

اختيار الأشخاص الموثوق بهم للصيانة: إذا احتاج جهازكم إلى صيانة أو إصلاح، لا تأخذوه إلا لشخص موثوق. تحتوي جميع الأجهزة على الكثير من البيانات الشخصية والحساسة، وسيكون لدى فرق الصيانة امكانية الوصول إلى كل شيء على الجهاز أثناء عملهم عليه.

3. استخدموا تطبيقات الرسائل المشفرة

- استخدموا تطبيقات مثل Signal للتواصل الآمن مع الآخرين.
- توفر هذه التطبيقات التشفير بين الطرفين، مما يعني أنكم والشخص الذي تتواصلون معه فقط يمكنكم قراءة الرسائل، مما يضمن خصوصية محادثاتكم.
- فعلوا خاصية الرسائل المؤقتة أو التلقائية الحذف، التي تقلل من خطر تخزين المعلومات الحساسة أو الوصول إليها في حالة مصادرة جهازكم أو اختراقه.

4. تأمين اتصال الإنترنت الخاص بكم

- **أمنوا الراوتر (Router)**: قد يستغل القراصنة ثغرات في أجهزة او أشياء نتجاهلها عادة او لم نكن نعلم انهم يستطيعون استغلالها للاختراق، مثل جهاز الراوتر. ضعوا الراوتر في مكان آمن لا يمكن للزوار أو المتسللين الوصول إليه بسهولة لمنع أي محاولات للتلاعب به. غيروا كلمة السر الافتراضية الخاصة بالراوتر (Admin) وأعيدوا تعيين كلمة مرور قوية خاصة بكم. فعلوا تشفير WPA3 أو WPA2 في إعدادات الراوتر لتحسين أمان شبكة الواي فاي.
- **لا تشاركوا شبكة الواي فاي الخاصة بكم:** مع الجيران أو الغرباء. تذكروا أن أي شخص لديه امكانية الوصول إلى شبكتكم يمكنه مراقبة نشاطكم عبر الإنترنت.
- استخدموا VPN خاصة في شبكات الواي فاي العامة:
- تقوم الشبكات الافتراضية الخاصة (VPN) بإنشاء اتصال مشفر وآمن بين أجهزتكم والإنترنت، مما يمنع المتنصتين من اعتراض بياناتكم. من شبكات VPN الموثوقة: Proton VPN, Psiphon, Tunnelbear.

5. ممارسة التصفح الآمن وحماية الخصوصية على وسائل التواصل الاجتماعي

- **فكروا قبل النقر:** تجنبوا النقر على الروابط المجهولة. كونوا حذرين من الروابط الموجودة في رسائل البريد الإلكتروني، أو الرسائل النصية، أو المواقع التي قد تؤدي إلى مواقع تصيد احتيالي.
- **تحققوا من وجود HTTPS في المواقع الإلكترونية:** لضمان تشفير المعلومات المرسلة بين متصفحكم والموقع الذي تزورونه.
- **قللوا المعلومات الشخصية التي تشاركونها عبر الإنترنت:** راجعوا إعدادات الخصوصية على منصات التواصل الاجتماعي واضبطوها لتقييد من يمكنه رؤية منشوراتكم وصوركم ومعلوماتكم الشخصية. اقبلوا طلبات الصداقة فقط من الأشخاص الذين تعرفونهم.
- **افصلوا بين حسابات العمل والحسابات الشخصية:** إذا أمكن، استخدموا أجهزة وحسابات مختلفة للأنشطة الشخصية والعملية. راقبوا نشاط الحسابات بانتظام، وافحصوا سجلات الوصول للحسابات لاكتشاف أي نشاط مشبوه. فعلوا تنبيهات الحساب للحصول على إشعارات حول تسجيلات الدخول، أو تغييرات لكلمات المرور، أو أي نشاط مريب.

6. احذروا من محاولات التصيد الاحتيالي

يستخدم المهاجمون رسائل البريد الإلكتروني، أو الرسائل النصية، أو المكالمات الهاتفية المخادعة لخداع ضحاياهم للكشف عن معلومات حساسة أو تنفيذ إجراءات تضر بأمنهم أو تتسبب بخسارة أموالهم. غالبًا ما تستهدف هذه الحيل الصحافيين/ات والناشطين/ات لإغرائهم بمشاركة معلومات أو مصادر حساسة. تحققوا من هذه الطلبات وتأكدوا منها باستخدام طريقة تواصل مختلفة، على سبيل المثال، إذا شككتم في بريد إلكتروني، تحققوا منه عبر مكالمة باستخدام تطبيق Signal.

- تحققوا من عنوان البريد الإلكتروني للمرسل وابحثوا عن أي تناقضات أو انتحال.
- تجنبوا النقر على الروابط المجهولة، مرروا الفأرة فوق الروابط للتحقق من وجهتها قبل النقر.
- لا تقوموا بتنزيل المرفقات المجهولة المصدر، فقد تحتوي على برمجيات ضارة.
- أبلغوا عن محاولات التصيد لمنظمتكم أو لمزود البريد الإلكتروني.
- علموا أنفسكم وأعضاء فريقكم كيفية التعرف على التصيد الاحتيالي، وابقوا على اطلاع حول الأساليب الشائعة المستخدمة.

7. النسخ الاحتياطي للبيانات بانتظام

- استخدموا مزيجًا من النسخ الاحتياطية السحابية والمحلية لتخزين نسخ من البيانات الحساسة والمهمة على أقراص خارجية مشفرة أو على منصات سحابية آمنة.
- قوموا بأتمتة النسخ الاحتياطي أو ضعوا جدولًا منتظمًا لإجراء النسخ الاحتياطي لتقليل خطر فقدان البيانات.
- اختبروا دائمًا النسخ الاحتياطية للتأكد من أنها تعمل بشكل صحيح ويمكنكم استرداد الملفات عند الحاجة.

8. حذف البيانات والتخلص من الأجهزة بشكل آمن

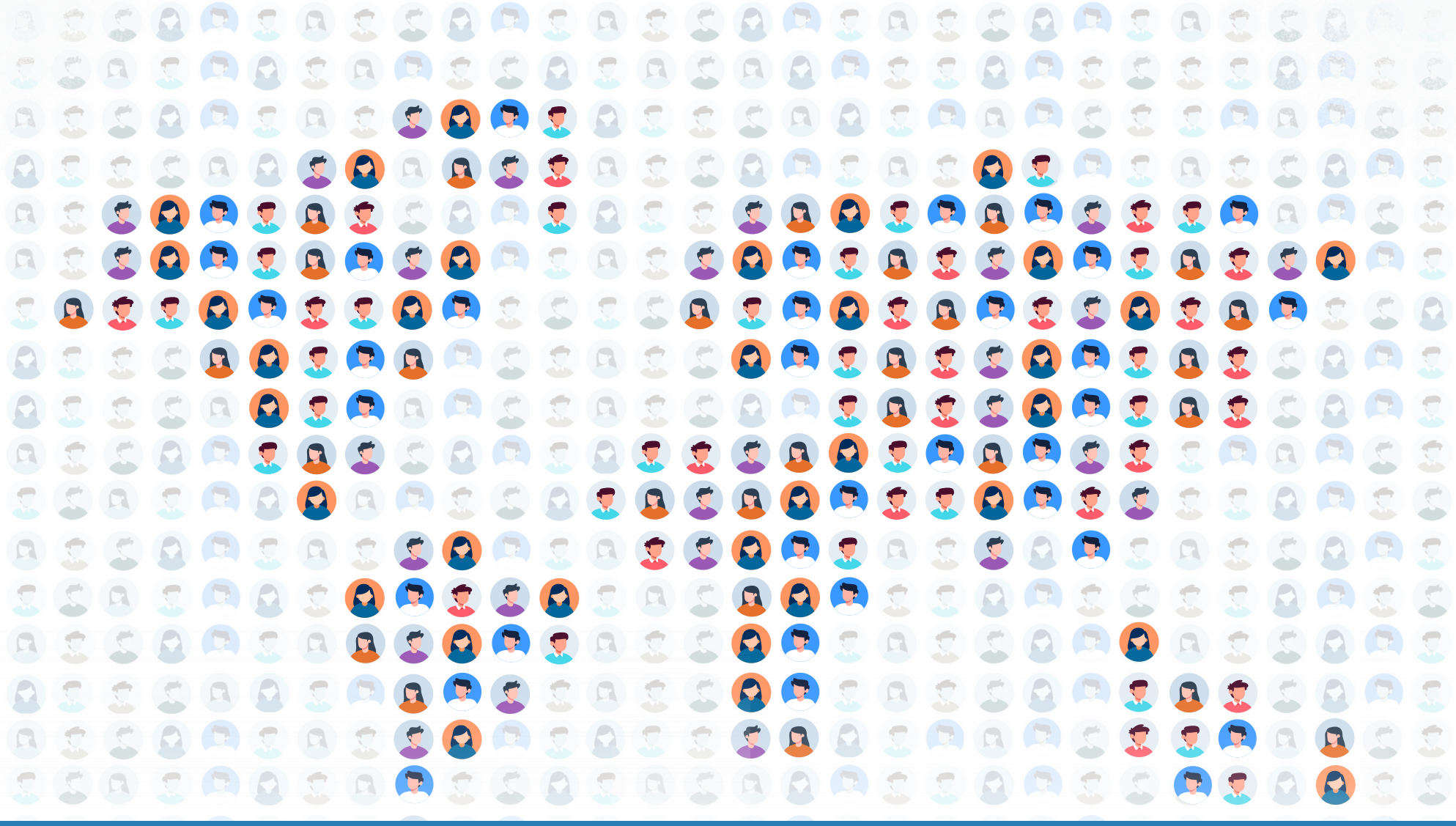
- معظم البيانات التي تحذفونها من أجهزتكم يمكن استردادها عند استخدام وظيفة الحذف العادية. إذا أردتم حذف البيانات بشكل دائم، يجب استخدام أدوات مثل Eraser أو BleachBit لحذف البيانات.
- قبل التخلص من الأجهزة أو بيعها أو إهدائها، تأكدوا من مسح جميع البيانات بشكل آمن.

9. تثقيف أنفسكم وجهات الاتصال الخاصة بكم

ابقوا على اطلاع حول أحدث التهديدات السيبرانية وإجراءات الحماية. إذا أتيحت لكم الفرصة، شاركوا في ورش عمل حضورية أو جلسات تدريب عبر الإنترنت مصممة خصيصًا للتعامل مع التهديدات الرقمية التي تواجه الصحافيين/ات والناشطين/ات.

10. الاستعداد للاستجابة للحوادث

- كونوا مستعدين لأسوأ السيناريوهات حتى لا تُفاجَؤوا. ضعوا بروتوكولًا واضحًا لما يجب القيام به في حالة حدوث خروقات بيانات أو حوادث سيبرانية.
- احتفظوا بقائمة تضم جهات اتصال لمتخصصي الأمن السيبراني والمنظمات التي يمكنكم التواصل معها عند الحاجة للمساعدة.
- راجعوا ومارسوا وقوموا بتحديث هذه البروتوكولات بانتظام.



مؤسسة مهارات

العنوان:
جديدة، المتن
لبنان

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

مهارات
Maharat