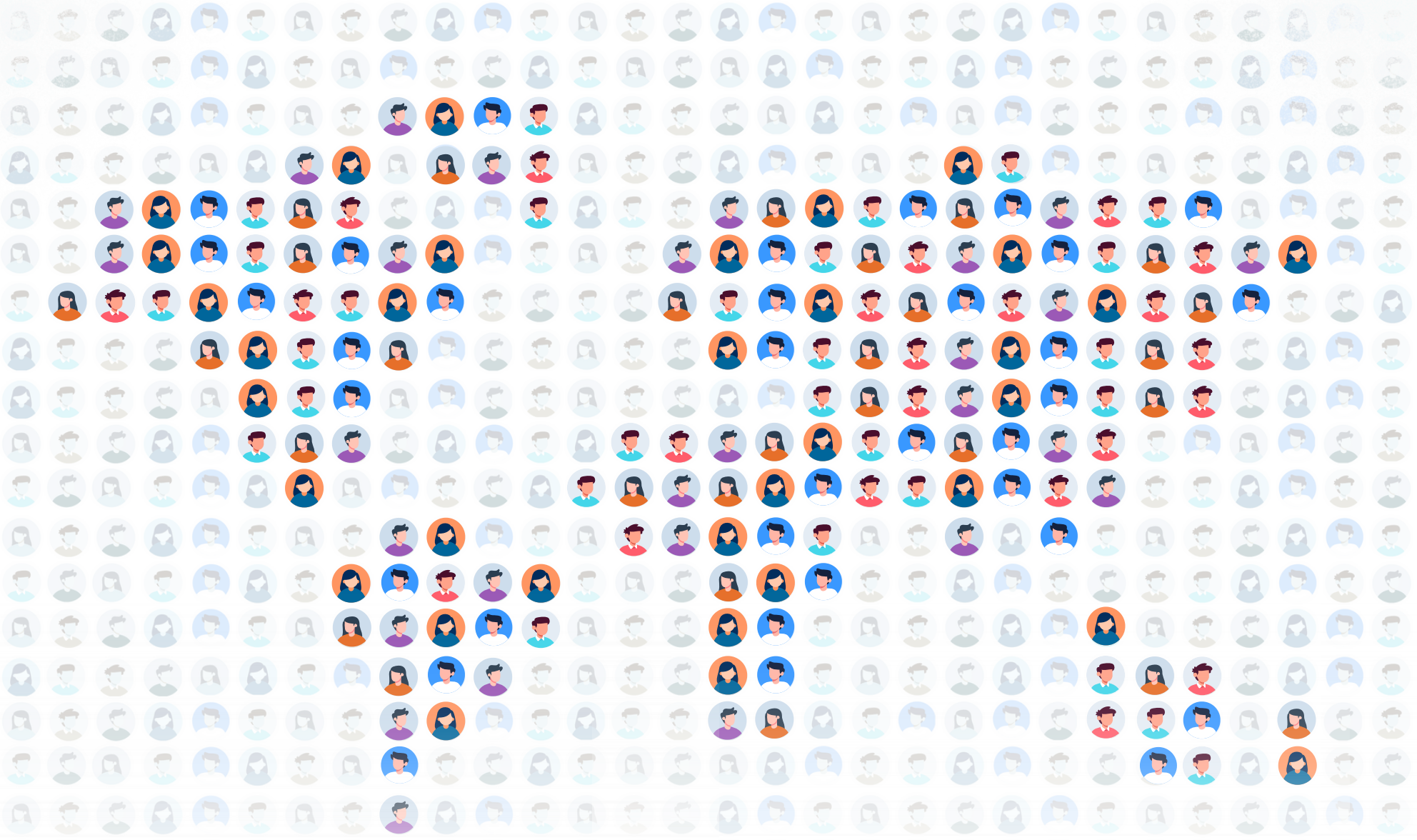


دليل الأمن الرقمي

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

٦

الأمان على وسائل التواصل الاجتماعي:

أفضل الممارسات لاستخدام وسائل التواصل الاجتماعي بأمان (إعدادات الخصوصية، مشاركة المعلومات الحساسة)

إعداد:
خبير في الأمن الرقمي بهاء نصر

وسائل التواصل الاجتماعي جزء من حياتنا اليومية

أصبحت وسائل التواصل الاجتماعي جزءًا أساسيًا من حياتنا اليومية. نستخدمها للبقاء على اتصال والحفاظ على العلاقات مع العائلة والأصدقاء؛ كما يستخدمها البعض **للتواصل المهني، أو للوصول إلى الأخبار والمعلومات، وآخرون للتعبير عن الذات والإبداع بالإضافة إلى الترفيه والاسترخاء.**

مع ازدياد اعتمادنا على وسائل التواصل الاجتماعي تصبح جزءًا لا يتجزأ من حياتنا اليومية؛ يمكن أن يؤدي ذلك إلى **مشاركة مفرطة للمعلومات الشخصية** عبر الإنترنت، مثل الصور، مواقع تواجدنا، اهتماماتنا، وهواياتنا، وغيرها من التفاصيل الشخصية.

لضمان استخدام وسائل التواصل الاجتماعي بأمان، علينا **ضبط إعدادات الخصوصية على كل منصة نستخدمها**، وضرورة التنبه للمعلومات التي نشاركها **وفهم المخاطر المرتبطة بأي تفاعل عبر الإنترنت.**

أفضل الممارسات لتحسين أمان وخصوصية حساباتنا على وسائل التواصل الاجتماعي

خلال أوقات الحرب، وقبل أي هجوم فعلي، تستخدم **القوات العسكرية وحدات خاصة للاستطلاع لجمع المعلومات عن العدو**: مدى جاهزيته، قدراته، واستكشاف المنطقة. المجرمون الإلكترونيون والقراصنة يستخدمون نفس تقنية "الاستطلاع". **الاستطلاع** هو المرحلة الأولى من عملية القرصنة، وتتضمن جمع أكبر قدر ممكن من المعلومات عن الهدف. عملية الاستطلاع تشبه عمل المحقق: يقوم القراصنة بجمع البيانات والمعلومات لفهم ضحاياهم ويستخدمون هذه المعلومات لتمنحهم ميزة تمكنهم من تصميم هجوم محدد ضد ضحاياهم.

1. كونوا انتقائيّين في المعلومات التي تشاركونها علنًا

تجنبوا الإفراط في مشاركة التفاصيل الشخصية: حدّوا من المعلومات التي تقدمونها عن موقعكم اليومي أو روتينكم. مشاركة تفاصيل مثل موقعكم الحالي أو عناوينكم الشخصية قد يزيد من مخاطر السرقة أو التتبع أو غيرها من الأخطار.

قلّلوا من مشاركة المحتوى الحساس: تجنبوا مشاركة المعلومات التي يمكن استخدامها لسرقة الهوية، مثل تاريخ ميلادكم الكامل، عنوانكم، أو بياناتكم المالية. حتى التفاصيل البسيطة يمكن أن يتم جمعها من قبل المجرمين السيبرانيين لتكوين صورة شاملة عنكم.

كونوا حذرين مع الصور: تجنبوا نشر صور لأشخاص آخرين دون إذنهم.

2. فكروا قبل النشر

تجنبوا الإفراط في مشاركة التفاصيل الشخصية

حدّوا من المعلومات التي تقدمونها عن موقعكم اليومي أو روتينكم. مشاركة تفاصيل مثل موقعكم الحالي أو عناوينكم الشخصية قد يزيد من مخاطر السرقة أو التتبع أو غيرها من الأخطار.

قلّلوا من مشاركة المحتوى الحساس

تجنبوا مشاركة المعلومات التي يمكن استخدامها لسرقة الهوية، مثل تاريخ ميلادكم الكامل، عنوانكم، أو بياناتكم المالية. حتى التفاصيل البسيطة يمكن أن يتم جمعها من قبل المجرمين السيبرانيين لتكوين صورة شاملة عنكم.

كونوا حذرين مع الصور

تجنبوا نشر صور لأشخاص آخرين دون إذنهم.

3. تعزيز أمان الحسابات

استخدموا كلمات مرور قوية وفريدة

أنشئوا كلمات مرور معقدة تتضمن مزيجًا من الأحرف والأرقام والرموز. تجنبوا استخدام نفس كلمة المرور لحسابات متعددة.

فعّلوا التحقق بخطوتين (2FA)

قوموا بتفعيل خاصية التحقق بخطوتين للحصول على جانب إضافي من الأمان. غالبًا ما يتطلب ذلك التحقق من تسجيل الدخول باستخدام طريقة ثانية، مثل رمز يتم إنشاؤه بواسطة تطبيق على هاتفكم.

راجعوا الأجهزة المتصلة بانتظا

تحققوا بانتظام من قائمة "الأجهزة التي تم تسجيل الدخول منها" في حساباتكم، وقوموا بتسجيل الخروج من الأجهزة التي لا تعرفونها أو التي لم تعودوا تستخدمونها.

تجنبوا فتح حساباتكم على أجهزة الآخرين أو الأجهزة العامة: لا يمكنكم التأكد من أمان هذه الأجهزة، وقد تعرض بياناتكم للخطر.

4. ضبط إعدادات الخصوصية

حدّدوا من يمكنه رؤية منشوراتكم على الإنترنت

اجعلوا رؤية ملفكم الشخصي تقتصر على "الأصدقاء فقط" لتقييد من يمكنه رؤية منشوراتكم، صوركم، ومعلوماتكم الشخصية.

راجعوا إعدادات الوسوم (Tags)

تحكموا بمن يمكنه الإشارة إليكم في الصور أو المنشورات. تسمح العديد من المنصات للمستخدمين بمراجعة الوسوم قبل ظهورها على ملفاتهم الشخصية.

راجعوا التطبيقات المثبتة في حساباتكم وصلاحياتها

تحققوا من الصلاحيات الممنوحة للتطبيقات الخارجية المرتبطة بحساباتكم على وسائل التواصل الاجتماعي. تخلصوا من أي تطبيقات طرف ثالث لا تستخدمونها.

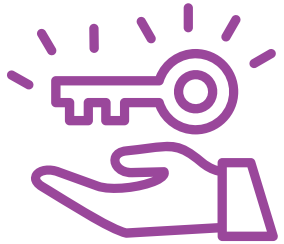
تحكموا بمن يمكنه التواصل معكم

ضعوا قيودًا على من يمكنه إرسال طلبات صداقة أو رسائل. على سبيل المثال، يمكنكم السماح فقط بـ "أصدقاء الأصدقاء" لإرسال الطلبات إذا كان ذلك ممكنًا.

قلّلوا من ظهور ملفكم الشخصي في محركات البحث

قوموا بتعطيل فهرسة محركات البحث لمنع ظهور ملفكم الشخصي على محركات البحث الخارجية مثل Google.

5. قللوا مشاركة المعلومات مع تطبيقات طرف ثالث



قيدوا وصول تطبيقات الطرف الثالث

حدّوا من الصلاحيات الممنوحة للتطبيقات الخارجية، خصوصًا إذا طلبت الوصول إلى قائمة أصدقائكم، تفاصيل ملفكم الشخصي، أو سجل منشوراتكم.

راجعوا سياسات جمع البيانات

تنبهوا لسياسات الخصوصية للتطبيقات والخدمات المرتبطة بوسائل التواصل الاجتماعي. قد تستخدم بعض التطبيقات بياناتكم بطرق قد لا تكونوا على علم بها أو مرتاحين لها.

اطفئوا خاصية مشاركة الموقع

تجنبوا مشاركة بيانات الموقع مع تطبيقات الطرف الثالث المتصلة بوسائل التواصل الاجتماعي، إلا إذا كان ذلك ضروريًا للغاية. بعض التطبيقات تجمع معلومات الموقع في الخلفية دون علمكم.

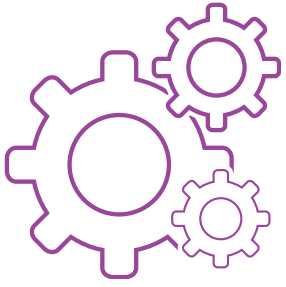
6. ابقوا على اطلاع بتحديثات الخصوصية

راجعوا سياسات الخصوصية بانتظام

تقوم منصات التواصل الاجتماعي بتحديث سياسات الخصوصية بشكل دائم. راجعوا هذه التحديثات لفهم كيفية استخدام معلوماتكم، وقوموا بتعديل إعداداتكم بما يتماشى مع ذلك.

تنبهوا لإشعارات الأمان

قد ترسل المنصات إشعارات للمستخدمين حول مشكلات أمنية محتملة أو تسريبات للبيانات. انتبهوا لهذه الإشعارات واتخذوا الإجراءات اللازمة إذا تأثرت حساباتكم.



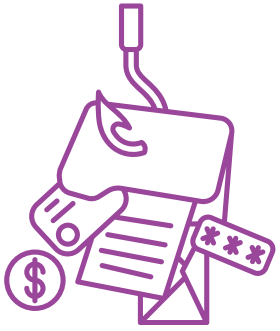
استخدموا أدوات مراجعة الخصوصية

توفر العديد من منصات التواصل الاجتماعي أدوات لمراجعة إعدادات الخصوصية وتحسينها، مع إرشادكم إلى أفضل الممارسات المرتبطة بالخصوصية والأمان.

7. كونوا حذرين مع التفاعلات عبر الإنترنت

تجنبوا التفاعل مع الحسابات غير المعروفة

قد يكون التعامل مع الغرباء، خاصة أولئك الذين يطلبون معلومات شخصية، خطرًا. تجنبوا قبول طلبات الصداقة أو الرسائل المباشرة من أشخاص لا تعرفونهم.



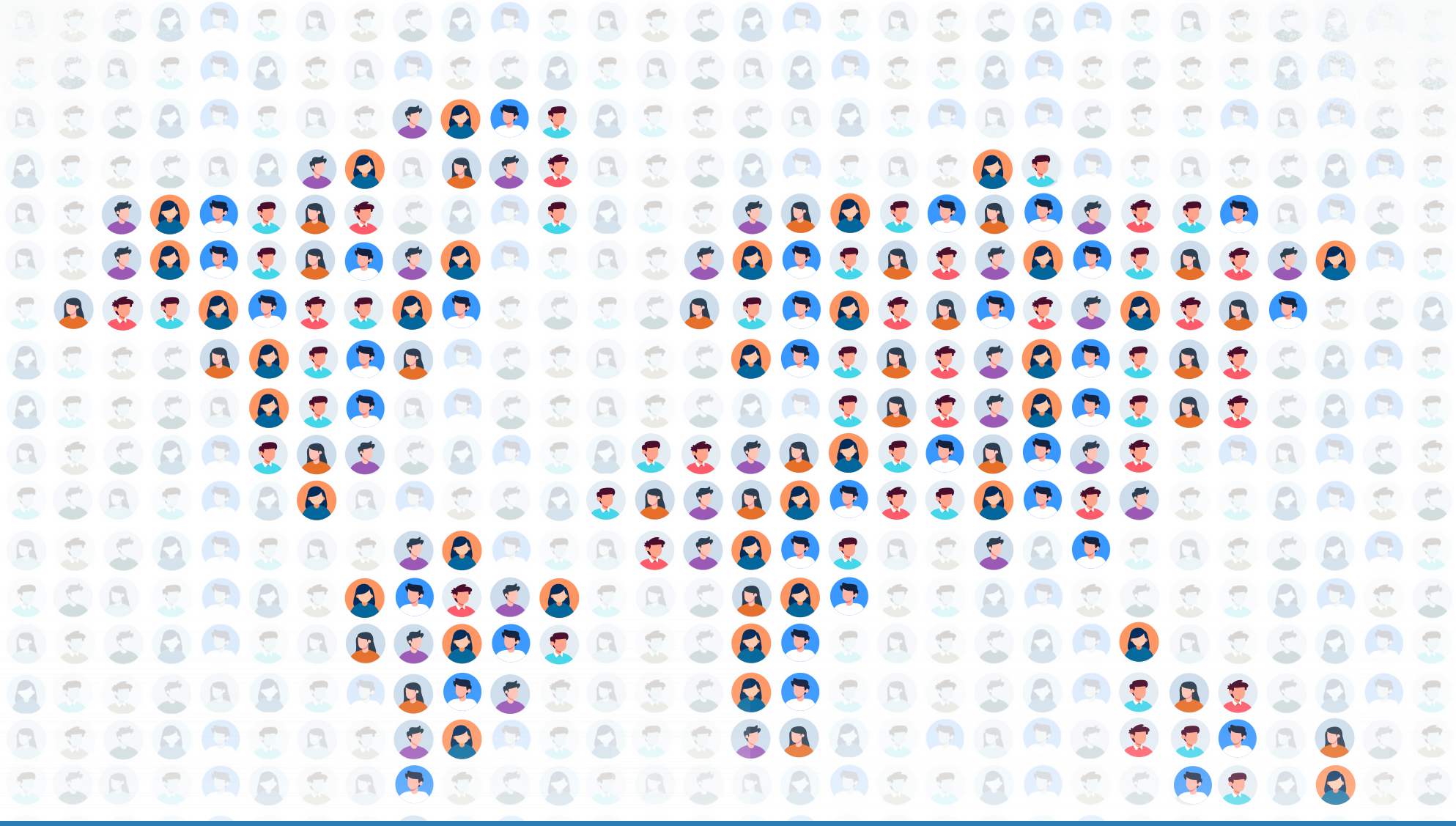
احذروا محاولات التصيد الاحتيالي

انتبهوا لعمليات الاحتيال التي تستخدم رسائل، روابط، أو صفحات وهمية لخداعكم للكشف عن معلومات تسجيل الدخول الخاصة بكم.

بلغوا عن المحتوى المشبوه

قوموا بالإبلاغ عن أو حظر المستخدمين والمحتوى الذي يبدو مريبًا أو ينتهك إرشادات المجتمع. يساعد ذلك في الحفاظ على بيئة آمنة على الإنترنت للجميع.

من خلال اتباع هذه الممارسات، يمكنكم تعزيز خصوصيتكم وحماية معلوماتكم الشخصية بشكل أفضل، مما يساعدكم على الاستمتاع بوسائل التواصل الاجتماعي بأمان وراحة بال أكبر.



مؤسسة مهارات

العنوان:
جديدة، المتن
لبنان

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

مهارات
Maharat