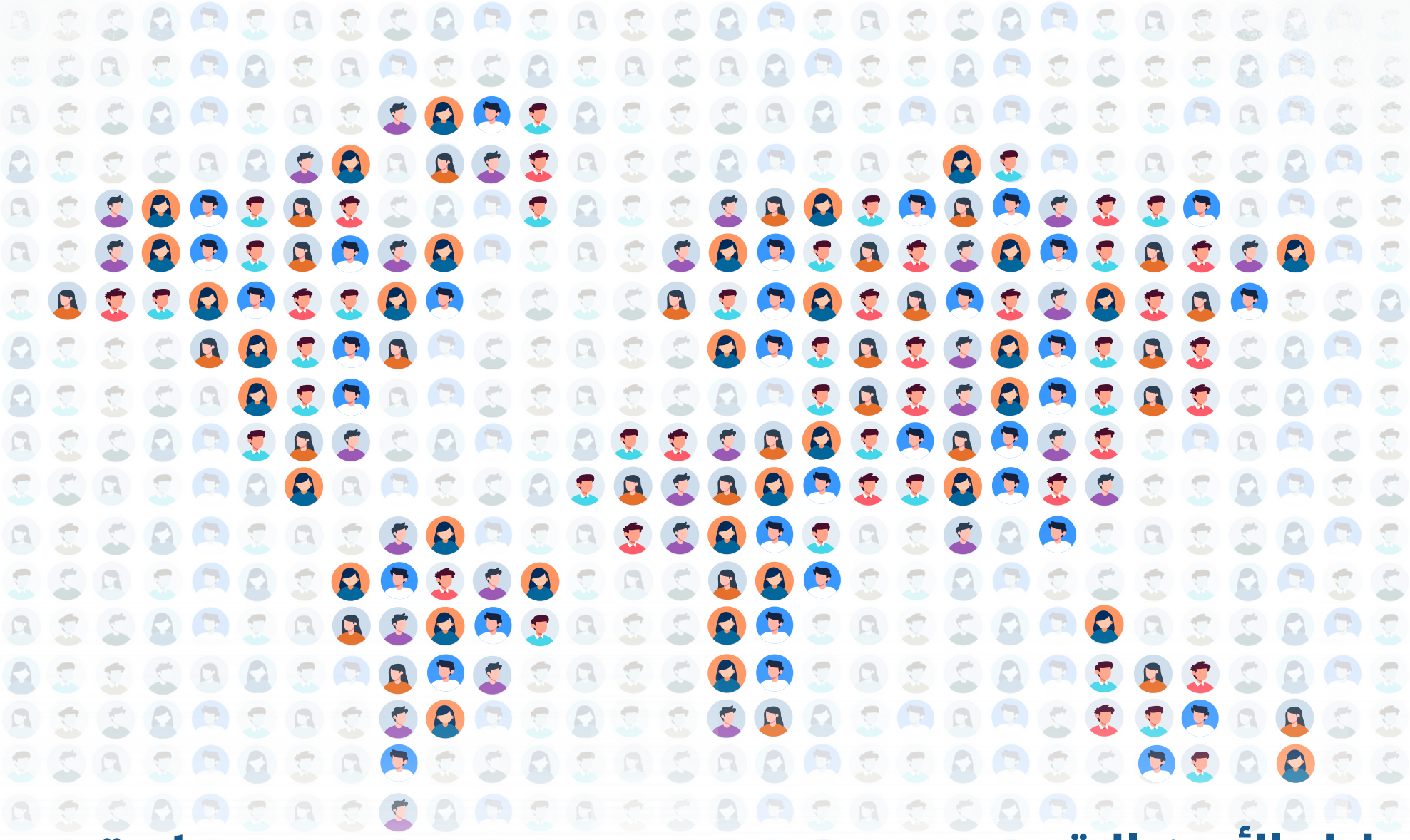


دليل الأمن الرقمي

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.

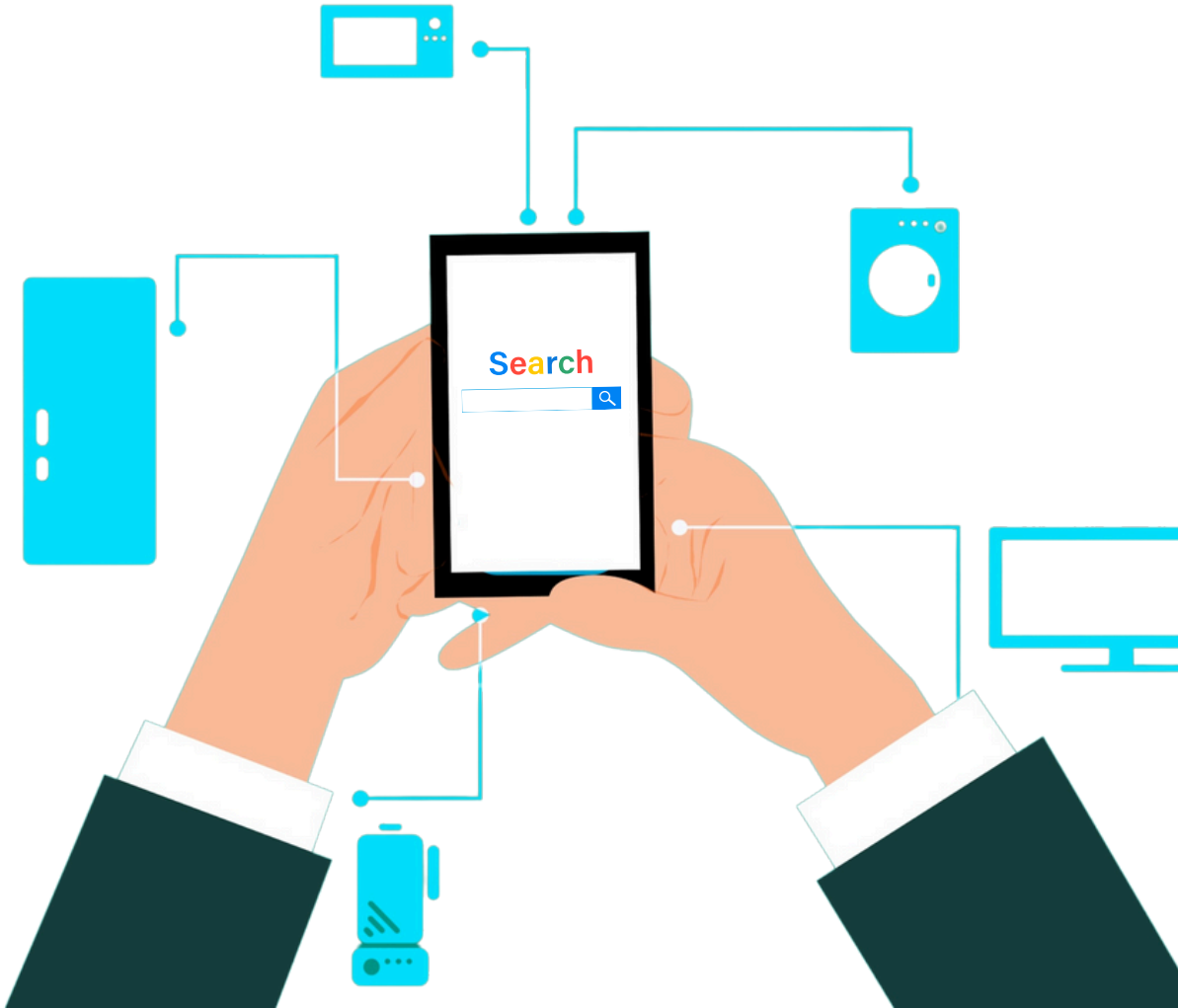
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

مهارات
Maharat

UN WOMEN

الجزء ٤

ممارسة عادات تصفح آمنة أمر ضروري لحماية معلوماتكم الشخصية وأجهزتكم وخصوصيتكم بشكل عام.



إعداد:
خبير في الأمن الرقمي بهاء نصر

لماذا تُعد السلامة على الإنترنت مهمة؟

لا شك أن الإنترنت يجعل حياتنا أسهل، سواء كنتم تطّلعون على أحدث الأخبار، أو تتواصلون مع الأصدقاء، أو تتصفحون وسائل التواصل الاجتماعي، أو تشاهدون مسلسلاتكم المفضلة. بالرغم من ذلك، ومع كل ما يقدمه الإنترنت، **يمكن ان يكون مكانًا خطيرًا إذا لم تكونوا حذرين**، خصوصًا في السنوات الأخيرة مع الازدياد المضطرد لتهديدات الأمن السيبراني والانتهاكات. **البرامج الضارة (مثل الفيروسات وأدوات الوصول عن بعد وأحصنة طروادة)، عمليات الاحتيال، رسائل البريد الإلكتروني الخبيثة**، والمحتوى غير المناسب ليست سوى أمثلة قليلة على التهديدات المحتملة أثناء تصفح الإنترنت. يمكن تشبيه التصفح الآمن بالنظر في الاتجاهين قبل عبور الشارع. الحفاظ على الأمان على الإنترنت أمر مهم جدًا.

لحسن الحظ، **هناك العديد من الطرق لحماية انفسكم ولجعل تجربة تصفح الإنترنت أكثر أمانًا وإرضاءً**، سواء كنتم تستخدمون جهاز كمبيوتر محمولا أو جهازًا لوحيًا أو هاتفًا ذكيًا. وهذه بعض النصائح لتصفح الانترنت بأمان:

كيفية تصفح الإنترنت بأمان

١- تحديث متصفح الويب بانتظام:

يستهدف القراصنة بشكل متكرر ثغرات متصفحات الويب، ولهذا السبب تقدم الشركات المصنعة للبرمجيات تحديثات دورية لإصلاح أي مشاكل وسد الثغرات الأمنية. تثبيت أحدث إصدار من المتصفح على جهازكم يساعد في حماية بياناتكم الشخصية ويمنحكم أحدث الميزات وإجراءات الأمان. إن تجاهل التحديثات قد يؤدي إلى تعرض متصفحكم للإختراق ويجعله هدفًا أسهل للقراصنة، لأن العديد من هجماتهم تستغل البرمجيات القديمة والثغرات المعروفة.

٢- فكروا قبل أن تضغطوا!

تجنبوا الضغط على الروابط والمرفقات المشبوهة، خاصة في رسائل البريد الإلكتروني وعلى وسائل التواصل الاجتماعي. صُممت روابط التصيد الاحتيالي لخداعكم للكشف عن معلوماتكم الشخصية أو تثبيت برامج ضارة. يفضّل كتابة عنوان الموقع يدويًا بدلاً من الضغط على الرابط.

انتبهوا إلى عنوان الويب. تحققوا من العنوان، وإذا ضغطتم على رابط، تأكدوا من أن العنوان لم يتغير. إذا تغيّر، فهذا يعني أنه قد نقلكم إلى عنوان ويب احتيالي حيث يمكن للمجرمين السيبرانيين مراقبة معلوماتكم والوصول إليها. غادروا الموقع فورًا ولا تُدخلوا أي معلومات شخصية.

في المتصفح، يظهر رمز قفل في بداية شريط العنوان للإشارة إلى أن الموقع آمن. ولكن لا تنخدعوا برمز القفل الذي يظهر داخل صفحة الويب نفسها، حيث يمكن للمجرمين السيبرانيين نسخ الصورة. لذلك، تحققوا مرتين من أن القفل موجود داخل إطار نافذة المتصفح نفسه.
اضغطوا مرتين على أيقونة القفل للحصول على مزيد من المعلومات عن الموقع. تحت القفل، يمكنكم العثور على معلومات الشهادة الخاصة بالموقع الذي تتصفحونه للتأكد من أنكم على موقع آمن وموثوق. تأكدوا من أن الشهادة سارية المفعول ومخصصة للموقع الذي تزورونه.

٣- استخدام شبكة VPN:

تقوم الشبكة الافتراضية الخاصة (VPN) بتشفير اتصالكم بالإنترنت، مما يُنشئ نفقًا آمنًا بين جهازكم وشبكة الإنترنت. هذا يخفي عنوان البروتوكول IP الخاص بكم ويحمي أنشطتكم عبر الإنترنت من مراقبة جهات خارجية، مثل القراصنة أو مزودي خدمة الإنترنت أو الجهات الحكومية.
عند استخدام شبكة عامة، مثل تلك الموجودة في الفنادق أو المطارات أو المقاهي، يجب دائمًا استخدام VPN، لأن هذه الشبكات قد تكون غير آمنة، مما يمكّن القراصنة من التجسس على نشاطكم عبر الإنترنت أو توجيهكم إلى مواقع ضارة.
تساعد شبكات VPN أيضًا على تجاوز الرقابة وتتيح لكم زيارة المواقع المحجوبة في البلد الذي تتواجدون فيه. ومع ذلك، من المهم اختيار VPN موثوق وآمن.

٤- استخدام كلمات مرور قوية وفريدة:

قوموا بإنشاء كلمات مرور معقدة تجمع بين الأحرف، والأرقام، والرموز، وتجنبوا إعادة استخدام كلمات المرور عبر مواقع مختلفة.
لا تحفظوا كلمات المرور في المتصفح. استخدموا مدير كلمات المرور حيث يمكنكم تخزين كلمات المرور بأمان في قاعدة بيانات مشفرة محمية بكلمة مرور قوية واحدة.

٥- تفعيل التحقق الثنائي (MFA):

أفضل طريقة لحماية حساباتكم عبر الإنترنت هي تفعيل التحقق الثنائي. تضيف هذه الخاصية طبقة إضافية من الأمان، حيث تتطلب التحقق من هويتكم باستخدام طريقة إضافية (مثل تطبيق المصادقة) للوصول إلى الحسابات الحساسة. هذا يجعل من الصعب على القراصنة اختراق حساباتكم.

٦- تجنب التحميل من مصادر غير موثوقة:

قوموا بتحميل التطبيقات والملفات فقط من المواقع الرسمية أو متاجر التطبيقات المعتمدة. قد تقدم المواقع غير الموثوقة برامج تحتوي على برمجيات ضارة، وبمجرد تثبيتها تفتح الباب أمام القراصنة للوصول إلى أجهزتكم وجميع البيانات والمعلومات الموجودة عليها.

٧- استخدام برامج مكافحة الفيروسات وجدران الحماية الموثوقة:

يمكن لممارسات التصفح غير الآمن أن تعرضكم لهجمات الفيروسات، مما قد يؤدي إلى اختراق ملفاتكم، وكلمات المرور، وحساباتكم، وأجهزتكم.
توفر برامج مكافحة الفيروسات وجدران الحماية دفاعات أساسية ضد البرمجيات الخبيثة وهجمات التصيد والتهديدات الأخرى. تأكدوا من أن هذه البرامج مفعلة ومحدثة على جميع أجهزتكم.

٨- تقليل مشاركة المعلومات الشخصية على وسائل التواصل الاجتماعي:

يستخدم المجرمون السيبرانيون المعلومات التي تتم مشاركتها على وسائل التواصل الاجتماعي أو المتوفرة عنكم عبر الإنترنت لسرقة الهوية أو تخمين أسئلة الأمان. تجنبوا مشاركة التفاصيل الحساسة، مثل العنوان الكامل، أو تاريخ الميلاد، أو أسماء أفراد العائلة، أو اهتماماتكم، أو أماكن تواجدكم. يمكن للقراصنة استغلال المعلومات المتوفرة عنكم على الإنترنت لشن هجمات مستهدفة ضدكم.

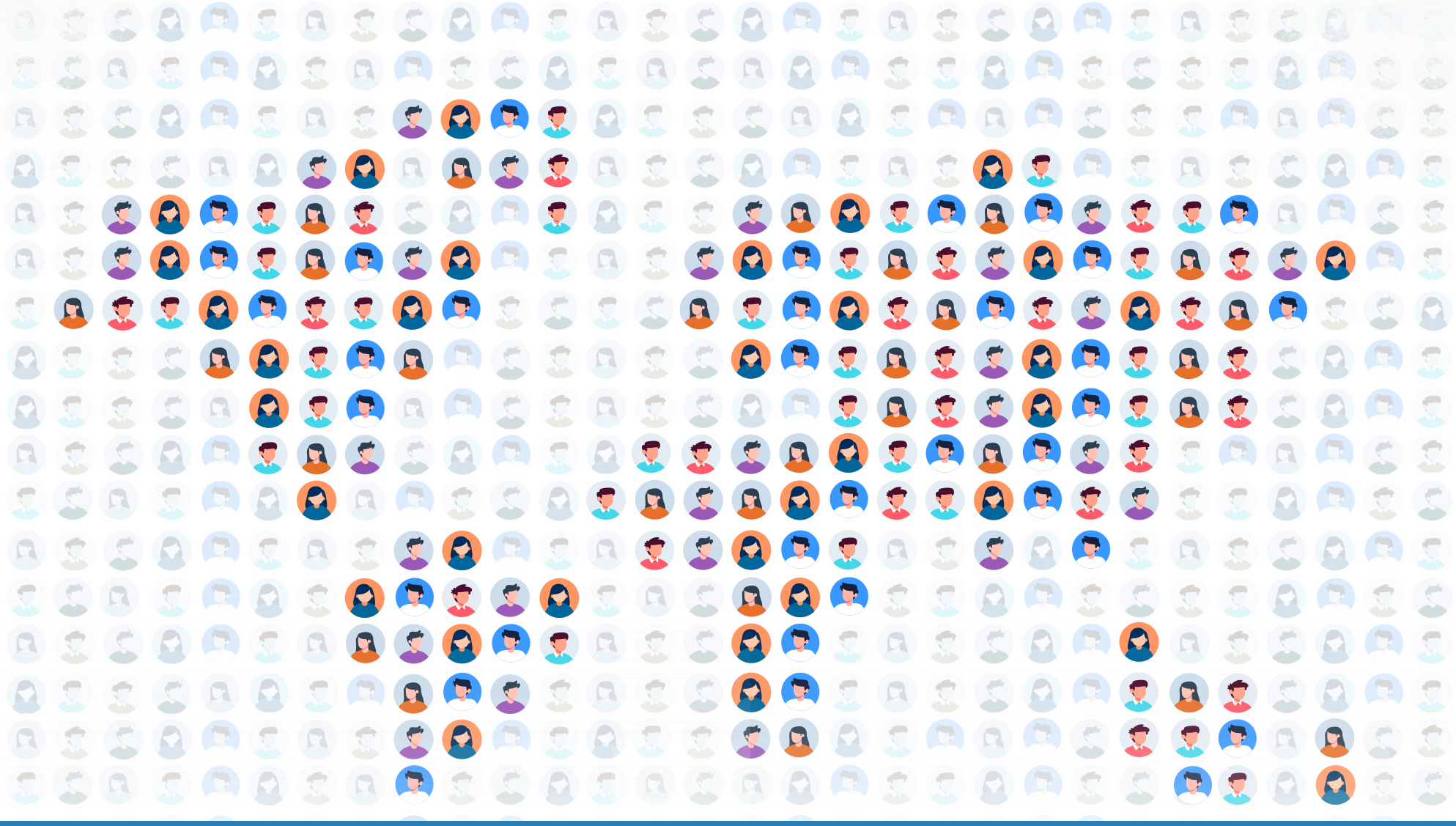
٩- التثقيف والتوعية حول التصيد الاحتيالي والهندسة الاجتماعية:

تُعد هجمات الهندسة الاجتماعية من التكتيكات التي يستخدمها المجرمون السيبرانيون لخداع الأفراد وإقناعهم بالكشف عن معلومات حساسة أو القيام بأفعال تضر بالأمن.
تعلموا كيفية التعرف على محاولات التصيد الاحتيالي، والتي غالبًا ما تتضمن عناصر مثل الإلحاح وطلب سرعة الاستجابة او التنفيذ أو مرفقات لم تطلبوها، أو طلبات للحصول على معلومات شخصية. إن تثقيف انفسكم والآخرين يقلل من مخاطر الوقوع ضحية هذه الهجمات.

١٠- توخي الحذر عند استخدام إضافات المتصفح:

إضافات أو ملحقات المتصفح هي برامج صغيرة تضيف ميزات إلى متصفح الويب الخاص بكم. من المهم تثبيت الإضافات التي تحتاجونها فقط والتي يُوصى بها من قبل خبراء الأمن الرقمي. تأكدوا من تثبيتها من الصفحة الرسمية أو متجر المتصفح. قد تحتوي بعض الإضافات على برامج ضارة أو خبيثة، أو قد تتعقب نشاطكم أثناء التصفح.

يمكن أن يكون الإنترنت مكانًا غير متوقع، وان خطأ صغيرا قد يسبب لكم الكثير من التوتر. ان اتباع عادات التصفح الآمن يقلل بشكل كبير من المخاطر. يجب أن تكون ممارسات التصفح الآمن أولوية للحفاظ على بياناتكم وخصوصيتكم من التهديدات السيبرانية الشائعة. استعيدوا السيطرة على أمنكم وخصوصيتكم من خلال اتباع نصائحنا العشر.



مؤسسة مهارات

العنوان:
جديدة، المتن
بيروت، لبنان

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

مهارات
Maharat