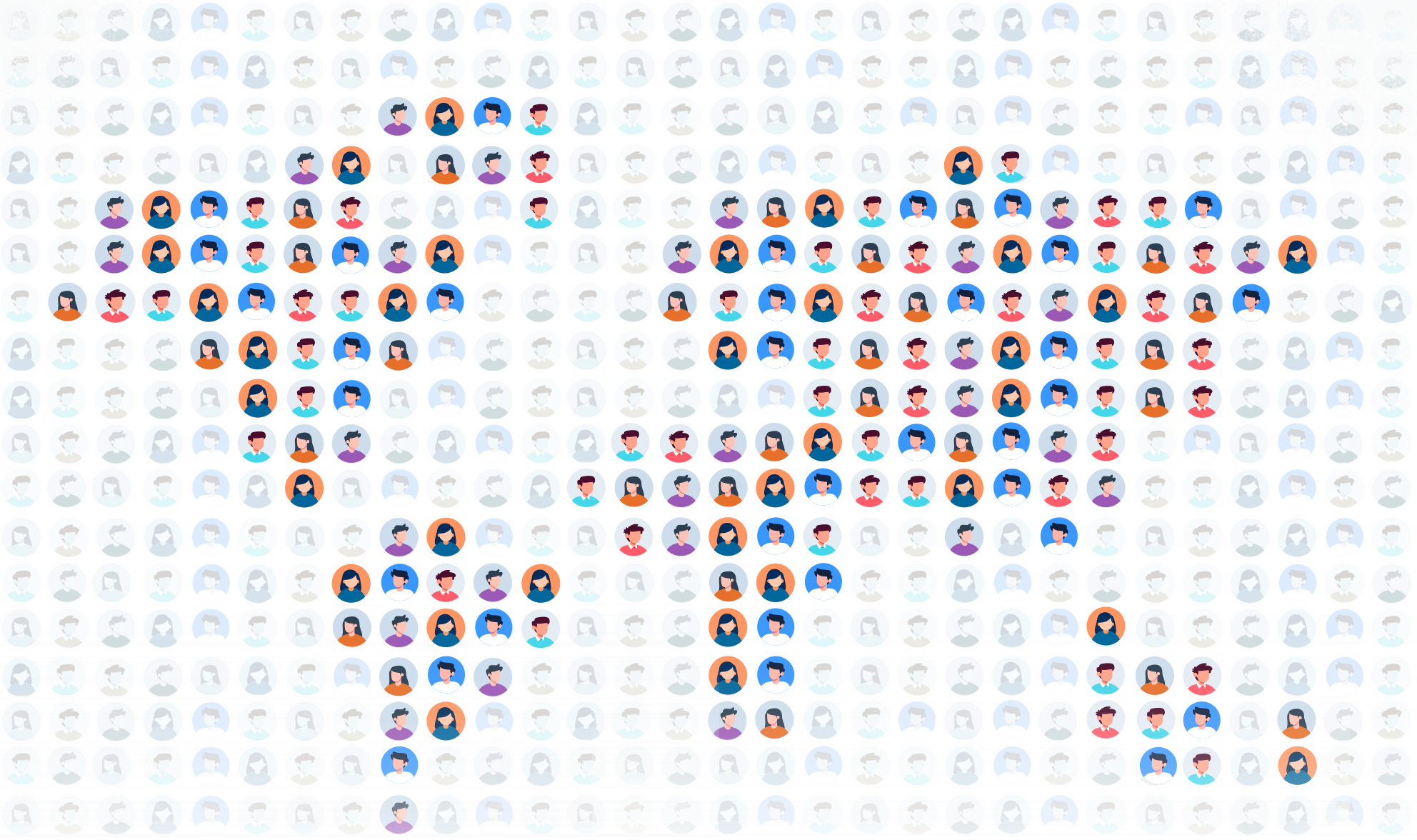


دليل الأمن الرقمي

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

0

التعرف على التهديدات الرقمية:

التعرف على التهديدات، التعامل مع الاختراقات، واستخدام أدوات الأمان

إعداد:
خبير في الأمن الرقمي بهاء نصر

التعرف على التهديدات الرقمية

في عالمنا المترابط اليوم، حيث تتغلغل التكنولوجيا في حياتنا اليومية، أصبح فهم وتحديد التهديدات الرقمية أكثر أهمية من أي وقت مضى. **يستخدم مجرمو الإنترنت تكتيكات متطورة لاستغلال الثغرات، وسرقة المعلومات الحساسة، وتعطيل الأنظمة.** وغالبًا ما تتجلى هذه التهديدات على شكل رسائل بريد إلكتروني احتيالية، أو روابط ضارة، أو رسائل خادعة، أو سلوك غير عادي للأجهزة. لحماية حياتكم الرقمية، **من الضروري التعرف على هذه التهديدات مبكرًا، والاستجابة بفعالية للاختراقات، واستخدام أدوات أمان قوية.**

أهمية النهج الاستباقي في الأمن الرقمي

أن تكون **استباقيًا يعني اتخاذ الإجراءات** قبل وقوع المشكلة. يساهم النهج الاستباقي في **تقليل خطر الاختراقات، والمساعدة في التخفيف من المخاطر المرتبطة بالتهديدات الرقمية والثغرات.** من خلال تحديد المخاطر المحتملة وتنفيذ تدابير الحماية المناسبة، يمكنكم تقليل تعرضكم وتعزيز أمانكم الرقمي بشكل عام.

يتطلب تبني النهج الاستباقي في الأمن الرقمي **تمكين أنفسكم بالمعرفة والمهارات اللازمة للتنقل بأمان في العالم الرقمي.** يشبه النهج الاستباقي اتخاذ احتياطات مسبقة لمنع حصول اي مشكلة مثل اقفال باب منزلكم قبل المغادرة. وعلى الرغم من أنه ليس هناك أي طريقة توفر حماية مطلقة، إلا أن التدابير الاستباقية تجعل منكم هدفًا أصعب للمهاجمين. وتساهم خطوات بسيطة في حماية معلوماتكم والمحافظة على خصوصيتها، مثل استخدام كلمات مرور قوية، تفعيل التحقق بخطوتين، تحديث البرامج، وضبط إعدادات الخصوصية.

بالإضافة إلى ذلك، فإن **تعزيز ثقافة الوعي الرقمي** – سواء على المستوى الشخصي أو داخل المؤسسات يمكن أن يساعد في تحديد التهديدات الناشئة ومنع الأخطاء المكلفة. البقاء على اطلاع على أحدث المخاطر السيبرانية واعتماد أفضل الممارسات يضمن أن تبقوا دائمًا متقدمين بخطوة على المهاجمين المحتملين.

فيما يلي بعض الأساليب الأكثر انتشارًا التي يستخدمها المجرمون السيبرانيون لاستهداف الأفراد والمنظمات:

محاولات التصيد الاحتيالي

تعتمد هجمات التصيد الاحتيالي والهندسة الاجتماعية على التلاعب النفسي والأساليب الاحتيالية لخداع الأفراد للكشف عن معلومات حساسة، او النقر على روابط ضارة، أو القيام بأفعال تعرض أمنهم للخطر. غالبًا ما تأتي هذه الهجمات على شكل رسائل بريد إلكتروني، رسائل نصية، أو مكالمات هاتفية تبدو وكأنها صادرة من جهات موثوقة مثل البنوك أو الشركات المعروفة.
لحماية أنفسكم، من الضروري التعرف على العلامات الشائعة لمحاولات التصيد:

رسائل بريد إلكتروني أو رسائل مشبوهة

غالبًا ما تحتوي على أخطاء إملائية أو قواعد لغوية غريبة، أو عناوين مرسلين غير متوقعة. وقد يستخدم فيها عبارات ترحيب عامة بدلاً من تحيات شخصية لكي تظهر شرعية. تحققوا دائمًا من هوية المرسل.

لغة ومطالب عاجلة

يستخدم المهاجمون الإلحاح لخلق حالة من الذعر والضغط عليكم للتصرف بسرعة دون تفكير. على سبيل المثال، "سيتم قفل حسابكم إذا لم تنقروا على هذا الرابط!"، او "انقروا الان واحصلوا على جائزة". انتبهوا من الرسائل حول سحوبات لوتو لم تشاركوا فيها او ميراث غير متوقع، اذ غالبا ما تكون عمليات احتيال.

روابط أو مرفقات غير عادية

تحققوا من الروابط قبل الضغط عليها. قد تشبه روابط التصيد المواقع الشرعية ولكنها تتضمن تغييرات طفيفة في العنوان (مثل استخدام ".net" بدلاً من ".com") أو استبدال الحروف بحروف مشابهة. تجنبوا تنزيل المرفقات من مصادر غير معروفة اذ يمكن ان تحتوي على برمجية خبيثة.

طلبات للحصول على معلومات شخصية

انتبهوا من الطلبات غير المرغوبة لبيانات التسجيل او تفاصيل شخصية او معلومات مالية. المواقع الشرعية لا تطلب هذه البيانات الحساسة عبر البريد الإلكتروني أو الرسائل النصية.

عروض غير واقعية

غالبًا ما يجذب المحتالون الضحايا بوعود بمبالغ كبيرة من المال، أو جوائز، أو مكافآت تبدو غير واقعية.

لتحسين قدرتكم على التعرف على هجمات التصيد والهندسة الاجتماعية، يمكنك استخدام موارد مثل اختبارات التصيد مثل

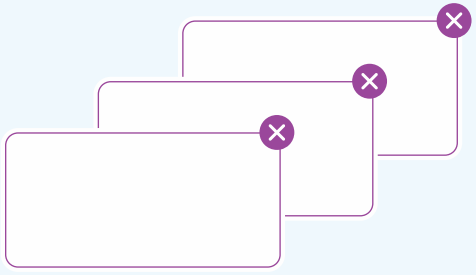
phishingquiz.withgoogle

shira.app

بالإضافة إلى ذلك، شاهدوا مقاطع فيديو عن "الهندسة الاجتماعية" على يوتيوب لفهم التكتيكات المخادعة بشكل أفضل وكيفية تجنب الوقوع ضحيةً فيها.

البرمجيات الضارة وبرامج الفدية

البرمجيات الضارة (Malware) هي البرامج التي تهدف إلى إلحاق الضرر بالأجهزة أو استغلالها، بينما تمثل برامج الفدية (Ransomware) نوعًا محددًا من البرمجيات الضارة التي تقوم بتشفير بياناتكم وتطلب دفع فدية لاستعادتها. إن التعرف على علامات الإصابة بالبرمجيات الضارة أو برامج الفدية أمر مهم لحماية أجهزتكم وبياناتكم. إليكم الاشارات الشائعة التي يجب الانتباه إليها:



النوافذ التي تظهر فجأة

إذا واجهتم نوافذ تظهر فجأة بشكل مستمر، خصوصًا تلك التي تتضمن تحذيرات أو عروضًا غير واقعية لدرجة يصعب تصديقها، فقد يكون ذلك علامة على وجود برمجيات ضارة. قد تظهر بعض النوافذ في شكل تحذيرات فيروسية لخداع المستخدمين لتنزيل برامج خبيثة مدعية أنها حلول.

الأجهزة البطيئة أو المعطلة

يمكن أن تؤدي البرمجيات الضارة إلى إبطاء كبير في أداء أجهزتكم، أو التسبب في تعطل التطبيقات، أو ظهور رسائل غريبة. إذا بدأت أجهزتكم في التصرف بشكل غير طبيعي، فقد تكون مصابة.

برامج أو إضافات جديدة مشبوهة

كونوا حذرين إذا لاحظتم وجود برامج أو إضافات للمتصفح لم تقوموا بتثبيتها أو لا تذكرون تثبيتها.

الملفات المقفلة أو رسائل الفدية

غالبًا ما تقوم برامج الفدية بتشفير الملفات وتعرض رسالة تطلب دفع فدية لاستعادة الوصول إليها.

اختطاف المتصفح

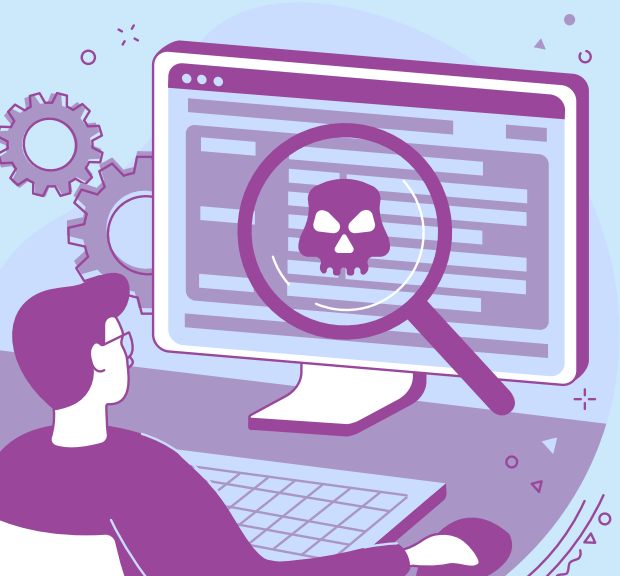
إذا تغيرت الصفحة الرئيسية أو محرك البحث الخاص بمتصفحكم دون موافقتكم، وبدأ يعيد توجيهكم إلى مواقع غير مقصودة، فقد يكون ذلك علامة على إصابة بالبرمجيات الضارة.

تعطيل برامج مكافحة الفيروسات أو أدوات النظام

بعض البرمجيات الضارة تقوم بتعطيل برامج مكافحة الفيروسات أو أدوات النظام مثل "إدارة المهام" (Task Manager) على أنظمة ويندوز أو "مراقبة النشاط" (Activity Monitor) على أجهزة ماك لتجنب اكتشافها. إذا بقيت هذه الأدوات معطلة رغم محاولات تفعيلها، قد تكون أجهزتكم مخترقة.

نشاط غير متوقع على البريد الإلكتروني أو وسائل التواصل الاجتماعي

قد تؤدي إصابة بالبرمجيات الضارة إلى إرسال رسائل بريد إلكتروني من حساباتكم أو نشر منشورات على وسائل التواصل الاجتماعي لم تقوموا بها.



التدابير الوقائية

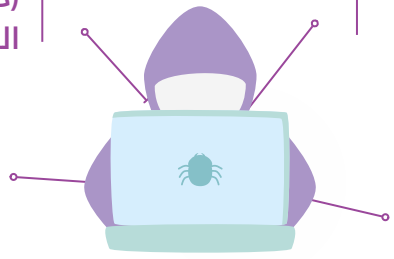
افحصوا الأجهزة للكشف عن البرمجيات الضارة

- استخدموا برامج مكافحة الفيروسات أو البرمجيات المضادة للبرمجيات الضارة: قوموا بإجراء فحص كامل لجهازكم باستخدام برامج موثوقة مثل Malwarebytes أو Windows Defender.
- اعزلوا الأجهزة المصابة: افصلوا الأجهزة المصابة عن الإنترنت لمنع انتشار البرمجيات الضارة أو تواصلها مع المهاجمين.
- إذا لم تكن لديكم الخبرة للتعامل مع البرمجيات الضارة، تواصلوا مع منظمات موثوقة يمكنها مساعدتكم.
- احرصوا على تثبيت التحديثات الأمنية بانتظام لتعزيز حماية أجهزتكم.

الوصول غير المصرح للحسابات

إذا لاحظتم علامات تشير إلى أن شخصًا آخر قد وصل إلى حساباتكم مثل:

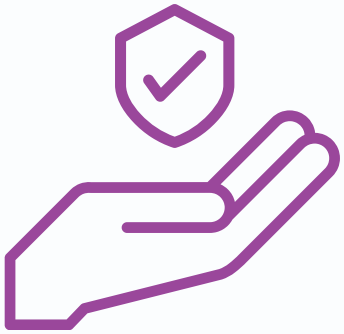
- إشعارات تسجيل الدخول من مواقع أو أجهزة غير معروفة.
- تغييرات في إعدادات الحساب (مثل كلمات المرور أو عناوين البريد الإلكتروني الاحتياطية).



- التحقق من إعدادات الحساب لمعرفة الأجهزة التي سجلت الدخول ومواقعها.
- مشتريات أو رسائل غير معروفة.

في حالة حدوث اختراق أمني، فإن اتخاذ إجراء سريع يمكن أن يحد من الضرر ويساعد في تأمين حساباتكم وأجهزتكم.

حماية الحسابات المخترقة

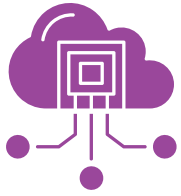


- غيروا كلمات المرور فورًا: إذا كنتم لا تزالون قادرين على الوصول إلى الحساب، قوموا بتغيير كلمة المرور إلى كلمة مرور قوية وفريدة. فعّلوا خاصية التحقق بخطوتين (2FA) لتوفير حماية إضافية.
- سجلوا خروجكم من جميع الجلسات: تتيح العديد من المنصات تسجيل الخروج من جميع الأجهزة. استخدموا هذه الميزة لطرد المستخدمين غير المصرح لهم.
- ابلغوا جهات الاتصال عن الاختراق: إذا تم اختراق بريدكم الإلكتروني أو حساباتكم على وسائل التواصل الاجتماعي، أبلغوا جهات الاتصال والزملاء لمنع وقوعهم ضحية لأي رسائل احتيالية تُرسل من حسابكم.
- إخطار المنصات ذات الصلة: أبلغوا مزود الخدمة أو المنصة عن الاختراق، حيث قد يكون لديهم خطوات استرداد إضافية أو نصائح لمساعدتكم.

نشاط الشبكة غير المعتاد

قد يشير نشاط الشبكة غير العادي إلى محاولات اختراق أو وجود برمجيات ضارة. أمثلة على ذلك:

ارتفاع كبير في استخدام البيانات



أجهزة غير معروفة متصلة بشبكتكم

لحماية أنفسكم من مثل هذه الهجمات

- قوموا دائمًا بتنزيل البرمجيات من المواقع الرسمية.
- كونوا حذرين مع مرفقات البريد الإلكتروني أو الملفات التي تصلكم عبر الرسائل أو وسائل التواصل الاجتماعي.
- لا تضغطوا على الروابط المشبوهة.
- تجنبوا إدخال أجهزة USB أو الكابلات التي لا تملكونها إلى أجهزتكم.

التعرف على المواقع المزيفة

يبتكر المجرمون السيبرانيون مواقع مزيفة تشبه المواقع الشرعية لسرقة المعلومات الحساسة.

تحققوا من HTTPS

رغم أن HTTPS يعني أن المعلومات المرسلة بين متصفحكم والموقع مشفرة، إلا أنه لا يضمن بالضرورة مصداقية الموقع. يمكن للمخترقين استخدام HTTPS أيضًا في مواقعهم المزيفة.

ابحثوا عن الأخطاء الإملائية والتناقضات

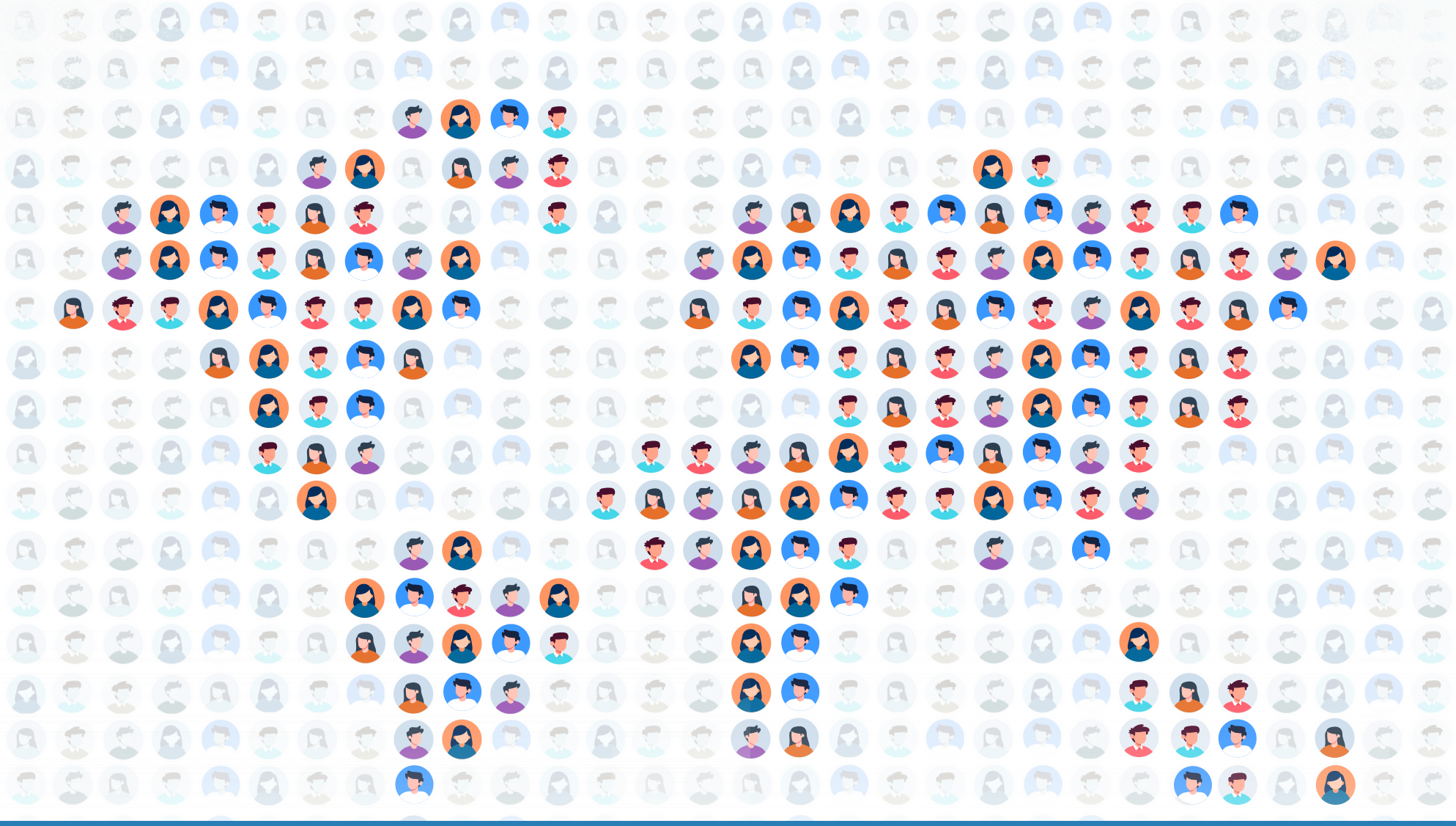
غالبًا ما تحتوي المواقع المزيفة على تصميمات ضعيفة الجودة، كلمات فيها أخطاء إملائية، أو ألوان غير متناسقة مع العلامة التجارية الرسمية.

تحققوا من عنوان URL

يقوم المجرمون السيبرانيون بإنشاء عناوين URL تشبه المواقع الحقيقية مع تغييرات طفيفة مثل تغيير حرف او اضافة بديلة (مثل "gmall.com" أو "facebouk.com" او"amazon.shop").
تأكدوا دائمًا من صحة تهجئة عناوين URL قبل إدخال معلومات حساسة.

أصبح التعرف على التهديدات الرقمية مهارة أساسية في عالمنا القائم على التكنولوجيا، لاسيما مع ارتفاع التهديدات المتقدمة المستمرة (APTs)، والتي يتم تنفيذها عادة بواسطة قراصنة ذوي مهارات عالية غالبًا ما يكونون تابعين لدول أو جهات مدعومة من الدول، ومع زيادة استخدام الذكاء الاصطناعي من قبل المجرمين السيبرانيين لتطوير هجماتهم، بما في ذلك رسائل التصيد الاحتيالي المولدة بالذكاء الاصطناعي والتزييف العميق (Deepfake).

ان البقاء على حذر تجاه محاولات التصيد، وإصابات البرمجيات الضارة، والمواقع المزيفة، مع تبني نهج استباقي للأمن السيبراني، يمكن أن يقلل بشكل كبير من تعرضكم للهجمات السيبرانية.
تذكروا دائمًا، الأمن السيبراني لا يتعلق فقط باستخدام الأدوات الصحيحة؛ بل يتعلق أيضًا بالوعي واكتساب عادات جيدة. من خلال تثقيف أنفسكم بانتظام حول التهديدات الناشئة، يمكنكم الاستعداد لمواجهة بيئة رقمية تتطور باستمرار.



مؤسسة مهارات

العنوان:
جديدة، المتن
لبنان

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

مهارات
Maharat