دليل السلامة الرقمية

Jordan Open Source Association | facebook

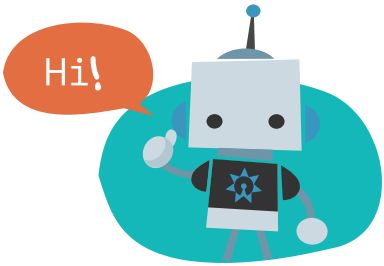
دليل السلامة الرقمية

الفهرس

Jordan Open Source Association | facebook

اهلا و سهلا في دليل السلامة الرقمية

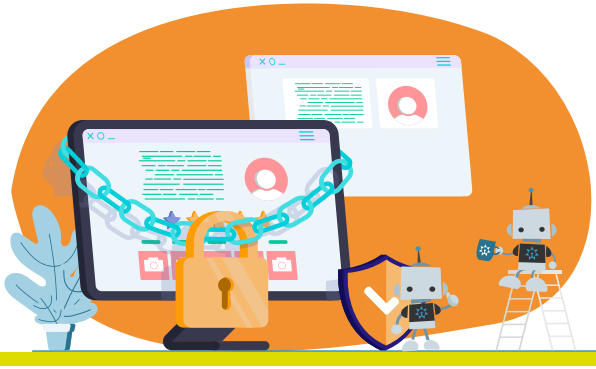
مصطلحات



من خلال هذا الدليل، سنقوم بالإشارة إلى (شركة فيسبوك) بصفتها الشركة، و (فيسبوك) بصفته تطبيق وسائل التواصل الاجتماعي.
يرجى العلم أن شركة فيسبوك تمتلك وتدير مجموعة تطبيقات التواصل التالية:

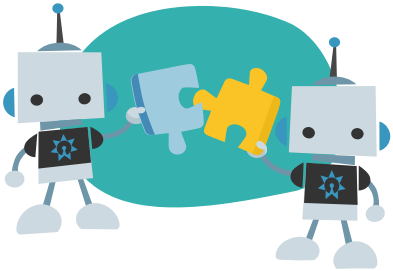
لمزيد من المعلومات حول شركة فيسبوك، يرجى زيارة: about.fb.com

Jordan Open Source Association | facebook



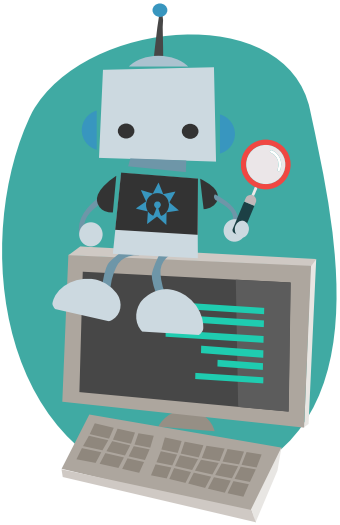
السلامة الرقمية في خمس خطوات

تعتبر سلامة المستخدم أمرا بالغ الأهمية لشركة فيسبوك. إذ أن الشركة تبذل قصارى جهدها لحماية المستخدمين في مجموعة التطبيقات التي تديرها، إلا أنه لا توجد منصة خالية من المخاطر وآمنة بشكل كامل. لهذا السبب، من المهم لك بصفتك مستخدم لهذه التطبيقات أن تعرف ما يمكن عمله لتخفيف المخاطر ولكي لا تكون ضحية للتهديدات الشائعة على الانترنت.



يزودك هذا الدليل بالإرشادات الأساسية لحماية المستخدمين من التهديدات الشائعة لمجموعة تطبيقات الشركة. هذه الإرشادات والنصائح مباشرة وليست بحاجة إلى معرفة متخصصة لاتباعها في هذا المجال. لقد صممت شركة فيسبوك منصاتها بهدف أن تمنح الناس قدرة التحكم في تجاربهم الخاصة ونأمل أن تساعد هذه النصائح المستخدمين لنلتقي معا في منتصف الطريق.

للمساعدة في فهم الفكرة العامة للسلامة الرقمية، دعنا نشبّهها بباب المنزل.



السلامة الرقمية في خمس خطوات

١. المصادقة الثنائية

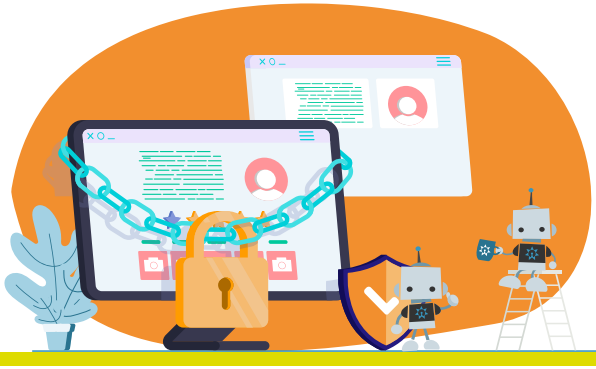
تشبه المصادقة الثنائية حماية منزلك بقفلين مختلفين بدلاً من قفل واحد. في كل وقت تريد تسجيل الدخول، فإنك تحتاج لاستخدام كلمة السر الخاصة بك، بعد ذلك الرمز الذي تم إرساله الى جهازك المحمول لديك، من أجل الدخول على الحساب الخاص بك. وفي هذه الطريقة، وحتى لو عرف شخص كلمة السر الخاصة بك، إلا أنه لا يستطيع الدخول الكامل لحسابك.

يمكن تفعيل خاصية المصادقة الثنائية بالخطوات التالية:

على فيسبوك، انقر على:
الإعدادات والخصوصية > الإعدادات > الأمان وتسجيل الدخول > استخدام المصادقة الثنائية

على انستجرام، انقر على:
الإعدادات > الأمان > المصادقة الثنائية

على واتساب، انقر على:
الإعدادات > الحساب > التحقق بخطوتين > تمكين



السلامة الرقمية في خمس خطوات

٢. تفعيل تنبيه تسجيل الدخول

يعمل تنبيه تسجيل الدخول مثل جهاز إنذار المنزل. في حال شك الشركة أن شخصا ما دخل بأسلوب غير مصرح إلى الحساب الخاص بك، أو شخصا ما دخل الى الحساب عبر جهاز غير معروف، ستستلم إشعار إلكتروني حول هذا النشاط غير الطبيعي

يمكنك أن تفعل تنبيهات تسجيل الدخول على فيسبوك:

على فيسبوك، انقر على:
الإعدادات والخصوصية > الإعدادات > الأمان وتسجيل الدخول تلقي تنبيهات بشأن تسجيلات الدخول غير المعروفة (تحت إعداد إجراءات أمان إضافية)

إليك طريقة التحقق من نشاط تسجيل الدخول:

على فيسبوك، انقر على:
الإعدادات والخصوصية > الإعدادات > الأمان وتسجيل الدخول > المكان الذي سجلت دخولك منه.

على انستجرام، انقر على:
الإعدادات > الأمان > نشاط تسجيل الدخول

و ايضا يمكن النقر على:
الإعدادات والخصوصية > الإعدادات > الأمان وتسجيل الدخول > تلقي تنبيهات بشأن تسجيلات الدخول غير المعروفة (تحت إعداد إجراءات أمان إضافية)

Jordan Open Source Association | facebook

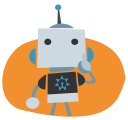
السلامة الرقمية في خمس خطوات

٣. استخدام كلمات سر قوية

بنفس الأسلوب، لن تستطيع حماية باب منزلك بواسطة عقدة رخوة، فلن تستطيع حماية الحساب الخاص بك بكلمة سر سهلة معرفتها أو من السهل تخمينها.

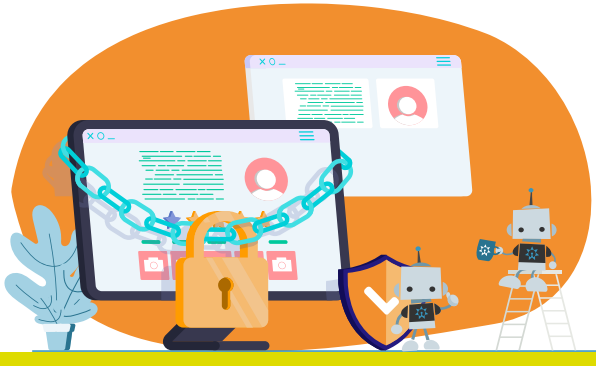
نوضح تاليا ما يمكن أن تفعله:

يجب أن تكون كلمة السر الخاصة بك أطول من ٨ أحرف، تحتوي على أرقام وحروف.

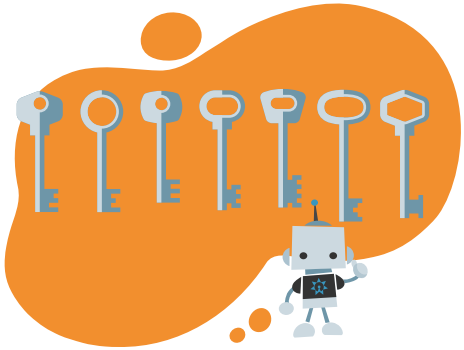


يجب أن تتمكن من تذكرها بسهولة، وفي نفس الوقت أن تكون من الصعب أن يعرفها أشخاص آخرون.

نصيحة : لا تختار اسم فرقة موسيقية تعرفها، بل جملة من نص أغنية من الأغنيات المفضلة لديك.



السلامة الرقمية في خمس خطوات



٤. استخدم كلمات سر مختلفة

تصور انك تستخدم نفس المفتاح للدخول إلى سيارتك، وبيتك ومكتبك. في حال تمكن اللص من الحصول على مفتاحك في أي وقت، فسيتمكن من فتح أي شيء آخر. نفس الشيء ينطبق على حساباتك على الانترنت، حماية هذه الحسابات بنفس كلمة السر سيجعل مهمة اللص سهلة للغاية.

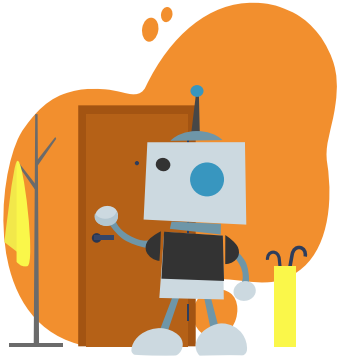
نذكر أدناه ما يمكن أن تقوم به:

اختر كلمة سر غير مستخدمة في أي مكان آخر على الانترنت.

في حال خفت من أن تنسى كلمات السر الخاصة بك، استخدم برنامج لإدارة كلمات السر. وهو تطبيق يعمل على تخزين جميع بيانات الاعتماد الخاصة بك على الانترنت. كما ينطبق على الجهاز المحمول وسطح المكتب.

لا تشارك كلمة السر الخاصة بك أو تكتبها في أي مكان. في حال اضطررت أن تفعل ذلك، يمكن تخزينها عبر تطبيق لإدارة كلمات السر.

السلامة الرقمية في خمس خطوات



٥- تذكر دائما بالتحقق من مصدر رسائل البريد الإلكتروني

عندما يقرع شخص ما جرس الباب، فإنك لن تفتح له الباب أولا ولكن تنظر عبر العين السحرية لتتأكد من أنه صديق أو قريب لك وتثق به. يمكن لأشخاص ينوون الشر بأن يحاولوا الوصول إلى معلوماتك عبر رسائل إلكترونية مضللة تظهر بأنها من فيسبوك أو انستجرام. يقومون باستخدام هذه الرسائل الإلكترونية لغرض معين أو أكثر: كسرقة معلومات تسجيل الدخول الخاصة بك بأن يطلبوا منك تعبئة نموذج، أو يحملون فيروس على الجهاز الخاص بك عن طريق إقناعك بالضغط على رابط.

للتحقق من مصدر رسائل البريد الإلكتروني:

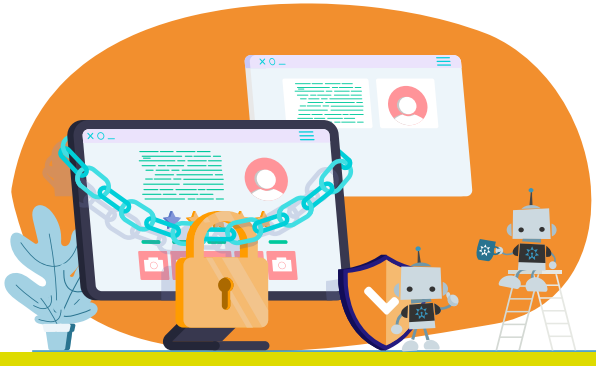
على فيسبوك، انقر على:
الإعدادات والخصوصية > الإعدادات > الأمان وتسجيل الدخول > عرض أحدث رسائل البريد الإلكتروني من فيسبوك

على انستجرام، انقر على:
الإعدادات > الأمان > رسائل البريد الإلكتروني الواردة من انستجرام

المصدر:

facebook.com/safety
https://www.facebook.com/about/basics/stay-safe-and-secure
https://www.facebook.com/about/basics/manage-your-privac
Instagram.com/safety
whatsapp.com/safetymessenger.com/privacy

Jordan Open Source Association | facebook



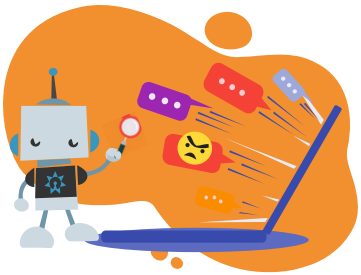
السلامة الرقمية للمستخدمين المستهدفين

يشمل المستخدمون المستهدفون لمخاطر عالية المدافعين عن حقوق الإنسان، والنشطاء، والمراسلين الصحفيين، بالإضافة إلى السياسيين وموظفيهم، والمؤثرين إعلاميا. في الغالب، فإن هؤلاء الأفراد مستهدفون في الهجمات الالكترونية. ويعزى ذلك إلى أن الدخول إلى حساباتهم ذو قيمة أعلى للمهاجمين.

على سبيل المثال، يخطط المدافعون عن حقوق الإنسان نشاطاتهم في المناصرة والمدافعة - وتعتبر هذه المعلومات ذات قيمة بالنسبة للسلطات. أيضا، فإن الصحفي الذي يجري تحقيقات حول الفساد يمكن أن يكون مستهدفا أيضا من جانب شركة ما.

إن التغيير في أساليب السلامة الرقمية، حتى في أبسط الممارسات، لا يعتبر سهلا. ولكن لا بد من الإشارة بأن دراسة حديثة أفادت بأن معظم اختراقات البيانات تعزى إلى خطأ إنساني وليست لثغرات أمنية. لذا، يعتبر تغيير السلوك ضروريا لحمايتك على الانترنت.

يجب على المستخدم االمستهدف التخطيط للتعرف على التهديدات المحتملة.



السلامة الرقمية للمستخدمين المستهدفين

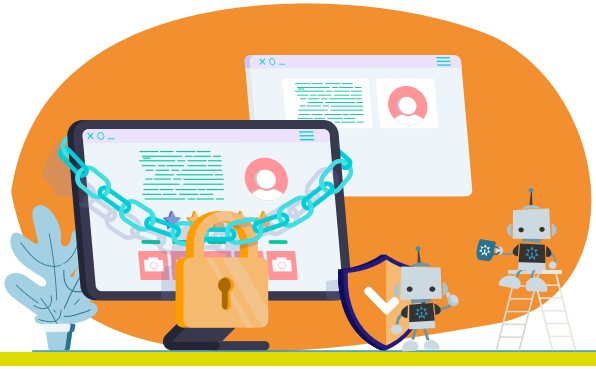
١. الحماية من اختراق الحساب

المصادقة الثنائية عن طريق تطبيق للمصادقة أفضل من المصادقة عن طريق الرسائل النصية

استلام رمز التحقق عبر رسالة نصية SMS يشبه إخفاء المفتاح الثاني تحت سجادة مدخل البيت، وكأنها على مرأى من الجميع. يعد استخدام تطبيق للمصادقة بكلمة مرور مؤقتة بديلاً أفضل بكثير، كما لو أنك تقوم بحماية المفتاح في قاصة حديدية. يوصى بشدة بتنزيل تطبيق موثق للمصادقة، ويفضل أن يكون مفتوح المصدر، وفي حال قمت بتفعيل المصادقة الثنائية على الفيسبوك والانستجرام، تقوم بطلب الرمز عبر التطبيق.

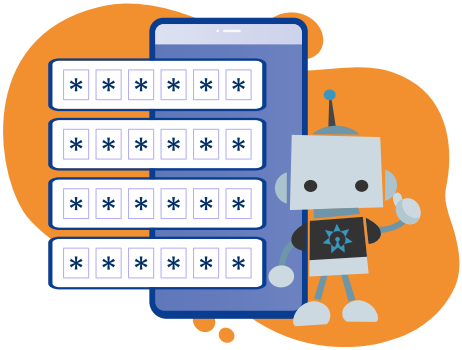
نظف أسنانك بالفرشاة، استخدم مدير كلمة السر

بالنسبة للمستخدمين المستهدفين، يعتبر استخدام تطبيق لإدارة كلمات السر ضروريا كتنظيف الأسنان بالفرشاة. لا يكتفي المهاجمون بتخمين كلمات المرور فحسب، بل يستخدمون برامج للكشف عن كلمات المرور من خلال تجربة كل الخيارات الممكنة لها، (ويمكن تشبيهها بكسر قفل الباب). لذا من الضروري أن تكون كلمة السر قوية ومميزة، وكذلك لكي لا تستخدم كلمة السر في أي مكان آخر. يقدم تطبيق إدارة كلمات السر المساعدة في تخزين كلمات السر الخاصة بك بشكل آمن، وكذلك استحداث كلمات سر لا تمتلكها. أنت تحتاج فقط أن تحفظ كلمة السر الرئيسية للدخول على تطبيق إدارة كلمات السر.



السلامة الرقمية للمستخدمين المستهدفين

هناك فائدة أخرى من استخدام تطبيق لإدارة كلمات السر وتتمثل في تخزين الملاحظات أيضًا بشكل آمن. لعلك تسأل عن متى يصبح ذلك ضروريا؟ عندما تفعّل خاصية المصادقة الثنائية، فإن تطبيقات شركة فيسبوك ستزّودك برموز للنسخ الاحتياطي تستخدم في حال فقدت القدرة على الدخول إلى جهازك أو التطبيق الذي ينتج كلمة المرور لمرة واحدة لك. يمكن تخزين هذه الرموز الاحتياطية بشكل آمن في تطبيق إدارة كلمات السر لديك.

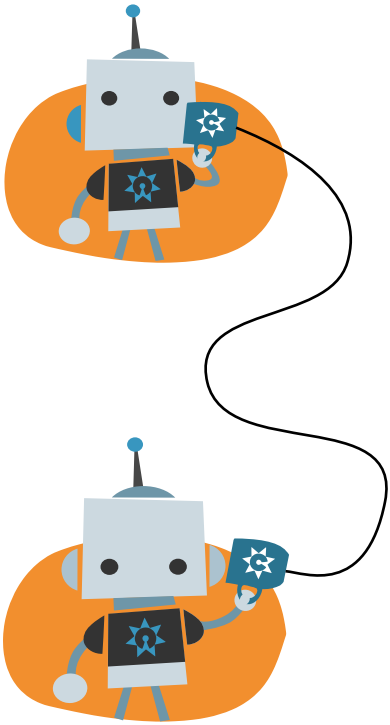


الهجمات التي لا تتطلب أي نشاط من المستخدم - Zero-click exploits

تعتبر الثغرات الأمنية أمرا لا مفر منه. تعمل الأبواب على تقديم حماية لا غنى عنها للبيوت، ولكنها ما تزال قابلة للكسر. تعامل شركة فيسبوك الأمن الرقمي بجدية تامة عند اكتشاف أي ثغرة أمنية، ستقوم الشركة بإشعارك في حال ما يكون الحساب الخاص بك مستهدفا أو كان مخترقا.

السلامة الرقمية للمستخدمين المستهدفين

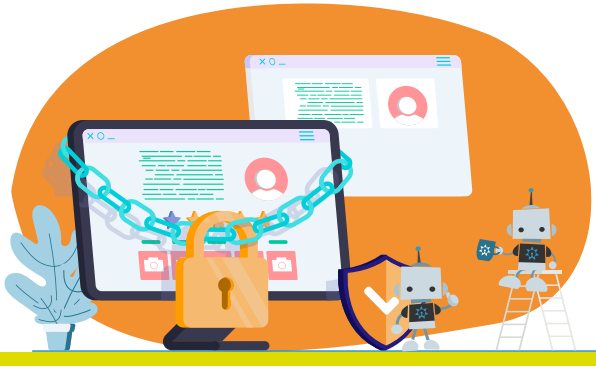
٢. الحماية من التطفل والمراقبة



التواصل الخاص

تُشارك بعض لحظاتك الشخصية على واتساب، ولهذا السبب قامت شركة فيسبوك ببناء التشفير التام (أو التشفير من طرف إلى طرف - end-to-end cryption) في أحدث إصدارات تطبيقها. عن طريق هذا التشفير، يتم تأمين رسائلك ومكالماتك بحيث لا يمكن لأي شخص آخر التنصت أو الاستماع إليها، بما فيها واتساب أيضا. يقصد بهذا النوع من التشفير أنه لا يمكن لأي شخص التنصت على الرسالة عند إرسالها ولغاية وصولها إلى الشخص المستلم لها. على تطبيق واتساب، يمكن إرسال «رسائل ذاتية الاختفاء»، لكي تكون الرسائل الجديدة في الدردشة تختفي تلقائيا بعد سبعة أيام. من أي دردشة على واتساب يمكن أن تضغط على اسم الشخص المتصل به ومن ثم الضغط على الرسائل ذاتية الاختفاء.

يقدم مسنجر ميزة تسمى الدردشة السرية، يمكن من خلالها أن تتحدث إلى شخص ما بطريقة مشفرة.



السلامة الرقمية للمستخدمين المستهدفين

النسخ الاحتياطي لبيانات المحادثة

دردشات مسنجر والرسائل المباشرة على انستجرام تُخزن للأبد على خوادم الشركة. إذا أرسلت معلومات حساسة عن طريق الخطأ، لديك عشر دقائق لتكون قادرا على حذف الرسالة بالنقر على الرسالة واختيار خيار الحذف. على تطبيق واتساب لديك حوالي ساعة لحذف الرسالة.

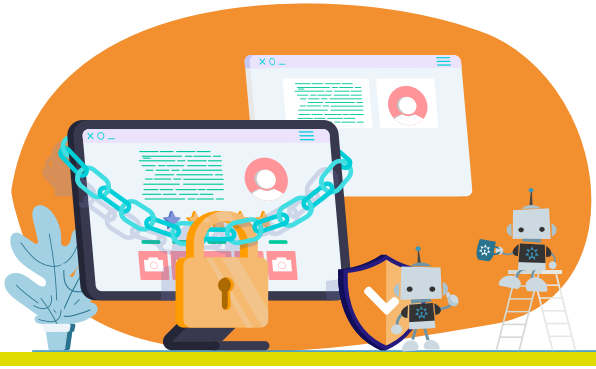
تُخزّن الدردشة عبر واتساب على جهازك محليا. يمكن أيضا أن تختار تخزين الدردشات على مزود السحابة الشخصية مثل iCloud وجوجل درايف Google Drive من المهم أن تعلم أن النسخ الاحتياطي غير محمٍ بالتشفير، لذا عليك التأكد أنك تأخذ بعين الاعتبار الأساليب الصحيحة لحماية النسخ الاحتياطية على السحابة مثل تفعيل المصادقة الثنائية (التحقق بخطوتين) واستخدام كلمة سر قوية ومميزة لحماية الحساب الخاص بك.

تهديدات شائعة على الانترنت

لكي تدرك كفاءة إجراءات السلامة المشار إليها أعلاه، من المهم للمستخدمين معرفة التهديدات الأكثر شيوعا التي قد يواجهونها في عالم الانترنت.

١. الحسابات المخترقة والمسروقة

مخترقو الحسابات على الانترنت -والذين يسمون عادة بالقراصنة Hackers- يمكنهم الحصول على دخول غير مفوض إلى حساب المستخدم، وغالبا ما يتم ذلك عن طريق معرفة أو تخمين كلمة السر الخاصة بالمستخدم. لذا تقوم شركة فيسبوك بمحاولة إقصاء القراصنة، وكذلك على المستخدمين أيضا اتخاذ الاحتياطات الضرورية لحماية كلمات السر الخاصة بهم وحساباتهم.



تهديدات شائعة على الانترنت

٢. الابتزاز

عندما يقوم المستخدم بالتواصل مع مستخدم آخر ومحاولة الحصول على المال أو أي منفعة أخرى، عن طريق التهديد بكشف معلومات خاصة أو معلومات قد تضر الضحية، يسمى هذا العمل (ابتزاز). عندما يُهدّد المستخدم بالكشف على صور ذات طبيعة جنسية، يشار إليها بالابتزاز الجنسي.

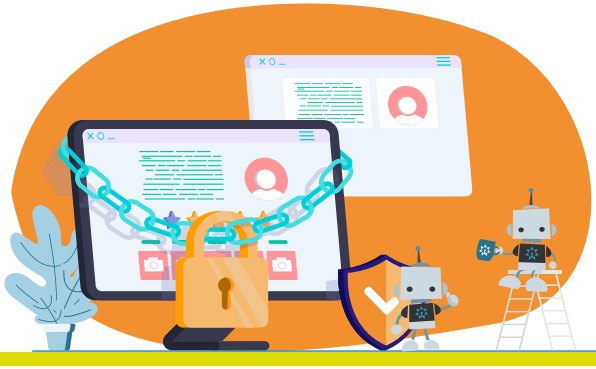
٣. الهندسة الاجتماعية

الهندسة الاجتماعية هي عملية تلاعب بشخص ما للقيام بعمل معين، أو الكشف عن معلومات شخصية غالبًا ما تكون حساسة. يقوم القراصنة في الغالب بإنشاء صداقات أو استخدام حيل نفسية لإقناع شخص ما لمشاركتهم بالصور، مشاركة كلمات السر... الخ. بدلا من العثور على ثغرة أمنية في البرنامج، يمكن للمهاجم أن يتظاهر زُورًا أنه شخص يقدّم الدعم الفني وأن لديه هدفا نبيلا لمساعدة المستخدمين ودعمهم عن طريق حماية حساباتهم، ويطلب منهم معرفة كلمات السر الخاصة بهم للسير لتحقيق هذا الهدف.

تهديدات شائعة على الانترنت

٤. هجمات التصيد

التصيـد يتمثل عندما تتنكر جهة وتظهر بأنهـا جهة موثوق بها ويحاول الحصول على معلومات حساسـة من مستخدم آخر ككلمات السـر الخاصة به أو معلومات عن بطاقة الائتمان. على سـبيل المثال، يتظاهر شـخص ما بكونه يعمل في محل تجاري، يرسـل لك رسالة تعلمك بأن لديهم خصم عـلى البضاعة في ذلك المحل. يطلب منك بعدها بالقيام بعملية الشـراء عبر واتساب، وإرسـال رقم بطاقة الائتمان الخاصة بك، تاريـخ الانتهاء، والرمز الأمني من أجل تكملة عملية البيع لك. مثال آخر، أن تسـتلم رسالة الكترونية تظهر انها من موقع فيسـبوك. تنص الرسـالة على تعرُّض الحساب الخاص بـك للتهديد وأن عليك الدخول فورا على حسـابك لحل المشكلة. تقوم بالضغط على إشـارة تسجيل الدخول من الرسالة وإضافة كلمة السـر الخاصة بك. في هذه الحالة فإنك تـزوّد بيانات الدخول هذه إلى القراصنة.



تهديدات شائعة على الانترنت

٥. روابط خبيثة

يمكن للمستخدم أن يستلم روابط بواسطة رسائل أو تعليقات تبدو وكأنها تروج لشيء حقيقي ولكن في الحقيقة تكون روابط خبيثة وتهدف إلى التصيد والاحتيال. في حال الضغط على الرابط، يتم تنزيل فيروس أو برنامج خبيث على جهاز المستخدم. الفيروس المستخدم في الغالب يعمل على سرقة البيانات الشخصية. للكشف فيما إذا كان الرابط خبيثًا، انسخ الرابط دون الضغط عليه ، انتقل إلى موقع VIRUSTOTAL.COM وألصقه في صندوق البحث. يقوم الموقع بالتأكد من الرابط ويطلعك فيما إذا كان الرابط غير صحيح، أو ليس جديرا بالثقة.

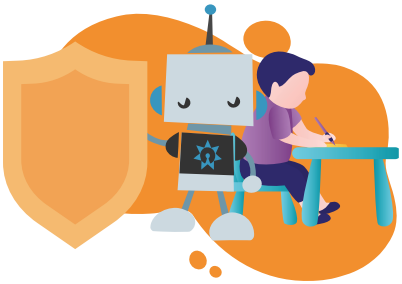
٦. انتحال الشخصية والحسابات المزورة

غالبًا ما يكتشف المستخدمون حسابات تبدو بأنها تخص شخصًا يعرفونه، أو تظهر بمعلومات، أو تبدو ببساطة بأنها مزورة. هذه الحسابات المزورة قد تكون تهديدا حيث أنها غالبا ما تكون مستخدمة لاكتساب ثقة مستخدمين آخرين وإضافة تابعين وأصدقاء، وقد تستخدم هذه الحسابات المزورة بعدها لتهديد المستخدم الذي ينتحلون شخصيته أو ابتزازه.

ما ذكر أعلاه يعتبر تهديدات عامة وشائعة على الانترنت. هناك تهديدات أكثر انتشارًا بين المستخدمين في منطقة الشرق الأوسط وشمال أفريقيا، لذا من المهم تسليط الضوء عليها كل على حدة، وتبيين أعراضها، والأساليب الممكنة للتقليل من حدتها. تعمل شركة فيسبوك على تطبيق سياسات، وأدوات والتكنولوجيا لمكافحة كل هذه التهديدات، منها:

تهديدات شائعة على الانترنت

٧. استغلال الأطفال

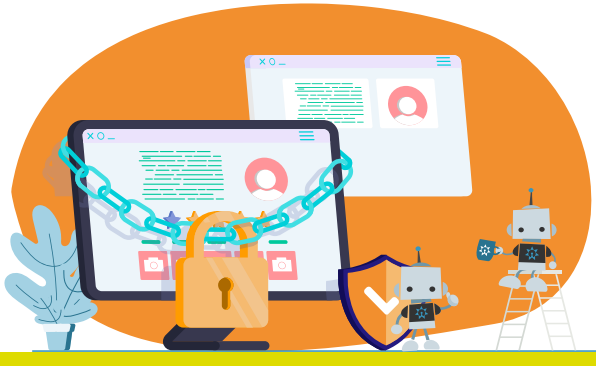


ما المقصود من استغلال الأطفال؟
لا تتسامح شركة فسيبوك مع أي سلوك أو محتوى يستغل الأطفال على الانترنت وتطور برامج الأمان والموارد التعليمية للمساعدة في جعل الانترنت مكانًا أكثر أمانًا للأطفال. للمستخدمين دور كبير في وقف ما يسمى باستغلال الأطفال. يمكن أن يصنف استغلال الأطفال على الانترنت إلى ثلاث فئات:

محتوى غير لائق: ويعني نشر وتوزيع مواد تحتوي على استغلال للأطفال. على سبيل المثال، القيام بإنشاء منشور يحتوى على صورة طفل يتعرض إلى إساءة جسدية، أو نشر فيديو عن أطفال يتعرضون للاستغلال الجنسي، أو مشاركة المحتوى الذي يحتوي على أي نوع من أنواع الإساءة الجسدية أو الاستغلال الجنسي للأطفال... الخ

سلوك غير لائق: يعني أي عمل يحرض أو يجبر الطفل على المشاركة في نشاط غير لائق. ويشمل على سبيل المثال التعليق على منشورات طفل بتعليقات غير لائقة، إزعاج الطفل وزرع شعور عدم الأمان في نفسه، التحرش بالطفل.... الخ

اتصال غير لائق: يعني إغراء طفل على الانترنت لغرض تحقيق اتصال جنسي. على سبيل المثال، الاتصال مع الطفل على الانترنت لغرض استغلاله إما على الانترنت أو في الواقع، و/أو إجباره للمشاركة في نشاط جنسي، بما فيه مشاركة صور أو أفلام حميمة معه.



تهديدات شائعة على الانترنت

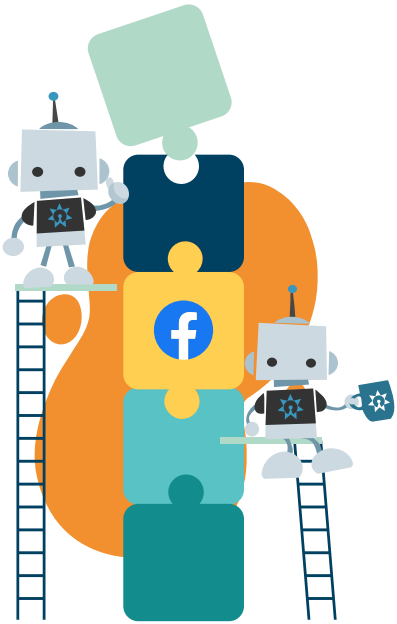
كيف تكافح شركة فيسبوك استغلال الأطفال؟
تتمثل إحدى مسؤوليات الشركة الأكثر أهمية في أن تبقى مجموعة التطبيقات آمنة فيما يتعلق باستغلال الأطفال. تعمل الشركة على تبني ممارسات متعددة لمكافحة استغلال الطفل على منصاتها.

السياسات | سياسات تقديم حمايات مميزة للقاصرين: تشترط منصات شركة فيسبوك على كل شخص أن يكون بعمر لا يقل عن ١٣ عاماً قبل أن يتمكن من إنشاء حساب (قد يكون شرط العمر هذا أعلى في بعض المناطق). يخالف التزويد بعمر زائف عند إنشاء حساب شروط خدمات شركة فيسبوك. وباستطاعة الناس الإبلاغ عن حساب يعود إلى شخص دون سن ١٣ عاماً. ولا تسمح شركة فيسبوك بالمحتوى الذي يستغل الأطفال جنسياً أو يعرضهم للخطر. وعندما تعلم شركة فيسبوك بوجود استغلال واضح للأطفال، تقوم بالإبلاغ عنه لدى المركز الوطني للأطفال المفقودين والمستغلين (NCMEC) وفقاً للقانون ساري المفعول. وتضع فيسبوك أيضاً قيوداً على تفاعل الأطفال بعمر ١٣ إلى ١٨ عاماً مع المستخدمين الآخرين وتضع قيوداً حسب العمر على المحتوى الذي يتفاعلون معه.

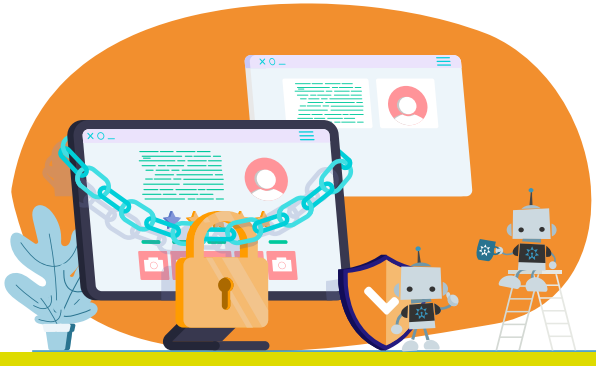
الأدوات والتكنولوجيا | عمليات الإزالة التلقائية: قامت شركة فيسبوك بتصميم منصتها لتعطي إلى الناس زمام التحكم بتجاربهم الخاصة – التحكم بما يريدون مشاركته ومع من يريدون أن يشاركوه والمحتوى الذي يرونه ويعيشون تجربته ومن يستطيع التواصل معهم. تمكن هذه الأدوات الأفراد من حماية أنفسهم من المحتوى غير المرغوب به والتواصل غير المرغوب به والتنمر والتحرش على الانترنت. وعندما يتعلق الأمر بالمستخدمين الذين تتراوح أعمارهم ما بين ١٣-١٨ سنة، فإن شركة فيسبوك نتخذ تدابير وقائية إضافية. لقد صممت الكثير من خصائصها لتذكير هؤلاء المستخدمين بمن يشاركون معه ولفرض قيود على التفاعلات مع

تهديدات شائعة على الانترنت

الغرباء. وتستخدم فيسبوك تقنية التعلم الآلي لتحديد المحتوى الذي يستغل الأطفال تلقائياً، وتتخذ إجراء استباقياً بإزالة ذلك من منصتها. كما تضيف فيسبوك أيضاً مواد استغلال الأطفال المؤكدة إلى بنك من الصور المشارَكة بحيث يتم التمكن من إزالة الصور المطابقة للمادة الموجودة في البنك بشكل تلقائي.



الشراكات | الشراكة مع الخبراء: لا تتسامح فيسبوك مع أي سلوك أو محتوى يستغل الأطفال على الانترنت ونطور برامج أمان وموارد تثقيفية مع أكثر من ٤٠٠ منظمة حول العالم للمساعدة على جعل الانترنت مكاناً أكثر أمناً للأطفال. وتضمن عمل شركة فيسبوك استخدام تقنية مطابقة الصور لمنع الناس من مشاركة صور استغلال الأطفال المعروفة، والإبلاغ عن المخالفات لدى المركز الوطني للأطفال المفقودين والمستغلين (NCMEC)، ويعمل المركز مع جهات تنفيذ القانون حول العالم لمساعدة الضحايا، وتعمل الشركة على مساعدة المؤسسة على تطوير برمجيات جديدة تساعد على جعل التقارير التي تشاركها مع منفذي القانون أولوية لها من أجل التعامل مع الحالات الأكثر خطورة أولاً.



تهديدات شائعة على الانترنت

٨. التنمر والتحرش

ما هو التنمر والتحرش؟
بصفتك مستخدم لإحدى التطبيقات من شركة فيسبوك، من المهم أن تدرك ما الذي يشكل تنمرا، إذا لم تكن متأكدا فيما إذا قُصد من شيء ما بأنه نكتة أو تنمر، فإنه يجب عليك أن تسأل نفسك فيما إذا ما يكون هذا التصرف يسبب لك الأذى. إذا كان الجواب بنعم، في هذه الحالة فإن السلوك يشكّل تنمرا.

التنمر هو عمل ما يؤدي إلى إلحاق الضرر أو إزعاج شخصاً ما. وهذا يمكن أن يشمل أيضًا الإهانة و تقليل من كرامة شخص ما.

التضييق هو سلوك تمييزي ومؤذي بطبيعته، وهو مبني على عرق شخص ما أو الديانة أو النوع أو التوجه الجنسي... الخ

على سبيل المثال فإن التنمر الإلكتروني يشتمل على:
نشر الإشاعات والأسرار حول شخص ما، ويهدف في الغالب إلى تحقير الشخص.
مثلا: أنك تنام مع كل الرجال في مكان العمل.

إرسال رسائل مؤذية أو تهديدات:
مثل انك غبي، تستحق الموت... الخ

خداع شخص ما بواسطة الفيديو أو مكالمة صوتية

نشر صور محرجة لصديق بهدف تحقيره.

تهديدات شائعة على الانترنت

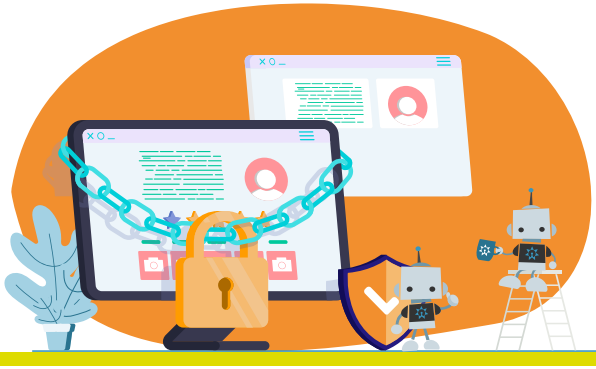
كيف توقف شركة فيسبوك التنمر والتحرش؟

الأدوات: منح المستخدمين مزيدا من التحكم:

قامت الشركة بطرح ميزات لمنح المستخدم القدرة على التحكم بوجودهم على الانترنت. مستخدمو فيسبوك وانستجرام يمكنهم إزالة التعليقات المؤذية والسيئة، والإبلاغ عن مستخدم ما بسهولة، بل والإبلاغ عن المستخدمين أو التعليقات عن الأصدقاء أو أعضاء المجموعة اللذين يتعرضون للتنمر والتحرش.

التكنولوجيا- إشعار المستخدمين عندما يقومون بكتابة تعليقات سيئة:

عندما يحاول المستخدم على انستجرام رفع صورة ما مع تعليق بقصد الإساءة، يعمل تطبيق انستجرام تلقائيا بتحري موضوع التعليق الذي يحتمل أن يكون مسيئا وتنبيه للمستخدم بأن التعليق يشبه محتوى آخر تم الإبلاغ عنه، وأن حسابه ربما يخالف إرشادات المجتمع.



٩. مشاركة الصور الحميمة بدون موافقة

ماذا تعني مشاركة الصور الحميمة بدون موافقة؟

يتمثل هذا الأمر عندما يقوم شخص ما بنشر صور حميمة دون الحصول على موافقة المرسل اليه. يشار الى هذا الأمر بـ "الانتقام الإباحي".

عندما يهدد شخص ما بنشر صور إباحية. ما لم يوافق الضحية على القيام بشيء ما في المقابل، مثل المشاركة بنشاط جنسي أو إرسال صور إباحية أكثر، فإن هذا الأمر يتم تصنيفه بصفته ابتزاز جنسي.

كيف توقف شركة فيسبوك ذلك؟

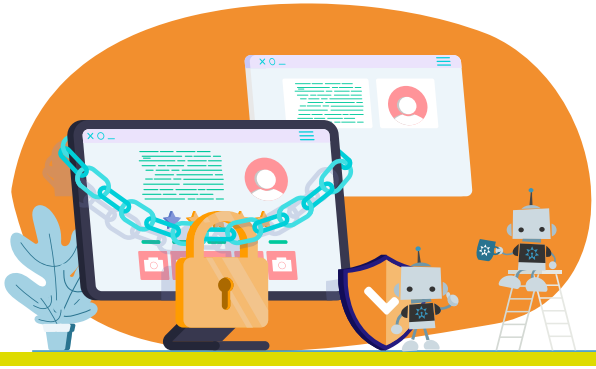
تكنولوجيا | تقنية مطابقة الصور:

تستفيد الشركة من التعلم الآلي وتكنولوجيا الذكاء الاصطناعي للعثور على الصور ومقاطع الفيديو التي تحتوي على عُري أو شبه عُري والكشف عنها تلقائيًا عند مشاركتها على فيسبوك وانستجرام دون موافقة.

تهديدات شائعة على الانترنت

الأدوات | الإبلاغ:
يمكنك أن تبلغ على فيسبوك وانستجرام ومسنجر عندما يشارك أحدهم صوراً حميمية لك دون موافقتك أو عندما يهدد بنشرها، وذلك عن طريق الإبلاغ عنه. يمكنك تعلم كيفية الإبلاغ عن الأمور على فيسبوك وانستجرام (يمكنك أيضاً تعلم كيفية الإبلاغ عن الرسائل على انستجرام). ويمكنك أيضاً أن تفعل ذلك على فيسبوك باستخدام رابط «الإبلاغ» الذي يظهر عندما تضغط على السهم الموجه إلى الأسفل أو "..." بجانب المنشور.

الأدوات | الصور:
إذا كنت متخوفاً من احتمال أن يقوم أحدهم بمشاركة صورك الحميمية على فيسبوك أو انستجرام أو مسنجر لكنه لم يفعل ذلك بعد، وكان لديك نفاذاً إلى الصور، يمكنك التواصل مع أحد شركائنا الموثوقين هنا لمساعدتك على منع أي شخص من مشاركة الصور.



تهديدات شائعة على الانترنت

العنف القائم على النوع الاجتماعي

ما هو العنف القائم على النوع الاجتماعي؟

يعتبر هذا الأمر سلوكا عنيفا وتهديدا موجه للمرأة على الانترنت. يمكن لهذا العنف أن يتخذ أنماط مثل: التتبع والمطاردة على الانترنت والابتزاز والخداع والتسلط على الانترنت والمضايقات والخطاب الذي يحض على الكراهية والتشهير وغير ذلك.

كيف توقف شركة فيسبوك هذا النوع من الأذى؟

القواعد: سياسات عملية:

مثلا، قامت الشركة بإعادة صياغة سياساتها بخصوص الخطاب الذي يحض على الكراهية بالتشاور مع خبراء سلامة المرأة. هذه السياسات واضحة وعملية بشكل أكبر وتأخذ بعين الاعتبار مقدار العنف غير اللائق الذي تصادفه المرأة على الانترنت.

تذكر الست نقاط

إذا وجدت نفسك في وضع يمكن لشخص ما التحرش بك، أو تهديدك أو التنمر عليك، أو نشر صور دون موافقتك، أو كان عنيفا في مواجهتك، تذكر قاعدة الست نقاط التالية:.

١ **لا تنتقم:** يميل المهاجمون إلى البحث عن ردة فعل من ضحاياهم.

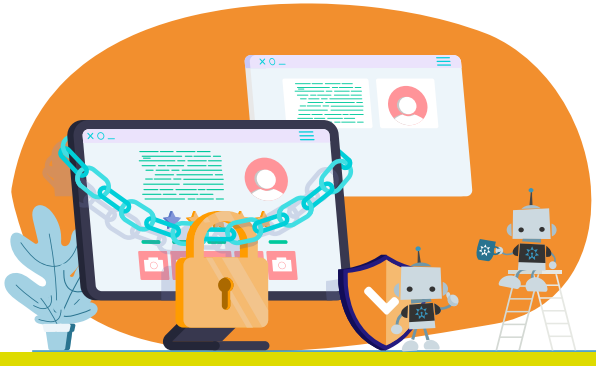
٢ **سجل:** قم بالتقاط صور الشاشة للهجمات واحتفظ بها، فقد تكون مفيدة.

٣ **أبلغ:** أبلغ عن حساب الشخص وأبلغ عن المنشورات والتعليقات المسيئة.

٤ **احذف:** قم بإلغاء الصداقة مع ذلك الشخص أو إلغاء متابعته.

٥ **امنع:** قم بحظر حساب الشخص بحيث لا يتمكن من التفاعل مع حساباتك.

٦ **تواصل:** إذا استمر التهديد، تأكد بإخبار أحد الأشخاص الذين تثق بهم. وإذا كان الأمر خطيراً، قم بإبلاغ الشرطة في منطقتك على الفور.



المصادر

السلامة الرقمية في خمس خطوات

facebook.com/safety
facebook.com/about/basics/stay-safe-and-secure
facebook.com/about/basics/manage-your-privacy
instagram.com/safety
whatsapp.com/safety
messenger.com/privacy

استغلال الأطفال

https://www.unicef.org/media/66616/file/Industry-Guidelines-for-Online-ChildProtection.pdf
https://www.facebook.com/communitystandards/child_nudity_sexual_exploitation
https://learning.nspcc.org.uk/child-abuse-and-neglect/child-sexual-exploitation
https://www.unicef.org/csr/files/pillars.pdf
https://about.fb.com/news/06/2020/fighting-child-exploitation-online/
https://www.facebook.com/safety
https://www.ceop.police.uk/Safety-Centre/what-is-online-child-sexual-abuse/
https://about.fb.com/news/10/2018/fighting-child-exploitation/

التنمر والتحرش

https://www.unicef.org/end-violence/how-to-stop-cyberbullying
https://www.facebook.com/safety/bullying/
https://about.fb.com/news/10/2018/protecting-people-from-bullying/
https://about.fb.com/news/12/2019/our-progress-on-leading-the-fight-against-online-bullying/
https://www.facebook.com/help/1163263651187512?_rdc=2&_rdr

مشاركة الصور الحميمة بدون موافقة

https://www.facebook.com/safety/notwithoutmyconsent
https://www.facebook.com/safety/StopSextortion/
https://about.fb.com/news/03/2019/detecting-non-consensual-intimate-images/
https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/are-you-victim-get-help-report-it-we-are-here

العنف القائم على النوع الاجتماعي

https://about.fb.com/news/10/2019/inside-feed-womens-safety/
https://about.fb.com/news/06/2017/giving-people-more-control-over-their-facebook-profile-picture/

Jordan Open Source Association | facebook

facebook

Jordan Open Source Association

facebook.com/safety

https://jordanopensource.org