تجنب التصيد الاحتيالي

التصيد الاحتيالي هو محاولة غير شريفة لخداع شخص ما بطريقة تعود بالنفع المالي على الشخص المُخادع على حساب الشخص المعرض للخداع. من المهم فهم بعض الأنواع الشائعة من التصيد الاحتيالي ومعرفة كيفية اكتشافه.

حالات التصيد الاحتيالي الشائعة

فيما يلي أربعة أمثلة على حالات التصيد الاحتيالي الشائعة، وهناك مئات الحالات الأخرى. بشكل عام، كن حذرًا من المكالمات أو رسائل البريد الإلكتروني أو الرسائل النصية التي تقدم إليك عروضًا جيدة جدًا لدرجة يصعب تصديقها، أو توجه تهديدات أو اتهامات، أو مليئة بالأخطاء الإملائية والنحوية، أو تطلب معلومات محددة للهوية الشخصية (PII).

المكاسب غير المتوقعة

في حالات التصيد الاحتيالي هذه، يتم الاتصال بالشخص المتعرض للخداع وإخباره بأنه قد ربح مبلغًا ماليًا أو سلعًا أو خدمات في مسابقة لم يشارك فيها، ويُطلب منه إرسال أموال أو معلومات PII من أجل المطالبة بمكاسبه، دون أن تأتي أبدًا هذه المكاسب. وباستخدام معلومات PII الخاصة بك، يمكن للشخص المُخادع أن يدخل إلى حسابك المصرفي ويحول مدخراتك إلى حسابه الشخصي.

الجمعيات الخيرية الزائفة

في حالات التصيد الاحتيالي هذه، يتم الاتصال بالشخص المتعرض للخداع من قبل شخص يتظاهر بأنه ممثل لجمعية خيرية، والذي يطلب المال بعد ذلك. ابحث دائمًا عن الجمعيات الخيرية عبر الإنترنت للتأكد من وجودها بشكل قانوني ولا تستخدم سوى بوابات التبرع الآمنة عند التبرع بالمال.

الضرائب المتأخرة

في حالات التصيد الاحتيالي هذه، يتم الاتصال بالشخص المتعرض للخداع من قبل شخص يدعي أنه يمثل دائرة الإيرادات الداخلية (IRS) أو جهة حكومية أخرى، ويهدده بالقبض عليه أو ترحيله في حالة عدم سداد الرسوم. لن تتصل بك دائرة IRS أبدًا لطلب معلومات PII، لذلك لا تعطها لأحد! إذا تلقيت مكالمة من هذا النوع، فابحث عن رقم هاتف المتصل في متصفح البحث على الويب. وهذا سيساعدك على معرفة ما إذا كان قد تم الإبلاغ عن هذا الرقم من قبل باعتباره مصدرًا للتصيد الاحتيالي. إذا انتابك التوتر، فأبلغ مدير الحالة الخاص بك بالحادثة.

عروض عمل مُبهمة

في حالات التصيد الاحتيالي هذه، يتم الاتصال بالشخص المتعرض للخداع من قبل شركة مزيفة تعرض عليه وظيفة قبل إجرائه لأي مقابلة شخصية أو تقدمه رسميًا إلى الوظيفة. لا تقم أبدًا بإعطاء معلومات PII الخاصة بك إلى أي جهة عمل محتملة إلا بعد التحقق أولاً من صفتها الشرعية.

ما هي المعلومات المحددة للهوية الشخصية؟

المعلومات المحددة للهوية الشخصية (PII) هي أي معلومات يمكن من خلالها الكشف عن هوية شخص ما على وجه التحديد. وتشتمل -على سبيل المثال لا الحصر- على ما يلي:

- أرقام الضمان الاجتماعي
- الأسماء الكاملة
- تواريخ الميلاد
- العناوين
- أرقام الحسابات المصرفية

ما هي بعض العلامات الدالة على أن هذه الرسالة هي حالة تصيد احتيالي؟

- لهجة غير رسمية
- طلب الحصول على بطاقة مسبقة الدفع

ماذا أيضًا؟

HIAS

مراقبة الأطفال

باعتبارك ولي أمر في عصر التكنولوجيا الرقمية، قد يكون من الصعب مراقبة نشاط أطفالك على الإنترنت. من المهم أن يتعرّض الأطفال للإنترنت، والذي سيكون جزءًا من حياتهم الاجتماعية والتعليمية والمهنية. ولكن في الوقت نفسه، **من المهم أيضًا حماية الأطفال من الجوانب الضارة للإنترنت، والتي تتضمن التنمر عبر الإنترنت والوصول لمحتوى غير مناسب والاستغلال المالي والمتصيدين عبر الإنترنت**. وتعتبر أدوات الرقابة والمتابعة الأبوية أمرًا ضروريًا لحماية أطفالك.

المصطلحات الأساسية

تشتمل برامج Android وiOS (المقدمة من Apple) الجديدة على أدوات رقابة أبوية مُدمجة. تتاح تطبيقات للرقابة الأبوية مجانًا، أو يمكن شراؤها، على منصات تثبيت التطبيقات *(لمزيد من المعلومات حول متاجر التطبيقات، يرجى الرجوع إلى القسم 1.1)*.

التنمر عبر الإنترنت

يتمثل التنمر عبر الإنترنت في إرسال أو نشر أو مشاركة محتوى سلبي أو ضار أو زائف حول شخص ما في رسائل نصية أو تطبيقات أو على وسائل التواصل الاجتماعي أو المنتديات أو الألعاب، والتي يمكن فيها للأشخاص عرض المحتوى والمشاركة فيه ومشاركته مع الآخرين.

المتصيدون عبر الإنترنت

المتصيدون عبر الإنترنت هم أشخاص بالغون يستخدمون الإنترنت سعيًا لاستغلال الأطفال من خلال الاستعانة بالتكنولوجيا الرقمية لتحديد مواقع الأطفال القصَّر واستهدافهم.

عوامل تصفية المحتوى

تسمح هذه الأدوات بالحد من وصول الأطفال إلى محتوى غير ملائم لأعمارهم. وتتاح عوامل تصفية المحتوى في العديد من التطبيقات والأجهزة والمتصفحات.

أدوات التحكم في الاستخدام

تعمل أدوات التحكم هذه على تقليص الوقت الذي يصل فيه الأطفال إلى تطبيقات معينة، والساعات التي يستخدمون فيها بعض التطبيقات المعينة، وما إذا كان بإمكانهم الوصول إلى التطبيقات أم لا.

أدوات المراقبة

تسمح هذه الأدوات لأولياء الأمور بتتبع موقع الأجهزة ومعرفة ما يفعله الأطفال بأجهزتهم والتعرف على الجوانب الأخرى لاستخدامها.

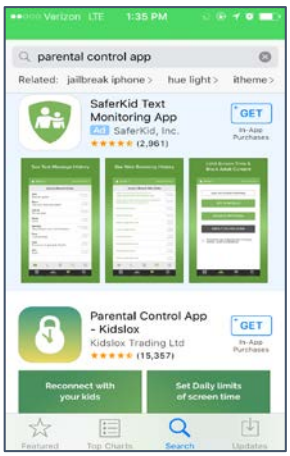
ما يجب أن تحذر منه

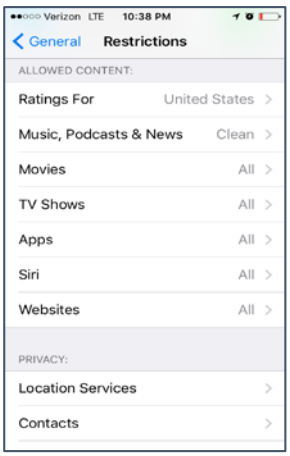
هناك طرق عديدة يمكن من خلالها استغلال الأطفال والشباب على الإنترنت. باعتبارك ولي أمر، سيساعدك فهمك للتنمر والمتصيدين عبر الإنترنت في منع هذا الأمر.

تتميز العديد من التطبيقات والألعاب بعمليات الشراء داخل التطبيق. وهي تسمح للأطفال بإجراء عمليات شراء مالية حقيقية. عند الإمكان، امنع عمليات الشراء داخل التطبيق عن طريق تحديث إعدادات الرقابة الأبوية وتجنب ربط معلومات حسابك المصرفي بمتجر التطبيقات.

يتاح المحتوى العنيف أو الجنسي أو غيره من أشكال المحتوى غير اللائق على نطاق واسع على شبكة الإنترنت. قم بالحد من تعرض طفلك من خلال مراجعة مواقع الويب والألعاب والتطبيقات قبل السماح لأطفالك باستخدامها.

يمكن الحد من تعرض طفلك للمحتوى الضار، ولكن لا يمكنك تجنب هذا الأمر تجنبًا تامًا. **تأكد من مناقشة السلامة على الإنترنت مع أطفالك مباشرة.** وسيستفيدون من هذه المهارات في جوانب أخرى من حياتهم.





إدارة بصمتك الرقمية

بصمتك الرقمية هي سجل إلكتروني يتضمن كل شيء تفعله على الإنترنت. **يتم حفظ جميع الرسائل النصية ورسائل البريد الإلكتروني ومنشورات وسائل التواصل الاجتماعي والصور وعمليات الشراء والبحث عبر الإنترنت إلى الأبد.** هناك طبقتان من هذه البصمة الرقمية. الطبقة الأولى هي المعلومات التي يمكن لأي مستخدم للإنترنت أن يصل إليها. أما الطبقة الثانية فهي المعلومات التي يمكن الوصول إليها من قبل مزود خدمة الإنترنت والشركات والحكومات ومجرمي الإنترنت. من المهم أن تعرف كيف يتم جمع هذه المعلومات وما يمكن استخدامها فيه وطريقة إدارتها.

المصطلحات الأساسية

الإعلانات الموجهة
إن العديد من مواقع الويب تستخدم بصمتك الرقمية الإجمالية من أجل الإعلان عن منتجات من مواقع الويب التي زرتها سابقًا.

الشبكة الافتراضية الخاصة (VPN)
تمنحك شبكة VPN الخصوصية عبر الإنترنت من خلال إنشاء شبكة خاصة من اتصال عام بالإنترنت. وتساعد شبكات VPN على منع مجرمي الإنترنت من اعتراض البيانات التي ترسلها من جهازك أو تستقبلها عليه. وتحتوي معظم أجهزة توجيه الإنترنت على شبكات VPN مُدمجة. إن إعداد شبكة VPN قد يكلفك رسومًا بسيطة شهريًا *(لمزيد من المعلومات حول أجهزة التوجيه، يُرجى الرجوع إلى القسم 1.2)*.

الاستعراض الخاص (وضع التصفح المتخفي)
حين تستخدم متصفحًا للإنترنت، قد يقوم المتصفح بتسجيل ما تقوم به ويحفظ كلمات المرور والمعلومات المالية وينزّل ملفات تعريف الارتباط من مواقع الويب التي سبق لك زيارتها. يساعد الاستعراض/التصفح الخاص في منع بعض من ذلك، وهو مهم بشكل خاص عند استخدام أجهزة الكمبيوتر العامة.

ملفات تعريف الارتباط
تشير ملفات تعريف الارتباط إلى البيانات المرسلة من متصفح للإنترنت ويتم حفظها على جهاز الكمبيوتر الخاص بك. وهذا يسمح لمواقع الويب بتذكر وتسجيل كلمات المرور وسجل التصفح الخاص بك. إذا حذرك أحد مواقع الويب من أنه يستخدم ملفات تعريف الارتباط، فإنك باستخدامك للموقع تمنحه إذنًا للوصول إلى إجمالي بصمتك الرقمية، مما قد يؤدي إلى ظهور إعلانات موجهة.

بصمتك الرقمية الأساسية

يمكن لأصحاب العمل ومالكي العقارات البحث عن حساب التواصل الاجتماعي الخاص بموظف أو مستأجر محتمل من أجل معرفة المزيد عنه.

إذا عثرت جهة عمل على حسابك على Twitter أو Facebook أو Instagram، فما الذي سيفكرون فيه؟

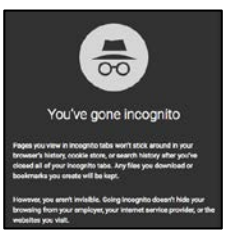
لإدارة بصمتك الرقمية الأساسية، يمكنك القيام بأمرين. أولاً، قم بضبط إعدادات الخصوصية المفضلة لديك على جميع حسابات وسائل التواصل الاجتماعي. ثانيًا، **لا تنشر شيئًا إلا إذا كنت لا تمانع في اطلاع الجميع عليه**. فهناك دائما فرصة لاحتمالية قيامهم بذلك!

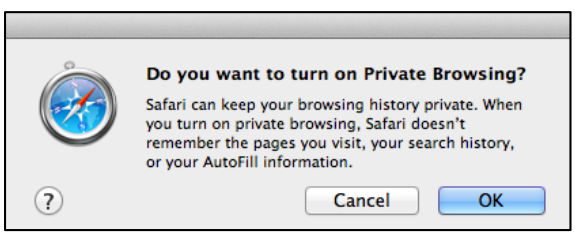
بصمتك الرقمية الإجمالية

إن بصمتك الرقمية لا تتشكل فقط من خلال ما تنوي نشره للجمهور العام. فالشركات وجهات إنفاذ القانون والحكومات ومجرمو الإنترنت يجمعون المعلومات من مستخدمي الإنترنت. **يُمكن استخدام معلوماتك بعدة وسائل، بدءًا من إنشاء إعلانات موجهة وصولاً إلى انتحال هويتك.**

ما هي الحالات التي قد تكشف فيها الشركات عن معلومات حول بصمتك الرقمية إلى سلطات إنفاذ القانون؟ وهل هذا قانوني؟

رغم أن مشاركة الشركات لبصمتك الرقمية يعتبر أمرًا قانونيًا، إلا أن بعض الشركات لديها سياسات ضد ذلك. يمكنك حماية بصمتك الإلكترونية من خلال استخدام خدمة شبكة VPN من أجل إخفاء وجودك عبر الإنترنت، ومن خلال التصفح في وضع الاستعراض الخاص من أجل منع ملفات تعريف الارتباط، ومن خلال توخي الحذر أيضًا فيما تقوم به عبر الإنترنت!





HIAS

البرامج الضارة والفيروسات والحماية من الفيروسات وجدران الحماية

هناك العديد من الوسائل التي من خلالها يمكن للمحتالين والمجرمين عبر الإنترنت الوصول إلى معلوماتك. بمجرد وصولهم إلى جهازك، أو تتبع المعلومات المحددة لهويتك الشخصية، يصبح بمقدورهم فتح خطوط ائتمانية باسمك وتحميل عمليات شراء على حسابك الجاري والاستيلاء على الأموال من حساب التوفير الخاص بك. تعتبر الفيروسات والبرامج الضارة من الأدوات الأساسية التي يستعين بها المجرمون في مساعيهم هذه. **حافظ على حماية جهازك وعلى سلامتك من خلال جدران الحماية وبرامج مكافحة الفيروسات الموثوقة!**

المصطلحات الأساسية

البرامج الضارة

البرامج الضارة هي أي شكل من البرامج الخبيثة المصممة للوصول إلى جهاز إلكتروني أو إتلافه. وعادة ما تصمم للاستيلاء على الأموال. تعتبر فيروسات الكمبيوتر نوعًا من البرامج الضارة التي تسمح لمجرمي الإنترنت بالوصول إلى معلوماتك المصرفية وتدمير رصيدك الائتماني *(لمزيد من المعلومات حول الائتمان، يُرجى الرجوع إلى القسم 4.1)*.

فيروس الكمبيوتر

فيروس الكمبيوتر هو برنامج، أو رمز، ضار يهدف إلى تغيير الطريقة التي يعمل بها أي جهاز. يمكن للفيروسات الانتشار بين الأجهزة المتصلة وسرقة كلمات المرور وتسجيل ضغطات لوحة المفاتيح وإتلاف الملفات وإرسال رسائل بريد عشوائي إلى جهات الاتصال على البريد الإلكتروني بل والهيمنة على الجهاز برمته. وتنتشر هذه الفيروسات من خلال مرفقات البريد الإلكتروني، والملفات والتطبيقات التي يتم تنزيلها، ومحتوى التواصل الاجتماعي الذي تتم مشاركته.

الحماية من الفيروسات

تُنتِج العديد من الشركات، مثل شركة Norton، برامج للحماية من الفيروسات. وتكلف حزم البرامج القابلة للتنزيل هذه رسومًا شهرية، ولكنها توفر حماية قوية ضد البرامج الضارة والفيروسات.

جدار الحماية

إن جدار الحماية هو أشبه ببرنامج لمكافحة الفيروسات ومخصص لاتصالك بالإنترنت. وهو يراقب حركة مرور الشبكة الواردة والصادرة ويتحكم فيها. كما أنه يضع حواجز بين الشبكات الداخلية الموثوق بها وغيرها من الشبكات الخارجية غير الموثوق بها.

علامات قد تدل على أن لديك فيروسًا

- كثرة النوافذ المنبثقة
- حدوث تغيرات على صفحتك الرئيسية
- رسائل بريد إلكتروني مرسلة من حسابك ولم تكتبها
- تكرار أعطال الكمبيوتر أو البرنامج
- تباطؤ الأداء عن سرعته المتوسطة
- وجود برامج غير معروفة على جهازك
- نشاط غير عادي

كيفية منع الفيروسات والبرامج الضارة

- لا تنقر على الإعلانات المنبثقة
- استخدم توصيلات عبر شبكات آمنة، ولا تقم بمشاركة الشاشة أو توصيل جهازك بأجهزة كمبيوتر ليست بها حماية من الفيروسات
- افحص الملفات دائمًا قبل تنزيلها
- استخدم برنامج موثوق للحماية من الفيروسات

HIAS

المعلومات المضللة

إن شبكة الإنترنت قد جعلت الوصول إلى المعلومات أمرًا سهلا. وهي تسمح أيضًا بالنشر السريع للمعلومات. وأصبح بإمكانك اليوم أن تعثر على المعلومات المتعلقة بالأحداث الجارية بسهولة عبر الإنترنت، ولكن **ليس كل ما تقرأه على الإنترنت يكون حقيقيًا**. سواء كنت تحصل على معلومات من وسائل التواصل الاجتماعي أو من مصدر إخباري، ينبغي لك دائما أن تتحقق مما تقرأه عبر الإنترنت حتى تتأكد من صحته.

الأخبار الكاذبة

الأخبار الكاذبة هي عبارة مستحدثة تصف المعلومات المضللة المنشورة على منصات التواصل الاجتماعي، مثل Facebook وTwitter. ويشيع استخدام هذه العبارة حاليًا بين الأفراد ووسائل الإعلام. ببساطة، يُقصد بالأخبار الكاذبة أي معلومات زائفة وليست لها حقائق أو مصادر أو اقتباسات يمكن التحقق منها. وقد تشير الأخبار الكاذبة إلى خطأ ما. على سبيل المثال، حين يقوم مصدر إخباري بمشاركة معلومات لم يتم التحقق منها، ثم يتبين له لاحقًا أنها معلومات كاذبة. وقد تكون الأخبار الكاذبة أيضًا في صورة معلومات خاطئة تتم مشاركتها عن عمد. بل قد يصف الناس شيئًا ما باعتباره أخبارًا كاذبة، على الرغم من صحته في واقع الأمر.

وبالنسبة للأشخاص حديثي العهد بالإنترنت، قد يتوهمون أن كثيرًا من الأخبار الساخرة حقيقية. والمعلومات المنشورة على المنصات الساخرة ليست واقعية. وتعتبر منصة Onion واحدة من المنصات الساخرة المعروفة – ويمكنك قراءة هذا المصدر على theonion.com.

ليس من السهل دائمًا التعرف على المعلومات المضللة. **احرص دائما على استخدام وسائل إعلام موثوقة وغير متحيزة لتكون مصدرك الإخباري.** ويمكنك أن تختار زيارة أحد تطبيقات الويب الموثوقة التالية لمتابعة الأخبار: New York Times، أو Wall Street Journal، أو Washington Post، أو الإذاعة العامة الوطنية (NPR)، أو Economist، أو New Yorker، أو Reuters، أو Atlantic، أو Politico *(لمزيد من المعلومات حول إذاعة NPR،*

في نهاية المطاف، لك الحرية في اختيار المصدر الإعلامي المفضل لديك. حاول دائمًا أن تقرأ وجهات نظر مختلفة. فعلى سبيل المثال، قد يكون المصدر الإعلامي المفضل لديك واحدًا من المصادر المدرجة أعلاه. وإذا كان الأمر كذلك، ففكر في قراءة مصدر إخباري دولي أيضًا، مثل بي بي سي (BBC). وهذا يقدم لك وجهتي نظر أمريكية ودولية حول الأخبار، وسيسمح لكل بتكوين آرائك المتعلقة بالسياسة والحكومة وغيرها من الأحداث الجارية بشكل أفضل.

اكتشاف المعلومات المضللة

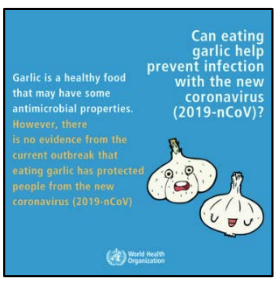
ليست هناك طريقة سهلة لاكتشاف المعلومات المضللة، ولكن يمكنك البدء باتباع الخطوات التالية:

- تشكك فيما تقرأه
- كن على دراية بالمنصات التي تقدم معلومات مضللة بشكل شائع
- تقصَّ الحقائق

كما يمكنك أيضًا استخدام تطبيقات، مثل تطبيق رويترز لتقصي الحقائق (Reuters fact check)، من أجل اكتشاف المعلومات المضللة: www.reuters.com/fact-check.

الوباء المعلوماتي

في مارس 2020، وصفت منظمة الصحة العالمية (WHO) المعلومات المضللة الموجودة على الإنترنت حول جائحة فيروس كورونا باعتبارها «وباءً معلوماتيًا». ولمكافحة المعلومات المضللة الموجودة على وسائل التواصل الاجتماعي، أطلقت منظمة الصحة العالمية حملة لدحض الشائعات المنتشرة حول فيروس كورونا. فعلى سبيل المثال، لم يثبت أن تناول الثوم يحمي الأشخاص من التقاط عدوى فيروس كورونا.



HIAS