

كيف تحارب التكنولوجيا الاتجار بالبشر؟

روبوت داخل الإعلانات الجنسية لمكافحة الاتجار بالبشر. هكذا قرر بعض موظفي شركة «مايكروسوفت» أن يتصدوا لمشتري الجنس على الإنترنت وتحذيرهم من عدم قانونية شراء الجنس وإحالتهم إلى الشرطة في حال أظهروا نية لممارسة الجنس مع قاصر. ينضم هذا البرنامج إلى برامج أخرى طورتها الشركات العاملة في مجال التكنولوجيا لمكافحة الاتجار بالبشر على الإنترنت. بعدما فتحت التكنولوجيا باباً تسويقياً واسعاً للمتاجرة

أيضا الشوفي

«التكنولوجيا لم تخلق الاستغلال الجنسي للأطفال... لكنها جعلته ديمقراطياً»، أي جعلته متاحاً للجميع. بهذه الجملة تحدد منظمة Thorn الصلة بين التكنولوجيا والاستغلال الجنسي. تقول أرقام المنظمة إن 63% من الأطفال الناجين من الاتجار بالبشر تم تسويقهم على الإنترنت في مرحلة ما أثناء وجودهم في عهدة الشبكات. أكثر من 57 ألف موقع على الإنترنت احتوى على صور اعتداء جنسي على الأطفال عام 2016، و60% من البشر المتاجر بهم يتم بيعهم إلى تجارة الجنس وغالبيتهم تحت سن 24 عاماً. في الولايات المتحدة وحدها تم تعقب 9 ملايين كمبيوتر عام 2011

تشارك ملفات إباحية للأطفال. في ظل هذه الأرقام المخيفة، كيف تحارب التكنولوجيا الاتجار بالبشر؟ يسعى موظفو «مايكروسوفت» إلى تصيد مشتري الجنس على الإنترنت ضمن مبادرة لمكافحة الاتجار بالبشر. فالروبوت الذي أطلقته الشركة مؤخراً هو عبارة عن برنامج chatbot يختبئ خلف إعلانات كاذبة للخدمات الجنسية، يتحدث مع الأشخاص الذين يدخلون إلى هذه الإعلانات طلباً للخدمات الجنسية، مدعياً أنه الفتاة الموجودة في الإعلان ويحببهم عن جميع الأسئلة من عمره. أو عمرها في هذه الحالة - جسدها، رغباتها الجنسية وأسعارها. وإذا لمس الروبوت نية في شراء خدمات جنسية، يقوم بإرسال رسالة صارمة للمشتري يحذره فيها من مخاطر شراء الجنس، ليتطور التحذير إلى بلاغ للسلطات في حال أظهر الشخص ميولاً انحرافية، مثل شراء خدمات جنسية من أشخاص قاصرين. اختبرت الشركة برنامجها في مناطق سيانل، أتلانتا وواشنطن، وهو جزء من مبادرة أطلقها ناشطون في مجال مكافحة الاتجار بالبشر، والذي يُعتبر الاتجار بالجنس أبرز وجوهه، بهدف تخفيض الطلب على الجنس من خلال تحذير المشتريين من أبعاد هذا الأمر وتأثيره على الضحية. فبعدما تكتمل الحادثة بين الروبوت والشاري، وعند تأكيد محاولة شراء خدمات جنسية، يرسل الروبوت الرسالة التالية «إن شراء الجنس من أي شخص هو عمل غير قانوني، ويمكن أن يسبب ضرراً

63% من الأطفال الناجين من الاتجار بالبشر تم تسويقهم على الإنترنت



جسماً على المدى الطويل للضحية، وكذلك دورة الاتجار بالبشر. ستتم مراجعة تفاصيل هذا الحادث بشكل أكبر، وقد يتم الاتصال بك من قبل سلطات إنفاذ القانون للاستجواب. لا تحاول شراء الجنس مرة أخرى، فإنه لن يحقق ما تبحث عنه». ينقل موقع wired أن الروبوت تبادل 14 ألف رسالة مع ألف شخص استجابوا للإعلانات المزروعة في المواقع، وقد تم توجيه رسائل تحذير إلى نصف هؤلاء لإظهارهم نية لشراء خدمات جنسية.

تقنيات الرؤية الحاسوبية: رصد، تحليل ومطابقة

في الواقع ليست هذه التكنولوجيا الأولى التي تطورها شركة «مايكروسوفت» لمكافحة الاتجار بالبشر، فقد طورت الشركة عام 2015 أداة PhotoDNA لمكافحة استغلال الأطفال جنسياً على شبكة

الإنترنت. يسمح البرنامج الصور التي تم تحميلها على وسائل الإعلام الاجتماعية وخدمات تبادل الصور، ويحدد الصور التي تصور اعتداءً جنسياً من أجل إزالتها عن الشبكة بهدف جعلها آمنة للجميع. تعمل هذه الأداة من خلال عملية تشفير وترميز تقوم على تقسيم الصور إلى مربعات وتعيين شيفرة لكل جزء، بحيث تتم مطابقة التشفير مع قاعدة بيانات تضم صوراً غير قانونية معروفة مأخوذة من المركز الوطني للأطفال المفقودين والمستغلين. وفي حين أنه كان بالإمكان كشف الصور غير القانونية إذا كانت مطابقة تماماً لصور الاعتداء الجنسي الموجودة في قاعدة البيانات، فإن تقنية التشفير أتاحت كشف هذه الصور حتى ولو تم التلاعب بها وتعديلها لتصبح مختلفة عن الصور في قاعدة البيانات. يستخدم تطبيق kik، وهي شبكة دردشة شعبية جداً بين المراهقين، أداة PhotoDNA للكشف عن الصور الشخصية التي تظهر استغلالاً جنسياً للأطفال في نفس الوقت الذي يجري فيه تحميلها على الشبكة، ما يتيح إزالتها فوراً وإبلاغ السلطات وإزالة حساب المستخدم، أكثر من 70 شركة وجمعية، من ضمنها فايسبوك وتويتر، تستخدم أداة PhotoDNA، وتقول الشركة إن 720 ألف صورة من بين 1,8 مليار صورة يتم تحميلها يومياً على الإنترنت تعذب غير قانونية وفيها استغلال جنسي للأطفال. 4 صور قد تساعد الشرطة على إنقاذ ضحية اتجار بالبشر. من هذه الفكرة

ينطلق تطبيق TraffickCam الذي أطلق العام الفائت. يقوم التطبيق على دفع الناس إلى التقاط 4 صور لغرف الفنادق التي يوجدون فيها، بحيث تحفظ هذه الصور في قاعدة بيانات يمكن للشرطة الوصول إليها بسهولة. لكن لماذا؟ يقوم المتاجرون بانتظام بنشر صور لضحاياهم في غرف الفنادق للإعلانات على الإنترنت. وهذه الصور هي أدلة يمكن استخدامها للعثور على مرتكبي هذه الجرائم ومقاضاتهم. لكن على

تقرير

هل تنجح الصين في بناء شبكة اتصالات كمومية؟

ستكون له آثار كبيرة في ما يتعلق بالأمن السيبراني ومنع الحكومات من اختراق الاتصالات، إذ يمهد الطريق نحو إقامة شبكة اتصالات كمومية Quantum Communication cryptography. هذا الإنجاز

أول مرة في العالم، نجحت الصين منذ أيام في إرسال بيانات سرية غير قابلة للاختراق من الفضاء إلى الأرض من خلال تقنية «التشفير الكمومي» Quantum cryptography. هذا الإنجاز



الصين تنجح في إرسال بيانات غير قابلة للكسر، من الفضاء إلى الأرض

أي محاولة لخرق «الفوتون» ستترك أثراً يمكن اكتشافه بسهولة



الفوتونات، أي الجسيمات التي تنقل الضوء، لنقل البيانات، بحيث تسمح لشخصين متباعدين بإنتاج مفتاح سري عشوائي معروف لهما فقط، يمكن استخدامه لتشفير وفك تشفير الرسائل. إن حمل البيانات عن طريق الفوتون يجعل التشفير «غير قابل للكسر»، لأن الفوتون لا يمكن أن يتم نسخه بشكل مطابق، وبالتالي فإن أي محاولة لقياسه ستترك أثراً يمكن اكتشافه بسهولة، وستنقله إلى محاولة لخرق الشبكة، في حين أن

التشفير النموذجي الذي يعتمد على الرياضيات التقليدية يعدّ مهبطاً في المستقبل من قبل الحوسبة الكمومية، حيث ستتمكن الحواسيب الكمومية، وهي أجهزة كمبيوتر أسرع وأقوى بكثير من الموجودة حالياً (مراجعة تقرير ما هو «الكوانتم كمبيوتر»؟، علي عواد، 20 تموز 2017)، من كسر المستويات الحالية للتشفير، وبالتالي فإن الحوسبة الكمومية قد تغير التشفير الذي نعرفه. تشرح هيئة bbc أن التواصل على الشبكة الكمومية يعمل بشكل مختلف؛ فإذا أردت أن ترسل رسالة آمنة، يتم أولاً إرسال مفتاح سري مرفق بجزيئات الضوء (الفوتون) على حدة. بعد حصول هذه العملية يتم إرسال الرسالة المشفرة التي يستطيع المتلقي قراءتها بمساعدة المفتاح السري المرسل مسبقاً. الميزة الأساسية لهذه التقنية هي أنه إذا حاول أي شخص اعتراض الفوتونات، فإنه حتماً سيقوم بتغييرها أو تدميرها، ما يعني أن أي محاولة للاختراق ستتم ملاحظتها على الفور، وبهذا المعنى