سام
للحقوق والحريات

ظاهرة انتحال الهوية الرقمية في اليمن..
الدوافع والتبعات

يناير 2023

www.samrl.org

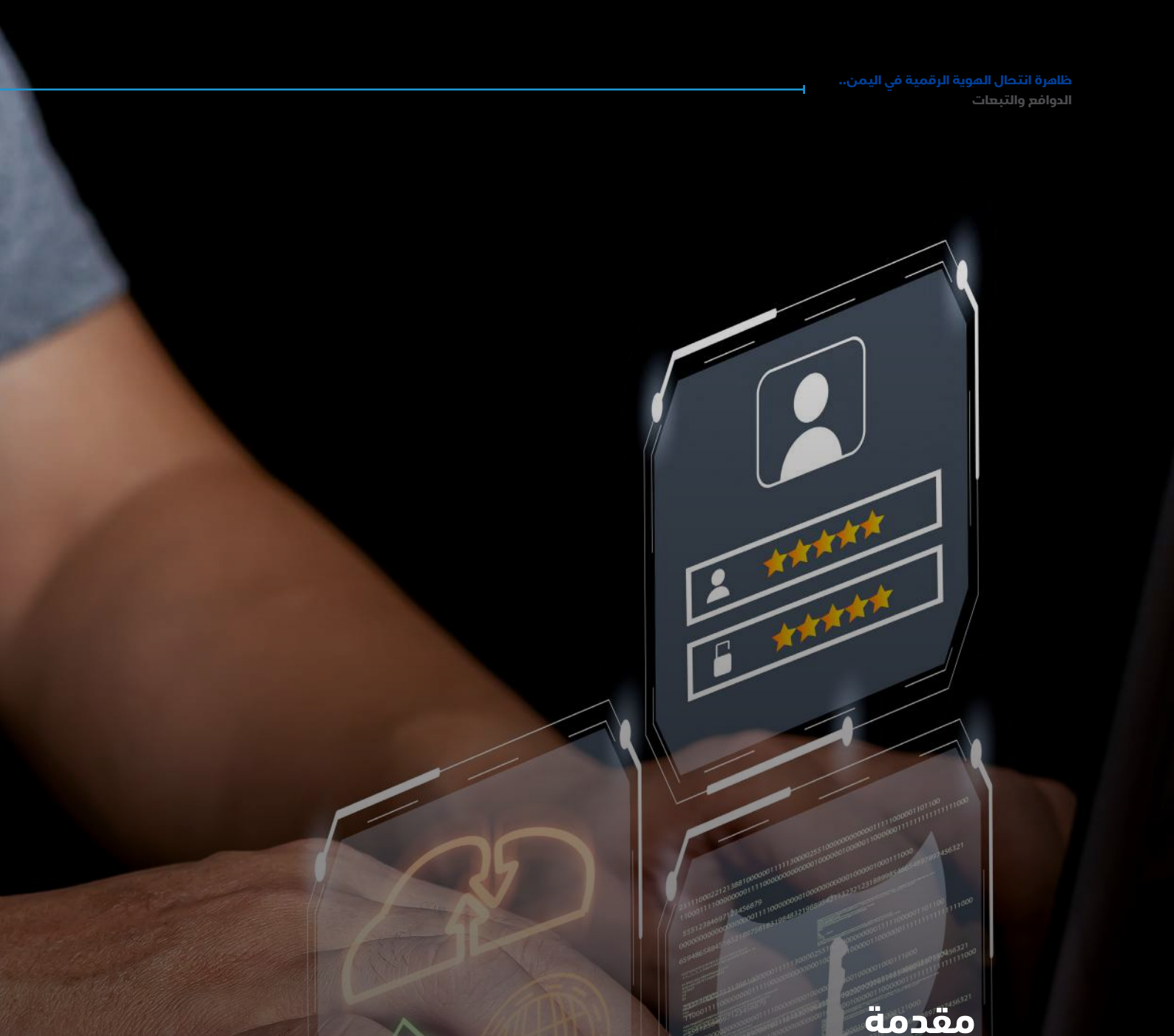
ظاهرة انتحال الهوية الرقمية في اليمن..
الدوافع والتبعات

سام
للحقوق والحريات

مشروع الحقوق الرقمية

نافذة حقوقية غير ربحية تابعة لمنظمة سام، بدعم من منظمة إنترنيوز، تهدف إلى التعريف بالحقوق الرقمية، ورصد الانتهاكات الرقمية بحق مستخدمي الفضاء الرقمي، حيث تعمل على مناصرة الحقوق الرقمية لليمنيين، بهدف الوصول إلى فضاء رقمي آمن وعادل وحر. تتيح النافذة تقديم البلاغات عن الانتهاكات الرقمية، كما تساهم في توثيقها وتشكيل قاعدة بيانات عنها. وتعمل على إصدار دراسات وأبحاث حول النشاط الرقمي، والحقوق الرقمية والأمان الرقمي، بالإضافة إلى تخطيط وإدارة حملات المناصرة المحلية والدولية.

violations@samrl.org



مقدمة

يعد انتحال الهوية الرقمية ظاهرة متنامية في اليمن، خاصة مع الاستخدام المتزايد لمنصات التواصل الاجتماعي، وما رافق ذلك من ظهور أشكال مختلفة من الانتحال، عبر إنشاء حسابات وهمية لأغراض مسيئة.

وقد أدى الصراع المستمر والاستقطاب السياسي الذي تشهده البلاد إلى زيادة انتشار الحسابات المزيفة على منصات التواصل الاجتماعي، والتي تستخدمها مختلف الأطراف لنشر الدعاية والتلاعب بالرأي العام والتأثير على الخطاب السياسي، وهو ما يستدعي الوقوف على هذه المشكلة، وإبراز تداعياتها على الأفراد والكيانات والمجتمع عموما.

إطار مفاهيمي

انتحال الهوية الرقمية هو شكل من أشكال سرقة الهوية لارتكاب احتيال أو خداع حيث يتظاهر شخص ما بأنه شخص آخر من خلال افتراض هوية هذا الشخص، عادةً من أجل الوصول إلى الموارد أو الحصول على بيانات، ومزايا أخرى باسم هذا الشخص وشهرته، أو استخدام هذه الهوية للتشهير بالشخصية المنتَحَلة وتشويه سمعتها والإضرار بها. Cyber Crime Chambers

يقع انتحال هوية أشخاص حقيقيين على وسائل التواصل الاجتماعي ضمن فئة أكبر من الهندسة الاجتماعية، وهي سلسلة من التكتيكات التي تعتمد على التلاعب النفسي، وخداع الضحايا. Bit Defender

إطار قانوني

لا يوجد قانون في اليمن ينظم الفضاء الرقمي، ويحدد عقوبات للجرائم الإلكترونية، وعليه فإن جريمة انتحال الهوية الرقمية ليست استثناءً، من حالة الفراغ التشريعي هذه، إلا أن قانون العقوبات تطرق للجريمة بشكل عام.

حيث تنص المادة (310) من القانون رقم (12) لسنة 1994م بشأن الجرائم والعقوبات، على التالي: «يعاقب بالحبس مدة لا تزيد على ثلاث سنوات أو بالغرامة من توصل بغير حق إلى الحصول على فائدة مادية لنفسه أو لغيرة وذلك بالاستعانة بطرق احتيالية (نصب) أو اتخاذ اسم كاذب أو صفة غير صحيحة».

الباحث والمستشار القانوني عبدالرحمن الزبيب، قال إن اليمن تعاني من ضعف في آليات التعامل مع الجرائم الإلكترونية، وإن وقعت جريمة إلكترونية فمن الصعوبة إثباتها والتحقيق فيها ومحاكمة مرتكبيها، بسبب عدم وجود قانون مكافحة الجرائم الالكترونية، حتى الآن، وعدم مواءمة المنظومة القانونية الوطنية مع الاتفاقيات الدولية المصادق عليها. (عدن الغد - يونيو 2021).

وإذا ما أخذنا نموذج عن كيفية تعامل دولة من الدول العربية مع جريمة الانتحال الإلكتروني، وما يستتبعه من جرائم أخرى- لاستلهام التجربة والاستفادة منها- نجد أن الإمارات، مثلا، قد حددت العقوبة، حيث نصت المادة (11) من قانون مكافحة جرائم تقنية المعلومات على أنه "يعاقب بالحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين كل من استولى لنفسه أو لغيره بغير حق على مال منقول أو منفعة أو على سند أو توقيع هذا السند، وذلك بالاستعانة بأي طريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة عن طريق الشبكة المعلوماتية أو نظام معلومات إلكتروني أو إحدى وسائل تقنية المعلومات".

السياق العام للظاهرة

أدى الصراع المستمر والاستقطاب السياسي في اليمن إلى زيادة انتشار الحسابات المزيفة على منصات التواصل الاجتماعي، والتي تستخدمها مختلف الأطراف لنشر الدعاية والتلاعب بالرأي العام والتأثير على الخطاب السياسي.

ومنذ 2011 تصاعد استخدام اليمنيين لمواقع التواصل الاجتماعي بشكل ملحوظ، وأصبحت أحد أهم وسائل التحشيد والاستقطاب السياسي في البلد، ولهذا بدأت فصائل سياسية منظمة خلق حسابات مزورة، بعضها تظهر طبيعتها المستعارة من خلال اسم الحساب غير الشخصي، وبعضها أسماء حسابات تبدو شخصية وبصور شخصية أحياناً وكان لها نشاط ملحوظ، ومع مرور الوقت يكتشف المستخدمون أنه حساب لشخصيات وهمية. (موقع المدنية - أبريل 2020)

وفي ظل الاستقطابات والتجاذبات السياسية الحادة، «تنشر مستويات عالية من الحسابات المزيفة المنسقة في اليمن والعراق -العديد منها مرتبط بأسباب سياسية أو جهادية- والتي تنشر معلومات مضللة وتثير العنف المحلي، غالبًا بين الجماعات المتحاربة». وفقا لـ تحقيق أعده الصحفي «مارك سكوت» لـ صحيفة «بوليتيكو» الأمريكية ونشر في أكتوبر 2021.

وعلى الرغم من أن تركيزنا ينصب على الحسابات الزائفة ذات المقاصد الخبيثة، إلا أن ثمة حسابات بأسماء مستعارة أنشئت بدون قصد الإضرار بالغير، إذ وبحسب تقرير لموقع يمن فيوتشر، فإن «نساء وفتيات وناشطات كثر كُنّ بداية دخولهن إلى منصات التواصل الاجتماعي يعبرن عن آرائهن بكل حرية، غير أنهن اضطررن مؤخراً إلى تغيير أسمائهن بأسماء مستعارة، جراء تعرضهن لمضايقات وعنف لفظي إضافة للتنمر. (يمن فيوتشر - سبتمبر 2021) وبالنظر إلى أن المجتمع اليمني مجتمع ذكوري مغلق -مع بعض الاستثناءات- تنتشر الأسماء المستعارة والحسابات المزيفة على فيسبوك، حيث ينشئ بعض الأولاد والبنات أسماءً مستعارة من أجل المتعة، لتجنب أي قيود اجتماعية، وينشئ آخرون حسابات مزيفة لخداع أصدقائهم ليعتقدوا أنهم يتحدثون مع فتيات. المونيتور - أكتوبر 2013

أنواع الانتحال الرائجة في الفضاء الرقمي اليمني

- انتحال شخصية حقيقية

ثمة آلاف من الحسابات والصفحات التي تنتحل هوية سياسيين وقادة عسكريين وشخصيات اجتماعية، وإعلاميين وصحفيين، ومشاهير، كنموذج بارز على هذا النوع من الانتحال، هناك أكثر من 30 صفحة وحساب، على فيسبوك، ومثلها على تويتر، تنتحل شخصية رئيس المجلس الرئاسي، رشاد العليمي.

- انتحال شخصية وهمية

توجد آلاف الحسابات والصفحات الزائفة، التي تتظاهر بأنها تمثل شخصيات حقيقية، على الواقع، حيث تظهر بأسماء وبيانات وصفات مألوفة، على سبيل المثال: د. حسين اليافعي، حساب على تويتر يحظى بأكثر من 112 ألف متابع، يصف نفسه بأنه رئيس الحراك الوطني الجنوبي ، ويدعي أنه أستاذ العلوم السياسية المساعد في جامعة عدن، غالبا ما يهاجم المجلس الانتقالي وينشر معلومات زائفة تماما، لكن تحقيق معمق أعدته منصة صدق اليمنية، بتاريخ أكتوبر 2021، كشف عن زيف الحساب، بالأدلة، واتضح أنه كان مسجلا باسم أحد الإعلاميين، قبل أن يتم تغييره إلى الاسم الحالي.

- انتحال هوية المؤسسات والكيانات

تم رصد العديد من الحسابات والصفحات -لا يتسع المجال لذكرها- التي تنتحل هوية: (الوزارات والمؤسسات الحكومية، والمنظمات العاملة في اليمن، والكيانات الإعلامية والإخبارية، والشركات التجارية، والمؤسسات الخاصة).

- الأسماء المستعارة

تنتشر الأسماء المستعارة بكثافة، على الفضاء الرقمي اليمني، البعض منها أنشئ بدوافع بريئة، كـ الحساسية الاجتماعية، والهروب من المضايقات، لكن الغالبية العظمى من هذه الحسابات لها مقاصد سيئة.

- سرقة الحسابات الشخصية

من الشائع في اليمن، أن يتم اختراق، حساب شخص ما على منصات التواصل الاجتماعي، والتحدث فيما بعد باسم الضحية، على سبيل المثال، في سبتمبر 2022 نبه ثلاثة وزراء سابقون في الحكومة المعترف بها دوليا (مروان دماج، عبد الرقيب فتح، سالم الحريزي) بأن مجهولين يستخدمون حساباتهم الشخصية القديمة على فيسبوك، بعد أن اخترقوها قبل سنوات، ويطلبون من جهات الاتصال، تحويل مبالغ مالية، على اعتبار أن من يطلب المساعدة المالية هم الوزراء.

دوافع انتحال الهوية الرقمية

- التلاعب بالرأي العام

ارتفعت وتيرة الاستخدام الموجّه لمواقع التواصل الاجتماعي بشكل كبير مع أحداث الربيع العربي منذ العام 2011، إذ أصبح أعضاء الجماعات والأحزاب السياسيّة يمارسون دور الدعاية والدعاية المضادة ونشر فضائح الطرف المنافس والإيقاع به، بالإضافة إلى نشر أفكار متعصّبة أحياناً تؤدّي إلى رفع وتيرة الانقسام الاجتماعي والاصطفاف الفكري والمناطقي اللذَين يتركان آثاراً سلبيّة بدأت بالانعكاس على الواقع. المونيتور - أكتوبر 2013

وعقب أي حدث سياسي مثلا، تبرز إلى العلن حسابات وصفحات شخصية، تنتحل هوية الشخصيات المحورية في ذلك الحدث، وتختلق التصريحات والآراء، لتحقيق غايات سيئة.

يستخدم أطراف الصراع في اليمن، الحسابات المزيفة على وسائل التواصل الاجتماعي للتلاعب بالرأي العام لنشر روايات متحيزة، تعمل على تضخيم أحداث ووجهات نظر معينة، من خلال التظاهر كأشخاص حقيقيين، أو تقمص شخصيات من الأطراف المعارضة، لنشر معلومات وتصريحات بهدف إحداث انقسام في صفوف تلك الأطراف.

- بث الشائعات وتشويه السمعة

تستخدم الحسابات المزيفة على منصات التواصل الاجتماعي كأداة لنشر الإشاعات ومشاركة المعلومات المضللة، وإيصالها إلى جمهور عريض من المتابعين، الذين باتوا محاصرين بأكوام من الأكاذيب، على كافة المستويات وليس على المستوى السياسي فحسب.

ولعل أبرز مثال على هذا الدافع، قيام أحد الحسابات على منصة تويتر، والذي حمل الاسم «سمية الخولاني» بنشر معلومات في

أبريل 2022 قال إنها تكشف عن وجود فساد واستغلال للفتيات من قبل المنظمات الإغاثية، وهو ما تلقفته المواقع الإخبارية، بدون تروٍ، فأعادت نشر تغريدات ذلك الحساب بشكل مكثف، علاوة على أن نشطاء مواقع التواصل الاجتماعي، دشنوا حملة شرسة ضد المنظمات، على خلفية المعلومات التي نشرها الحساب المذكور، دون أن يقدم دليلا واحدا على ادعاءاته، ليتضح فيما بعد أن الحساب مزيف تماما.

- تنفيذ هجمات التصيد الاحتيالي

تزايدت هجمات التصيد الاحتيالي في الفضاء الرقمي اليمني، باطراد ملحوظ، حيث يستخدم مجهولون حسابات وهمية -في العادة- للإيقاع بضحاياهم، إما عبر إرسال لينكات خبيثة -والتي عادة ما تكون مرفقة برسائل مغرية كالحصول على مساعدة من منظمة ما، أو جوائز مالية، رصيد إنترنت...إلخ- أو تسجيل بيانات الولوج للحساب عبر صفحات فيسبوك زائفة، تم إنشاؤها بقصد اختراق حساب الهدف والحصول على بياناته،أو إرسال رسائل من حسابات وهمية تطلب معلومات شخصية، أو نشر روابط لمواقع مزيفة، ومن ثم ابتزازه بطلب أموال أو تحقيق رغبات لا أخلاقية.

على سبيل المثال، ظهرت إعلانات ممولة على مواقع التواصل الاجتماعي، لجذب أكبر عدد من الضحايا، عبر عروض خيالية تقدم في الإعلان للباحثين عن وظائف. تقوم هذه العملية على انتحال أسماء شركات كبرى عبر صفحات مزورة في «فيسبوك» أو «واتساب»، يتضمن الإعلان حاجة هذه الشركات لشباب وشابات للعمل لديها، وترفق ذلك برابط لتعبئة بيانات المتقدم، فيفاجأ المتقدمون برابط وهمي، أو «هاكر»، وتبدأ بالتالي عملية الابتزاز، بحسب ما ذكره تقرير صادر عن درج ميديا (بتاريخ ديسمبر 2021).

- القيام بعمليات الابتزاز

غالبًا ما تُستخدم الحسابات الزائفة على وسائل التواصل الاجتماعي للقيام بعمليات ابتزاز، من خلال الاتصال بالضحية والمطالبة إما بدفع مبالغ مالية مقابل (عدم مشاركة المعلومات أو الصور الشخصية)، أو الاستجابة لمطالب لا أخلاقية، بعد أن يتم الحصول على المعلومات والصور من خلال القرصنة أو التصيد الاحتيالي، أو إنشاء محتوى مزيفًا لابتزاز الضحية.

وكنموذج لهذا النوع من الدوافع، ما كشف عنه الناشط في حماية وأمن المعلومات مختار عبد المعز، في يونيو 2022، عن تعرض ثلاث فتيات للابتزاز، بعد استدراجهن من قبل محتال يمني أنشأ حسابا وهميا على فيسبوك، وانتحل شخصية رجل أعمال خليجي، لافتا إلى أن المبتز هدد الفتيات، في حال عدم الاستجابة لمطالبه ودفع مبلغ مالي بإيصال الأمر إلى أهاليهن.

- ممارسة الاحتيال المالي

يتخفى المحتالون خلف ستار الحسابات والصفحات الزائفة لتنفيذ عمليات احتيال، عبر الاتصال بالضحية والمطالبة بالدفع مقابل توفير خدمة معينة، أو للوصول إلى المعلومات والفرص الحصرية، وقد يدعي المحتال أنه يمثل مؤسسة حكومية أو شركة مشروعة ويطلب معلومات حساسة.

في يوليو 2022، كشف اليوتيوبر «أحمد غازي» عن عملية «احتيال مالي» تستهدف مغتربين يمنيين في السعودية، عبر تطبيقات التعارف والزواج، ولفت إلى أن أفراد وقعوا ضحايا خطوبة وزيجات وهمية تم توثيقها بعقود زواج مزورة، والتي بموجبها دفعوا مبالغ مالية لمحتالين يمنيين، انتحلوا شخصيات فتيات، منوها بأن عصابات محترفة تقف خلف هذا الاحتيال.

في منتصف يناير 2023 قالت منصة صدق اليمنية إنها أغلقت -بالتعاون مع ميتا- مجموعة من الحسابات (33 حسابا) على منصة فيسبوك كانت تحمل أسماءً وهمية، وتضع في الغالب صور نساء منقبات، وتنشر نفس الفيديوهات التي تظهر فيها عوائل فقيرة لاستعطاف الناس، والنصب عليه، وأخذ الأموال منهم.

وهذه ليست المرة الأولى التي تقوم المنصة بإغلاق حسابات من هذا النوع بعد إبلاغ ميتا، ففي يونيو 2020 أغلقت المنصة شبكة من حسابات الاحتيال التي تحمل عدة أسماء بنفس الرقم وتطلب أموال كمساعدة للمحتاجين، وتستغل فيديو قديم لحالة مرضية حقيقية، كان قد تُكفل بعلاجها في عام 2017.

وفي أكتوبر 2022 كشف ناشطون عن وقائع احتيال مالي، تعرض لها عدة أشخاص من قبل حساب وهمي على فيسبوك باسم «شذى المخلافي» -تدعي أنها ناشطة إعلامية وحقوقية مقيمة في أمريكا- والذي استلب الضحايا مبالغ مالية تتراوح ما بين 30 ألف إلى 40 ألف دولار، بحيلة استصدار إقامة في أمريكا.

الآثار المترتبة على الانتحال

يقول ماكس هاينماير، مدير وحدة تعقُّب التهديدات في دارك تريس Darktrace (وهي شركة تكنولوجيا معلومات أمريكية بريطانية متخصصة في الدفاع السيبراني) إن تهديد الحسابات المزيفة على منصات التواصل الاجتماعي حقيقي، ويمثل مشكلة كبيرة، إذ يمكن استخدامها في الكثير من الأمور السيئة أو الشريرة، بما في ذلك إنشاء رسائل غير مرغوب فيها أو تنفيذ عمليات احتيال أو التحريض على العنف أو تنظيم الإرهاب أو أي سلوك آخر. (Protocol - مايو 2020)

مما لا شك فيه أن الحسابات المزيفة على وسائل التواصل الاجتماعي تساهم بشكل كبير في خلق بيئة معادية على الإنترنت، من خلال نشر خطاب الكراهية والتحريض على العنف، ومضايقة الآخرين والتنمر عليهم، وقذفهم والتشهير بهم، وتعزيز الأيديولوجيات المسببة للانقسام والاستقطاب، ناهيك عن استخدام هذه الحسابات في تضخيم وجهات النظر المتطرفة، وكل ذلك، يجعل من بيئة الإنترنت بيئة سامة وعدائية.

كما تتسبب الحسابات المزيفة في إلحاق أضرار فادحة بالأفراد والكيانات، على كافة المستويات، (نفسيا، واجتماعيا، وماليا... الخ)، على سبيل المثال: «السهولة في الحصول على شخصية وهمية باستخدام ايميل على صفحات التواصل الاجتماعي تساعد المبتزين في الاستمرار فى اصطياد ضحاياهم و ممارسة كل أنواع الابتزاز والذي قد يصل بالبعض بتنفيذ تهديده و نشر صور الضحية على الحساب الوهمي في فيسبوك دون الكشف عن هويتهم أو حتى تتبعهم». (منصة دكة - ديسمبر 2022).

وفي هذاالسياق، يحذر الناشط مختارعبد المعز -في منشور على فيسبوك (مارس 2022)- من الانجرار خلف الحسابات الوهمية، ويرى أنها أُنشئت خصيصا للإساءة للأشخاص، مشيرا إلى أن أحد الحسابات الوهمية تسبب في سجن أكثر من ناشط في محافظة إب، من ضمنهم الصحفي ماجد ياسين.

ويمكن أن تؤدي هذه الحسابات إلى تقويض التماسك المجتمعي، من خلال نشر معلومات مضللة ومغرضة، وخلق زخم للمحتوى المثير للعداوة، بالإضافة إلى تغذية التوترات والنزاعات، وتقويض الثقة بين الأطراف المختلفة، وبالتالي تضعف الروابط الاجتماعية وتزيد من تفاقم الانقسامات القائمة. بالإضافة إلى ذلك، فإن استخدام الحسابات المزيفة للتلاعب بالرأي العام، ينتج رؤية مشوهة للواقع، حيث يتعرض الأفراد لوجهة نظر واحدة، وتغيب عنهم الرؤى الأخرى المختلفة.

دور الجهات المحلية في مكافحة الانتحال

بشكل عام «يغيب الدور الحكومي المناط به تنفيذ إجراءات الرقابة والضبط المفترض اعتمادها لملاحقة الجريمة الإلكترونية في اليمن، وذلك بسبب تفكك الدولة وتعدد السلطات الحاكمة في البلد بفعل أزمة الصراع»، بحسب تقرير نشره الموقع بوست في أكتوبر 2022.

وفي ظل عدم وجود نصوص صريحة تحكم الجرائم الإلكترونية في اليمن يضطر القاضي الى إخضاع الأفعال وتجريمها وفق القواعد العامة للقانون الجنائي وهي بالتأكيد قاصرة من أن تشمل كافة أوجه النشاط الإجرامي الالكترونية تعقيداته وتطوراته ناهيك عن قلة خبرة المنظومة الأمنية والقضائية في الأمور التقنية"، وفق تصريح أدلى به المحامي والناشط الحقوقي مازن سلام لـ منصة دكة (ديسمبر 2022).

وهنا، يبرز دور منصات تدقيق الحقائق في مكافحة الحسابات الزائفة، والإطاحة بـ منشئيها، وكنموذج، تقوم منصة صدق اليمنية بتتبع هذه الحسابات، وكشف الجهات/ الأشخاص الذين يقفون خلفها، وبالتعاون مع Meta ميتا، يتم إغلاق العديد من الحسابات والصفحات الوهمية على الفيسبوك.

كما يضطلع النشطاء والمختصين بدور بارز في التصدي لظاهرة الانتحال، كـ الخبير في الأمن الرقمي «فهمي الباحث» و «مختار عبد المعز» و»أحمد غازي». «يقول الباحث... في حال صادفت محتوى عنيفا أو تم إبلاغي بحساب وهمي يمارس أي نوع من الانتهاك أتوجه برسالة عبر البريد الإلكتروني إلى الفريق المختص في شركة فيسبوك للإبلاغ مع توضيح السبب " و لكن الإشكال الحقيقي بحسب المهندسة نور خالد العاملة في منظمة يوديت أحد المنظمات المعتمدة أيضا لتقديم البلاغات، يكمن في الحاجز الثقافي بين دوله محافظه كاليمن و بين فريق فيسبوك المراجع للبلاغات، وتقول نور "عادة ما نواجه صعوبة في إقناع الفريق بخصوصية ثقافتنا تجاه انتشار صور النساء لا نجد تفاعل أو إجراءات تقييد من الفريق كونه يعتبر الصورة محتوى غير منتهك". (منصة دكة - ديسمبر 2022).

دور منصات التواصل الاجتماعي

تقوم منصات التواصل الاجتماعي، من وقت لآخر، بإغلاق شبكة من الحسابات والصفحات الزائفة، بسبب انخراطها في سلوك منسق غير أصيل، وانتحالها لهوية شخصيات من المجتمعات الأصلية. على سبيل المثال، أزالت Meta ميتا، في يوليو 2020، 69 حسابًا و28 صفحة و 15 مجموعة على فيسبوك، و10 حسابات على إنستغرام في اليمن، تنتحل هوية وزارات حكومية في السعودية، منها وزارة المالية ووزارة العمل، واستهدفت اليمنيين وشاركت روايات تنتقد الحوثيين.

وفي يناير 2019 قامت ميتا Meta بـ إزالة 783 صفحة ومجموعة وحسابات بسبب الانخراط في سلوك منسق غير أصيل مرتبط بإيران، والقيام بمجموعات متعددة من الأنشطة المتصلة بالمجتمعات الأصلية في عدة بلدان، بما في ذلك اليمن. وعادةً ما مثّل مديرو الصفحة ومالكو الحسابات أنفسهم على أنهم مواطنين محليين، باستخدام حسابات مزيفة.

وفي يوليو وأغسطس 2022 أزالت شركتا تويتر و»ميتا» (Meta) المالكة لفيسبوك مجموعتين متداخلتين من الحسابات المرتبطة بالبنتاغون، والتي نفذت حملات خداع وتضليل بهدف تعزيز الرواية الأميركية الرسمية للأحداث والتطورات السياسية المهمة بما يخدم مصالح واشنطن. وحدد التقرير حالات متعددة لحسابات تشارك المحتوى وتعرض أنماط نشر منسقة على فيسبوك وإنستغرام وتويتر، على سبيل المثال، في 23 سبتمبر/أيلول 2021 نشر ملف شخصي على فيسبوك يستخدم شخصية مزيفة وصفحة على الموقع اسمها «هنا اليمن» (Here Is Yemen) فيديو مع تعليقات متطابقة حول عمليات إعدام جماعي مزعومة خطط لها قادة الحوثيين في اليمن، وتمت المشاركة من حسابات مزيفة أخرى خلال دقيقتين فقط. (الجزيرة نت - سبتمبر 2022)

لكن هذا ليس كافيا، فثمة أعداد مهولة من الحسابات والصفحات الوهمية، التي تشارك محتوىً مسيء ومثير للانقسام، ولم تتخذ إدارة المنصة (فيسبوك، أو تويتر) أي إجراء حيالها، على الرغم من حملات الإبلاغ عن تلك الحسابات.

إحدى نقاط الضعف في آلية استجابة فيسبوك وتعاطيها مع الحسابات الوهمية، والمحتوى الذي تنشره، تكمن في اعتماد المنصة على مجتمع المستخدمين الخاص بها للإبلاغ عن مثل هذا المحتوى، وتأخر الاستجابة لغاية وصوله إلى مستوى معين من الشعبية، في حين أنه من الأسهل استخدام الذكاء الاصطناعي لمراقبة المحتوى النصي في الوقت الفعلي. (بتصرف: Brookings - أبريل 2019)

هذه الإستراتيجية أكثر كفاءة وفعالية من حيث التكلفة لشركات التواصل الاجتماعي، وهذا يعني أيضًا أنه كلما اكتسب الحساب المزيف مزيدًا من الاهتمام، زادت احتمالية وضع علامة عليه، لإلقاء نظرة فاحصة.[1]

إضافة إلى ذلك، «تمتلك قنوات التواصل الاجتماعي حوافز تجارية قليلة جدًا للتخلص من الحسابات المزيفة، حيث يعتمد نموذج الإعلان بالكامل على متوسط عدد المستخدمين الشهري، خاصةً عندما تولد هذه الحسابات المزيفة تفاعلاً عبر الإعجابات ونقرات النقر وإعادة التغريد التي تؤثر على خوارزمية المحتوى الشائع المعروض للمستخدمين». Forbes - ديسمبر 2020

(1) نيويورك تايمز - ديسمبر 2020

طرق اكتشاف الحسابات الزائفة

أصبح منتحلو الشخصية أكثر ذكاءً وهم يجعلون تتبع حسابات وسائل التواصل الاجتماعي المزيفة أكثر صعوبة هذه الأيام. ومع ذلك، إذا كان الحساب مزيفًا، فهناك دائمًا علامة أو بضع علامات، ذلك أن كل إجراء عبر الإنترنت يترك بصمة رقمية، وعندما لا يتم إخفاء هذه البصمة بخبرة أو يصبح الجاني متخلفًا في تغطية آثاره، يمكن لمحققي وسائل التواصل الاجتماعي تتبعه واكتشافه. (Bosco Legal - أكتوبر 2022)

من خلال اتباع هذه الخطوات، يمكنك معرفة ما إذا كان الحساب زائفًا أم حقيقيا:

- ابحث عن مشتركات

استخدم محركات البحث للتحقق مما إذا كان الشخص المذكور موجودًا على الشبكات الاجتماعية الأخرى التي تستخدم نفس الاسم. تحقق مما إذا كانت صور الملف الشخصي المستخدمة متشابهة، وتحقق أيضًا من تطابق السير الذاتية للملف الشخصي وتفاصيل الاتصال والموقع، وافحص إذا ما كانت الحسابات تشترك في محتوى مماثل، وعليه، إذا تمكنت من اكتشاف درجة كبيرة من التداخل، فأنت على الأرجح تتعامل مع حساب حقيقي. يمكنك أيضًا دراسة صور الملف الشخصي للحصول على تلميحات، من خلال استخدم طريقة البحث العكسي عن الصور -خدمة تقدمها Google و Bing و Yandex- لمعرفة ما إذا كانت الصورة المستخدمة في الملف الشخصي تصور شخصًا آخر غير المطالب به ، أو إذا ظهرت الصورة في مكان آخر عبر الإنترنت. ولكن ضع في اعتبارك أن هذه مفاتيح وليست أدلة دامغة لقياس ما إذا كان الحساب صحيحًا أم لا. (دي دبليو - يوليو 2022)

- السلوك عبر الإنترنت

انتبه إلى وقت إنشاء ملف تعريف الوسائط الاجتماعية. إذا تم إنشاؤه وظل نشطًا لسنوات، فقد يكون حقيقيًا. ومع ذلك، فهذه ليست طريقة مؤكدة لقياس المصداقية... ادرس أيضًا نوع المحتوى المنشور بواسطة الحساب. هل تتطابق مع الشخص أم تبدو خارجة عن الشخصية؟، أيضًا إذا قام شخص ما بتغيير موقعه باستمرار، فإن هذا يجب أن يثير الاستغراب، إلا إذا كان الفرد يعمل كمدون سفر أو في صفة مماثلة. (دي دبليو - يوليو 2022)

- الاهتمامات

كن على دراية بقضايا المتصيدين المفضلة وكن مشككًا فيها. فهم قد يكونون أكثر اهتمامًا بإحداث الفوضى، لكنهم يظهرون أيضًا تفضيلات واضحة بشأن بعض القضايا[1]...

(1) . (The Conversation - يونيو 2020)

- تحقق أيضا من المؤشرات التالية:

- إذا كان هناك العديد من التحديثات والمحتوى المنشور ولكن القليل من المحادثات والتفاعل مع الأصدقاء.
- إذا تلقيت طلبًا لتحويل الأموال أو الكشف عن معلومات حساسة، فهذا تكتيك يستخدمه المحتالون.
- إذا أرسل رابطا عشوائيا، أو شارك نفس الرابط بشكل متكرر في فترة زمنية قصيرة، أو قدم معلومات مضللة حول وجهة الارتباط. (Europol - ديسمبر 2021)

ما الذي يتوجب فعله؟

لن يكون ثمة حلول ومعالجات ممكنة لظاهرة انتحال الهوية الرقمية، ما لم يستشعر الجميع مسؤوليته تجاه هذه الظاهرة، بدءًا بالمستخدم، وانتهاءً بإدارة المنصات الاجتماعية، نفسها، وعليه؛ فإننا سنطرح الحلول المتاحة كـ توصيات للأطراف المعنية.

للجمهور:

الامتناع عن متابعة الحسابات الوهمية أو التفاعل معها بأي حال، والإبلاغ عنها فورًا، ولتكن حذرا من التجاوب مع طلبات تحويل الأموال، أو الكشف عن أي معلومة شخصية، أو الضغط على أي رابط مرفق، تحت أي ظرف.

للمؤسسات الإعلامية والصحفية:

ينبغي لوسائل الإعلام والصحفيين والإعلاميين والناشطين، ألا يستقوا معلومات أو مادة إخبارية من الحسابات الزائفة، أو يتداولوا محتواها، إلا في سياق التنبيه، كما ينبغي القيام بدور توعوي، في كشف الحسابات الزائفة وفضح منشئيها، وإطلاع الجمهور على التكتيكات والوسائل التي يتبعها المتصيدون في ممارسة الجريمة الإلكترونية من خلال انتحال شخصية وهمية.

- للمنظمات والمؤسسات المانحة:

الاستثمار في دعم المنصات المعنية بـ «مكافحة الجريمة الإلكترونية»، وتزويدها بالإمكانيات اللازمة، وبالأخص «مبادرات» التحقق من المعلومات وكشف التضليل.

- لأطراف الصراع:

وينبغي لأطراف الصراع ألا تنخرط في صراع إلكتروني تعوزه الأخلاقيات والممارسات القيمية، وألا تلجأ إلى استخدام حسابات وهمية في نشر دعايتها وتعزيز تصوراتها للأوضاع، وتشويه الطرف الآخر.

- لمنصات التواصل الاجتماعي:

اتخاذ نهج استباقي للكشف عن الحسابات المزيفة وإزالتها من خلال تطبيق أنظمة آلية للكشف والإبلاغ، واستخدام وسطاء بشريين لمراجعة وإزالة الحسابات الزائفة، والتعاطي مع طلبات المراجعة بجدية ومسؤولية. بالإضافة إلى عقد شراكة مع المبادرات المحلية المعنية بـ «تدقيق الحقائق»، والعمل مع المنظمات المحلية لتعزيز الوعي بالمشكلة، وتوفير التعليم والتدريب للمستخدمين حول كيفية التعرف على الحسابات الزائفة والإبلاغ عنها.

- للسلطات:

العمل على إصدار «قانون الجرائم الإلكترونية»، على أن يخضع الأمر لنقاشات معمقة مع مختلف الأطراف ذوي المصلحة، بحيث تكون نصوص القانون محددة وواضحة ودقيقة وذات صلة، وبما لا يسهم في تقييد حرية الرأي والتعبير أو يؤدي إلى انتهاك خصوصية الأفراد وإلحاق الضرر بهم، كما يتوجب الدفع لإنشاء مركز وطني للاستجابة للحوادث السيبرانية، والاستعانة بخبراء ومختصين في هذا الحقل، فضلا عن إعادة تأهيل وتدريب القضاة والمحققين وكافة الأشخاص المعنيين بمعالجة الجريمة الإلكترونية

خاتمة

تشكل ظاهرة انتحال الهوية الرقمية في اليمن مصدر قلق متزايد يتطلب اهتمامًا فوريًا من قبل المعنيين، بما يسهم في تخفيف الأضرار الناجمة عن هذه الأنشطة الاحتيالية، من خلال اتباع الإرشادات الموصى بها، واتخاذ إجراءات استباقية لحماية تواجدنا على الإنترنت.


سام
للحقوق والحريات

ظاهرة انتحال الهوية الرقمية في اليمن..
الدوافع والتبعات

يناير 2023

violations@samrl.org
www.dg.samrl.org

Digital.Rights.Yemen
@SamDigitalRight

سام
للحقوق والحريات

www.samrl.org
info@samrl.org