

# انتحال الشخصيات السعودية في تويتر

الدوافع والآليات وأساليب المواجهة  
«دراسة تحليلية»



# المحتويات

03 مقدمة

03 موضوع الدراسة

05 نتائج الدراسة

• 05 أساليب انتحال الشخصيات السعودية

• 06 دوافع انتحال الشخصيات السعودية

• 08 أساليب الكشف عن الحسابات الوهمية

• 13 سبل الحماية من انتحال الشخصيات

14 خاتمة

## مقدمة..



يُمثّل انتحال الشخصيات عبر شبكات التواصل الاجتماعي، أو استخدام ملفات التعريف المزيفة، واحداً من أكثر الطرق شيوعاً لتنفيذ هجمات سرقة البيانات عبر هذه الشبكات، حيث يُقدّم المستخدمون أنفسهم في حسابات تنتحل هوية شخصيات حقيقية أو وهمية، وهو ما يبرز إشكالية حقيقية تُهدّد الأفراد والمجتمعات، لما تتضمنه من مظاهر التشهير والنشر غير المشروع، خاصة أن تلك الشبكات لا توقّر ميزات التحقق من الشخصية، وما إذا كان الحساب المنسوب إليها تحت إشرافها وتحكمها، إذ من الممكن أن يستخدم شخص ما هوية مزورة لشخص حقيقي، ليستفيد من سمعته أو ماله أو صلاحياته.

وقد انتشرت هذه الأساليب بصورة كبيرة في المملكة في الفترة الأخيرة، من خلال انتحال شخصيات شهيرة ولها مكانتها المرموقة في المجتمع، واستغلال مكانتها لتنفيذ عمليات غير مشروعة، ما يستوجب دراسة ظاهرة الانتحال، ووضع تصوّر علمي فعّال لمواجهتها.

## موضوع الدراسة:

ترصد هذه الدراسة أساليب ودوافع انتحال الشخصيات السعودية على شبكة التواصل الاجتماعي «تويتر»، وتحدّد آليات كشف الحسابات الوهمية التي تُستخدم في عملية الاحتيال، لوضع تصوّر فعّال لمواجهة تلك الهجمات الإلكترونية، ويحتلّ هذا الأمر أهمية مجتمعية كبيرة تتمثل في الحفاظ على قيم المجتمع وحماية خصوصية مستخدمي الشبكات الاجتماعية، وخاصة المشاهير وقادة الرأي في المجتمع، والذين يتمّ استغلال هوياتهم بشكل واضح في الهجمات الإلكترونية، لتحقيق منافع مادية أو معنوية، أو لأغراض الترويج ونشر الأفكار وترسيخ الاتجاهات والتأثير على الأفراد.

اعتمدت الدراسة على المنهج الاستقرائي لتحديد المفاهيم والدوافع والأدوات التي تُستخدم في عمليات انتحال الشخصيات عبر الشبكات الاجتماعية، من خلال مراجعة الأدبيات والدراسات العلمية وتحليل محتوى آراء الخبراء والمُؤرّدين حول موضوع الانتحال، بالإضافة إلى المنهج الوصفي لرصد وتحليل الصفحات التي تُستخدم هويات الشخصيات السعودية من المشاهير على «تويتر»، للتعرف إلى الأساليب والأدوات التي يعتمد عليها منتحلو الهوية، وتحديد آليات معرفة الهويات الحقيقية وكشف الانتحال.

## 39 حساباً..

شملت عينة الدراسة استخدمت أسماء أميرات سعوديات.

وتضمّنت عيّنة الدراسة حسابات تويتر لشخصيات سعودية مرموقة، يتكرّر استخدام أسمائها في حسابات مختلفة، ما يشير إلى وهمية أغلبية تلك الحسابات، ومن بينها أسماء أميرات من العائلة المالكة، للشعبية البارزة التي يحظين بها في المجتمع السعودي، ومشاركتهم في المناسبات الاجتماعية والإنسانية والشأن العام، ما دعا المنتحلين لاستغلال ثقة الشعب بهنّ، بإنشاء حسابات وهمية متعدّدة بأسمائهنّ.

شملت عيّنة الدراسة 39 حساباً على شبكة تويتر، استخدمت أسماء أميرات سعوديات، تم اختيارهنّ بطريقة عمّدية، وكانت موزّعة وفقاً للجدول التالي:

الإجمالي	الحسابات غير الموثقة	الحسابات الموثقة	اسم الشخصية
9	9	-	سمو الأميرة حصة بنت سلمان بن عبد العزيز آل سعود
8	8	-	سمو الأميرة البندري بنت عبد الرحمن الفيصل آل سعود
4	3	1	سمو الأميرة ريما بنت بندر بن سلطان آل سعود
5	4	1	سمو الأميرة الجوهرة بنت طلال بن عبدالعزيز آل سعود
9	9	-	سمو الأميرة سحاب بنت عبدالله بن عبد العزيز آل سعود
1	-	1	سمو الأميرة فهدة بنت سعود بن عبد العزيز آل سعود
1	-	1	سمو الأميرة لمياء بنت ماجد بن سعود بن عبدالعزيز آل سعود
1	-	1	سمو الأميرة ريما بنت طلال بن عبدالعزيز آل سعود
1	-	1	سمو الأميرة ريم بنت الوليد بن طلال بن عبدالعزيز آل سعود

اعتمدت الدراسة على تحليل محتوى الخصائص المميزة لحسابات تويتر عيّنة الدراسة، المتمثلة في معلومات وبيانات ملفات تعريف مستخدمي تلك الهويات وعلاقتها وطبيعة تغريداتها، والمشاركات التي تتم من خلال تلك الحسابات، وتحليل القواسم المشتركة بين الأنشطة المنسقة لتلك الحسابات، بالإضافة إلى تحليل السمات المميزة للحسابات الشرعية عن المزيفة، وقد تم الاعتماد على مقياس مؤشر جودة مستخدمي تويتر (TUQI) لفرز خصائص المستخدم.

## نتائج الدراسة

### أولاً: أساليب انتحال الشخصيات السعودية

تعددت الأساليب المستخدمة في انتحال الشخصيات السعودية الشهيرة على شبكة تويتر، وتمثلت أكثر الأساليب استخداماً في: إنشاء ملف تعريف مزيف تماماً، وانتحال شخصية ذلك المستخدم لاحقاً، والوصول إلى موارده، والاستفادة من السيطرة المكتسبة على برنامج شبكة تويتر الخاص به، كمنصة انتشار لمهاجمة أصدقائه الموثوقين ونشر الرسائل نيابةً عنه، والوصول إلى معلومات المستخدم الخاصة مثل العمر ووجهات النظر، ومكان الوجود الحالي أو المستقبلي، وأخيراً تحديد موقع الضحايا الذين ينوي المنتحل التغيير بهم في معاملات غير حقيقية.



وقد نتج عن استخدام هذه الأساليب انتشار الحسابات المزيفة للشخصيات السعودية الشهيرة، والتي تحتوي على بيانات وتفصيل الشخصيات الحقيقية، بهدف الحصول على امتياز مادي أو معنوي أو لأغراض أخرى.

وتُعدّ الشخصيات العامة في المملكة، سواء السياسية أو الإعلامية أو الرياضية أو الأدبية، الأكثر تعرّضاً للانتحال الشخصيات على تويتر، لتحقيق الأهداف الاحتيالية - أياً كان نوعها - وتزداد الخطورة في حال انتحلت شخصيات سياسية واعتبارية لها قيمتها في المجتمع، بطريقة تُسيء للشخصيات وتتقوّل على لسانها، ما دعا الكثير من تلك الشخصيات إلى التبرؤ من تلك الحسابات ونفي الصلة بها، وتوثيق حسابات شخصية حقيقية، كما لجأ البعض إلى استخدام طريقة بث الفيديو الخاص «كيك - keek» عبر تويتر، بهدف إثبات الشخصية، خاصةً بعد أن **نجح بعض المنتحلين في تقمص الشخصية المنتحلة**، وإقناع رواد تويتر بأنّه بالفعل الشخص المشهور، وذلك إمّا:

● بحثاً عن التسلية.

● أو تعمّد الإساءة وترويج الشائعات.

● أو لأغراض تتعلّق بالاحتيال المالي.

ما يستوجب إيجاد حلول مرنة تحدّ من هذه التجاوزات.

ولا يقتصر خطر الانتحال في تويتر على المشاهير السعوديين فقط، بل يصل هذا الانتحال لأيّ مستخدم آخر، أو حتى إنشاء حسابات وهمية لا تمتّ بصلة لشخص

حقيقي، والتي عادةً ما تُستخدم لعدم الإفصاح عن الهوية الحقيقية أثناء الممارسات الإلكترونية، سواء لحاجات نفسية ومعنوية يتحرّج البعض من القيام بها بالهوية

## انتحال الشخصيات

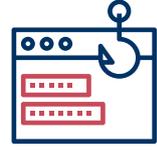
في تويتر لا يقتصر خطره على المشاهير السعوديين فقط.

الحقيقية، أو حتى لنشر الآراء والإيديولوجيات، من خلال إغراق الهاشتاقات بتغريدات متتابعة ومتكررة من حسابات مختلفة ومتنوعة، تدور حول فكرة واحدة واتجاه واحد، وتسعى إلى تبني قضايا ونشرها على مستوى الرأي العام السعودي، وإيهامه بأن هناك رأياً قوياً يمثل عدداً

كبيراً من الناس، وأن ما تطرحه وتتبناه عبر تغريداتها هو الرأي الصحيح والمقبول، أو توجيه المغردين السعوديين نحو النقاش في هذه الموضوعات أو القضايا التي تطرحها الحسابات الوهمية، وصرّهم عن هاشتاقات أو قضايا أخرى أكثر أهمية، ومن ثم تحفيز القنوات الإعلامية لتناول هذا الرأي العام الوهمي، من خلال بعض المؤشرات، كزيادة نسب التفاعل في هاشتاق معين.

## ثانياً: دوافع انتحال الشخصيات السعودية

تختلف دوافع وأسباب انتحال الشخصيات عبر الشبكات الرقمية، باختلاف أهداف وطبيعة المنتحل وثقافته، ومدى ما يملكه من خبرة ومهارة في مجال البرمجيات والحاسب الآلي، إلا أن السيناريو النموذجي لاستخدام الهويات الرقمية المزورة - سواء المزيفة أو الوهمية - يتمثل في سعي المهاجم الإلكتروني إلى بناء الثقة



مع الهدف (المستهدفين من المستخدمين الأبرياء على شبكات التواصل الاجتماعي)، ومن ثم استغلال تلك الثقة - بعد ذلك - في التفاعل المباشر للحصول على معلومات الاهتمامات الشخصية، وجمع مزيد من المعلومات تُفيد في صناعة الهجمات الإلكترونية، مثل هجمات التصيد العشوائي الاحتيالي، ونشر البرامج والأنشطة الضارة أو الارتباط بها، بالإضافة إلى المساعدة في تصعيد تلك الهجمات الاحتيالية.

ومن خلال تحليل عينة من آراء المغردين السعوديين حول أسباب انتحال الشخصيات في تويتر، أكد المغردون على أنه سلوك مرضي، ناتج عن ظهور التقنية التي أوجدت ثقافة فرعية مَهَّدت لظهور وانتشار أنماطٍ من الانحرافات السلوكية التقليدية والمستحدثة، والتي تُسبب حرجاً اجتماعياً، وذلك السلوك يُعبّر عن شخصيةٍ مضادةٍ للمجتمع، تُسوّ لها نفسها انتحالاً صفةٍ إحدى الشخصيات المشهورة، للتواصل مع أكبر عدد من المعجبين، كما أنه ناتج عن خلل وشعور بالنقص، أو الحقد ومحاولة الإضرار بالشخصية التي يتم انتحالها، بترويج شائعات أو رسائل مخالفة لفكرها ومبادئها، بهدف تشويه صورتها، أو تشويه سمعة المجتمع الذي إليه تنتمي.

## ويمكن إجمال دوافع انتحال الشخصيات بالتالي:

● **الدوافع المادية:** تُعدّ الرغبة الجامحة في تحقيق الثراء لدى العديد من المُنتحلين، من الدوافع الرئيسية لاستخدام هذا الأسلوب، نظراً للأرباح الطائلة التي يُمكنُ جنيهاً من هذه الأعمال بأقلّ جهد، من خلال عمليات استغلال البيانات والابتزاز والاحتيال وغيرها، مُستغلّين الفرص التي أتاحتها التقنيات المعلوماتية. **وتُعدّ أخطر أنواع انتحال الشخصيات** تلك التي تهدف إلى سرقة مستخدمي تويتر والاحتيال عليهم، وانتحال صفة شخصيات عامة بهدف جمع التبرعات أو الاشتراك في مشاريع تجارية وهمية من قبل أصحاب هذه الحسابات المُنتحلة.

● **الدوافع الذاتية:** وتتخذ أشكالاً عدة، مثل الرغبة في إثبات الذات والتغلب على تقنية الأنظمة الحاسوبية وتحقيق الانتصار عليها، وذلك **بدافع التحدي لإثبات القدرات الذاتية، وإشباع شعور البحث** عن القوّة دون وجود دافع الحقد أو التخريب، وكذلك الرغبة في الحصول على المعلومات الجديدة عن التطوّر التكنولوجي وكلّ ما يحتويه عالم الكمبيوتر والشبكات الإلكترونية من أسرار، والتي تدفع الكثير من الأشخاص إلى ارتكاب جرائم إلكترونية للبحث واكتشاف الأنظمة التقنية، تحت دعاوى ضرورة عدم وجود قيود في سبيل الحصول على أيّ نوع من المعلومات.

● **الدوافع الاجتماعية:** وتعبّر عن التأثير على الرأي العام، من خلال عمليات السيطرة والتوجيه وترتيب الأولويات، أو الهجوم على أشخاص أو جماعات أو مؤسسات، وتكوين رأي عام مضافاً أو معارضة مصطنعة لآراء وأفكار واتجاهات هؤلاء الأشخاص أو الجماعات أو المؤسسات، **بههدف تشويه الصورة، أو الرغبة في الانتقام** من شخص أو جهة أو مؤسسة لسبب ما، وفي بعض الأحيان يكون دافع المزاج والدعابة هو المقصد من استخدام هذا السلوك الإجرامي.

● **الدوافع السياسية:** وهي الأشدّ خطراً لكونها تستهدف مجموعات أو شعوباً بأكملها، وتُستخدم فيها أساليب حرب المعلومات ونشر الشائعات والتشكيك في الدول، عبر هجمات إلكترونية منظمة من قبل جهاتٍ تقدّم دعماً مالياً لمجموعات من الأفراد، مقابل عدد متفق عليه من التغريدات بشكل دوري، أو عن طريق حسابات تُدار بشكل آلي (socialbots) لتحقيق أهداف تلك الجهات، والتي من أهمّها **التحكّم والسيطرة على مصادر المعلومات**، وبالتالي السيطرة على الإعلام والرأي العام، من خلال هجمات إلكترونية ميسرة تستخدم نهجاً واحداً واضحاً، وبلغة وطريقة سردية واحدة.

## ثالثاً: أساليب الكشف عن الحسابات الوهمية

استندت الدراسة في تحديد آليات الكشف عن الحسابات الوهمية في تويتر، على الخصائص المميزة لحسابات الوسائط الاجتماعية الخاطئة الفردية، إلى جانب روابطها الاجتماعية، والقواسم المشتركة بين الأنشطة المنسقة لحسابات وسائط اجتماعية مزيفة متعدّدة.



وتُظهر النتائج وجود **نوعين رئيسيين من الحسابات الوهمية:**

- الحسابات المزيفة (Sybils).
- الحسابات التي تتزايد قائمة متابعيها باستمرار، نتيجة استغلال أسماء وشخصيات المشاهير.

وتحدّدت أهمّ أساليب الكشف عن الحسابات الوهمية، في تحليل واستخلاص ميزات وخصائص الملفات الشخصية الفردية والمشاركات وعلاقتها، وذلك بمساعدة:



● مصنّفات النصوص وخوارزميات التعلّم الآلي.

● مكوّنات الكشف التي تقيّم انتظام التغريدات.

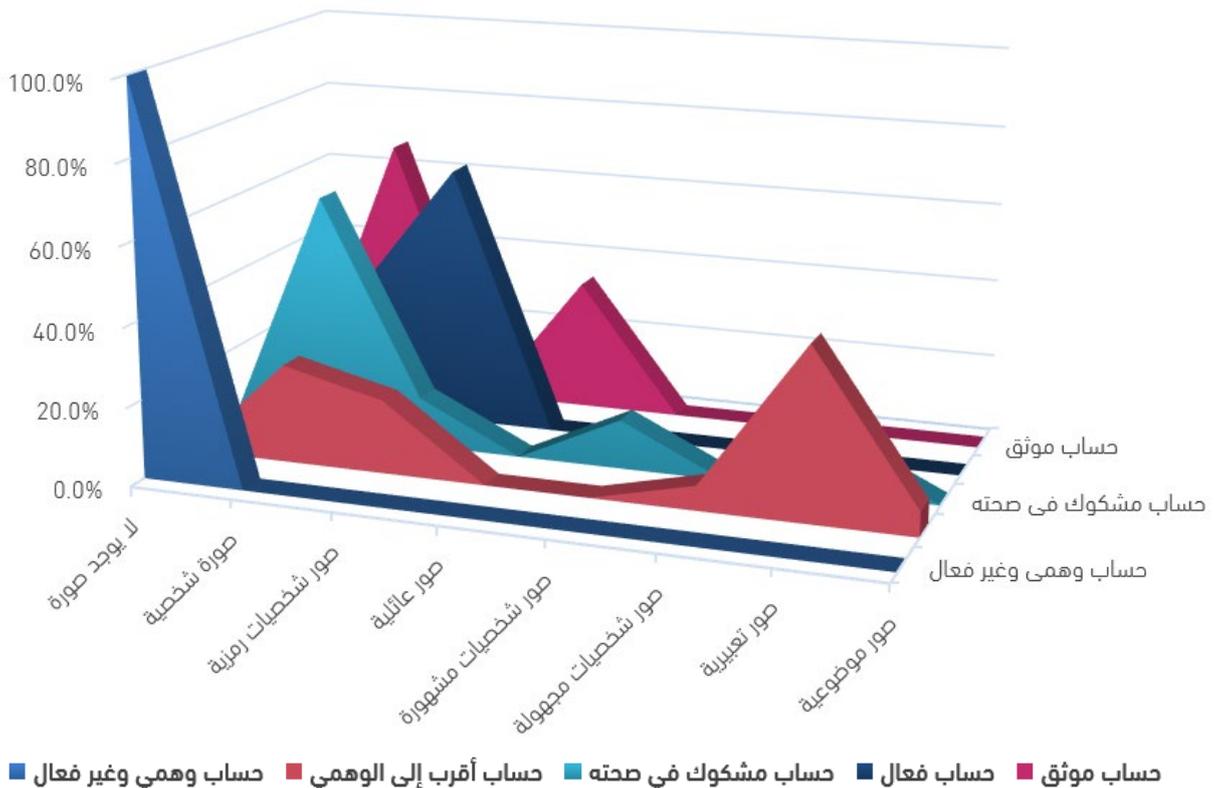
● عدد اللغات المحكية والتعليم والمهارات.

● عدد الاتصالات وأنواعها.

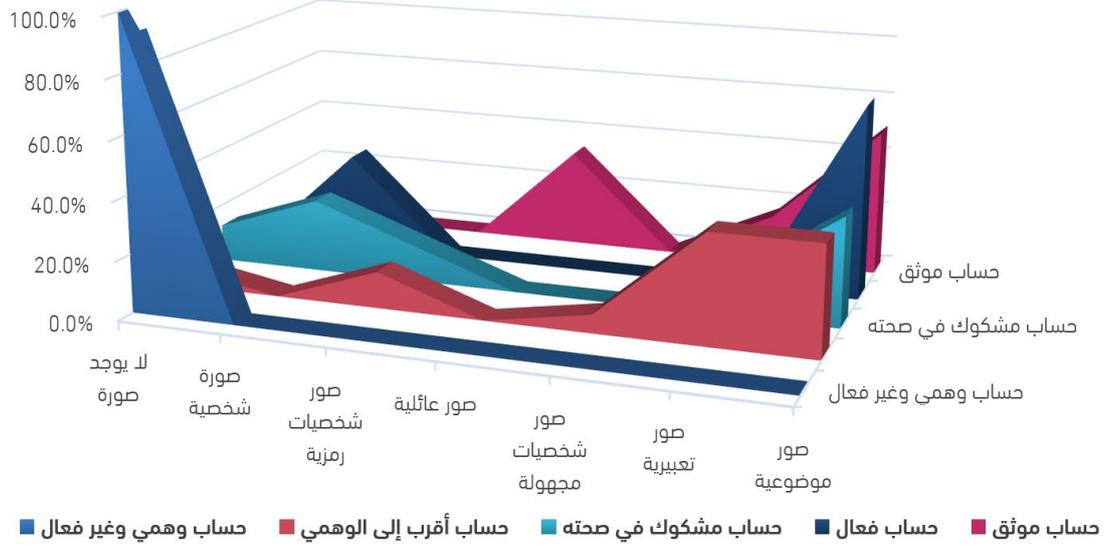
● بعض خصائص الحساب، باستخدام واجهات برمجة التطبيقات، من خلال تحليل بيانات المستخدمين وميزات الملفات الشخصية وعلاقتها، إلى جانب استخدام ميزات تشابه الرسائل، ووجود أنماط وراء البحث عن الأصدقاء لإضافتهم، والتوقيات والجوار، مع الاعتماد على الملاحظة التي تشير إلى أن ملفات التعريف المزيفة (Sybil) تتّصل عادةً بملفات التعريف المزيفة الأخرى، بدلاً من الملفات الشخصية المشروعة.

وفي هذا السياق استخدمت الدراسة هذه الأساليب لتحليل الحسابات الاجتماعية - عينة الدراسة - على تويتر، في محاولةٍ للكشف عن الخصائص المميزة للحسابات الحقيقية والوهمية، وكشفت نتائج التحليل الكيفي لسمات البيانات التعريفية، اعتماداً على الحسابات الوهمية أو غير الحقيقية على استخدام الألقاب وصيغ التفضيم والتقدير في التعريف بالحسابات (اسم المستخدم)، وظهور أرقام أو رموز أو حروف لا تُعبّر عن أيّ دلالات في الأسماء التعريفية، مع وجود عدد من الحسابات التي أظهرت مراجعةً أسمائها التعريفية صفةً الحساب المزيف، بسبب دلالتها على هوية المنتحلين الحقيقية، ومنها حسابات متكرّرة لنفس الشخص، في حين أظهرت الحسابات الموثوقة اعتماداً واضحاً على استخدام الأسماء الحقيقية للشخصية، كمعزّفات مباشرة، في كلٍّ من (اسم المستخدم) دون أي ألقاب، و(الاسم التعريفي) دون مبالغة في استخدام رموز أو أرقام، وأظهر تحليل الميزات المستند للرسوم البيانية، فروقاً واضحة في استخدامات الصور التعريفية وصور الغلاف للحسابات عينة الدراسة، وفقاً لدرجة موثوقيتها وصحتها، حيث كانت الحسابات الوهمية أقرب لعدم استخدام صور تعريفية أو غلاف بشكل واضح، بينما كانت الحسابات الموثوقة حريصةً بشكل واضح على استخدام الصور الشخصية - سواءً لصاحب الحساب فقط أو الصور التي تجمع الشخصية بأفراد العائلة - كصورةٍ تعريفية، دون اهتمام بالأنواع الأخرى للصور، كما كانت الصور الموضوعية أو العائلية عنصراً مميزاً لصور غلاف تلك الحسابات الموثوقة.

شكل رقم (1) الصور التعريفية في حسابات تويتر



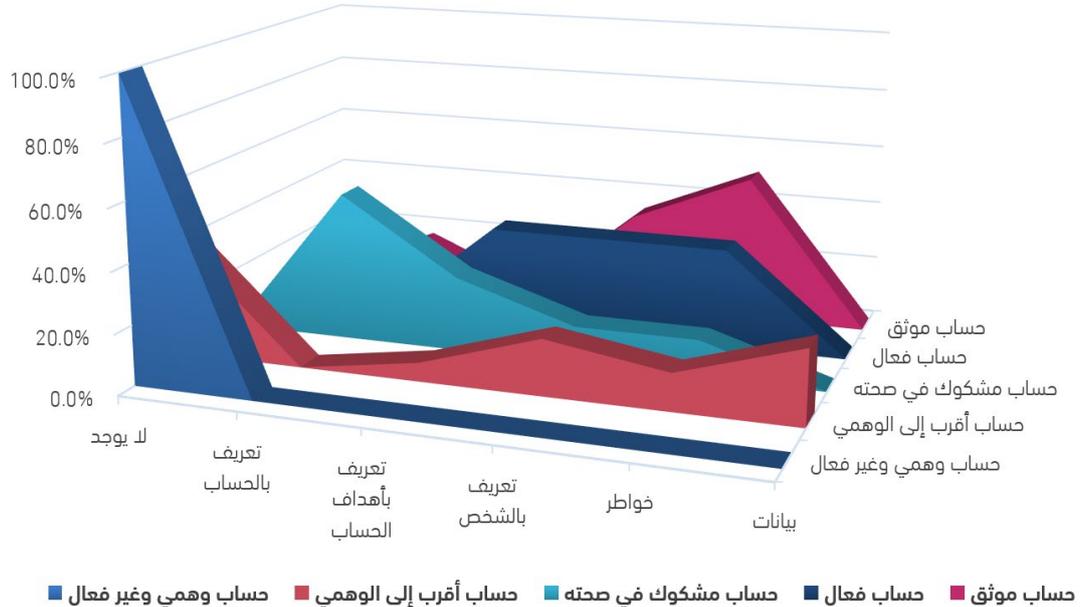
شكل رقم (2) صور الغلاف في حسابات تويتر



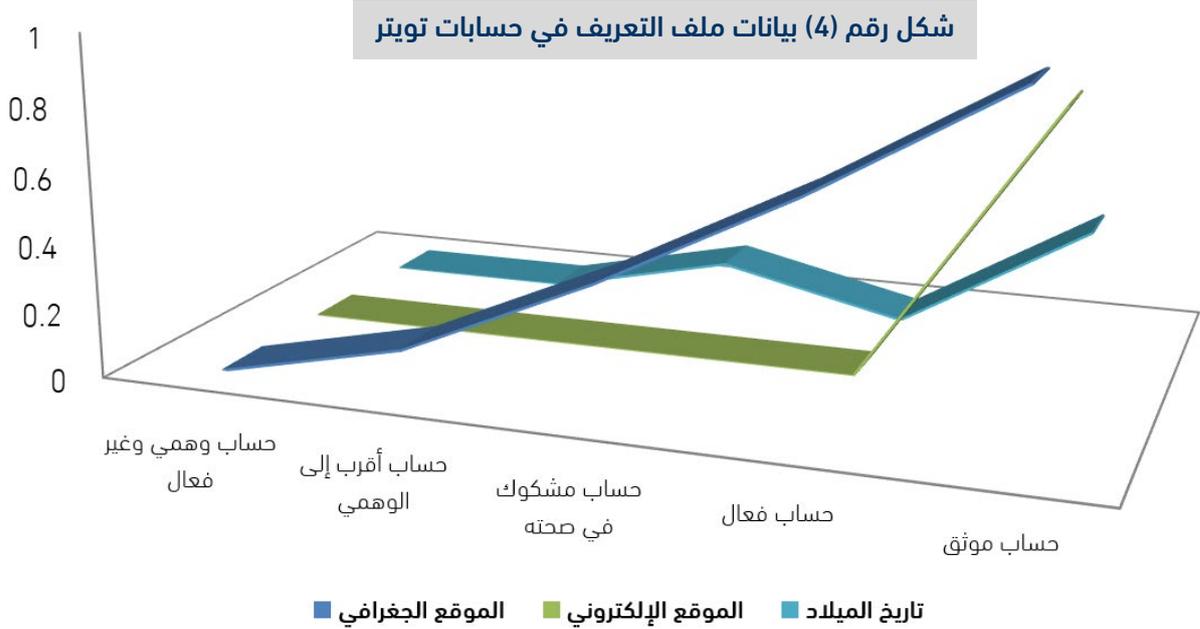
وتنوّعت استخدامات الحسابات الوهمية لبيانات النبذة التعريفية، بين استخدام الخواطر العامة والبيانات غير المفهومة، أو محاولات اكتساب صفة شرعية للحساب، من خلال محاولات التعريف بالحساب، والتأكيد على أنه حساب رسمي، أو التعريف بالشخصية المُنتقلة، بينما خلت نسبة كبيرة من أي بيانات تعريفية.

فيما كانت النبذة التعريفية للحسابات الموثقة مختصرة وواضحة، إما للدلالة على صفة الشخصية، أو التأكيد على رسمية الحساب، أو لخواطر اجتماعية ذات صفة عائلية. ويظهر الرسم البياني التالي أنماط استخدام النبذة التعريفية بشكل أكثر تفصيلاً، وفقاً لتصنيفات الحسابات عينة الدراسة:

شكل رقم (3) النبذة التعريفية في حسابات تويتر

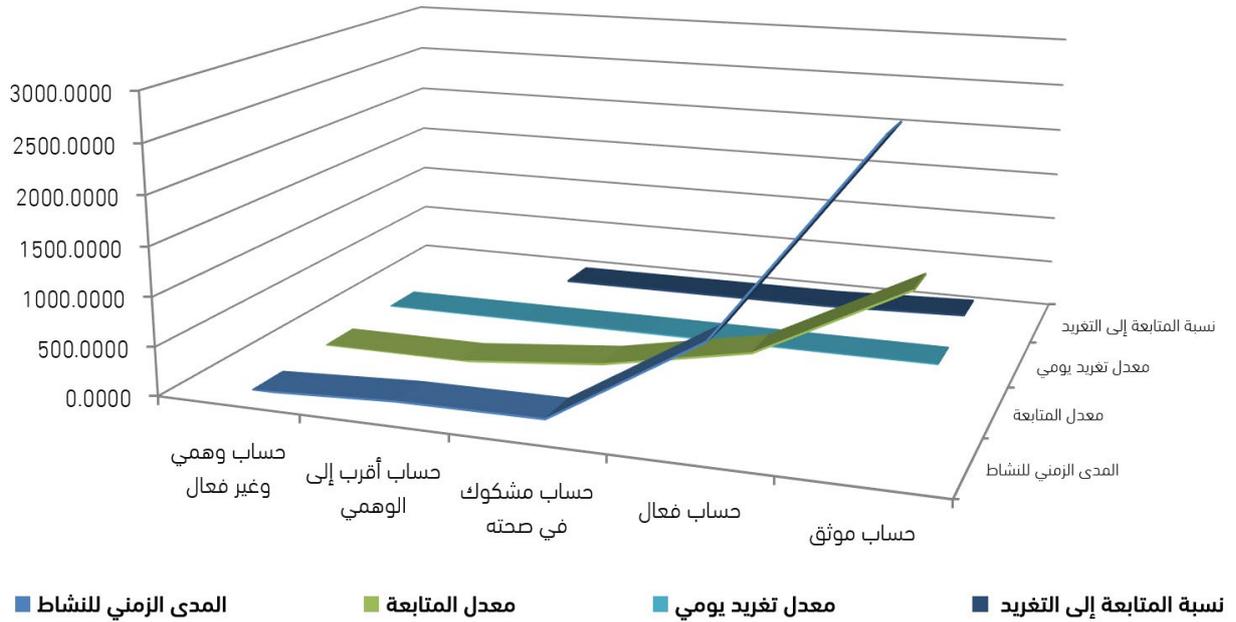


لم تستخدم الحسابات غير الموثقة أيّ بياناتٍ أخرى في ملفات التعريف بشكل واضح، فيما أظهرت الحسابات الموثقة استخداماً كاملاً لبيانات الموقع الجغرافي، واستخداماً شبه كامل لبيانات الموقع الإلكتروني، وفي بعض الحالات تمّ إظهار بيانات تاريخ الميلاد.



أظهرت الملاحظة الكيفية لخصائص الحسابات عيّنة الدراسة، وجود مدى زمني طويل يكتسب صفتي القَدَم والاستمرارية لأنشطة الحسابات الموثقة، صاقبته مُعدّل متابعة مرتفعة، وهي النتيجة المنطقية لثقة المتابعين في الحساب، واستمرار النشاط بشكل يومي لفترات طويلة، على عكس الحسابات غير الموثقة، والتي أنشئ أغلبها بتواريخ حديثة ونشاطٍ زمني محدود، وبالتالي صاقب هذا النشاط مُعدّل متابعة منخفض، فيما لم تُظهر بيانات مُعدّل التغريد اليومي أو نسبة المتابعة إلى التغريد، أيّ مؤشرات واضحة يُمكن الاعتمادُ عليها للتمييز بين الحسابات، حسب درجة موثوقيتها وفعاليتها، وهو ما يوضّحه الشكل البياني التالي:

شكل رقم (5) معدلات النشاط في حسابات تويتر



واستناداً للبيانات السابقة، يُمكن فهم عدم ظهور محتوى تغريدات أو وسائط، أو حتى حالات إعجاب في كثير من الحسابات غير الموثقة والتي تكتسب صفة الوهمية، بالإضافة إلى كون المحتويات التي ظهرت في الحسابات غير الحقيقية ذات سمة عاطفية تعمل على استمالة المستخدمين من خلال إجراءات المساعدات الإنسانية والمسابقات الاحتيالية بتغريدات متكررة، والمحتويات ذات الطابع الديني لاستغلال تعاطف المستخدمين ونزعاتهم نحو التقرب من كل ما هو ديني، أو نشر محتويات إنشائية وخواطر - يعتمد أغلبها على الصور - لمجرد الظهور على الشبكة، أو استغلال صور الملوك والأمراء في الترويج للصفحة، وكانت جميعها تغريدات مباشرة، ولا يوجد أي حرص على التفاعل من خلال الردود أو إعادة التغريد أو غيرها.

في حين أظهرت الحسابات الموثقة اهتماماً واضحاً بأشكال التفاعل المتاحة في شبكة تويتر، سواء إعادة التغريد أو الردود أو استخدام الوسائط والإعجابات وغيرها، مع التركيز على مراعاة موثوقية المحتوى المنشور، وخدمته لأهداف الشخصية وصورتها وحيثيتها وانتماؤها ومرجعياتها، ومراعاة الصالح العام للمملكة، من خلال مضمون مُتزن يستخدم صيغ الإخبار عن الشخصية أو المؤسسة التي تنتمي إليها الشخصية وأهم نشاطاتها، والأحداث الهامة، والتعبير عن الحالات الشعورية والتفاعل الاجتماعي والمشاركات والاهتمامات الإنسانية.

## رابعاً: سبل الحماية من انتحال الشخصيات

رصدت الدراسةُ عدداً من سُبلِ حماية مستخدمي شبكات تويتر من انتحال الشخصيات، على غرار طول الأمن في العالم الواقعي، والتي لجأ إليها العديد من مُشغلي شبكات التواصل الاجتماعي، وشركات الأمن التجاري، والباحثين الأكاديميين، من خلال استخدام مجموعة متنوعة من طول الأمن والخصوصية التي تُوفّر عدة طبقات من الحماية ضد هذه التهديدات، تتمثل في:



● ضبط إعدادات الخصوصية: وهي طبقة الحماية الأولى التي تُعدّ بمثابة وظيفة إحكام الغلق، وتُسهّل إلى منع المتسللين غير المرغوب فيهم من الدخول إلى المشاركات والتفاصيل الشخصية لمستخدمي شبكات تويتر، من خلال مجموعة من إعدادات الأمان والخصوصية المختلفة المُعدّة من قبل مشغلي الشبكة. كما قامت شركات الأمان والباحثون الأكاديميون المتخصصون، بتطوير طول تساعد هؤلاء المستخدمين في تحسين إعدادات الخصوصية، ومنها ما يعمل تلقائياً على فحص المعلومات المنشورة للمستخدمين، ومنعهم من تحميل منشورات تحتوي على المعلومات الحساسة، مثل (The Social Privacy Protector) - (ZoneAlarm Privacy Scan).

● طول برامج أمان الإنترنت: وتُعدّ بمثابة وظيفة إنذار الأمن، وتهدف إلى منع المستخدمين من اختراق حسابات الشبكة الاجتماعية، أو جمع المشاركات والتفاصيل الشخصية للمستخدمين، بالإضافة إلى برمجيات اكتشاف التصيد الاحتيالي والحسابات الاجتماعية المزيفة.

● مراقبة النشاط عبر الإنترنت: من خلال برامج المراقبة المختلفة مثل Net Nanny MinorMonitor - وهي بمثابة الكاميرات الأمنية التي تعمل على مراقبة المحيط المكاني.

● تفعيل آليات التوثيق والمصادقة: وهي المسؤولة عن التأكد من أن الأشخاص الحقيقيين فقط من يمكنهم تسجيل الدخول إلى الشبكة.

● الإمكانيات المتاحة لمشغلي الشبكات الاجتماعية: والتي تُوفّر لهم إمكانية تحديد التهديدات المحتملة بناءً على هيكل الشبكة الاجتماعية بالكامل، إلى جانب عناوين IP الخاصة بالمستخدمين، وأوقات تسجيل الدخول، وأنماط السلوك، والاستفادة من طوبولوجيا الرسم البياني لشبكة التواصل الاجتماعي الكاملة، من أجل تحديد المؤيدين المزيفين.

## خاتمة..

يُعاني المجتمعُ السعودي من خطر انتشار الحسابات الوهمية التي تؤثر على طبيعة الحراك المجتمعي في المملكة، ويقف وراءها أشخاص وجماعات وجهات، تستخدمها لتنفيذ أعمال احتيالية، أو الإساءة لشخصيات عامة والنيل منها، أو الإضرار بمصلحة البلاد ومحاولة تفريق وحدة شعبها.

وتقدّم الدراسة مجموعة من الأدوات التي يمكن من خلالها تمييز هذه الحسابات، أبرزها:

**التأكد من البيانات التعريفية للحساب**، حيث أن عدم وجود نبذة موجزة للتعريف بالحساب، أو وجود اسم تعريفي يحوي حروفاً ورموزاً أو بيانات غير مفهومة، قد يكون مؤشراً واضحاً على عدم صحة هذا الحساب.

**تشابه هذه الحسابات في عدد التغريدات** ونوعية المتابعة والقدى الزمني للنشاط، حيث تُعدّ حالات ضعف المتابعة مع زيادة نسبة التغريد، وحادثةُ تاريخ إنشاء الحساب، بمثابة مؤشرات هامة للشك في صحة الحساب.

**التشابه والتقارب في عدد التغريدات ومضمونها**، والتي قد تدلّ على سلوكيات غريبة لا يصحّ أن تصدر عن شخصية عامة، مثل إعادة المتابعة من حساب يحمل اسم شخصية عامة بشكل مفاجئ، أو استلام دعوات من قبلها للانضمام إلى مجموعات اجتماعية، أو الدخول إلى روابط معينة، أو طلب المساعدة في مأزق مالي.

ولتجنّب خطر تلك الحسابات، تُوصي الدراسة باستخدام مجموعة متنوّعة من حلول الأمن والخصوصية، المتمثلة في عمليات ضبط **إعدادات الأمان والخصوصية في الحسابات**، وتفعيل آليات التوثيق والمصادقة، والاستعانة بالبرمجيات الخاصة بعمليات الأمان والمراقبة، مع التأكد من معلومات الحساب قبل نقل أيّ تغريدة، خاصة إذا كانت مثيرة للجدل، وعدم دعم الحسابات التي تنتحل الشخصيات مهما كان هدفها أو مبررها، وعدم التردّد في الإبلاغ عن تلك الحالات الإجرامية.

# مركز القرار

للداسات الإعلامية



..نخطو  
بقرارك



تابع حسابنا على تويتر



 [www.alqarar.sa](http://www.alqarar.sa)

   @alqarar\_sa