سياج
SIYAJ

2026

دراسة رصدية تحليلية · الإصدار الثاني

التصيّد الاحتيالي وانتحال الجهات الحكومية لتزوير الوثائق الرسمية في المملكة العربية السعودية

بوابات تحقق مزيفة ورموز استجابة سريعة مضلِّلة:
قراءة في بيانات رصدٍ استمر 51 يوماً وشمل نحو 4.7 مليار اسم نطاق

Phishing and Impersonation of Saudi Government Entities for Forging Official Documents: An Observational Analytical Study

إعداد

م. تركي عبدالله الشهري

مؤسس منصة سياج

فترة الرصد

20 سبتمبر – 9 نوفمبر 2026

البيانات محدّثة حتى 9 نوفمبر 2026

4.7 مليار
اسم نطاق رُصد في سجلات شفافية الشهادات

150
موقعاً منتحِلاً مؤكداً، منها 17 بوابة تزوير

247
شهادة صحية مزوّرة في سجلات موقع واحد خلال 37 يوماً

58
موقعاً أُبلغت بها الهيئة الوطنية للأمن السيبراني في 26 بلاغاً

بيانات الدراسة

العنوان: التصيّد الاحتيالي وانتحال الجهات الحكومية لتزوير الوثائق الرسمية في المملكة العربية السعودية: دراسة رصدية تحليلية

الباحث: م. تركي عبدالله الشهري، مؤسس منصة سياج

الإصدار: الثاني، نوفمبر 2026

مصدر البيانات: قاعدة بيانات منصة سياج، لقطة 9 نوفمبر 2026، الساعة 23:08 بتوقيت الرياض

طريقة الاستشهاد المقترحة

الشهري، تركي عبدالله. (2026). **التصيّد الاحتيالي وانتحال الجهات الحكومية لتزوير الوثائق الرسمية في المملكة العربية السعودية: دراسة رصدية تحليلية**. منصة سياج.

Alshahri, T. A. (2026). **Phishing and impersonation of Saudi government entities for forging official documents: An observational analytical study**. Siyaj.

المحتويات

- **الملخص** — 3
  Abstract
- **أبرز النتائج** — 4
  النتائج الرئيسة ونافذة الرصد في صفحة واحدة

01 **المقدمة وإطار الدراسة** — 5
المشكلة، والأسئلة، والأهداف، والأهمية، والحدود، والمصطلحات

02 **الدراسات السابقة** — 7
دراسات وتقارير عن السياق السعودي، وأدبيات التزوير بالذكاء الاصطناعي

03 **منهجية الدراسة** — 8
مصادر البيانات، والعينة، وإجراءات الإبلاغ، والاعتبارات الأخلاقية

04 **النتائج** — 10
بوابات التزوير، وثلاث دراسات حالة، والجهات المستهدفة، والأساليب، والإبلاغ

05 **الذكاء الاصطناعي وتحوّل التزوير** — 18
ما توثقه التقارير الدولية وما يتسق معه في بيانات الرصد

06 **مناقشة النتائج** — 20

07 **التوصيات** — 21
حلول التحقق، وتوصيات الجهات، وتوصيات بحثية

08 **الخاتمة** — 22

- **المراجع** — 23
- **الملاحق** — 24
  قنوات التحقق الرسمية، ومؤشرات بوابات التزوير المؤكدة

تنويه: سياج مبادرة سعودية مستقلة، وليست جهة حكومية، ولا تمثّل أي جهة ورد اسمها في هذه الدراسة. تُعرض أسماء النطاقات الضارة بصيغة معطّلة `[.]` لمنع فتحها بالخطأ، ولا تتضمن الدراسة أي بيانات شخصية.

الملخص

Abstract

تهدف هذه الدراسة إلى وصف أنماط انتحال الجهات الحكومية السعودية عبر النطاقات الإلكترونية، وبيان توظيفها في التصيّد الاحتيالي وفي تزوير الوثائق الرسمية. اعتمدت الدراسة المنهج الوصفي التحليلي، من خلال رصد سلبي لسجلات شفافية الشهادات الرقمية شمل نحو 4.7 مليار اسم نطاق في الفترة من 20 سبتمبر إلى 9 نوفمبر 2026، ومراجعة تحليلية للنطاقات المشتبه بها.

أظهرت النتائج بنية تقنية منظمة لتزوير الوثائق تقوم على بوابات تحقق مزيفة ترتبط بها رموز الاستجابة السريعة (QR) المطبوعة على الوثائق المزورة، وصُنّف 17 موقعاً بوابات تزوير تنتحل جهات منها منصة بلدي ومنصة قوى والمركز السعودي للأعمال. وكشفت سجلات موقع آخر ينتحل منصة بلدي عن 247 شهادة صحية مزورة صدرت خلال 37 يوماً، **91%** منها لعاملين في منشآت الغذاء، ونُسبت إلى 15 أمانة. وتركّز التصيّد المؤكد في انتحال الخدمات الحكومية، إذ انتحلها 121 من 150 موقعاً مؤكداً (**81%**)، وثبت الانتحال في 31 من 37 اسماً محسوماً يحمل اسم منصة بلدي، في حين لم يثبت انتحال علامة تطابق كلمة شائعة مثل saudia رغم كثرة ظهورها. وكان **26%** من النطاقات المؤكدة المعروف تاريخ تسجيلها مسجلاً منذ أكثر من عام عند رصده، ولم يُظهر سوى **11%** من المواقع المؤكدة في عينة التحليل نموذج إدخال للفاحص الآلي، بما يرجّح إخفاء المحتوى عنه.

وتناقش الدراسة ما توثقه التقارير الدولية من خفض أدوات الذكاء الاصطناعي التوليدي لكلفة تزوير الوثائق ونسخ المواقع، وتوصي بنقل التحقق من الوثائق من الرابط المضمَّن في الرمز إلى تطبيقات الجهات المصدرة مع توقيع رقمي لبيانات الرمز، أو إلى تحقق بعد الدخول عبر النفاذ الوطني الموحد.

الكلمات المفتاحية

التصيّد الاحتيالي · انتحال الهوية المؤسسية · تزوير الوثائق · رموز الاستجابة السريعة · بوابات التحقق المزيفة · الذكاء الاصطناعي التوليدي · سجلات شفافية الشهادات · المملكة العربية السعودية

Abstract

This study describes how Saudi government entities are impersonated through web domains and how such impersonation is used for phishing and for forging official documents. Using a descriptive-analytical design, it draws on passive monitoring of Certificate Transparency logs covering about 4.7 billion domain names between 20 September and 9 November 2026, followed by analyst review of suspicious domains. Results show an organised infrastructure of fake verification portals linked to the QR codes on forged documents; 17 sites impersonating entities such as Balady, Qiwa and the Saudi Business Center were classified as forgery portals. The records of another site impersonating Balady showed 247 forged health certificates issued in 37 days, 91% of them for food-establishment workers, attributed to 15 municipalities (amanas). Sites impersonating government services accounted for 81% (121) of the 150 confirmed sites, and 26% (24 of 91) of confirmed domains with a known registration date were over a year old when detected. The study discusses how generative AI lowers the cost of document forgery and site cloning, and recommends moving verification away from links encoded in QR codes to issuers' official apps that check digitally signed QR data, or to verification after signing in through Nafath, Saudi Arabia's national single sign-on.

أبرز النتائج
Key findings at a glance

4.7 مليار
اسم نطاق رُصد في سجلات شفافية الشهادات خلال 51 يوماً

15,422
اسم مضيف مشتبه به سُجّل في سجل الرصد، دخل 7,151 منها قائمة التحقق

150
موقعاً مؤكداً: 133 موقع تصيّد و17 بوابة تزوير، على 97 نطاقاً مسجلاً

58
موقعاً في 26 بلاغاً رسمياً إلى الهيئة الوطنية للأمن السيبراني

81%
من المواقع المؤكدة تنتحل خدمات حكومية (121 من 150)

84%
من الأسماء المحسومة التي تحمل اسم بلدي ثبت انتحالها (31 من 37)

26%
من النطاقات المؤكدة المعروف تاريخ تسجيلها عمرها أكثر من عام (24 من 91)

11%
فقط من المواقع المؤكدة في عينة التحليل أظهرت نموذج إدخال للفاحص الآلي (7 من 61)

ثلاث دراسات حالة من بيانات الرصد

247
شهادة صحية مزوّرة في سجلات موقع واحد ينتحل بلدي، 91% منها لمنشآت الغذاء، منسوبة إلى 15 أمانة

9
نطاقات تحمل اسم قوى أو أجير رُصدت خلال 21 يوماً، منها بوابتا تزوير لتصاريح العمل

2:21
ساعتان و21 دقيقة بين رصد نطاق جديد ينتحل قوى وإبلاغ الهيئة عنه

نافذة الرصد: 20 سبتمبر – 9 نوفمبر 2026



الخلاصة

لم يعد انتحال الجهات الحكومية مقتصراً على سرقة بيانات الدخول، بل امتد إلى انتحال آلية التحقق من الوثائق ذاتها: وثيقة مزورة تحمل رمزاً يفتح صفحة تحقق مزيفة تُظهر أن الوثيقة "سارية". ولأن هذه الصفحات لا تطلب كلمة مرور، فإنها تفلت من أغلب أدوات مكافحة التصيّد. والحل الجذري ليس ملاحقة المواقع وحدها، بل تغيير طريقة التحقق نفسها.

01 المقدمة وإطار الدراسة

Introduction and study framework

شهدت المملكة العربية السعودية تحولاً واسعاً نحو الخدمات الحكومية الرقمية ضمن مستهدفات رؤية المملكة 2030، فأصبحت وثائق مثل الشهادة الصحية للعاملين، وتصاريح العمل، وشهادات الاشتراك في التأمينات الاجتماعية، وشهادات السجل التجاري تُصدر إلكترونياً، ويُتحقق منها عبر رموز الاستجابة السريعة المطبوعة عليها.

وقد أتاح هذا التحول فرصاً جديدة للمحتالين. فلم يعد التصيّد مقتصراً على سرقة بيانات الدخول، بل امتد إلى انتحال بوابات التحقق نفسها، بحيث تظهر الوثيقة المزورة سارية عند مسح رمزها. وتكمن خطورة هذا النمط في أثره المباشر على السلامة العامة وسوق العمل: فالشهادة الصحية المزورة تسمح بعمل أشخاص غير مفحوصين في منشآت الغذاء، وتصريح العمل المزور يُستغل في تشغيل العمالة غير النظامية، وشهادة الاشتراك المزورة تُمرَّر في التوظيف والتعاقدات وطلبات التمويل.

ويزيد من حدّة هذا النمط أن أدوات الذكاء الاصطناعي التوليدي باتت تخفض كلفة إنتاج وثائق ومواقع بالغة الإتقان يصعب على المستخدم غير المتخصص تمييزها، كما يوضح الفصل الخامس.

مشكلة الدراسة وأسئلتها

تتمثل مشكلة الدراسة في أن أدوات مكافحة التصيّد السائدة صُممت لاكتشاف نماذج سرقة بيانات الدخول والبطاقات المصرفية، أما بوابات التحقق المزيفة فلا تطلب مثل هذه البيانات، فتمر دون اكتشاف، مع ندرة الدراسات الميدانية التي ترصد هذا النمط في المملكة. وتسعى الدراسة إلى الإجابة عن الأسئلة التالية:

1. ما أنماط انتحال الجهات الحكومية السعودية المستخدمة في تزوير الوثائق الرسمية؟
2. ما حجم نشاط التزوير الذي تكشفه حالة موثقة لموقع واحد؟
3. ما الجهات الأكثر استهدافاً بالتصيّد المؤكد؟
4. ما الأساليب التقنية التي يتبعها المهاجمون لإطالة بقاء مواقعهم؟
5. كيف يغيّر الذكاء الاصطناعي التوليدي كلفة التزوير ونسخ المواقع؟
6. ما الآليات المقترحة للحد من تزوير الوثائق عبر رموز الاستجابة السريعة؟

أهداف الدراسة

- توصيف البنية التقنية لبوابات التحقق المزيفة والجهات التي تنتحلها.
- قياس حجم نشاط التزوير في حالة موثقة، وتوزيعه على القطاعات والمناطق.
- تحديد الجهات الحكومية الأكثر عرضة للانتحال، والأساليب التقنية المستخدمة.
- تقديم توصيات عملية للجهات المصدرة والجهات الرقابية.

أهمية الدراسة

تستمد الدراسة أهميتها من اعتمادها على بيانات رصد ميدانية حديثة ومقيسة، ومن تناولها نمطاً لم يُدرَس بشكل كافٍ في السياق السعودي. وتفيد نتائجها الجهات المصدرة للوثائق، والمفتشين، وأصحاب العمل، ومنصات التوصيل والتوظيف، والجهات المعنية بالأمن السيبراني.

حدود الدراسة

الحدود الزمانية: من 20 سبتمبر إلى 9 نوفمبر 2026. **الحدود الموضوعية:** النطاقات الإلكترونية التي تحاكي جهات سعودية وظهرت في سجلات شفافية الشهادات الرقمية، ولا تشمل الدراسة الرسائل النصية أو حسابات وسائل التواصل الاجتماعي.

مصطلحات الدراسة

جدول 1: مصطلحات الدراسة وتعريفاتها الإجرائية

المصطلح	التعريف الإجرائي
التصيّد الاحتيالي	انتحال جهة موثوقة عبر موقع إلكتروني أو رسالة بهدف الحصول على بيانات أو أموال أو تضليل المستخدم
بوابة التحقق المزيفة	موقع يحاكي صفحة التحقق الرسمية لجهة مصدرة، ويُظهر الوثيقة المزورة على أنها سارية، أو يُصدر وثائق مزورة
رمز الاستجابة السريعة (QR)	رمز مطبوع على الوثيقة يفتح عند مسحه رابطاً للتحقق منها
سجلات شفافية الشهادات	سجلات عامة تُقيَّد فيها شهادات التشفير (TLS) فور إصدارها للمواقع
اسم المضيف	الاسم الكامل الظاهر في الشهادة، مثل `ajeer.qiwa-sa[.]info`
النطاق المسجّل	الاسم الذي يُشترى من المسجّل، مثل `qiwa-sa[.]info`، وقد تتفرع منه أسماء مضيفين متعددة
الموقع المؤكد	اسم مضيف صنّفته المنصة تصيّداً أو بوابة تزوير بعد مراجعة تحليلية، أو آلياً بربطه بحملة مؤكدة
الاسم المحسوم	اسم انتهت مراجعته بقرار: مؤكَّد أو مستبعَد
الذكاء الاصطناعي التوليدي	أدوات تُنتج نصوصاً وصوراً وشيفرات ومواقع كاملة من وصف نصي مختصر

02 الدراسات السابقة

Prior work

ركّزت الدراسات والتقارير السابقة عن المملكة على التصيّد الهادف إلى سرقة بيانات الدخول والأموال، ولم تتناول بوابات التحقق المزيفة من الوثائق.

دراسات وتقارير عن السياق السعودي والخليجي

1. **تقرير Group-IB (2022):** رصد أكثر من 1,000 نطاق احتيالي تنتحل شركة سعودية رائدة في الاستقدام خلال 16 شهراً، استدرجت الضحايا عبر إعلانات وسائل التواصل والرسائل النصية، ثم جمعت بياناتهم ورسوماً مالية وبيانات دخول مصرفية وحكومية.
2. **تقرير CloudSEK (2022):** وصف حملة تنتحل منصة أبشر عبر روابط في رسائل نصية، تجمع بيانات الدخول ورمز التحقق لمرة واحدة، ثم بيانات الدخول المصرفية.
3. **دراسة اليحيى وويز (2021):** درست استجابة الأفراد في المملكة للتصيّد وفق نظرية السلوك المخطط، ووجدت أن الاتجاه الشخصي يتنبأ بالاستجابة للرسائل التي تنتحل صفة السلطة.
4. **تقرير Group-IB (2026):** رصد أكثر من 400 مورد تصيّد في دول الخليج، تُستدرج إليها الضحايا عبر إعلانات بحث مدفوعة وتنسخ مواقع خدمات حكومية وتأمينية، واستُخدمت لصرف بطاقات مسروقة عبر بوابات دفع حكومية بمبالغ احتيالية مؤكدة تقارب 2.01 مليون دولار.

أدبيات التزوير ونسخ المواقع بالذكاء الاصطناعي

تتفق تقارير جهات إنفاذ القانون ومزوّدي الأمن على أن الذكاء الاصطناعي التوليدي خفّض كلفة إنتاج الوثائق المزورة والمواقع المنسوخة. فقد حذّر مكتب التحقيقات الفيدرالي الأمريكي (2024) من توظيفه في إنتاج وثائق هوية وبطاقات اعتماد حكومية ومصرفية مزورة، ورصدت شركة Okta (2025) استخدام أداة توليد مواقع لبناء صفحات تصيّد عاملة من أوامر نصية بسيطة. ويعرض الفصل الخامس هذه الأدبيات بالتفصيل.

الفجوة البحثية

تضيف هذه الدراسة بُعداً لم تتناوله الدراسات السابقة: استغلال انتحال الجهات الحكومية في تزوير الوثائق والتحقق منها لا في سرقة البيانات فقط، مع قياس حجم النشاط في حالة موثقة، وربطه بما توثقه الأدبيات الدولية عن أثر الذكاء الاصطناعي.

03 منهجية الدراسة
Methodology

اعتمدت الدراسة المنهج الوصفي التحليلي، بالاستناد إلى بيانات منصة سياج، وهي منصة سعودية مستقلة ترصد انتحال الجهات السعودية آلياً عبر سجلات شفافية الشهادات. وجُمعت البيانات على خمس مراحل:

01 الرصد السلبي
قراءة مستمرة لسجلات شفافية الشهادات العامة
2.67 مليار شهادة

02 مطابقة الأسماء
مقارنة كل اسم بأسماء الجهات السعودية بالعربية والإنجليزية
4.88 مليون اسم مشابه

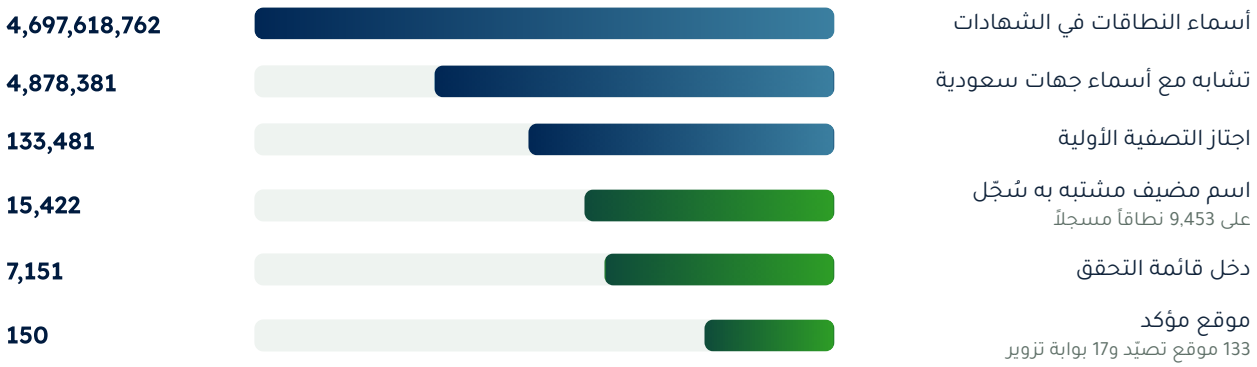
03 التسجيل والفحص
تسجيل الأسماء المشتبه بها وفحص المحتوى العام دون أي تفاعل آخر
15,422 مشتبهاً

04 المراجعة والتصنيف
حسم الأسماء المحالة للمراجعة، أو تصنيفها آلياً بربطها بحملة مؤكدة
150 مؤكداً

05 الإبلاغ
إحالة المؤشرات المؤكدة إلى الهيئة الوطنية للأمن السيبراني
26 بلاغاً

شكل 1: قمع الرصد من سجلات الشهادات إلى المواقع المؤكدة

مقياس لوغاريتمي



المصدر: عدّادات منصة سياج وقاعدة بياناتها، 20 سبتمبر - 9 نوفمبر 2026. عدّادات الأيام السبعة الأولى (20–26 سبتمبر) تقديرية، ثم سُجّلت آلياً.

عينة الدراسة

جدول 2: عينة الدراسة اسم المضيف هو وحدة العد ما لم يُذكر غير ذلك

البيان	العدد
أسماء المضيفين المشتبه بها المسجّلة	15,422 اسماً على 9,453 نطاقاً مسجلاً، دخل 7,151 منها قائمة التحقق
الأسماء المحسومة بالمراجعة (20 سبتمبر – 4 نوفمبر)	764 اسماً، منها 85 مؤكدة و679 مستبعدة
عينة التحليل (مجمّدة في 4 نوفمبر)	607 أسماء: 61 مؤكدة و546 مستبعدة، على 266 نطاقاً مسجلاً
المواقع المؤكدة حتى 9 نوفمبر	150 اسماً: 133 موقع تصيّد و17 بوابة تزوير، على 97 نطاقاً مسجلاً
المواقع المبلّغ عنها للهيئة الوطنية للأمن السيبراني	58 موقعاً في 26 بلاغاً (30 سبتمبر - 9 نوفمبر)
دراسة حالة: سجلات موقع لتزوير الشهادات الصحية	247 سجلاً، حُلّلت بصيغة مجمّعة فقط

وأُفردت عينة مستقلة للتحقق النهائي من النتائج، ولم تُستخدم في بناء أدوات التحليل ولا في حساب نسب عينة التحليل. **المعالجة الإحصائية:** استُخدمت التكرارات والنسب المئوية، مع فترات ثقة دقيقة بمستوى **95%** وفق طريقة كلوبر-بيرسون، تُعرض بين معقوفين بعد كل نسبة.

إجراءات الإبلاغ

تُحال المواقع المؤكدة إلى الهيئة الوطنية للأمن السيبراني في بلاغات رسمية بنية موحدة، كما في البلاغ الأول عن شهادات التأمينات:

الجهة والنطاقات	الجهة المنتحَلة، وأسماء النطاقات بصيغة معطّلة
آلية الاحتيال	كيف تُصدر الوثيقة المزورة، وإلى أين يقود رمزها، وما الذي تعرضه الصفحة المزيفة
الأثر	المعاملات التي تمر بالوثيقة المزورة، والخطر على الثقة بآلية التحقق
المطلوب	الحجب، والتنسيق مع المسجّلين ومزوّدي الاستضافة، وتنبيه الجهة المنتحَلة
المرفقات	ملفات مؤشرات قابلة للمعالجة الآلية بصيغتي CSV وSTIX، ولقطات للصفحات عند توفرها

الاعتبارات الأخلاقية

- اقتصر الرصد الآلي في منصة سياج على المحتوى العام للصفحات، دون إدخال بيانات أو أي تفاعل آخر مع المواقع.
- لا تتضمن الدراسة أي بيانات شخصية. وما ورد عن موقع تزوير الشهادات الصحية مصدره سجلات الموقع نفسه (247 سجلاً حتى مساء 9 نوفمبر 2026)، وكان البلاغ رقم 24 المرفوع إلى الهيئة صباح اليوم نفسه قد أشار إلى 241 منها؛ وتُعرض في صورة أعداد مجمّعة فقط، دون أسماء أو أرقام هويات أو صور.
- أُحيلت المؤشرات المؤكدة إلى الهيئة الوطنية للأمن السيبراني قبل النشر، وتُعرض أسماء النطاقات بصيغة معطّلة [.].

04 النتائج
Results

أولاً: تزوير الوثائق وبوابات التحقق المزيفة

أظهرت النتائج بنية تقنية منظمة لتزوير الوثائق الرسمية؛ إذ صُنّف **17 اسم مضيف** على 15 نطاقاً مسجلاً "بوابات تزوير"، إضافة إلى **8 أسماء مضيفين** قيد المراجعة بوصفها بوابات تزوير محتملة، ومواقع أخرى مؤكدة تصيّداً تعرض محتوى الوثائق نفسها. وتعمل هذه المواقع بأحد أسلوبين: إصدار وثيقة مزورة عبر نموذج إلكتروني، أو عرض نتيجة "سارية" عند مسح رمز الاستجابة السريعة المطبوع على الوثيقة.

شكل 2: آلية التزوير عبر بوابة التحقق المزيفة

كما وصفتها البلاغات



المسار الحالي: الرمز رابط حرّ لا يحمل أي ضمان لسلامته، ويمكن لأي جهة إنشاء رمز يفتح صفحة تحاكي الصفحة الرسمية.

المسار المقترح: المسح من داخل تطبيق رسمي يسترجع السجل من النظام مباشرة، فلا قيمة لأي رمز مزيف مهما بلغت دقته.

المصدر: البلاغ رقم 1 المرفوع إلى الهيئة الوطنية للأمن السيبراني في 30 سبتمبر 2026 بشأن شهادات الاشتراك في التأمينات الاجتماعية، والبلاغ رقم 2 بشأن الشهادات الصحية.

جدول 3: الوثائق المستهدفة والمواقع المرصودة التصنيف كما في قاعدة البيانات

الجهة المنتحَلة	الوثيقة	المحتوى المرصود	نماذج النطاقات	التصنيف
منصة بلدي	الشهادة الصحية، بيانات الرخص	"إصدار شهادة صحية"، بطاقة شهادة صحية	appsbalady-govsa.pages[.]dev ccs.balady.gov.sa-sa[.]info balady.govsa[.]app	بوابة تزوير
منصة قوى / أجير	تصاريح العمل المؤقت	"التحقق من تصريح أجير" (في qiwa-sa[.]net)	ajeer-hrsd-qiwa-gov-sa[.]online ajeer-hrsd-qiwa.gov-sa[.]store	بوابة تزوير تصيّد
التأمينات الاجتماعية	شهادة الاشتراك	نتيجة تحقق تفيد بأن الاشتراك "فعّال" (البلاغ 1)	gosi.gov.sa-sa[.]info gosi-gov-sa[.]online	تصيّد
المركز السعودي للأعمال	السجل التجاري	محاكاة صفحة التحقق بالرمز	qrsaudibusiness-govsa[.]org	بوابة تزوير

الجهة المنتحَلة	الوثيقة	المحتوى المرصود	نماذج النطاقات	التصنيف
جهات صحية	الشهادات الطبية	"MED Certificate"	`alriyadh-gov-sa[.]com` ونطاقان مرتبطان واسم فرعي	بوابة تزوير
المركز الوطني للرقابة على الالتزام البيئي	التصاريح البيئية	"إصدار التصريح البيئي للمصانع والورش"	`dhamen-sa.pages[.]dev`	بوابة تزوير
وزارة الداخلية	معاملات الأحوال المدنية	"استخراج موافقة زواج ومعاملات التجنيس"	`moigov-sa[.]com`	تصيّد
وزارة التعليم	الشهادات الجامعية	"استعلام رسوم الشهادة الجامعية"	`moegovsa[.]org`	تصيّد

وتشترك بوابات التزوير في ثلاثة ملامح: تسمية تحاكي النطاق الحكومي `gov.sa`، واستضافة سريعة الإنشاء، وغياب أي طلب لكلمة مرور. ولأن هذه المواقع لا تطلب كلمة مرور، فإن معايير الفحص التي تبحث عن نماذج كلمات المرور تصنّفها غالباً "سليمة". فعند تطبيق قاعدة تجريبية لرصد بوابات التحقق المزيفة على الصفحات المحفوظة، رصدت القاعدة 19 موقعاً، كانت 14 منها قد صُنّفت سابقاً "سليمة"، مع العلم أن بين هذه المواقع نتائجَ إيجابية زائفة معروفة.

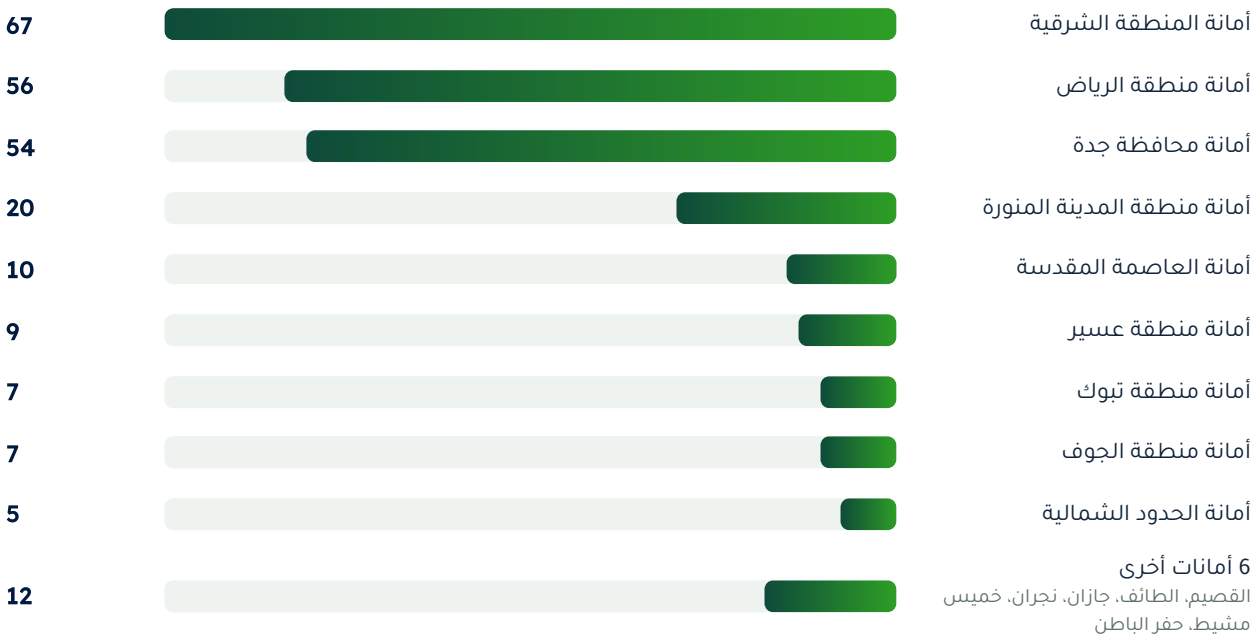
ثانياً – دراسة الحالة الأولى: موقع لتزوير الشهادات الصحية باسم بلدي

رصدت منصة سياج موقعاً ينتحل الهوية البصرية والاسم الرسمي لمنصة بلدي (`services-balady-gov-sa[.]fun`)، مصنّفاً في قاعدة البيانات موقعَ تصيّد مؤكداً)، ويُصدر "شهادات صحية موحّدة" مزوّرة مزوّدة برموز استجابة سريعة تحاكي صفحات التحقق الحكومية. وأُبلغت به الهيئة الوطنية للأمن السيبراني صباح 9 نوفمبر 2026 (البلاغ رقم 24، وأشار حينها إلى 241 شهادة). وتكشف سجلات الموقع حتى مساء اليوم نفسه، المعروضة هنا بصيغة مجمّعة فقط، حجم نشاط موقع واحد، إذ تبلغ حصة منشآت الغذاء [86–94%] **91%** من شهاداته:

247	37	15	91%
شهادة صحية مزوّرة في سجلات الموقع حتى مساء 9 نوفمبر 2026	يوماً (4 أكتوبر - 9 نوفمبر)، صدرت خلالها شهادات في 35 يوماً، بمتوسط 6.7 يومياً	أمانة نُسبت إليها الشهادات، لكل منها شعارها الخاص	لعاملين في منشآت الغذاء (224 من 247)

شكل 3: توزيع الشهادات على الأمانات

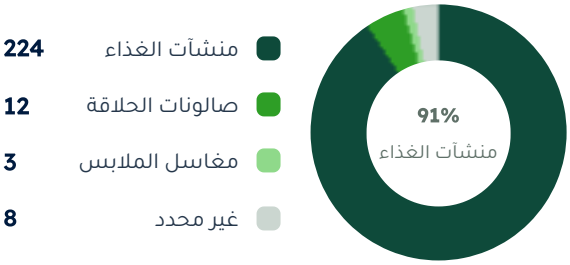
عدد الشهادات من 247



المصدر: سجلات الموقع حتى مساء 9 نوفمبر 2026، أعداد مجمّعة.

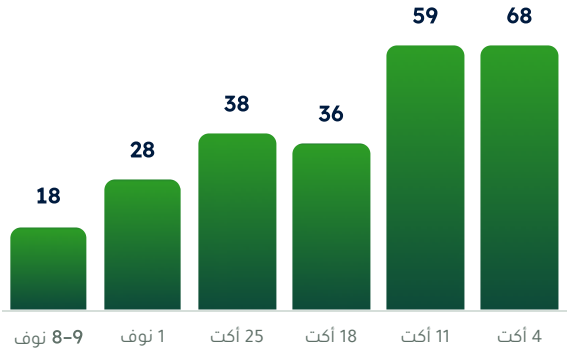
شكل 4: البرنامج التثقيفي المسجّل

من 247



شكل 5: الشهادات المصدرة أسبوعياً

الأسبوع يبدأ الأحد



الأسبوع الأخير يومان فقط (8 و9 نوفمبر).

وتوزعت الشهادات على 65 مسمى وظيفياً كما وردت في السجلات، أكثرها: عامل تحميل وتنزيل (53)، وعامل (27)، وعامل مطبخ (19)، وبائع (10)، وصانع حلويات (10)، وسائق خاص (7)، وحلاق (6) وحلاق رجالي (6). وبلغت ذروة الإصدار 26 شهادة في يوم واحد، وتضمنت جميع السجلات صورة شخصية لحامل الشهادة، وهو ما يمنح الوثيقة المزورة مظهر الوثيقة الأصلية.

ملامح الاحتراف في هذه الحالة

اختار الموقع شعار الأمانة المطابقة لكل شهادة من بين 15 شعاراً، وقدّم أكثر من نوع من الوثائق، منها الشهادة الصحية الموحدة وشهادة لعاملي التوصيل. ووجّه رموز الاستجابة السريعة عبر صفحة وسيطة على GitHub Pages تعيد توجيه الماسح إلى صفحة التحقق المزيفة، وهو ما يتيح للمزوّر تغيير الوجهة إذا حُجب نطاقه دون الحاجة إلى إعادة طباعة الوثائق.

الأثر على الصحة العامة: تعني هذه الأرقام وجود 224 شهادة منسوبة إلى عاملين في منشآت الغذاء، يُرجَّح أنها صدرت دون فحص طبي أو برنامج تثقيفي، ويمكن أن تجتاز الرقابة عند مسح رمزها. وهذا موقع واحد فقط من المواقع المرصودة.

ثالثاً – دراسة الحالة الثانية: شهادات الاشتراك في التأمينات الاجتماعية

رُصد النمط ذاته في شهادات الاشتراك في التأمينات الاجتماعية. فبحسب البلاغ الأول المرفوع إلى الهيئة في 30 سبتمبر 2026، يُصدر المحتالون شهادة اشتراك مزورة بتصميم يحاكي الشهادة الرسمية وتتضمن رمز استجابة سريعة، وتُقدَّم إلى الجهات أو المدققين بصفتها إثباتاً لاشتراك المنشأة أو الموظف. وعند مسح الرمز يُوجَّه المدقق إلى نطاق منتحِل، مثل `gosi.gov.sa-sa[.]info`، بدلاً من `gosi.gov.sa`، فتعرض الصفحة أن الاشتراك "فعّال".

8/8	12	4
نطاقات محسومة تحمل اسم التأمينات ثبت انتحالها في عينة التحليل	موقعاً مؤكداً ينتحل التأمينات الاجتماعية على 11 نطاقاً مسجلاً	بلاغات عن تزوير شهادات الاشتراك (1 و7 و11 و16)، أحدها عن موقع "سُجّل قبل ساعة"

ويتمثل أثر هذا النمط، بحسب البلاغ، في تمرير اشتراكات وهمية أو منتهية في معاملات تعتمد على إثبات التأمينات، مثل التوظيف والتعاقدات وطلبات التمويل، وفي تقويض الثقة في آلية التحقق عبر رمز QR للمستندات الحكومية عموماً.

رابعاً – دراسة الحالة الثالثة: حملة أجير وقوى، والإبلاغ خلال ساعتين

تكشف بيانات الرصد عائلة من النطاقات تنتحل منصة قوى وخدمة أجير لتصاريح العمل المؤقت: **9 نطاقات مسجلة رُصدت أول مرة خلال 21 يوماً** (20 أكتوبر - 9 نوفمبر)، بأسماء متقاربة على امتدادات مختلفة؛ منها 6 مؤكدة، بينها بوابتا تزوير، و3 قيد المراجعة.

جدول 4: أسماء المضيفين المرصودة باسم قوى وأجير اسم واحد لكل نطاق مسجّل

اسم المضيف المرصود	أول رصد	الحالة
`qiwalogin[.]com`	20 أكتوبر	تصيّد مؤكد "Check Work Permit, Contract"
`ajeer-hrsd-qiwa.gov-sa[.]store`	21 أكتوبر	بوابة تزوير
`ajeer-hrsd-qiwa-gov-sa[.]online`	21 أكتوبر	بوابة تزوير ومعه اسم فرعي للتحقق
`ajeer.qiwa-sa[.]info`	26 أكتوبر	قيد المراجعة

اسم المضيف المرصود	أول رصد	الحالة
ajeer-hrsd.qiwa-gov-sa[.]online	28 أكتوبر	تصيّد مؤكد
ajeer.qiwa-sa[.]co	5 نوفمبر	قيد المراجعة
qiwa-sa[.]net	6 نوفمبر	تصيّد مؤكد — "أجير	التحقق من تصريح أجير"
ajeer.qiwa-sa[.]online	9 نوفمبر	قيد المراجعة
ajeerqiwa[.]net	9 نوفمبر	تصيّد مؤكد — أُبلغ عنه بوصفه موقعاً لتزوير شهادات قوى

رصد ajeerqiwa[.]net لحظة إطلاقه

سُجّل النطاق في 9 نوفمبر 2026، وصدرت له شهادة تشفير في اليوم نفسه، فرصدته منصة سياج فور ظهور الشهادة في سجلات الشفافية. وبعد المراجعة أُحيل إلى الهيئة الوطنية للأمن السيبراني بوصفه موقعاً "لتزوير شهادات قوى"، بعد ساعتين و21 دقيقة من رصده.

9 نوفمبر 2026
تسجيل النطاق
لدى المسجّل Spaceship

19:27:43 بتوقيت الرياض
ظهور الشهادة ورصد النطاق آلياً
درجة الخطورة 81.3 من 100، والجهة المنسوبة: منصة قوى

21:49:10
تأكيد المحلل
عنوان الصفحة: "Employee Admin"

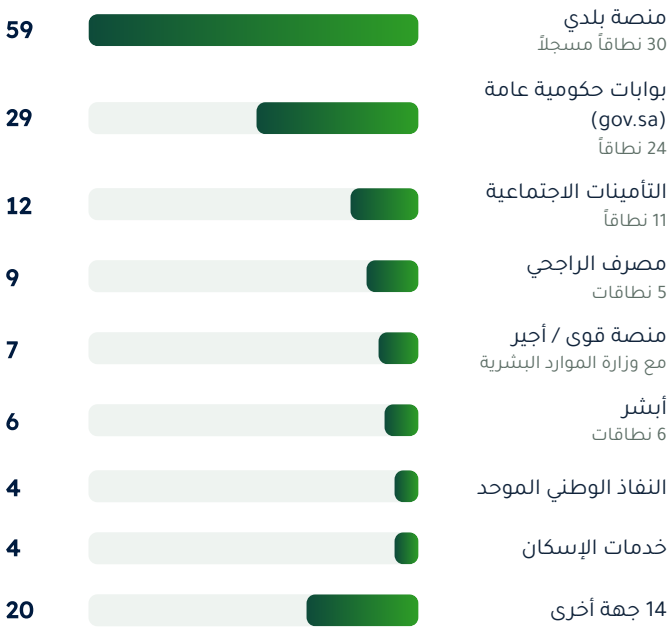
21:49
البلاغ رقم 26 إلى الهيئة
بعد ساعتين و21 دقيقة من الرصد

خامساً: الجهات المستهدفة

تركّز التصيّد المؤكد في الخدمات الحكومية، إذ ينتحلها 121 من 150 موقعاً مؤكداً ([73–87%] **81%**)، وتصدّرت منصة بلدي القائمة بـ59 موقعاً على 30 نطاقاً مسجلاً.

شكل 6: المواقع المؤكدة حسب الجهة

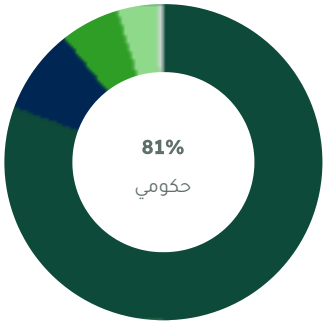
من 150



المصدر: قاعدة بيانات منصة سياج، 9 نوفمبر 2026.

شكل 7: القطاع المنتحَل

من 150



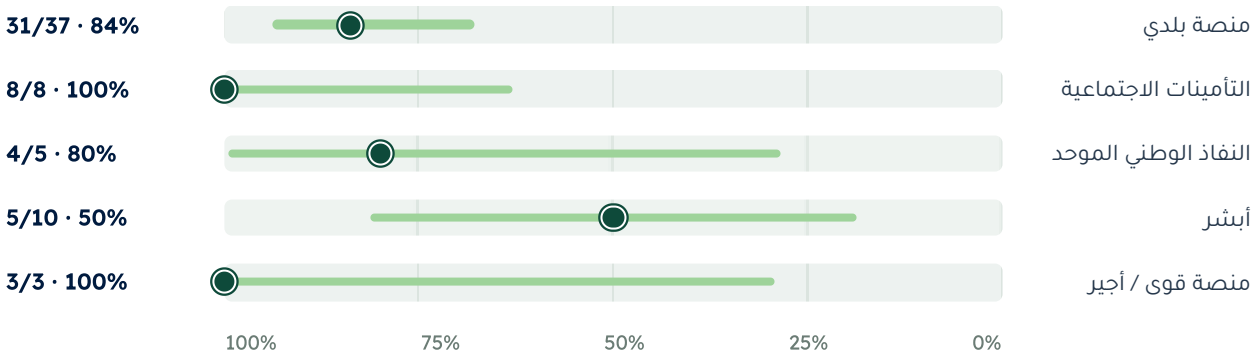
121	حكومي
13	مصرفي ومالي
9	خدمات
6	شركات
1	أخرى

التصنيف القطاعي من حقل الفئة في سجل الرصد، ويختلف عن تصنيف الجهة في الشكل 6 الذي تنتمي فيه 131 موقعاً إلى جهات حكومية.

ولا يعني تكرار اسم الجهة في النطاقات أنها مستهدفة. فقد نُسب 731 اسم مضيف مرصوداً إلى الخطوط السعودية، منها 601 تحمل كلمة "saudia"، دون أي انتحال مؤكد للناقل الجوي؛ إذ تستخدمها منشآت مشروعة بمعنى "السعودية"، والنطاق المؤكد الوحيد الذي حمل هذه الكلمة (`saudiavisagov[.]org`) كان ينتحل خدمة التأشيرات الحكومية. ويقابل ذلك ارتفاع نسبة الثبوت في أسماء الخدمات الحكومية التي يتعامل معها المستفيد بشكل متكرر:

شكل 8: نسبة ثبوت الانتحال في الأسماء المحسومة حسب الجهة

عينة التحليل، فترة ثقة 95%



المصدر: قرارات المراجعة التحليلية، 20 سبتمبر - 4 نوفمبر 2026، للأسماء المحسومة التي تحمل اسم الجهة. تتسع فترة الثقة كلما قل عدد الحالات.

سادساً: الأساليب التقنية للمهاجمين

تبيّن أن المهاجمين يجمعون بين محاكاة النطاق الحكومي، وإخفاء المحتوى، والاستضافة سريعة الإنشاء، والأسماء المتقاربة على امتدادات متعددة، وأساليب أخرى وثقتها البلاغات:

جدول 5: الأساليب التقنية المرصودة المصدر: قاعدة البيانات والبلاغات

الأسلوب	النتيجة المقيسة أو الموثقة	مثال
محاكاة بنية النطاق الحكومي داخل نطاق أجنبي	نمط متكرر في بوابات التزوير المؤكدة	`ccs.balady.gov.sa-sa[.]info`
استخدام الاسم السابق للوزارة	اسم momra داخل نطاق يحاكي gov.sa (البلاغ 2)	`ebalady.momra.govsa[.]app`
نطاقات مسجّلة منذ أكثر من عام	24 من 91 نطاقاً مؤكداً معروف تاريخ تسجيله عند رصده (**26% [18–37%]**)، وفي عينة التحليل 14 من 61 موقعاً (**23% [13–36%]**)	`appbaladygovsa[.]org` مسجّل منذ أكتوبر 2024
إخفاء المحتوى عن الفحص الآلي	لم يظهر نموذج إدخال إلا في 7 من 61 موقعاً مؤكداً (**11% [5–22%]**)، وإعادة توجيه لإخفاء المحتوى (البلاغ 2)	`appbalady[.]info` نشط منذ ديسمبر 2024
استضافة سريعة الإنشاء	3 من 17 بوابة تزوير على Cloudflare Pages	`servicesbaladygovsa.pages[.]dev`
وسيط للرموز وتخزين سحابي للصور	صفحة على GitHub Pages تعيد توجيه الرمز، وصور الشهادات على خدمة Cloudinary (البلاغ 24)	تغيير الوجهة دون إعادة طباعة الوثيقة
أسماء متقاربة على امتدادات متعددة	رُصد الاسم `balady-gov-sa` أول مرة على 8 امتدادات و4 أسماء فرعية مجانية بين 29 سبتمبر و29 أكتوبر، وبعضها مسجّل قبل ذلك	`balady-gov-sa[.]cc` مسجّل منذ أغسطس 2024
دمج علامتين وطلب الدخول عبر نفاذ	نطاق ينتحل مصرفاً والمركز السعودي للأعمال ويطلب الدخول عبر النفاذ الوطني الموحد (البلاغ 13)	`account.alrajhi[.]world`
خدمات أسماء فرعية تحاكي .sa	نطاقان يبيعان أسماء فرعية قريبة من `.sa` (البلاغ 22)	`gov.sa[.]cyou`
تهيئة النطاق لحملات بريد جماعي	سجل SPF لخدمة إرسال جماعي، ونطاق فرعي لتتبع النقرات، دون سجل DMARC (البلاغ 3)	`qiddiya[.]top`

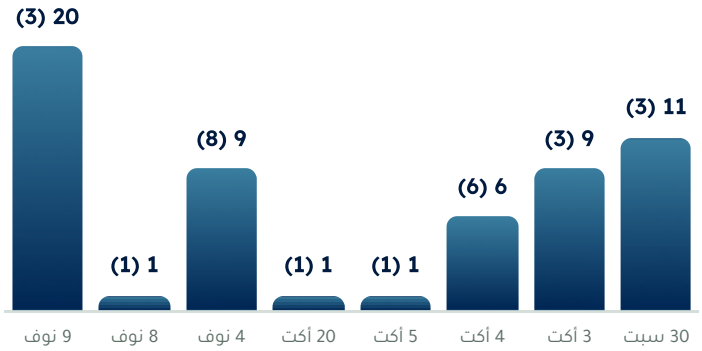
يُضعف استخدام النطاقات المسجلة منذ أكثر من عام الافتراضَ الشائع بأن النطاق الحديث هو وحده مؤشر الخطر. كما يجعل إخفاءُ المحتوى الفحصَ الآلي للصفحات غيرَ كافٍ منفرداً، ويستدعي الجمع بينه وبين تحليل أسماء النطاقات وبلاغات المستفيدين. أما توجيه الرموز عبر وسيط فيعني أن حجب النطاق وحده لا يُبطل الوثائق المطبوعة.

سابعاً: الإبلاغ والاستجابة

أُبلغت الهيئة الوطنية للأمن السيبراني عن **58 موقعاً في 26 بلاغاً** بين 30 سبتمبر و9 نوفمبر 2026، أظهر 16 موقعاً منها على الأقل محتوى صريحاً لإصدار الوثائق أو التحقق منها، وفق عناوين صفحاتها أو تصنيفها بوابات تزوير. وكان بلاغان منها (8 و10) استباقيين عن نطاقات لم يُفعَّل محتواها بعد، وتناولت بلاغات أخرى (5 و11 و12 و13 و26) نطاقات سُجّلت قبل ساعات أو أيام وكانت نشطة.

شكل 9: المواقع المبلّغ عنها حسب اليوم

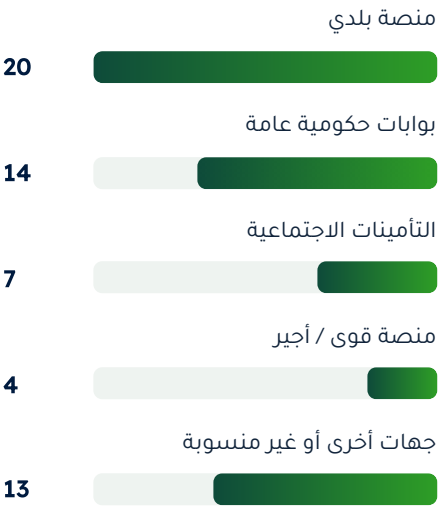
المواقع (البلاغات)



المصدر: سجل البلاغات المرسلة من منصة سياج إلى الهيئة الوطنية للأمن السيبراني، 26 بلاغاً.

شكل 10: المواقع المبلّغ عنها حسب الجهة

من 58



المصدر: سجل البلاغات.

وقد تشير عودة الأسماء نفسها بعد البلاغات إلى مجموعة منظمة تستبدل نطاقاتها بأخرى جديدة، مع أن بعض نطاقاتها قديم: فقد سُجّل `appbaladygovsa[.]org` في أكتوبر 2024، وذكر البلاغ رقم 2 أن `appbalady[.]info` نشط منذ ديسمبر 2024. وفي بلاغ واحد بتاريخ 9 نوفمبر (رقم 25) أُبلغ عن 19 نطاقاً رُصد أغلبها منذ مطلع أكتوبر، وترجّح القرائن أن أغلبها يعود إلى مجموعة واحدة، لتطابق أنماط التسمية وعناوين الصفحات ("إصدار شهادة صحية"، "Certificate Generator"، "التحقق من تصريح أجير"، "MED Certificate") واستخدام استضافات سريعة الإنشاء مثل Cloudflare Pages. وهذا يعني أن حجب النطاقات بمفرده لا ينهي النشاط، بل يلزم معه معالجة آلية التحقق التي يعتمد عليها التزوير.

05 الذكاء الاصطناعي وتحوّل التزوير

Generative AI and the shift in forgery

كان إتقان وثيقة رسمية أو نسخ موقع حكومي يتطلب مهارة في التصميم والبرمجة. أما اليوم فتوثق تقارير جهات إنفاذ القانون ومزوّدي الأمن أن أدوات الذكاء الاصطناعي التوليدي خفّضت هذه الكلفة إلى أوامر نصية قليلة، وأن إتقان الصياغة والتصميم لم يعد مؤشراً كافياً على المشروعية.

أولاً: وثائق مزورة شبه مطابقة

244%
ارتفاع تزوير الوثائق رقمياً على أساس سنوي، ليشكّل 57% من احتيال الوثائق (Entrust, 2024)

15 دولاراً
سعر صورة بطاقة هوية مزيفة لدى خدمة تزعم إنتاج 20,000 وثيقة يومياً (404 Media, 2024)

311%
ارتفاع احتيال وثائق الهوية الاصطناعية في أمريكا الشمالية، الربع الأول 2025 مقارنة بسابقه (Sumsub, 2025)

- حذّر مكتب التحقيقات الفيدرالي الأمريكي في 3 ديسمبر 2024 من أن المجرمين يستخدمون الذكاء الاصطناعي التوليدي لإنتاج وثائق هوية مزورة، كرخص القيادة وبطاقات الاعتماد المنسوبة إلى جهات إنفاذ القانون أو الجهات الحكومية أو المصرفية، لأغراض الاحتيال وانتحال الصفة.
- ورصدت شبكة مكافحة الجرائم المالية بوزارة الخزانة الأمريكية في نوفمبر 2024 ارتفاعاً في بلاغات النشاط المشبوه التي تصف استخدام وسائط التزييف العميق، ولا سيما وثائق الهوية المزورة، للالتفاف على التحقق من الهوية.
- واستخدم صحفيو موقع 404 Media بطاقة هوية مزيفة من خدمة تدّعي استخدام "الشبكات العصبية" لاجتياز التحقق من الهوية في منصة تداول العملات المشفرة OKX.
- وفي المقابل، تشير Sumsub (2026) إلى أن 2% من الوثائق المزيفة التي رصدتها خلال ستة أشهر من 2025 أُنتجت بأدوات توليدية، وهي نسبة صغيرة لكنها تنذر بوثائق تجتاز الفحص البصري والآلي.

ثانياً: مواقع منسوخة في دقائق

40%
نحو 40% من حالات إساءة استخدام خدمات الذكاء الاصطناعي في التصيّد كانت لمولّدات المواقع (Unit 42, 2025)

4,000
أكثر من 4,000 بلاغ شهرياً عن منصة واحدة لتوليد المواقع بحلول أكتوبر 2025، مقابل أقل من 250 في يناير (Netcraft, 2026)

1–2
أمرٌ أو أمران نصيّان يكفيان لبناء موقع تصيّد كامل الوظائف (Proofpoint, 2025)

- رصدت شركة Okta في يوليو 2025 مهاجمين يستخدمون أداة توليد مواقع لبناء صفحات تصيّد عاملة تنسخ صفحات الدخول لعلامات عدة من أوامر نصية بسيطة، وخلصت إلى أن المؤسسات لم تعد قادرة على الاعتماد على تدريب المستخدمين لاكتشاف التقليد غير المتقن.

- وأفادت Microsoft في أبريل 2025 بأن مواقع التجارة الإلكترونية الاحتيالية يمكن إنشاؤها في دقائق بأدوات لا تتطلب معرفة تقنية تُذكر، وأنها كثيراً ما تحاكي مواقع مشروعة بما يصعّب على المستهلك تمييزها.
- ورصدت Netcraft في 2024 ارتفاع عدد المواقع التي تحتوي على نصوص مولّدة آلياً إلى 3.95 ضعف ما كان عليه خلال خمسة أشهر، وخلصت إلى أن النص المكتوب بلغة احترافية لم يعد مؤشراً قوياً على مشروعية الموقع.
- غير أن Unit 42 لاحظت أن صفحات التصيّد المبنية بمولّدات المواقع ما زالت بدائية نسبياً حتى الآن، وهو ما يعني أن الأثر الأكبر متوقع في السنوات القادمة.

ثالثاً: ما يتسق مع ذلك في بيانات الرصد

لا تملك الدراسة دليلاً مباشراً على الأداة التي أُنشئت بها المواقع المرصودة، ولا تنسب أي موقع بعينه إلى الذكاء الاصطناعي. غير أن خصائص عدة في البيانات تتسق مع ما توثقه التقارير السابقة:

إتقان القوالب

شهادات صحية بشعار الأمانة المطابقة من بين 15 شعاراً، وصورة شخصية، ورمز تحقق، وأكثر من نوع من الوثائق.

سرعة الإطلاق

نطاق ينتحل قوى سُجّل وصدرت شهادته وظهرت صفحته في اليوم نفسه، و9 نطاقات متقاربة الأسماء خلال 21 يوماً.

كثافة الإنتاج

247 شهادة مزورة في سجلات موقع واحد خلال 37 يوماً، بذروة 26 شهادة في يوم واحد.

محاكاة بأخطاء قليلة

عناوين صفحات تطابق أسماء الخدمات الرسمية، مثل "التحقق من تصريح أجير" و"إصدار شهادة صحية".

الدلالة

إذا أصبح إنتاج وثيقة أو موقع مطابق للأصل في متناول أي شخص، فإن التوعية القائمة على "تمييز الأخطاء" تفقد جزءاً كبيراً من فاعليتها، ويكمن الحل في جعل التحقق نفسه غير قابل للتقليد: قناة رسمية لا يستطيع المزوّر محاكاتها. وفي هذا السياق، تحث الهيئة السعودية للبيانات والذكاء الاصطناعي على التأكد من موثوقية المواقع قبل مشاركة البيانات والوثائق، وتُدرج إرشاداتها بشأن التزييف العميق، بحسب تغطية Arab News، الاحتيالَ بانتحال الشخصية أولَ ثلاثة تهديدات ضارة رئيسة.

06 مناقشة النتائج

Discussion

تشير النتائج إلى اتساع استغلال انتحال الجهات الحكومية: من سرقة بيانات الدخول، كما وصفها تقريرا **Group-IB** و**CloudSEK**، إلى انتحال آلية التحقق من الوثائق ذاتها. وفي هذا النمط لا يكون حامل الوثيقة هو المتضرر المباشر، بل المفتش أو صاحب العمل الذي يثق بنتيجة مسح الرمز، ثم المجتمع الذي يتعامل مع عامل غير مفحوص في منشأة غذاء.

وتكشف دراسة الحالة الأولى أن موقعاً واحداً قادر على إصدار نحو 250 وثيقة خلال خمسة أسابيع، موزعة على مناطق المملكة. وإذا تكرر هذا النمط في بوابات أخرى، فقد يكون حجم التزوير الفعلي أكبر مما تكشفه أعداد النطاقات وحدها. كما أن تركّز **91%** من الشهادات في منشآت الغذاء يربط الظاهرة مباشرة بالصحة العامة.

> **الحل الجذري ليس ملاحقة المواقع وحدها، بل تغيير طريقة التحقق نفسها.**
>
> فالنطاق المحجوب يُستبدل خلال أيام، أما الرمز الذي لا يُقرأ إلا من تطبيق رسمي فلا يمكن تقليده.

ويتسق تركّز الاستهداف في الجهات الحكومية (**81%** [73–87%] من المواقع المؤكدة) مع ما توصلت إليه دراسة اليحيى وواير من أن الاتجاه الشخصي يتنبأ باستجابة الأفراد للرسائل التي تنتحل صفة السلطة. ويشير عدم ثبوت أي انتحال للخطوط السعودية بين 601 اسم مضيف تحمل كلمة "saudia" إلى أن تكرار الاسم ليس مؤشراً كافياً، وأن المهاجمين يختارون الخدمات التي يتعامل معها المستفيد بشكل متكرر.

ويدل استخدام النطاقات المسجلة منذ أكثر من عام، مع إخفاء المحتوى والأسماء المتقاربة وتوجيه الرموز عبر وسيط، على أن الاعتماد على مؤشر واحد لا يكفي. ويضاف إلى ذلك ما توثقه الأدبيات من أن الذكاء الاصطناعي التوليدي يجعل الوثيقة المزورة والموقع المنسوخ أقل أخطاءً، فتفقد التوعية القائمة على تمييز الأخطاء جزءاً من فاعليتها. فالمعالجة الفاعلة تتطلب تكامل الرصد التقني المبكر مع بلاغات المستفيدين، ومع معالجة آلية التحقق نفسها لدى الجهات المصدرة.

حدود التفسير: تعكس أعداد المواقع المؤكدة ما رصدته منصة سياج عبر سجلات شفافية الشهادات، ولا تشمل المواقع التي تعمل دون شهادة تشفير جديدة أو تُنشر عبر الرسائل ووسائل التواصل. وتمثّل دراسات الحالة مواقع بعينها ولا تُعمّم نسبها على جميع بوابات التزوير، كما أن تصميم الدراسة مقطعي لا يقيس اتجاهاً زمنياً.

07 التوصيات
Recommendations

أولاً: حلول مقترحة للتحقق من الوثائق

تقترح الدراسة نقل التحقق من "فتح الرابط المضمَّن في الرمز" إلى قنوات رسمية لا يستطيع المزوّر محاكاتها:

01 تطبيق رسمي لفحص الرموز

يمسح المفتش الرمز من داخل تطبيق الجهة، أو خدمة موحدة في تطبيق حكومي قائم، فيسترجع التطبيق السجل من النظام الرسمي مباشرة دون فتح أي رابط.

يُبطل أثر بوابات التحقق المزيفة كلياً

02 التحقق بعد الدخول عبر النفاذ الوطني الموحد

لا تُعرض نتيجة التحقق إلا لمستخدم موثّق يبدأ من القناة الرسمية، مع تسجيل كل عملية تحقق.

يصعّب محاكاة الخدمة، ويوفر سجلاً للمتابعة

03 التوقيع الرقمي لبيانات الرمز

يحمل الرمز بيانات الوثيقة موقّعة رقمياً من الجهة المصدرة، ويتحقق التطبيق الرسمي من التوقيع.

يكشف أي تعديل أو رمز منشأ خارج الجهة

04 قصر روابط التحقق على النطاقات الرسمية

تُعلن كل جهة نطاقات التحقق المعتمدة، وكلها تنتهي باللاحقة sa.، ويُعدّ مزوّراً كلُّ رمز يفتح نطاقاً لا ينتهي بها، حتى لو تضمّن اسمه gov.sa في بدايته أو وسطه.

يسهّل التمييز الفوري للمفتش والمواطن

ثانياً: توصيات للجهات المعنية

الجهات المصدرة للوثائق

تبنّي أحد الحلول السابقة، والتنبيه على الوثيقة نفسها بأن التحقق يتم عبر القناة الرسمية فقط، وإبطال الوثائق التي يُكشف تزويرها.

الهيئة الوطنية للأمن السيبراني

معاملة بوابات التحقق المزيفة بأولوية التصيّد نفسها، وإدراج مؤشراتها في خدمة "تحقق" لفحص الروابط، والتنسيق مع الجهات المصدرة لحجب عائلات النطاقات المتكررة.

المفتشون وأصحاب العمل

عدم الاعتماد على الصفحة التي يفتحها الرمز، والتحقق من نطاقها قبل قبول النتيجة، والإبلاغ عن أي وثيقة مشتبه بها.

منصات التوصيل والتوظيف

التحقق من الشهادات الصحية وتصاريح العمل عبر واجهات الجهات الرسمية مباشرة، لا عبر صورة الوثيقة أو رمزها.

مزوّدو الاستضافة والنطاقات

الاستجابة السريعة لبلاغات انتحال الجهات الحكومية، بما في ذلك صفحات إعادة التوجيه الوسيطة التي تستخدمها الرموز.

الجمهور

التوعية بأن الخدمات الحكومية لا تُباع عبر وسطاء أو مواقع غير رسمية، وأن إتقان الوثيقة أو الموقع ليس دليلاً على صحته.

ثالثاً: توصيات بحثية

- توسيع الدراسة لتشمل الرسائل النصية ومنصات التواصل الاجتماعي وإعلانات البحث المدفوعة.
- قياس أثر تطبيق التوقيع الرقمي للرموز على انتشار بوابات التحقق المزيفة.
- تطوير مؤشرات لرصد المحتوى المولّد آلياً في مواقع انتحال الجهات الحكومية.
- دراسة طولية لمتابعة المهاجمين وعائلات النطاقات عبر فترات أطول.

08 الخاتمة
Conclusion

تناولت هذه الدراسة ظاهرة انتحال الجهات الحكومية في المملكة العربية السعودية عبر مواقع إلكترونية مزيفة، وخلصت إلى أنها لم تعد مقتصرة على سرقة بيانات الدخول، بل امتدت إلى نمط أشد خطورة يتمثل في بوابات تحقق مزيفة تُستخدم لإضفاء صفة رسمية على وثائق مزوّرة، كالشهادات الصحية وتصاريح العمل وشهادات الاشتراك في التأمينات.

وقد أسفر الرصد خلال الفترة من 20 سبتمبر إلى 9 نوفمبر 2026 عن تأكيد 150 موقعاً منتحِلاً، منها 17 بوابة تزوير، والإبلاغ عن 58 موقعاً في 26 بلاغاً رسمياً إلى الهيئة الوطنية للأمن السيبراني. وكشفت سجلات موقع واحد عن 247 شهادة صحية مزوّرة خلال 37 يوماً، معظمها لعاملين في منشآت الغذاء. وتركّز الاستهداف على عدد محدود من الجهات، في مقدمتها منصة بلدي (59 موقعاً) والبوابات الحكومية العامة (29) والتأمينات الاجتماعية (12)، تليها مصرف الراجحي (9) ومنصة قوى (7)، وهو ما يشير إلى أن الوثائق الأكثر طلباً في سوق العمل هي الأكثر عرضة للتزوير.

وتؤكد النتائج، ومعها ما توثقه الأدبيات عن أثر الذكاء الاصطناعي التوليدي، أن الحل الجذري لا يكمن في ملاحقة المواقع المزيفة وحدها، إذ يمكن إنشاء بدائل لها بسرعة وبإتقان متزايد، بل في تغيير طريقة التحقق نفسها؛ بحيث يتم التحقق من الوثيقة عبر تطبيق رسمي أو بعد تسجيل الدخول عبر النفاذ الوطني الموحد، لا عبر رابط مضمَّن في رمز مطبوع على الوثيقة. وبذلك يفقد الرمز المزيف قيمته مهما بلغت دقة تقليده.

وتأمل الدراسة أن تُسهم نتائجها في دعم جهود الجهات المختصة في حماية الثقة بالوثائق الرسمية، وأن تكون منطلقاً لدراسات لاحقة أوسع نطاقاً.

المراجع
References

المراجع العربية

1. الهيئة الوطنية للأمن السيبراني. (2025، 30 ديسمبر). **إطلاق خدمة "تحقق"**. nca.gov.sa
2. الهيئة الوطنية للأمن السيبراني. (د.ت). **الأدلة الإرشادية لتطبيق ضوابط الأمن السيبراني**. الرياض. nca.gov.sa
3. وزارة البلديات والإسكان. (د.ت). **الاستعلام عن حالة شهادة صحية**. منصة بلدي. balady.gov.sa
4. وزارة الموارد البشرية والتنمية الاجتماعية. (د.ت). **إصدار تصاريح أجير**. hrsd.gov.sa

المراجع الأجنبية

1. 404 Media. (2024, February 5). Inside the underground site where 'neural networks' churn out fake IDs. 404media.co
2. Alyahya, T., & Weir, G. R. S. (2021). Understanding responses to phishing in Saudi Arabia via the Theory of Planned Behaviour. 2021 National Computing Colleges Conference (NCCC). IEEE. strathprints.strath.ac.uk/78717
3. Arab News. (2026, May 9). SDAIA issues deepfakes guidelines to regulate responsible AI use. arabnews.com/node/2642878
4. CloudSEK. (2022, updated 2023). Phishing campaign targeting the Saudi government service portal Absher. cloudsek.com
5. Entrust Cybersecurity Institute. (2024, November 19). Deepfake attacks strike every five minutes amid 244% surge in digital document forgeries [Press release]. securityinfowatch.com
6. Federal Bureau of Investigation, Internet Crime Complaint Center. (2024, December 3). Criminals use generative artificial intelligence to facilitate financial fraud (I-120324-PSA). ic3.gov
7. Financial Crimes Enforcement Network. (2024, November 13). FinCEN issues alert on fraud schemes involving deepfake media targeting financial institutions. fincen.gov
8. Group-IB. (2022, November 9). Hired Hand [Press release]. group-ib.com
9. Group-IB. (2026, October 5). Paid in full: How card fraudsters in the GCC use government payment portals to cash out stolen cards. group-ib.com
10. Microsoft. (2025, April 16). Cyber Signals Issue 9: AI-powered deception: Emerging fraud threats and countermeasures. microsoft.com
11. Netcraft. (2024, August 29). Scam sites at scale: LLMs fueling a GenAI criminal revolution. netcraft.com
12. Netcraft. (2026, July 28). How the rise of AI 'vibe coding' introduced a new phishing shortcut for cybercriminals. netcraft.com
13. Okta Threat Intelligence. (2025, July 1). Okta observes v0 AI tool used to build phishing sites. okta.com
14. Palo Alto Networks Unit 42. (2025, August 19). Fashionable phishing bait: GenAI on the hook. unit42.paloaltonetworks.com
15. Proofpoint. (2025, August 20). Cybercriminals abuse AI website creation app for phishing. proofpoint.com
16. Riyadh Daily. (2026, April 5). SDAIA urges verifying website reliability before sharing data, documents, biometrics. alriyadhdaily.com
17. Sumsub. (2025, June 12). Synthetic identity document fraud surges 300% in the U.S.: Sumsub warns e-commerce, healthtech and fintech at risk. sumsub.com
18. Sumsub. (2026, January 15). AI fake IDs and the new KYC risk. sumsub.com

الملاحق
Appendices

الملحق أ: قنوات التحقق الرسمية من الوثائق

تقدّم الجهات الحكومية السعودية خدمات التحقق من وثائقها عبر نطاقات تنتهي باللاحقة .sa. وعليه، فإن أي رمز استجابة سريعة أو رابط على وثيقة حكومية يقود إلى نطاق خارج القائمة التالية يستدعي التحقق من الوثيقة مباشرة لدى الجهة المصدرة.

جدول 6: النطاقات الرسمية للتحقق من الوثائق

الجهة المصدرة	أبرز الوثائق	النطاقات الرسمية
منصة بلدي / وزارة البلديات والإسكان	الشهادة الصحية، الرخصة البلدية، رخصة البناء	balady.gov.sa momah.gov.sa
منصة صحة / وزارة الصحة	الإجازة المرضية، التقرير الطبي	seha.sa moh.gov.sa
منصة قوى / أجير / وزارة الموارد البشرية	تصريح أجير، رخصة العمل، عقد العمل	qiwa.sa hrsd.gov.sa
المؤسسة العامة للتأمينات الاجتماعية	شهادة الاشتراك، شهادة الراتب	gosi.gov.sa
المركز السعودي للأعمال / وزارة التجارة	السجل التجاري	saudibusiness.gov.sa mc.gov.sa
مقيم / المديرية العامة للجوازات	الإقامة، تأشيرة الخروج والعودة	muqeem.sa absher.sa moi.gov.sa
الإدارة العامة للمرور	المخالفات، رخصة القيادة، استمارة المركبة	absher.sa moi.gov.sa
وزارة الخارجية / المنصة الموحدة للتأشيرات	التأشيرة، تصديق الوثائق	mofa.gov.sa enjazit.com.sa ksavisa.sa
منصة نسك / وزارة الحج والعمرة	تصريح الحج، تصريح العمرة	nusuk.sa haj.gov.sa
وزارة التعليم	الشهادة الجامعية، معادلة الشهادات	moe.gov.sa
الهيئة السعودية للتخصصات الصحية	التصنيف والتسجيل المهني	scfhs.org.sa
الهيئة السعودية للمهندسين	الاعتماد المهني الهندسي	saudieng.sa
وزارة العدل / ناجز	الوكالات، الوثائق العدلية	najiz.sa moj.gov.sa
منصة إيجار	عقد الإيجار	ejar.sa
المركز الوطني للرقابة على الالتزام البيئي	التصريح البيئي	ncec.gov.sa
هيئة الزكاة والضريبة والجمارك	شهادة التسجيل الضريبي، شهادة الزكاة	zatca.gov.sa
توكلنا / الهيئة السعودية للبيانات والذكاء الاصطناعي	الهوية الرقمية	tawakkalna.sa sdaia.gov.sa

ملاحظة: جُمعت هذه النطاقات من المواقع الرسمية للجهات في نوفمبر 2026، وقد تضيف الجهات نطاقات فرعية جديدة تحت النطاقات نفسها.

الملحق ب: مؤشرات بوابات التزوير المؤكدة

أسماء المضيفين السبعة عشر المصنّفة "بوابة تزوير" في قاعدة بيانات منصة سياج حتى 9 نوفمبر 2026، بصيغة معطّلة:

جدول 7: بوابات التزوير المؤكدة

#	اسم المضيف	الجهة المنتحَلة	أول رصد
1	ccs.balady.gov.sa-sa[.]info	منصة بلدي	4 أكتوبر
2	appbaladygovsa[.]org	منصة بلدي	4 أكتوبر
3	qrsaudibusiness-govsa[.]org	المركز السعودي للأعمال	10 أكتوبر
4	balady[.]sbs	منصة بلدي	16 أكتوبر
5	appsbalady-govsa.pages[.]dev	منصة بلدي	18 أكتوبر
6	appbaladygovsa[.]com	منصة بلدي	19 أكتوبر
7	balady.govsa[.]app	منصة بلدي	20 أكتوبر
8	ajeer-hrsd-qiwa.gov-sa[.]store	منصة قوى / أجير	21 أكتوبر
9	ajeer-hrsd-qiwa-gov-sa[.]online	منصة قوى / أجير	21 أكتوبر
10	verify.ajeer-hrsd-qiwa-gov-sa[.]online	منصة قوى / أجير	22 أكتوبر
11	servicesbaladygovsa.pages[.]dev	منصة بلدي	27 أكتوبر
12	ccs.balady.gov.sa-sa[.]space	منصة بلدي	28 أكتوبر
13	dhamen-sa.pages[.]dev	المركز الوطني للرقابة على الالتزام البيئي	4 نوفمبر
14	alriyadh-gov-sa[.]net	جهات صحية	6 نوفمبر
15	alriyadh-gov-sa[.]info	جهات صحية	7 نوفمبر
16	www.eservices.alriyadh-gov-sa[.]com	جهات صحية	9 نوفمبر
17	alriyadh-gov-sa[.]com	جهات صحية	9 نوفمبر

أول رصد هو تاريخ إدراج اسم المضيف في قائمة المراجعة بمنصة سياج. وتضم القائمة أيضاً 8 أسماء مضيفين قيد المراجعة بوصفها بوابات تزوير محتملة لم تُدرج هنا.

سياج

السور الذي يحمي الثقة الرقمية

منصة سعودية مستقلة ترصد المواقع التي تنتحل الجهات الحكومية والبنوك والعلامات السعودية لحظة ظهورها في سجلات الشهادات، وتبلّغ عنها الجهات المختصة.

كيف تتحقق من وثيقة حكومية؟

01

من التطبيق الرسمي

افتح تطبيق الجهة المصدرة أو منصتها، وتحقق من الوثيقة من داخله.

02

انظر إلى نهاية النطاق

نطاق التحقق الرسمي ينتهي بـ .sa، ووجود gov.sa في وسط الاسم لا يكفي.

03

بعد الدخول عبر نفاذ

إن أمكن، تحقق بعد تسجيل الدخول عبر النفاذ الوطني الموحد.

contact@siyaj.net

siyaj.net

© 2026 م. تركي عبدالله الشهري · منصة سياج