أكاديمية طويق
Tuwaiq Academy

أبشر طويق

المسار

ابتكار وتطوير الخدمات

محروس
Mahroos

خدمة للتحقق من انتحال هوية الجهات الحكومية

المحتويات

01 وصف ومواءمة الفكرة للمسار

02 المشكلة وحلّها

03 البيانات المستخدمة

04 كيفية توفير هذا البيانات وكيفية استخدامها

05 التقنيات المستخدمة

06 الاختبار / التحقق

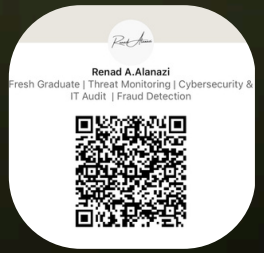
07 العرض التوضيحي / المحاكاة

08 التحديات والخطط المستقبلية

أعضاء الفريق

سيرا الهطلاني

نورة العمّار



ريناد العنزي

حماية موثوقة
من انتحال الجهات الحكومية

بدء الفحص

وصف ومواءمة الفكرة للمسار

هي خدمة تحقق تستهدف أي محتوى يدعي أنه صادر من جهة حكومية، سواء:

- رسالة SMS
- إيميل
- رابط
- رقم
- موقع إلكتروني

الهدف كشف أي انتحال لهوية حكومية قبل أن يتفاعل معه المواطن أو المقيم

وتمكين الجهات المختصة من رصد محاولات انتحال الهوية الحكومية واتخاذ الإجراءات اللازمة حياله

وتنسجم الفكره مع مسار ابتكار وتطوير خدمات لكونها قابلة للتكامل مع المنصات الوطنية مثل أبشر أو توكلنا ، وقد تم اختيار توكلنا كنقطة عرض أولية للنموذج لاعتبارات تشغيلية تتعلق بالاستخدام اليومي وسهوله الوصول

المشكلة وحلّها

محروس
Mahroos

رغم أن كثيرًا أصبحوا أكثر وعيًا بأنماط الاحتيال، إلا أن ليست كل محاولات الاحتيال واضحة للجميع.

-كبار السن

-محدودو المعرفة التقنية

-المقيمين الذين لا يعرفون شكل الرسائل الحكومية الأصلية

خصوصا أن أساليب الانتحال أصبحت متقنة لدرجة تجعل التمييز يدويًا أمرًا صعبًا حتى على الأشخاص الحذرين

فالمحتالون يتعمدون استخدام أساليب دقيقة يصعب ملاحظتها

ولهذا تبرز الحاجة إلى خدمة تحقق حكومية معتمدة, تتيح للمواطن و المقيم عدم التعرض للاحتيال بانتحال الجهات الحكومية

المشكلة وحلّها

محروس
Mahroos

لا يكتفي بحماية المواطن أو المقيم من الاحتيال

بل يحول كل عملية تحقق إلى إنذار مبكر تساعد الجهات المختصة في كشف وإيقاف الاحتيال قبل انتشاره.

وتخدم ايضا الجهات المختصه في 4 وظائف رئيسيه استراتجيه

1) رصد مبكر للأنماط الاحتيالية

يكتشف أي روابط أو رسائل احتيالية جديدة فور ظهورها.

2) تحديد الجهات الأكثر تعرضًا للانتحال

يوضح الجهات الحكومية التي تُستهدف بشكل متكرر لاتخاذ إجراءات حماية أسرع.

3) معرفة المناطق والفئات الأكثر استهدافًا

يحدد أماكن انتشار الاحتيال والفئات الأكثر عرضة للهجمات.

4) إنشاء قاعدة بيانات وطنية للانتحال

يبني سجلاً موحدًا لحملات وأساليب الانتحال لدعم التحليل والاستجابة السريعة

محروس يوفر نقطة تحقق وطنية فورية تكشف للمستخدم ما إذا كانت الرسالة أو الرابط حقيقيًا أو احتيالًا، قبل وقوع الضرر. كما يزوّد الجهات المختصة ببيانات عن محاولات الانتحال، وتحليل للأنماط المستجدة، مما يمكّنها من التدخل السريع ورفع مستوى الأمان الرقمي

البيانات المستخدمة

يعتمد محروس على ثلاثة أنواع رئيسية من البيانات للتحقق من صحة الرسائل والروابط

بيانات حكومية رسمية

- النطاقات الحكومية المعتمدة
- الروابط الرسمية

البيانات نستخدمها كأساس للمقارنة وكشف أي اختلاف يدل على الانتحال.

بيانات محاولات الاحتيال

- روابط مشبوهة تم الإبلاغ عنها سابقًا
- كلمات أو صيغ تستخدم عادة في الاحتيال

البيانات تساعد بتعرف على أساليب المحتالين

بيانات يدخلها المستخدم

- نص الرسالة
- الرابط
- الرقم

يبدأ دور الذكاء الاصطناعي

دور الذكاء الاصطناعي في محروس

قراءة لقطات الشاشة تلقائيًا

المستخدم يصور الشاشة ← يرفع الصورة ← الذكاء الاصطناعي:

- يقرأ النص داخل الصورة
- يتعرف على شكل الرسالة ولغتها

بدون ما يحتاج المستخدم ينسخ أو يلصق .

كشف الروابط المموهة

المحتال يغيّر حرف واحد في الرابط الحكومي (مثال: Absher → Absherr).

الذكاء يكتشف هذه الاختلافات الصغيرة فورًا

تحليل الأنماط الجديدة (تعلم مستمر)

كل محاولة احتيال جديدة تُستخدم لتقوية الخدمة وتحديث قاعدة البيانات.

يساهم هذا التكامل بين البيانات الرسمية والذكاء الاصطناعي في رفع دقة الكشف وتقليل فرص الاحتيال قبل وقوع الضرر.

كيفية توفير هذا البيانات وكيفية استخدامها

كيفية توفير البيانات

يتم الحصول على بيانات الجهات الحكومية الرسمية من قواعد بيانات موثوقة ومعتمدة.

- استخدام واجهات ربط (API) موحدة لتحديث البيانات المرتبطة بالنطاقات والروابط وأرقام التواصل المعتمدة.
- يستقبل محروس محتوى المستخدم (النص/الرابط/الرقم/لقطة الشاشة) ويحلل بشكل فوري دون أي تدخل يدوي.
- تُسجل محاولات الاحتيال المبلغ عنها لتكوين قاعدة بيانات دقيقة تُستخدم في رصد الأنماط الجديدة.

كيفية استخدام البيانات

يقوم محروس بتحليل المحتوى المدخل (النص أو لقطة الشاشة) لاكتشاف النقاط المريبة.

- مطابقة الرسالة أو الرابط مع القوالب الرسمية والروابط الحكومية المعتمدة.
- تقييم مستوى الخطورة باستخدام تقنيات الذكاء الاصطناعي لمعرفة هل المحتوى: رسمي أو انتحال .
- إرسال تنبيه للمستخدم، مع تمرير البيانات مجهولة الهوية للجهات المختصة لرصد محاولات الاحتيال الجديدة

التقنيات المستخدمة في بناء النموذج الأولى

تصميم واجهة المستخدم

- Figma
- تصميم النموذج الأولي (Prototype)
- بناء تجربة مستخدم بسيطة وواضحة بأسلوب مشابه لواجهات توكلنا
- إنشاء تدفقات الاستخدام (User Flows) للمراحل من الفحص إلى النتيجة

تقنيات محرك التحقق (Verification Engine) (Backend)

- Google Colab
- nGrok
- Postman

الاختبار / التحقق

- أثبت النظام فعاليته بالتصنيف بشكل صحيح في كل مره تم استخدامه للتحقق من بيانات مسجلة في قاعدة البيانات.
- تصميم واجهة المستخدم الأولية في Figma لاختبار تجربة المستخدم وسهولة التفاعل.

رابط github

العرض التوضيحي

التحديات والخطط المستقبلية

التحديات

- غياب بيانات تجريبية واسعة .
- اختبار الـ Endpoints: تم استخدام Postman / curl للطلبات من نوع POST بدل المتصفح الذي يرسل فقط GET
- التكامل مع تطبيقات الجهات الحكومية بشكل مباشر يحتاج وصول إلى واجهات برمجية (APIs).

ما نحتاجه للمساعدة

- توفير بيانات إضافية من الجهات الرسمية لفحص وتحليل أكبر.
- إمكانية الوصول إلى APIs رسمية أو بيئات اختبار للروابط والرسائل الحكومية.
- التعامل مع عدد كبير من الطلبات بشكل آمن وفعّال.

العمل المستقبلي / خارطة الطريق

- تدريب نماذج الذكاء الاصطناعي للكشف عن محاولات التصيّد الاحتيالي بما يتجاوز القواعد البسيطة.
- لوحة تحكم للجهات المختصة لمراقبة المحاولات المشبوهة في الوقت الفعلي.
- عرض مدى قوة الاشتباه (مثال: تشابه بنسبة 85%).
- دعم متعدد اللغات: اكتشاف الرسائل بالعربية والإنجليزية.
- تنبيهات المستخدمين: إشعار المواطنين عند اكتشاف نشاط مشبوه.

أبشر طويق

محروس
Mahroos

يكشف الانتحال ... ويقطع طريق الاحتيال

شكراً

أكاديمية طويق
Tuwaiq Academy