الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

التصيد الاحتيالي والهندسة الاجتماعية

الفئة المستهدفة
الجمهور العام

كُتَيّب المُدَرّب

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

التصيد الاحتيالي والهندسة الاجتماعية

الفئة المستهدفة

الجمهور العام

كُتَيّب المُدَرّب

تمهيد

السَّلامة الرقميَّة ركيزة أساسيَّة لضمان أمْن المعلومات، وحماية الأفراد والمجتمعات من التهديدات السيبرانية المتزايدة باستمرار.

تم تصميم هذا الكُتَيِّب بهدف توعية فئات المجتمع بمبادئ السلامة الرقمية وأفضل الممارسات التي تساعد على تجنُّب المخاطر في البيئة الرقمية.

يهدف الكتيّب إلى تعزيز الوعي بأبرز التهديدات التقنية التي قد نواجهها في حياتنا اليومية؛ مثل: التصيُّد الاحتيالي، والهندسة الاجتماعية، واستعراض أكثر صورهما شيوعًا، مثل: الرسائل الاحتيالية، والمكالمات المزيَّفة، وانتحال صفة الجهات الرسمية، مع تقديم إرشادات عملية تساعد الأفراد على التصرُّف السليم عند التعرُّض لمحاولات خداع أو الاشتباه بنشاطٍ مريبٍ.

وتُعدّ هذه الجهود جزءًا من المبادرة الوطنية للسلامة الرقمية التي تُنظّمها الوكالة الوطنية للأمن السيبراني، لبناء بيئة رقمية آمِنَة لجميع فئات المجتمع.

المبادرة الوطنيّة للسلامة الرقميّة

Digital Safety National Initiative

تعريف المبادرة

مجموعة من فعاليات التوعية في مجال السلامة الرقمية والأمن السيبراني؛ تستهدف المجتمع المحلي على اختلاف الشرائح العُمرية والاجتماعية والقطاعات المهنية.

تعمل المبادرة على نشر الوعي بالسلامة الرقمية والاستخدام الآمِن لشبكة الإنترنت والتطبيقات التكنولوجية المختلفة، وتوضيح المخاطر المحتمَلة؛ وذلك بهدف بناء مجتمع آمِن سيبرانيًّا ومتمكّن تكنولوجيًّا.

الشرائح المستهدَفة

تستهدف المبادرة مختلف شرائح المجتمع، مع تركيزها على الفئات التالية:

01 السنة الأولى

- ذوو الاحتياجات الخاصة
- طلبة الجامعات
- العمالة الوافدة
- مؤسسات المجتمع المدني
- القطاع المالي والمصرفي
- كبار القَدْر
- المرأة والأسرة

02 السنة الثانية

الدبلوماسيون

الإعلاميون

الجمهور العام

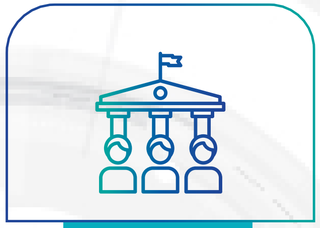
المرأة (العنف الرقمي ضد المرأة)

العاملون في المجال الصحي

المؤسسات العقابية والنيابة والمؤسسات الإصلاحية

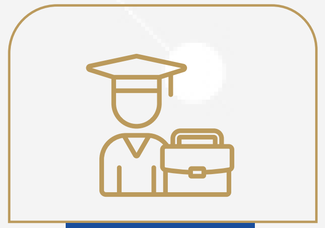
الرياضيون

03 السنة الثالثة



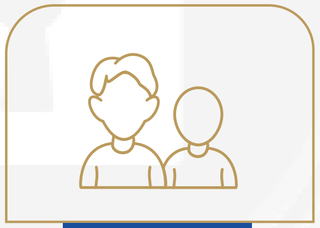
العاملون في وزارتي الدفاع والداخلية

العاملون في قطاع الطاقة



العاملون في قطاع التعليم

ذوو الاحتياجات الخاصة



اليافعون والشباب

الجمهور العام

أدوات التوعية

تعتمد المبادرة على أدوات توعية متنوّعة ومتكاملة، تشمل ما يلي:

دليل السلامة الرقمية

كُتَيّبات توعية مطبوعة

شرائح العرض (للمُدرّبين)

فيديوهات التوعية (أنيميشن)

فيديوهات التوعية (تمثيلية)

الألعاب السيبرانية

بوابة التوعية السيبرانية

الروبوت التفاعلي

وِرَش التوعية

01 المحور الأول

التصيُّد الاحتيالي

مفهوم التصيُّد الاحتيالي

هو أحد أكثر أساليب الاحتيال الرقمي شيوعًا، ويعتمد على انتحال صفة جهات موثوقة أو رسمية؛ بهدف دَفْع المستخدِم إلى الإفصاح عن معلومات شخصية أو مالية، أو تنفيذ إجراء يُعرِّضه للخطر الرقمي.

السمات الرئيسية

- محاكاة الرسائل أو المواقع الرسمية من حيث الشكل، اللغة، والعناصر البصرية
- استخدام لغة مُطمئنة أو مُقْلِقَة لدَفْع الشخص إلى الرَّدّ
- الاعتماد على الخداع النفسي بدلًا من الأساليب التقنية
- استهداف مستخدمين نشطين يعتمدون على الخدمات الرقمية في معاملاتهم اليومية
- الانتشار الواسع بسبب سهولة التنفيذ وتكرار القوالب

الرسائل النصية القصيرة الاحتيالية

تصل هذه الرسائل عبر الهاتف المحمول، وغالبًا ما تعتمد على صياغة مختصرة وعاجلة؛ تهدف إلى خَلْق شعور بالضغط والاستعجال، ودَفْع المتلقّي إلى التفاعل دون تفكير.

العناصر المكررة في هذه الرسائل

- استخدام عبارات مثل: "أوْقَفْنا حسابك"، "ربحت معنا"، "تم شحن الطرد"...
- غياب التفاصيل الدقيقة أو معلومات التواصل الرسمية
- فَرْض مهلة زمنية قصيرة لاتخاذ الإجراء
- إدراج روابط مختصرة بصيغة يصعب التحقُّق منها
- توجيه المستخدِم إلى صفحة تطلب إدخال بيانات أو تحميل تطبيق خارجي

الاتصالات الهاتفية الاحتيالية

يعتمد هذا الأسلوب على إجراء مكالمة هاتفية مباشرة، يقدّم فيها المحتال نفسه بصفته موظفًا رسميًّا، مستفيدًا من نبرة الصوت الواثقة واللغة المنظَّمة لبناء مصداقية زائفة.

الأسلوب المستخدَم

- الادعاء بالانتماء إلى بنك، جهة حكومية، أو مؤسسة خدمية
- استخدام لغة رسمية وهدوء مُبالَغ فيه؛ لإشعار المتلقّي بالأمان
- إثارة موضوعات حساسة مثل تحويلات مشبوهة أو إجراءات قانونية
- طلب بيانات الحساب أو رموز التحقُّق بشكل مباشر
- محاولة إنهاء المكالمة بسرعة لمنع التحقق أو الاستشارة

رسائل WhatsApp الاحتيالية

يُستغل تطبيق واتساب WhatsApp على نطاق واسع في إرسال رسائل احتيالية تنتحل أسماء مؤسسات معروفة، أو جهات خدمية، بهدف الحصول على بيانات شخصية أو مالية بحجة وجود تحديث، مشكلة تقنية، أو إجراء عاجل.

الخصائص الشائعة لهذه الرسائل

1. تحتوي على شعارات حقيقية أو مأخوذة من مواقع رسمية
2. تبدأ بتحية عامة غير موجّهة بالاسم
3. تتضمّن رابطًا يشير إلى صفحة شبيهة بموقع معروف
4. مُطالَبة المستخدم بإدخال بيانات حساسة مثل رقم الهوية أو المعلومات البنكية
5. طلب كلمة المرور لمرة واحدة عبر واتساب WhatsApp

المواقع الإلكترونية المُزيَّفة

يتم إعداد صفحات إلكترونية تحاكي مواقع البنوك أو الجهات الحكومية؛ من حيث التصميم والعناوين، مع تغييرات طفيفة.

السمات التي تُميِّز هذه المواقع

01
التشابه الكبير في الألوان والشعارات والعناوين

02
استخدام روابط تتضمن حروفًا إضافية أو تغييرات بسيطة في التهجئة

03
عدم وجود شهادة أمان (https) أو رمز القفل بجانب الرابط

04
تضمين نموذج لتسجيل الدخول أو تحديث البيانات

رسائل الجوائز والهدايا المُزيَّفة

تُرسَل هذه الرسائل بهدف إقناع الشخص بأنه فاز بجائزة قيِّمَة، بهدف استدراجه إلى تقديم بياناته أو دفع مبالغ مالية رمزية.

العناصر الأساسية

- عرض جوائز مغرية مثل أجهزة ذكية، مبالغ مالية، أو رحلات
- استخدام عبارات تحفيزية ومباشرة مثل "مبروك، أنت الفائز"
- طلب إدخال بيانات شخصية عبر رابط خارجي
- المطالبة بدفع رسوم بسيطة تحت مسمى "تكاليف الشحن"
- إنهاء الاتصال أو المراسلة فور استلام البيانات أو المبلغ

انتحال هوية مؤسسات رسمية

يعتمد هذا الأسلوب على استخدام أسماء جهات رسمية أو معروفة لإضفاء مصداقية وهمية على عملية الاحتيال؛ ما يزيد من احتمالية استجابة المتلقي.

المظاهر المستخدَمة في هذا النوع من الاحتيال

- ذِكْر أسماء بنوك، جهات حكومية، أو مؤسسات معروفة
- إرسال رسائل أو إجراء مكالمات بتصميم أو لغة قانونية
- الحديث عن مخالفات، تجميد حسابات، أو تحقيقات وهمية
- استخدام التهديد غير المباشر لدفع المستخدم إلى التفاعل
- توجيه الطلب بسرعة قبل أن يُتاح للضحية التحقُّق

التصيُّد عبر وسائل التواصل الاجتماعي

تُستخدم منصات التواصل الاجتماعي كوسيلة فعّالة للوصول إلى الضحايا، سواء عبر حسابات مخترقة أو حسابات مزيفة تم إنشاؤها لهذا الغرض.

الأساليب الشائعة

- إرسال رسالة من حساب لصديق يقول "أحتاج مساعدتك"
- مشاركة روابط تبدو طبيعية مثل "انظر هذا الفيديو"
- طلب تحويل مبلغ مالي من خلال محادثة مباشرة
- انتحال شخصية مؤسسات وتقديم عروض مُزيَّفة
- استخدام أساليب ودية ولغة عادية لبناء الثقة قبل الاحتيال

رسائل تنتحل شخصية الأقارب

تصل هذه الرسائل من أرقام مجهولة، ويدّعي مُرسلها أنه أحد الأقارب، وغالبًا ما يُستخدَم هذا الأسلوب لطلب تحويل مالي عاجل.

الخطوات التي يعتمدها المحتال في هذا النوع

- الادعاء بتغيير رقم الهاتف مع تقديم صفة عائلية
- الادّعاء بأنه في موقف طارئ يتطلب مساعدة مالية
- مَنْع الشخص من التحقُّق من هويته بحجة "السرية" أو "الحرج"
- استخدام معلومات عامة مثل الاسم الأول لإقناع الضحية
- طلب التحويل إلى رقم حساب أو خدمة دفع سريع
- استخدام اسم حساب مُشابه للأقارب بمواقع التواصل الاجتماعي

حملات التبرع الاحتيالية

تظهر هذه الحملات في شكل منشورات أو رسائل إنسانية، وتهدف إلى استغلال التعاطف العام لجمع تبرعات لحالات غير حقيقية.

الأساليب المستخدَمة في هذا النمط

- نشر صور أو مقاطع مؤثرة لحالات طبية أو كوارث
- استخدام لغة عاطفية تدعو إلى المساعدة العاجلة
- تقديم أرقام حسابات أو هواتف شخصية
- غياب أيّ جهة موثوقة أو توثيق رسمي
- اختفاء الصفحات أو الرسائل بعد جمع الأموال

التصيُّد عبر الإعلانات المموَّلة

أصبحت الإعلانات المموَّلة إحدى القنوات غير المباشرة للتصيّد الاحتيالي؛ حيث يستغل المحتالون ثقة المستخدِم بنتائج البحث والإعلانات الظاهرة في الصدارة، لإنشاء مسارات احتيالية تبدو شرعية من حيث الشكل والمحتوى.

المنهجية المعتمدة

- تصميم إعلانات تحاكي الهوية البصرية لشركات أو منصات معروفة
- استغلال خوارزميات الإعلانات للوصول إلى فئات محددة
- توجيه المستخدِم إلى مواقع مُهيَّأة لجمع البيانات بدلًا من تقديم الخدمة
- الاعتماد على قرارات سريعة ناتجة عن البحث اللحظي
- صعوبة التمييز بين الإعلان التجاري الحقيقي والمحتوى الاحتيالي

التصيُّد عبر البريد الإلكتروني

يتجاوز هذا النوع من التصيُّد الرسائل العامة، ويَستهدف المستخدِم في سياق مهني أو مؤسسي، مستفيدًا من طبيعة العمل التي تتطلب الاستجابة السريعة والتعامل مع مستندات وروابط بشكل يومي.

سمات هذا النمط

- محاكاة أسلوب المراسلات الداخلية أو الرسمية
- استغلال ضغط الوقت والمسؤولية الوظيفية
- استخدام تسلسل منطقي في الطلبات لخفض مستوى الشكّ
- الاعتماد على أخطاء طفيفة في عناوين البريد يصعب ملاحظتها
- إدراج مرفقات أو روابط ضمن سياق مهني مألوف
- استخدام هوية بصرية قريبة من هوية جهة رسمية أو خاصة

التصيُّد المرتبط بالخدمات الحكومية الرقمية

مع التحوُّل نحو الخدمات الحكومية الرقمية، ظهرت محاولات تصيُّد تستند إلى الشرعية المؤسسية، مستغلة الثقة العالية التي يمنحها المستخدم للمنصات الرسمية.

آليــة العمــل

- بناء واجهات رقمية تحاكي البوابات الحكومية
- استخدام لغة تنظيمية تُوحي بالإلزام القانوني
- ربط التفاعل بعواقب إدارية مثل إيقاف الخدمة
- طلب تحديث بيانات بحجة الامتثال أو التحقق
- استثمار الخوف من فقدان الخدمة كعامل ضغط

التصيُّد عبر العروض الوظيفية الوهمية

يستهدف هذا النوع الأفراد الباحثين عن فرص عمل، من خلال نشر إعلانات أو إرسال رسائل تعرض وظائف مغرية دون متطلبات واضحة.

مؤشرات النمط الاحتيالي

1. وعود مهنية غير متناسبة مع متطلبات الوظيفة
2. تسريع إجراءات القبول دون تقييم فِعلي
3. نقل التواصل خارج القنوات المهنية المعتادة
4. طلب معلومات حساسة تحت ذريعة التوظيف
5. فرض رسوم غير مبرَّرة في مراحل مبكرة

التصيُّد المرتبط بالتجارة الإلكترونية

يرتبط هذا الأسلوب بسلوك الشراء الرقمي، ويعتمد على إقناع المستخدم بأن الخلل في عملية الدفع أو الشحن يتطلب تدخّلًا فوريًّا.

الأساليب المستخدمة

- توجيه المستخدم لإعادة إدخال بيانات البطاقة
- استخدام صور منتجات مأخوذة من متاجر حقيقية
- اختفاء المتجر أو الحساب بعد إتمام عملية الدفع
- إنشاء متاجر إلكترونية مؤقتة بأسعار مغرية
- إرسال رسائل حول مشكلات في الدفع أو الشحن

التصيُّد بالذكاء الاصطناعي

يُشير هذا النوع من التصيُّد إلى استخدام تقنيات الذكاء الاصطناعي في تنفيذ عمليات احتيالية رقمية أكثر تطوُّرًا، تُركِّز على محاكاة السلوك البشري والتواصل الواقعي؛ بهدف خداع المُستخدِم ودَفْعه للإفصاح عن معلومات مُهمَّة أو اتخاذ قرارات غير آمِنة.

السمات الرئيسية

- استخدام أنظمة ذكية لتوليد رسائل مُقنِعة وطبيعية
- مُحاكَاة تفاعلات بشرية يصعب تمييزها عن الحقيقية
- تقليل الأخطاء اللُّغوية والمؤشرات التقليدية للاحتيال
- رَفْع مستوى الإقناع مقارنةً بأساليب التصيُّد التقليدية

أساليب التصيُّد باستخدام الذكاء الاصطناعي

أسهم الذكاء الاصطناعي في نقل التصيُّد الاحتيالي من نماذج عامة إلى هجمات دقيقة ومُخصَّصة، تعتمد على تحليل سلوك المُستخدِم وسياقه الرقمي؛ ما يزيد من احتمالية نجاح عملية الاحتيال، ويُقلِّل من فرص اكتشافه مُبكرًا.

أبرز الأساليب المُستخدَمة

تحليل البيانات الشخصية	الرسائل النصية المُولّدة بالذكاء الاصطناعي	مُحاكَاة الأسلوب اللغوي	استنساخ الصوت	التزييف العميق
التكيُّف الآلي مع ردود الضحية	تقليل المؤشرات التقليدية للتصيُّد الاحتيالي	استغلال الثقة في الأنظمة والردود المؤتمتة	توسُّع نطاق الهجمات وسرعة تنفيذها	مُحاكاة موقع إلكتروني لجهة حكومية أو خاصة

تحليل البيانات الشخصية

يعتمد المحتالون على تقنيات الذكاء الاصطناعي في جمع وتحليل البيانات المتاحة عن المُستخدِمين؛ لبناء صورة دقيقة تساعد في تصميم رسائل احتيالية متوافقة مع اهتماماتهم وظروفهم.

مصادر البيانات الشائعة

01 المعلومات المنشورة عبر وسائل التواصل الاجتماعي

02 البيانات الوظيفية أو المهنية المتاحة علنًا

03 أنماط التفاعل الرقمي وسلوك الاستخدام

04 العلاقات الاجتماعية والمناسبات الشخصية المُعلَنة

الرسائل النصية المُولّدة بالذكاء الاصطناعي

تُصاغ هذه الرسائل باستخدام نماذج لُغوية ذكية تُحاكي أسلوب التواصل المحلي، وتُوجَّه للمستخدِم برسائل تبدو طبيعية وذات صلة مباشِرة بوضعه الشخصي أو الخدمي.

الأساليب المُستخدَمة

01

تخصيص محتوى الرسالة وَفْق اسم المستخدِم أو نشاطه

02

استخدام لغة مألوفة تُقلِّل من مستوى الشكّ

03

تضمين روابط أو تعليمات تبدو منطقية ومعتادة

مُحاكَاة الأسلوب اللُّغوي

يُوظَّف الذكاء الاصطناعي في تقليد أسلوب الكتابة الخاص بالمؤسسات أو الأشخاص الحقيقيّين، بما يشمل الصياغة الرسمية ونبرة الخطاب؛ لإضفاء مصداقية زائفة على الرسائل الاحتيالية.

الخصائص اللغوية المُستغَلَّة

- استخدام عبارات رسمية مُشابِهة للمراسلات الأصلية
- تقليد التوقيعات والأسلوب الإداري أو المهني
- محاكاة أسلوب أشخاص معروفين لدى الضحية
- تقليل الأخطاء التي قد تكشف الطابع الاحتيالي

استنساخ الصوت

تُستخدَم تقنيات الذكاء الاصطناعي في استنساخ أصوات أشخاص حقيقيّين، مثل: الأقارب أو المسؤولين؛ لإجراء مكالمات هاتفية تُقنِع الضحية بتنفيذ طلبات مالية أو إفشاء معلومات حساسة.

خصائص هذا الأسلوب

- محاكاة نَبْرة الصوت وطريقة الحديث بدقَّة عالية
- استغلال الثقة المُسبَقة في الصوت المألوف
- تقديم طلبات عاجلة تحت ذريعة الطوارئ
- تقليل فرص الشكّ أو التحقُّق
- صعوبة التمييز بين الصوت الحقيقي والمُزيَّف

التزييف العميق

يُستخدَم التزييف العميق (Deepfake) لإنشاء مقاطع فيديو تُظهِر أشخاصًا حقيقيّين وهم يُقدّمون طلبات أو تعليمات مزيَّفة، مُستغلّين الثقة البصرية كأداة إقناع فعّالة.

الأساليب المُستخدَمة

- تركيب وجوه وأصوات على مقاطع فيديو واقعية
- انتحال شخصيات قيادية أو معروفة
- إرسال الفيديوهات عبر تطبيقات المراسلة
- استغلال الصدمة أو المفاجأة لدفع الضحية للاستجابة

التكيُّف الآلي مع ردود الضحية

يعتمد المحتالون على أنظمة ذكية قادرة على تحليل ردود المستخدِم، وتعديل أسلوب التواصل تلقائيًّا؛ للحفاظ على استمرار التفاعل وتقليل الشكّ.

آليات التكيُّف

- تحليل نبرة الردود ومستوى التردُّد
- تغيير أسلوب الخطاب حسب تفاعُل الضحية
- زيادة الإلحاح أو التهدئة عند الحاجة
- تقديم مُبرّرات إضافية لإقناع المستخدِم
- تعديل السيناريو بما يتناسب مع مُجريات الحوار

تقليل المؤشرات التقليدية للتصيُّد الاحتيالي

يسهم الذكاء الاصطناعي في تقليل العلامات الشائعة التي كان يعتمد عليها المستخدِمون لاكتشاف الرسائل الاحتيالية؛ مما يجعل التمييز بين المحتوى الحقيقي والمزيّف أكثر صعوبةً.

وذلك من خلال

01 خلوّ الرسائل من الأخطاء اللغوية والإملائية

02 استخدام صياغة مُتَّسقة ومنطقية

03 تجنُّب العبارات المبالَغ فيها أو المكشوفة

04 محاكاة الأسلوب الرسمي أو الشخصي بدقَّة

استغلال الثقة في الأنظمة والردود المؤتمتة

يعتمد هذا الأسلوب على استثمار ثقة المستخدِم في الأنظمة الرقمية المؤتمتة، مثل الردود الآلية والمساعدات الافتراضية؛ لإضفاء طابع رسمي وتقني على عملية الاحتيال.

أساليب الاستغلال

01

الادّعاء بأن الرسالة صادرة عن نظام ذكي رسمي

02

استخدام مصطلحات تقنية لزيادة المصداقية

03

تقديم الطلب على أنه إجراء آلي إلزامي

04

تقليل فرص الاعتراض أو الاستفسار

05

توجيه المستخدِم لتنفيذ الإجراء دون تفاعُل بشري

توسُّع نطاق الهجمات وسرعة تنفيذها

يُمكِّن الذكاء الاصطناعي المحتالين من تنفيذ عدد كبير من الهجمات المُتقَنة في وقت قصير، مع الحفاظ على مستوى عالٍ من الجودة والإقناع.

مظاهر التوسُّع

- تنفيذ هجمات مُتعدّدة في وقت متزامن
- استهداف فئات مختلفة برسائل مُخصَّصة
- تقليل الجهد البشري المطلوب للتنفيذ
- زيادة سرعة الانتشار عبر القنوات الرقمية
- صعوبة تتبُّع مصدر الهجمات

التمييز بين المحتوى الحقيقي والمزيَّف

مع تطوُّر تقنيات الذكاء الاصطناعي، أصبح من الصعب الاعتماد على الشكل أو الأسلوب وحده للتمييز بين المحتوى الحقيقي والاحتيالي؛ ما يرفع مستوى الخطورة التي يواجهها المستخدِمون.

مُبرّرات الصعوبة

- محاكاة دقيقة للأسلوب اللغوي والبصري
- غياب الأخطاء التي كانت تكشف الاحتيال سابقًا
- تَطابُق المحتوى مع السياق اليومي للمستخدِم
- استخدام مصادر وسيناريوهات واقعية
- استغلال الثقة في التقنيات الحديثة

علامات التصيُّد الاحتيالي

تظهر علامات التصيُّد الاحتيالي في الرسائل أو المكالمات التي تهدف إلى دفع المستخدِم لاتخاذ إجراء سريع دون تحقُّق، مُستغلَّة الخوف أو الاستعجال أو الثقة الزائفة للحصول على معلومات حسَّاسة.

المؤشّرات الشائعة

- طلب عاجل لتحديث بيانات أو تأكيد معلومات
- استخدام لغة تُوحي بالتهديد أو إيقاف الخدمة
- فرض مُهْلة زمنية قصيرة للتفاعل
- مطالبة بتنفيذ إجراء غير معتاد
- غياب التفاصيل الواضحة أو الرسمية

مُؤشّرات المحتوى والروابط المشبوهة

يرتبط التصيُّد الاحتيالي غالبًا بروابط أو مرفقات تُستخدَم لنقل المستخدِم إلى صفحات مُزيَّفة أو تحميل محتوى ضار، مع مُحاكاة شكل المواقع أو الرسائل الرسمية.

أبرز العلامات

- روابط مُختصرة أو عناوين إلكترونية غير دقيقة
- اختلاف بسيط في اسم الجهة أو عنوان الموقع
- مرفقات غير متوقَّعة أو غير مُبرَّرة
- طلب إدخال معلومات حساسة عبر رابط خارجي
- غياب وسائل تواصُل رسمية للتحقُّق

02 المحور الثاني

الهندسة الاجتماعية

مفهوم الهندسة الاجتماعية

مجموعة من الحِيَل التي يستخدمها المحتال للتَّلاعب بالشخص نفسيًّا من أجل الحصول على معلومات سرية، دون الحاجة إلى تقنيات مُعقَّدة.

الركائز الأساسية لهذا النوع من الهجمات

- بناء علاقة ثقة مُزيَّفة مع الضحية
- استغلال حُسن النية والرغبة في المساعدة
- استخدام موقف اجتماعي أو عاطفي لدَفْع الشخص إلى التجاوب
- إدخال الضحية في حوارٍ يبدو طبيعيًّا، ثم التدرُّج بطلب المعلومات
- توظيف مواقف اجتماعية أو عاطفية لدفع الشخص إلى اتخاذ قرار غير مدروس
- الإيحاء بمعرفة سابقة أو اهتمام شخصي لتعزيز الانطباع المزيّف

الفرق بين الهندسة الاجتماعية والتصيُّد الاحتيالي

تُركِّز الهندسة الاجتماعية على التفاعل الإنساني المباشر، بينما يعتمد التصيُّد غالبًا على وسائط رقمية مثل الروابط أو الرسائل.

الاختلافات الأساسية

01 التصيُّد يتم عبر رسالة أو رابط إلكتروني، بينما الهندسة الاجتماعية تعتمد على المحادثة المباشرة

02 الهندسة الاجتماعية تُستخدم في الواقع اليومي، الهاتف، أو اللقاءات، أكثر من البريد الإلكتروني

03 المحتال في الهندسة الاجتماعية يُقدِّم نفسه على أنه شخص حقيقي يتفاعل معك

04 في الهندسة الاجتماعية يتم بناء الاحتيال على مراحل وليس في رسالة واحدة

استخدام العاطفة وسيلةَ ضَغْط

يعتمد المحتال في الهندسة الاجتماعية على إثارة مشاعر محدّدة لدى الضحية لدَفْعه إلى اتخاذ قرارات سريعة.

المشاعر الأكثر استخدامًا في هذا السياق

الخوف

من مشكلة قانونية، تهديد، أو تجميد حساب

الثقة

من خلال الحديث بلغة رسمية أو مهنية

الإلحاح

وضع الضحية تحت ضغط الوقت

الإحراج

من خلال طلب شخصي يصعب رفضه

العطف

بإظهار الحاجة الماسة للمساعدة

التدرُّج في الطلبات للوصول إلى الهدف

لا يبدأ المحتال بطلب كلمة المرور مباشرة، بل يستخدم أسلوبًا تدريجيًّا، يبدأ بأمور بسيطة، ثم ينتقل إلى ما هو حسّاس.

مراحل التـــــدرج

- يبدأ بطلب غير ضارّ مثل الاسم أو تأكيد رقم الهاتف
- يستمر بإظهار التعاون والاهتمام
- يطلب في الخطوة التالية تفاصيل أكثر دقة
- يُقدّم مُبرِّرات مُقنِعَة لكل طلب
- يُنهي المحادثة بعد حصوله على ما يريد دون إثارة الشك

انتحال صفة الموظفين والمتخصصين

يتقمَّص المحتال دور موظف في جهة معروفة، مثل البنك أو الدعم الفني؛ ليكسب ثقة الضحية بسرعة.

الصفات والوسائل المعتمدة

01 استخدام لغة متخصّصة تُوحي بالخبرة

02 ذِكْر أسماء جهات معروفة لإضفاء المصداقية

03 توفير "معلومات" عامة لإقناع الضحية بأنه يعرفه

04 الادعاء بوجود خطأ تقني يستوجب الدخول إلى الحساب

05 استخدام أدوات تكنولوجية مثل البريد الرسمي المزوّر أو عرض الشاشة

المقابلات الهاتفية والشخصية المُزيَّفة

يتم التواصل مع الضحية من خلال مكالمة هاتفية أو حتى لقاء شخصي مباشر، مع تقديم سيناريو مقنع.

الخصائص المتكررة

- يرتدي المحتال لباسًا رسميًّا أو يُعرّف بنفسه كموظف دعم
- يزور المنزل بحجة الصيانة أو متابعة اشتراك خدمي
- يطلب من الشخص إدخال رمز أو فتح جهازه لتحديث النظام
- يتظاهر بتقديم المساعدة الفنية لحلّ مشكلة معينة
- يغادر فور الحصول على البيانات أو الوصول إلى الجهاز
- الاتصال من خلال هاتف شخصي بدلًا من هاتف رسمي معرّف

حِيَل الدعم الفني الوهمي

يتصل المحتال، ويدّعي أنه من فريق الدعم الفني لشركة الهاتف أو مزوّد الإنترنت، ويتحدَّث بلغة فنية لإقناع الضحية.

الخطوات المعتادة في هذا الأسلوب

- الإشارة إلى مشكلة في الاتصال أو حساب الخدمة
- **طلب الدخول إلى جهاز الحاسوب أو الهاتف**
- استخدام أدوات تحكُّم عن بُعد (مثل تطبيقات الدعم)
- إقناع الضحية بإعطاء رموز أو كلمات مرور
- استخدام الجلسة للوصول إلى البيانات أو تغيير كلمات المرور

الهندسة الاجتماعية عبر تطبيقات المراسلة

تُستخدم تطبيقات مثل واتساب WhatsApp أو تيليجرام Telegram لبناء علاقة مُزيَّفة، ثم خداع الشخص لاحقًا، خاصةً في حالات التواصل الأولي.

المراحل التي يتبعها المحتال

- بَدْء الحديث باسم مستعار أو حساب مزيف
- التحدُّث بهدوء وودّ، مع خلق صلة اجتماعية
- استخدام صور وعبارات تُوحي بالثقة
- الانتقال إلى الحديث عن "فرصة"، "مشكلة"، أو "طلب مساعدة"
- تقديم طلب مباشر للحصول على المال أو البيانات

03 المحور الثالث

الوقاية من التصيُّد الاحتيالي والهندسة الاجتماعية

المبادئ العامة للوقاية الرقمية

الوعي بأن الخداع لا يأتي دائمًا من جهات مجهولة، بل قد يصدر عن أطراف تتحل صفة أقارب أو مؤسسات موثوقة

التوقُّف للحظة والتفكير قبل اتخاذ أيّ إجراء

عدم التفاعل السريع مع الرسائل أو المكالمات غير المتوقعة

الرجوع إلى العائلة أو شخص موثوق عند الشك

تجنُّب مشاركة المعلومات إلا بعد التأكُّد من هوية الطرف الآخر

الوقاية من التصيُّد الاحتيالي المدعوم بالذكاء الاصطناعي

تتطلَّب الوقاية من التصيُّد الاحتيالي باستخدام الذكاء الاصطناعي مستوًى مُتقدّمًا من الوعي الرقمي، وعدم الاكتفاء بالثقة في شكل الرسالة أو أسلوبها؛ نظرًا لقدرة هذه التقنيات على محاكاة التواصل الحقيقي بدقَّة عالية.

إجراءات وقائية أساسية

- تجنُّب مشاركة أي معلومات حساسة دون تأكُّد
- عدم الاستجابة الفَوْرية للرسائل أو المكالمات غير المتوقَّعة
- الشكّ في الرسائل شديدة الإقناع أو المخصَّصة بدقَّة
- التحقُّق من مصدر الطلب عبر قنوات رسمية مُستقلَّة
- اعتماد التمهُّل كخطوة أُولَى قبل أي تفاعُل

الوقاية من التزييف العميق (Deepfake)

يُعدّ التزييف العميق من أخطر تطبيقات الذكاء الاصطناعي في الاحتيال، إذ يعتمد على خداع المستخدم بصريًّا عبر مقاطع فيديو تبدو واقعية؛ ما يستدعي الحذر وعدم الاعتماد على المظهر وحده.

أساليب الوقاية

- عدم الاعتماد على الفيديو وحده كمصدر موثوق
- التحقُّق من أي طلب عبر اتصال مباشِر مُستقل
- الانتباه للحركات غير الطبيعية أو اختلاف نبرة الصوت
- عدم الوثوق بمقاطع الفيديو التي تتضمَّن طلبات عاجلة
- الإبلاغ عن المقاطع المشبوهة للجهات الرسمية المختصَّة

الوقاية من الاحتيال الهاتفي

تعتمد عمليات استنساخ الصوت على تقليد أصوات أشخاص موثوقين؛ ما يجعل المكالمة الهاتفية أداة خداعٍ قوية تستوجب الحذر وعدم الاستجابة العاطفية.

إجراءات الحماية

01 عدم تنفيذ أي طلب مالي عبر مكالمة هاتفية

02 إنهاء المكالمة والاتصال بالشخص الحقيقي مُباشرةً

03 عدم الوثوق بالمكالمات العاجلة غير المعتادة

04 عدم مشاركة رموز التحقُّق أو المعلومات الشخصية

الوقاية من المحتوى التفاعلي المزيَّف

تستغلّ الرسائل التفاعلية المدعومة بالذكاء الاصطناعي ثقة المستخدِم في المحادثات الطبيعية؛ ما يتطلَّب وعيًا مستمرًّا بأساليب الخداع الحديثة.

ممارسات وقائية

- عدم مشاركة البيانات عبر المحادثات الفَوْرية
- التحقُّق من الحسابات قبل التفاعل معها
- تجنُّب الروابط المُرسَلة ضمن سياق محادثة طويلة
- الحذر من الوثوق السريع بالعلاقات الافتراضية مع الغرباء
- التحديث المعرفي المستمر بأساليب الاحتيال المُتطوّرة

التأكّد من هوية المرسِل أو المتصل

غالبية عمليات الاحتيال تبدأ من جهة مجهولة تدّعي أنها معروفة. ولهذا فإنّ التحقّق من هوية الطرف الآخر يُعدّ أمرًا أساسيًّا.

أساليب تساعد على التحقق من الهوية

- مراجعة الرقم الهاتفي عبر محركات البحث أو التواصل مباشرة مع الجهة الرسمية
- الاعتماد على المصادر الرسمية فقط، مثل المواقع المعتمدة أو أرقام خدمة العملاء
- التأكّد من أن البريد الإلكتروني أو الحساب الرقمي تابع فعليًّا للجهة التي يدّعيها المرسِل
- الانتباه للفروق الدقيقة في أسماء الحسابات، العناوين، أو أسلوب الصياغة
- طرح أسئلة لا يمكن الإجابة عنها إلا من الطرف الحقيقي

التعامل مع الروابط والمرفقات

تُستخدم الروابط كأدوات خفية لنقل الشخص إلى صفحات مُزيَّفة أو تحميل برمجيات ضارَّة، لذلك من الضروري الانتباه قبل التفاعل معها.

الاحتياطات التي تتعلّق بالروابط والمرفقات

- عدم الضغط على الروابط في الرسائل المجهولة
- فَحْص الرابط بالنظر إلى بدايته (https) وتطابقه مع العنوان الأصلي
- فتح المواقع عبر الكتابة اليدوية بدلًا من النقر
- استخدام برنامج حماية (مضاد فيروسات) للمساعدة في الكشف عن التهديدات
- حذف الرسائل التي تحتوي مرفقات غير معروفة المصدر

خطوات وقائية على المستوى الشخصي

تطبيق عدد من العادات اليومية البسيطة يمكن أن يُقلِّل من احتمالية الوقوع ضحية للهندسة الاجتماعية والتصيُّد الاحتيالي.

ممارسات شخصية مفيدة للحماية

- عدم حفظ كلمات السر في دفاتر أو أوراق مكشوفة
- استخدام أرقام سرية لا ترتبط بالاسم أو تاريخ الميلاد
- تعيين كلمات مرور طويلة ومُعقّدة، والحرص على تغييرها بصفة دورية
- عدم الحديث عن الأمور المالية أو البنكية مع أيّ شخص مجهول
- تجنُّب نشر معلومات خاصة على الحسابات العامة في الإنترنت

التحقُّق من الرسائل والمكالمات قبل التفاعل

تعتمد الرسائل والمكالمات الاحتيالية على خلق شعور بالاستعجال أو الخوف لدى الضحية، لذلك فإن التمهّل والتحقّق يُفْقِد المحتال عنصر الضغط الذي يعتمد عليه.

أساليب عملية للتحقق

- التواصل مع الجهة المزعومة عبر رقمها الرسمي قبل أيّ تفاعل
- عرض الرسالة أو المكالمة على أحد أفراد العائلة للمراجعة
- البحث عن محتوى الرسالة أو الرقم عبر الإنترنت للتحقّق من سُمعته
- تحليل أسلوب الخطاب: هل يتضمّن تهديدًا، استعجالًا، أو عاطفة مُفرِطة؟
- عدم الاستجابة لأيّ طلب مالي صادر عن شخص غير معروف شخصيًّا

حماية الحسابات الشخصية

يستهدف المهاجمون الحسابات البنكية، والبريد الإلكتروني، ومنصات التواصل الاجتماعي، باعتبارها بوابات للوصول إلى معلومات حساسة أو أموال.

خطوات عملية لتعزيز حماية الحسابات

- استخدام كلمات مرور قوية تجمع بين الحروف والأرقام والرموز
- تفعيل خاصية التحقق بخطوتين كلما أمكن
- تجنُّب تسجيل الدخول من أجهزة أو شبكات عامة
- تسجيل الخروج بعد استخدام الحسابات في الأماكن المشتركة
- تحديث كلمات المرور بانتظام وعدم إعادة استخدامها عبر أكثر من حساب

التعامل مع محاولات الدعم الفني المُزيَّفة

بعض المحتالين يتواصلون على أنهم من فِرَق الدعم الفني لمزوّدي الإنترنت أو الخدمات الرقمية.

الإشارات التي تدل على أن الدعم مُزيَّف

- الاتصال غير المسبق من شخص يطلب التحكم بجهازك
- الطلب الفوري باستلام كلمات مرور أو رموز تحقُّق
- التحدث بلُغة تقنية مُفْرِطة لإرباك المستمع
- الإصرار على تنفيذ خطوات معينة بسرعة
- عدم وجود توثيق رسمي للطلب أو للمكالمة

التصرُّف عند الشك بعملية احتيال

عند الشعور بأن الرسالة أو الاتصال غير طبيعي، هناك خطوات يمكن اتباعها لتجنُّب الضرر أو التفاعل مع الهجوم.

الإجراءات الأساسية عند الاشتباه

- إنهاء المكالمة أو حذف الرسالة فورًا
- عدم الرد أو فتح الروابط المُصاحِبة
- التواصل مع أحد الأبناء أو الأقارب لمراجعة الوضع
- الإبلاغ عن الحادثة للجهات المعنية
- مراقبة الحسابات البنكية والإلكترونية؛ للتأكد من عدم التلاعب بها

تثقيف النفس بشكل مستمر

التهديدات الرقمية تتطور باستمرار، ومن المهم أن يبقى الشخص على معرفة مستمرة بالأساليب الجديدة التي يستخدمها المحتالون.

طرق بسيطة للبقاء على اطلاع

- متابعة نشرات توعية من مؤسسات رسمية
- المشاركة في جلسات توعية أو ورش عمل محلية
- قراءة المقالات المبسطة التي تتناول الموضوع
- الاستفادة من أفراد العائلة في شرح المصطلحات الجديدة

المراجع

1. Cybersecurity and Infrastructure Security Agency (CISA). Malware, phishing, and ransomware., on site: https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware
2. Cybersecurity Asia. The rise of cyber crime targeting older adults., on site: https://cybersecurityasia.net/rise-cyber-crime-targeting-older-adults/
3. Dey, Saswata et al. AI-powered phishing detection: Integrating natural language processing and deep learning for email security. World Journal of Advanced Engineering Technology and Sciences. December 2023. On site: https://wjaets.com/node/2428
4. Ernest, Nonum et al. Social Engineering: Understanding Human Factors in Cyber Security. International Journal of Convergent and Informatics Science Research, May 2025, on site: https://harvardpublications.com/hijcisr/article/view/326

5. Federal Trade Commission (FTC). Fake prize, sweepstakes, and lottery scams., on site: https://consumer.ftc.gov/articles/fake-prize-sweepstakes-and-lottery-scams

6. Kosinski, Matthew. IBM. What is phishing?, on site: https://www.ibm.com/think/topics/phishing

7. National Cyber Security Centre (NCSC). Phishing., on site: https://www.ncsc.gov.uk/guidance/phishing

8. National Cyber Security Centre (NCSC). Spot phishing scams., on site: https://www.ncsc.gov.uk/collection/phishing-scams/spot-scams

9. U.S. General Services Administration, Office of Inspector General (GSA OIG). Scam Alert: Beware of fake websites that mimic legitimate official U.S. government websites., on site: https://www.gsaig.gov/news/scam-alert-beware-fake-websites-mimic-legitimate-official-us-government-websites

10. University of Florida. Deepfake Phishing. On site: https://it.ufl.edu/security/learn-security/deepfakes/deepfake-phishing/

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

للتواصل مع الأكاديمية الوطنية للأمن السيبراني

16555 - 40466379 - 51045944

www.ncsa.gov.qa academy@ncsa.gov.qa