الأولمبياد الدولية
للأمن المالي

الجانب المظلم
للذكاء الاصطناعي

#الذكاء الاصطناعي

الذكاء الاصطناعي Artificial intelligence

أنظمة حاسوبية قادرة على أداء مهامّ يستطيع الذكاء البشري القيام بها

الذكاء الاصطناعي هو مجموعة من التقنيات التي تُمكّن الأنظمة من:

- فهم الطلبات المصاغة باللغة الطبيعية
- تحليل البيانات والتعامل معها واستخلاص المعلومات المطلوبة
- تمييز الأنماط والرموز والصور
- التعلّم من كميات ضخمة من البيانات
- اتخاذ القرارات والتكيّف مع ظروف مختلفة

مجالات تطبيق الذكاء الاصطناعي

القطاع المصرفي

- الاستثمار التلقائي
- التقييم الائتماني وتقدير المخاطر
- اتخاذ القرارات بسرعة وكفاءة

الطب والرعاية الصحية

- خطط علاجية فردية
- تطوير أدوية جديدة
- تحليل البيانات

البحث العلمي

- الكشف السريع عن الأنماط
- تسريع الأبحاث
- إيجاد حلول قائمة على التحليل

التعليم

- تكييف المحتوى حسب الطالب
- كشف فجوات المعرفة
- إعداد مهام إضافية

حماية الأمن السيبراني

مواجهة الذكاء الاصطناعي لعمليات الاحتيال

- يكشف المخططات الاحتيالية ويُحبطها
- يخفّف الضغط عن الضحايا الحقيقيين

مثال :"الجدّة السيبرانية " ـــنموذج ذكاء اصطناعي تابع لشركة اتصالات

- تتواصل مع المحتالين باسم عميل المسنّ
- تُلهي المحتالين عن الضحايا الحقيقيين، وتستنزف وقتهم ومواردهم

الجانب الآخر للذكاء الاصطناعي

مجال عالي الخطورة

- تزايد عدد الضحايا من القُصَّر
- هجمات عبر المكالمات والرسائل (بصفة المدارس والجهات الحكومية وشركات الاتصالات)
- الاحتيال عبر حسابات اللاعبين امتحانات الدولة الرسمية

المخاطر المالية

- تزايد الاحتيال السيبراني باستخدام الذكاء الاصطناعي
- سرقة الأموال والبيانات
- أتمتة المخططات الإجرامية

مكافحة

- الهيئة الفيدرالية للرقابة المالية في روسيا
- أجهزة الاستخبارات المالية في دول رابطة الدول المستقلة
- المجموعة الأوراسية لمكافحة غسل الأموال وتمويل الإرهاب

محاولات احتيال تمّ إحباطها

222
مليار روبل
نوفمبر 2025

عمليات دون موافقة العملاء

21
مليار روبل
9أشهر من عام 2025

27,5
مليار روبل
عام2024

غسل الأموال

الاحتيال السيبراني

حسابات مصرفية وهمية

تحويلات متكرّرة ودمج الأموال

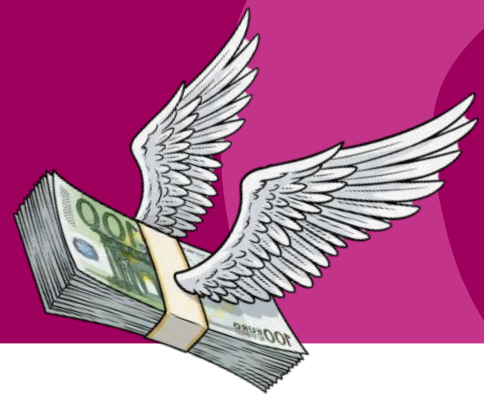
تمويه التدفقات المالية

منصّات العملات المشفّرة

إضفاء الشرعية على العائدات غير المشروعة /تمويل الأنشطة الإجرامية

يُعدّ التهديد عابرًا للحدود

من هو «الدروبّر »؟



الدروبّر

شخص يستغل بطاقاته المصرفية لسحب الأموال المسروقة أو تمريرها إلى جهات أخرى

توريط الشباب

طرق الاستدراج (حيل نفسية):

- **الإلحاح** — «الفرصة متاحة اليوم فقط»
- **التبسيط** — «الأمر سهل ويمكن لأي شخص القيام به»
- **إيهام الشرعية** — «كل شيء قانوني»
- **التدرّج** — البدء بمبالغ صغيرة ثم زيادتها تدريجيًا
- **التأثير الاجتماعي** — «المئات يعملون معنا بالفعل»

الفئات التي يتم توريطها

- مراهقون ابتداءً من سنّ 14عامًا
- الطلاب في المدارس والجامعات
- العاطلون عن العمل

أكثر من مليون دروبّر

حجم المشكلة في روسيا

وفقًا لبيانات البنك المركزي الروسي

المسؤولية القانونية

ممارسة إنفاذ القانون

- في عام 2025فُتِحَت أول قضية جنائية ضدّ مُنظّم شبكة دروبّرات
- التعاون مع وزارة الداخلية يُعدّ أساسًا للإعفاء من المسؤولية
- تمّ الكشف عن المنظّم استنادًا إلى إفادات دروبّر مُوقوف

مسؤولية جنائية مباشرة

أُقرّت بشأن مخططات الدروبّر ضمن التعديل على المادة 187من القانون الجنائي الروسي

العقوبة الجنائية

- **السجن لمدة تصل إلى 3 سنوات** —مقابل نقل البيانات المصرفية
- **السجن لمدة تصل إلى 6 سنوات** —للمنظّمين (مديري شبكات الدروبّرات)

الديب فيك :تهديد جديد

الديب فيك

(من الإنجليزية: **Deepfake** - «التزييف العميق»)

فيديوهات أو تسجيلات صوتية أو صور ينشئها الذكاء الاصطناعي، يظهر فيها شخص وهو يقوم بأفعال أو يقول أشياء لم تحدث في الواقع

كيف تعمل هذه التقنية:

- مكالمات تحت غطاء استطلاعات الرأي مع تسجيل الصوت
- يقوم الذكاء الاصطناعي بنسخ ملامح الوجه والصوت
- إنشاء ديب فيك صوتي

تكفي بضع ثوانٍ من التسجيل لإنتاج ديب فيك صوتي

أول قضية بارزة

عام 2019، المملكة المتحدة

استخدم المحتالون الذكاء الاصطناعي لنسخ صوت المدير التنفيذي لشركة طاقة

آلية الهجوم

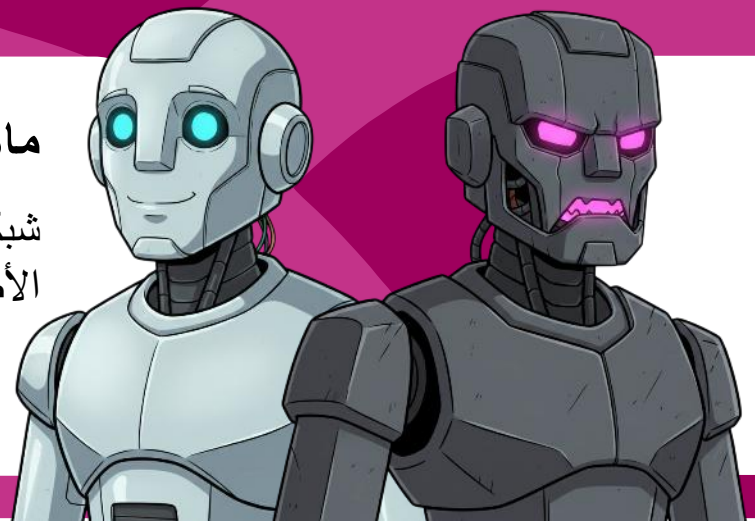
يتصل «صوت المدير» بأحد موظفيه

ويصدر تعليمات عاجلة بتحويل مبلغ مالي إلى أحد المورّدين

€220 000

تمّ تحويلها إلى حسابات المحتالين

«التوأم الشرير» (Evil Twin)



ما يتم سرقته

- أسماء المستخدمين وكلمات السر
- بيانات البطاقات المصرفية
- المراسلات وسجلّ التصفّح

ماهية الهجوم

شبكة Wi-Fi مزوّرة تُحاكي الشبكة الأصلية

كيف تعمل هذه الآلية

التصيّد الاحتيالي
صفحة دخول مزيّفة

Man-in-the-Middle
اعتراض كامل لحركة البيانات

اتصال الضحية بالشبكة
في المقاهي والمطارات ومراكز التسوّق

استنساخ الشبكة
الاسم نفسه (SSID) مع إشارة أقوى

هجوم «التوأم الشرير» في المطار

السيناريو:

- اتصلت تلميذة بشبكة Wi-Fi تحمل اسم المطار
- كانت الشبكة في مقدّمة القائمة
- وتبيّن أن الرمز كان كلمة مرور لمرة واحدة

الأخطاء الجسيمة:

- تجاهل التحذيرات من أن الشبكة غير آمنة
- إدخال رقم الهاتف
- إدخال رمز التحقّق المرسل عبر تطبيق المراسلة

النتيجة:

- فقدان الوصول إلى حسابها في تطبيق المراسلة
- تعريض البيانات الشخصية للاختراق

هامّ!

لا تُستخدم رموز التحقّق الواردة عبر تطبيقات المراسلة عند التسجيل في شبكة Wi-Fi

التصيّد الاحتيالي بالذكاء الاصطناعي (AI-Phishing)

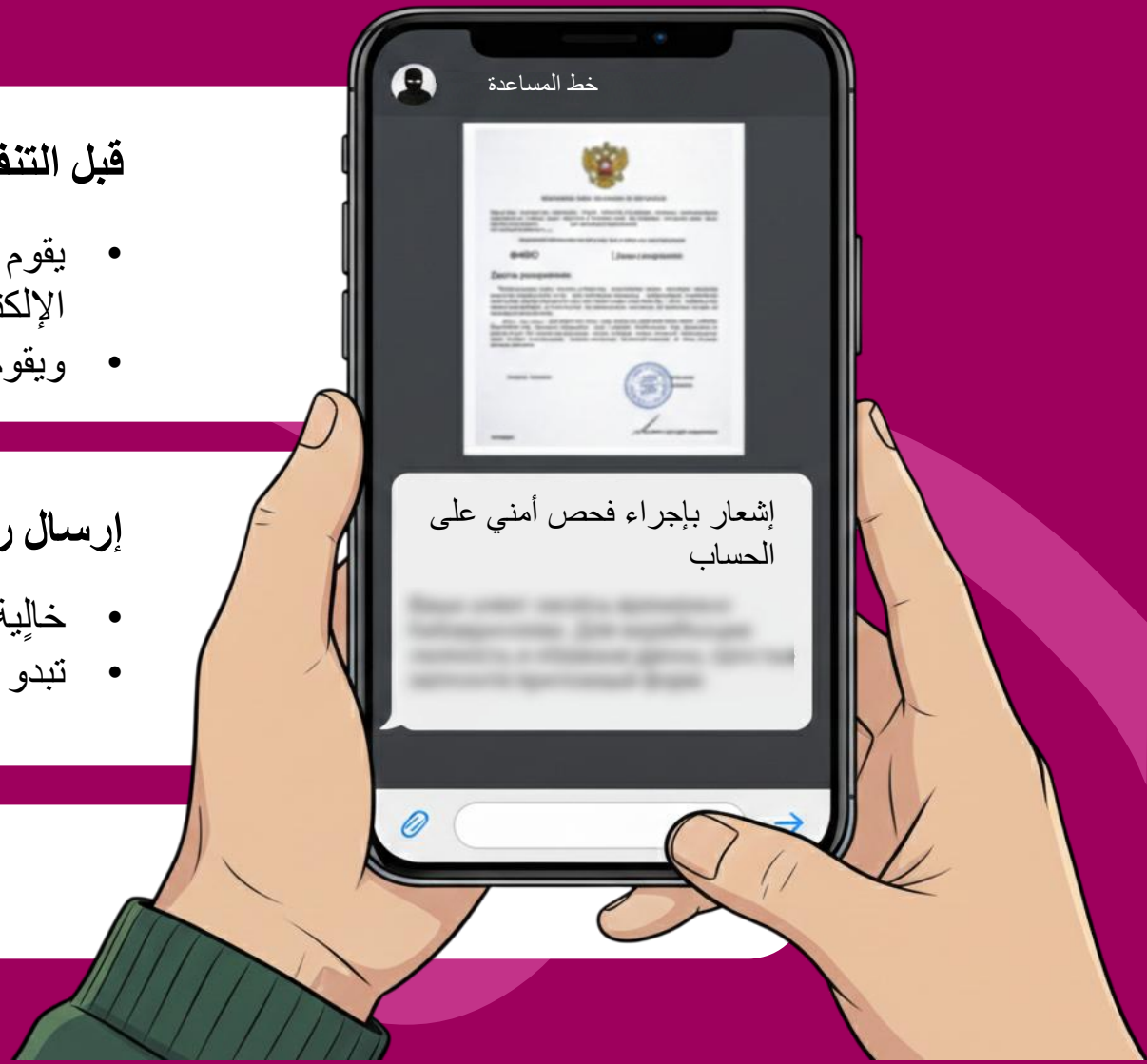
قبل التنفيذ

- يقوم الذكاء الاصطناعي بتحليل بيانات من وسائل التواصل الاجتماعي والمواقع الإلكترونية والتسريبات
- ويقوم بتوليد رسائل ومراسلات مُحكمة الصياغة تبدو مقنعة

إرسال رسالة شخصية

- خالِية من الأخطاء والعبارات النمطية
- تبدو وكأنها مراسلة رسمية حقيقية

النتيجة ـــ خسارة الأموال



الفيشينغ الصوتي بالذكاء الاصطناعي (AI Vishing)

الاحتيال الصوتي باستخدام الذكاء الاصطناعي

مصطلح إنجليزي مركّب من Voiceو Phishingويعني »التصيّد الصوتي«

- نسخة صوتية من تقنية التزييف العميق
- يقوم الذكاء الاصطناعي بنسخ الصوت اعتمادًا على بضع ثوانٍ من التسجيل
- ويتيح إجراء حوار مباشر مع الضحية

يجعل الذكاء الاصطناعي الاحتيال يبدو واقعيًا للغاية

الاحتيال العاطفي

آلية الاحتيال

- يدير الذكاء الاصطناعي محادثات مع آلاف الأشخاص في الوقت نفسه
- ويخلق وهم الثقة، مستفيدًا من بيانات وسائل التواصل الاجتماعي لتخصيص التواصل

كيف تعمل هذه الآلية

استعراض «النجاح» من خلال الصور ولقطات الشاشة الهدايا

→

عرض فرص استثمارية
رهانات، عملات مشفّرة، مخططات هرمية

→

مراسلات
أسئلة شخصية
رسائل صوتية

الأمان في شبكات Wi-Fi العامة

تجنّبوا إدخال كلمات السر وبيانات البطاقات عبر الشبكات العامة

إذ يمكن لشبكات Wi-Fi العامة اعتراض حركة البيانات

تجنّبوا استخدام الشبكات غير الآمنة

غالبًا ما تكون شبكات «التوأم الشرير» مفتوحة

انتبهوا إلى التحذيرات

فهي تشير إلى وجود تهديد حقيقي

استخدموا المواقع التي تعمل ببروتوكول HTTPS فقط

رمز القفل يشير إلى أن الاتصال محميّ بتشفير شامل (من طرف إلى طرف)

فعّلوا المصادقة متعددة العوامل (MFA)

كلمة مرور +رمز تحقّق لمرة واحدة

لا داعي للذعر!

طريقة بسيطة وفعّالة للحماية من تزييف الصوت بالذكاء الاصطناعي

1. **أغلقوا المكالمة** عند أول شكّ
2. **أعيدوا الاتصال بالقريب أو الصديق** عبر الرقم المحفوظ في جهات الاتصال للتحقّق
3. **استخدموا كلمة سرّ** عائلية لتأكيد الهوية
4. **اطرحوا أسئلة شخصية** لا يعرفها إلا المقرّبون

(مثل: «ما اسم كلبنا؟»)

التزموا بالنظافة الرقمية!

حافظ على توازنك العاطفي

- أيّ معلومة تثير مشاعر قوية وتدفعك إلى اتخاذ إجراء فوري غالبًا ما تكون خدعة
- ناقش الأمر مع شخص مقرّب منك

كيف تحمي صوتك من الاستنساخ بالذكاء الاصطناعي

- **اجعل الوصول إلى حساباتك في وسائل التواصل الاجتماعي** مقتصرًا على الأصدقاء فقط
- **لا تنشر تسجيلات** صوتك في الأماكن العامة

(مثل المنشورات المؤقتة والبث المباشر)

التفكير النقدي هو خطّ الدفاع الأوّل

تذكّروا :المؤسسات الحكومية (مثل البنك المركزي أو الجهات الأمنية أو السلطات الضريبية)لا تناقش قضايا مهمّة عبر الهاتف

اقطع التواصل مع أي جهة تثير الشك

كيف تتصرّف عند التعرّض للاحتيال

- **لا تحوّل أي أموال** إلى شخص لم تلتقِ به وجهًا لوجه
- عند الحاجة، **أبلغ الجهات المختصّة** وإدارة المنصّة
- **أنهِ المكالمة** فور الحديث عن المال أو الرهانات أو العملات المشفّرة
- **فكّر بعقلانية** ولا تتسرّع
- **قم بحظر** المحتال فورًا

الاحتيال العاطفي هو لعبة تقوم على استغلال الثقة،

وفي النهاية تكون أموالك هي الثمن

الدروبّرات وسطاء في المخططات المالية الاحتيالية

من هم الدروبّرات؟

- أشخاص يستقبلون أموالًا مسروقة
- يقومون بتحويلها أو سحبها لصالح منظّمي المخطّط
- يسلّمون بطاقاتهم مع بيانات الدخول إلى الخدمات المصرفية عبر الإنترنت

يشارك الدروبّرات في جريمة جنائية

حيازة أو نقل بطاقة مصرفية من قبل أشخاص لا يُعدّون عملاء لدى البنك — «وتُعاقَب هذه المخالفة بالسجن لمدة تصل إلى 6 سنوات مع فرض غرامة مالية

المادة 187من القانون الجنائي للاتحاد الروسي» :التداول غير المشروع لوسائل الدفع«

إحصاءات حول ظاهرة الدروبّرات في روسيا

الدروبّرات يشكّلون حلقة محورية في إضفاء الشرعية على الأموال المسروقة

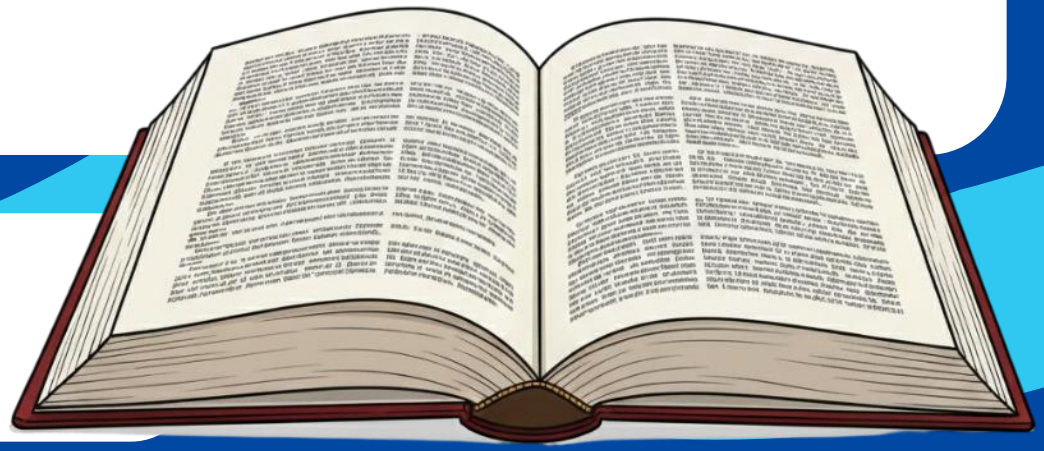
يمكن أن يُحالوا إلى المسؤولية الجنائية بموجب **المادة 174 من القانون الجنائي للاتحاد الروسي «إضفاء الشرعية (غسل الأموال) على أموال أو ممتلكات أخرى حصل عليها آخرون بطرق غير مشروعة»**

> 1 مليون

عميل من الدروبّرات في البنوك

~ 20%

من المراهقين غير مدركين للعواقب



الوعي والحذر أمران في غاية الأهمية

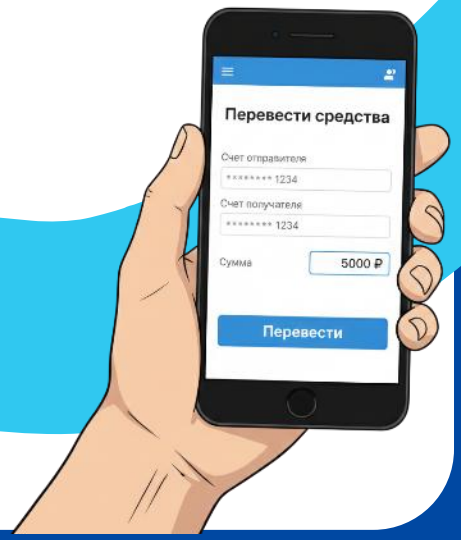
أنواع الدروبّرات حسب وظائفهم

الساحبون نقدًا

- يسحبون الأموال من أجهزة الصرّاف الآلي ←
- ثم يسلّمونها للمنظّمين

الناقلون

- يتلقّون تحويلات ←
- ويُعيدون توجيهها إلى حسابات أو محافظ أخرى



المودِعون

- يستلمون أموالًا نقدية ←
- يُودِعونها في الحساب ←
- ثم يُحوّلونها إلى جهات أخرى

استدراج الدروبّرات باستخدام الذكاء الاصطناعي

آلية عمل المخطّط

استهداف الفئات الهشّة اجتماعيًا
(كالطلاب، والعاطلين عن العمل، والباحثين عن مصدر دخل سريع)

تقوم **الشبكات العصبية و NLP** بتحليل البيانات المتاحة علنًا (من الشبكات الاجتماعية والمنتديات والأسواق الإلكترونية)

التواصل الأوّلي
(باستخدام روبوتات المحادثة وصور رمزية مُولَّدة بتقنية التزييف العميق)

تحليل الجوانب النفسية للضحية
(المنشورات وأسلوب التواصل ← مدى القابلية للتأثير والطمع)

«فرصة ربح سهلة»

سيناريو نمطي:

- لا يتطلّب خبرة أو مؤهلات
- العمل من المنزل لمدة ساعتين إلى ثلاث ساعات يوميًا
- شرط أساسي :وجود بطاقة مصرفية أو حساب للخدمات المصرفية عبر الإنترنت

قد ينخرط الشخص، من غير وعي، في دور الدروبّر ويصبح شريكًا في جريمة

«تحويل بالخطأ»

آلية عمل المخطّط

تحويل الأموال إلى الحسابات التي يحدّدها المحتالون

اتصال هاتفي يطلب بشكل عاجل إعادة المبلغ إلى «الحساب الصحيح»

يصل مبلغ إلى الحساب على أنه تحويل تمّ بالخطأ

أرسلت المبلغ بالخطأ، رجاءً حوّله على هذا الرقم

رسالة SMS من: رقم غير معروف
المبلغ: 50,000 روبل

الحلّ الصحيح الوحيد:

- المبادرة إلى التواصل مع البنك فورًا
- والالتزام الكامل بتعليماته

«مسؤول اليانصيب»

ما يحدث في الواقع:

- يصبح الشخص المُستقطَب دروبّرًا دون أن يدرك ذلك
- الأموال الموجودة على البطاقة هي أموال مسروقة من ضحايا آخرين
- تُصنَّف التحويلات على أنها »جوائز«، لكنها تُحوَّل في الواقع إلى:
  —دروبّرات آخرين أو أشخاص مُستخدَمين كواجهة
  —أو مباشرةً إلى المحتالين

كيف تتمّ الاستدراج:

- عرض «عمل تقني»
- المهمّة: توزيع الجوائز المالية على «الفائزين»

الدور المحوري للدروبّر:

- يقسّم التدفقات المالية غير المشروعة ويُموّه مسارها
- ويُعقّد بشكل كبير كشف المخطّط من قبل البنوك والجهات المختصّة

الاستدراج عبر وسائل التواصل الاجتماعي

كيف تتمّ عملية الاستدراج:

- استخدام حساب يبدو حقيقيًا مع صور مسروقة
- إرسال رسائل تعرض عملًا جانبيًا أو مساعدة في «مشروع اجتماعي»
- إقناع الضحية بأن الأمر قانوني
- طلب تحويل الأموال عبر بطاقته المصرفية الشخصية

كيف يتم اختيار الضحية:

- يحلّل الذكاء الاصطناعي حسابات وسائل التواصل الاجتماعي، مثل المنشورات عن البحث عن عمل أو المشاركة في السحوبات
- ويتم اختيار الأشخاص الأكثر عرضة للاستغلال

القصص الوهمية الشائعة:

- «مسؤول عن إدارة التبرّعات»
- مساعد لأحد صُنّاع المحتوى على المنصّات الرقمية
- متطوّع يتولّى استقبال التبرّعات

لا تعتمد أي جهة قانونية على بطاقة شخص غير مرتبط بها رسميًا

المسؤولية الجنائية في روسيا الاتحادية

المواد التي تنصّ على العقوبة عن نشاط الدروبّرات:

- **المادة** 174 من القانون الجنائي لروسيا الاتحادية «إضفاء الشرعية (غسل الأموال) على أموال أو ممتلكات أخرى حصل عليها آخرون بطرق غير مشروعة»
- **المادة** 187 من القانون الجنائي لروسيا الاتحادية «التداول غير المشروع لوسائل الدفع»
- **المادة** 159 من القانون الجنائي لروسيا الاتحادية «الاحتيال»

تذكّر الأهمّ:

- **الدروبّرية** ليست فرصة ربح، بل **فعل مُجرَّم قانونًا**
- **وتشمل المسؤولية** الجنائية المنظّمين و**المشاركين** على حدّ سواء

قواعد السلامة

في حال ملاحظة مؤشرات على الاستدراج:

- أوقف جميع أشكال التواصل مع المحتالين
- لا تُحوّل أي أموال، حتى لو استلمت تحويلًا مشبوهًا
- قم بحظر بطاقتك المصرفية وأبلغ البنك فورًا
- احتفِظ بنسخ من المراسلات والبيانات المصرفية وأرقام المحتالين
- توجّه إلى الجهات المختصّة وأبلغها بالواقعة

كل عروض «الربح السهل» تثير الشك

وخاصةً إذا طُلِب منك تقديم بيانات شخصية أو منح الوصول إلى بطاقاتك المصرفية

التاريخ والخصائص

3يناير 2009

تمّ توليد أول كتلة في شبكة بيتكوين

ما هي العملة المشفَّرة:

- أموال رقمية تعمل من دون تدخل البنوك المركزية أو الجهات الحكومية
- تعتمد على تقنية البلوك تشين —وهي سجلّ لامركزي للمعاملات

أهمّ الأصول المشفَّرة لعام 2026

نموّ استثنائي في القيمة:

العائد في الماضي ≠عائدًا في المستقبل

الروبل الرقمي vs العملات المشفَّرة

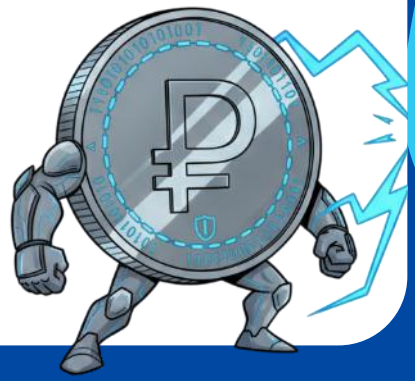
العملات المشفَّرة

- لامركزية —لا تخضع لرقابة موحّدة من قبل الدول أو البنوك
- تُستخدم كأصل أو ممتلكات، وليست دائمًا وسيلة دفع قانونية
- ذات طابع مستعار — (Pseudonymous) ترتبط بعنوان محفظة عام، مع وجود مخاطر أمنية

أصلٌ لامركزيّ عالي التقلّب

الروبل الرقمي

- يكمّل وسائل الدفع النقدية وغير النقدية
- يخضع لإشراف البنك المركزي لروسيا الاتحادية، ويتم الوصول إليه عبر التطبيقات المصرفية والإنترنت البنكي
- يتطلّب إجراءات اعرف عميلك (KYC) الإلزامية للحدّ من الاحتيال وغسل الأموال



أصلٌ حكومي خاضع للرقابة

العملات المشفَّرة والاحتيال

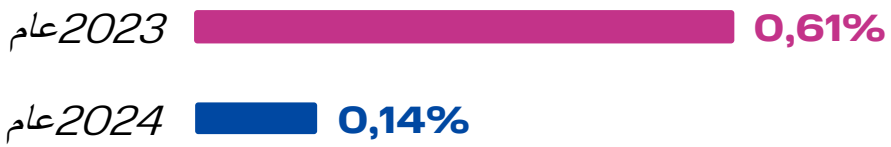
استخدامها في الأنشطة الإجرامية:

- الاتجار بالمخدرات، المقامرة غير المشروعة، وسرقة الملكية الفكرية
- غسل الأموال والمخططات الهرمية المالية
- استخدام العملات المشفَّرة كوسيلة لجمع الأموال والاستثمارات مع وعود بعوائد سريعة

تحظى العملات المشفَّرة بإقبال من الشباب،

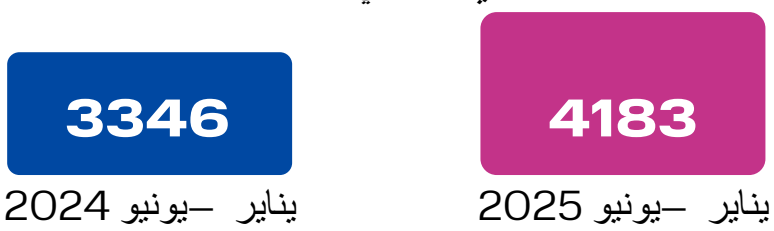
إلا أنها تُستخدم أحيانًا كوسيلة للاحتيال، خاصةً مع الاستعانة بالذكاء الاصطناعي لتحقيق انتشار واسع .

نسبة المعاملات الإجرامية



جهات يُشتبه في نشاطها غير القانوني

بيانات البنك المركزي الروسي



مخطّط الاحتيال الثلاثي عبر منصّات P2P

آلية عمل المخطّط

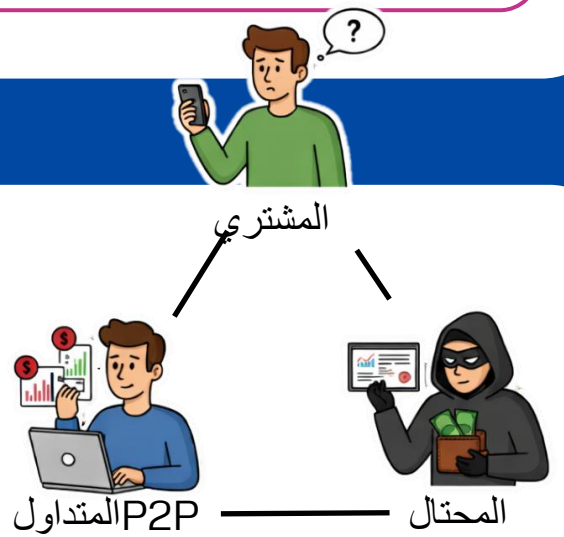
تحويل المبلغ إلى أحد متداولي P2P
شراء عملات مشفَّرة لصالح المحتالين

←

تغيير بيانات التحويل
بطاقة أحد متداولي P2Pبدلًا من بطاقة البائع

←

إعلان وهمي
عرض سلعة بسعر أقل من السعر المتداول في السوق



آليات تقليل المخاطر

- تحقّق من تقييمات وسجلّ المتعاملين قبل إتمام الصفقة
- اختر وسائل دفع موثوقة ومعتمدة
- بع السلع عبر منصّات تجارية موثوقة فقط

عملية احتيال عملة SQUID المشفَّرة

مؤشّرات الخطر

- عدم القدرة على بيع الرمز
- غياب الإدراج في منصّات التداول المعروفة
- وجود أخطاء واضحة في الموقع الإلكتروني

ماذا حدث

- رُوّج لرمز SQUID على أنه سيُستخدم في لعبة إلكترونية مستوحاة من مسلسل شهير
- **خلال يومين ارتفع سعره بنسبة 44,000٪ ليصل إلى 2,860 دولارًا**
- بعد ذلك انهارت قيمته إلى 0
- سحب المحتالون أكثر من 3 ملايين دولار، وتضرّر أكثر من 40,000 مستثمر

هامّ

- قبل الاستثمار، تحقّق من هوية القائمين على المشروع ومن المعلومات المتاحة عنه
- الحذر والتفكير النقدي = خطّ الدفاع الأوّل ضدّ الاحتيال المالي

مخطّط بيتكونكت الهرمي

آلية الاحتيال

- أموال المستثمرين الجدد ← تُستخدم لدفع «الأرباح» للمستثمرين السابقين ومنح المكافآت ← ثم تُحوَّل إلى جيوب المنظّمين

لم يكن هناك أي روبوت تداول فعلي

ضمان عوائد مرتفعة
+
مكافآت إحالة
=
مؤشّر واضح على احتيال مالي

آلية المخطّط

- التستّر كمنصّة عملات مشفَّرة تدّعي استخدام الذكاء الاصطناعي في التداول
- الوعد بأرباح مرتفعة مع مخاطر منخفضة للغاية
- برنامج إحالة يمنح عمولات تتراوح بين **15–7**٪ من ودائع المشاركين الجدد

النتائج

- تضرّر مستثمرون من أكثر من **40 دولة**
- تجاوزت الخسائر **17 مليون دولار**

مخطّط فينيكو الهرمي

السمات المميّزة

- جميع العمليات كانت تُجرى بعملة بيتكوين وTether
- كان إيداع الأموال بالعملات التقليدية (الفيات) محظورًا
- ازدادت شعبية المخطّط بفضل العروض الكبيرة التي بدت «مغرية»

آلية المخطّط

- الوعد بالتخلّص من القروض عبر الاستثمار
- الادّعاء باستخدام «نماذج رياضية» والذكاء الاصطناعي لتقليل المخاطر
- إمكانية شراء شقّة أو سيارة مقابل 35٪ فقط من قيمتها
- ودائع بعائد يتراوح بين 20–30٪ شهريًا

عوائد مرتفعة + عدم إمكانية استخدام الأموال التقليدية = مؤشّر واضح على الاحتيال

قواعد السلامة

مؤشّرات المخطّطات الهرمية المالية

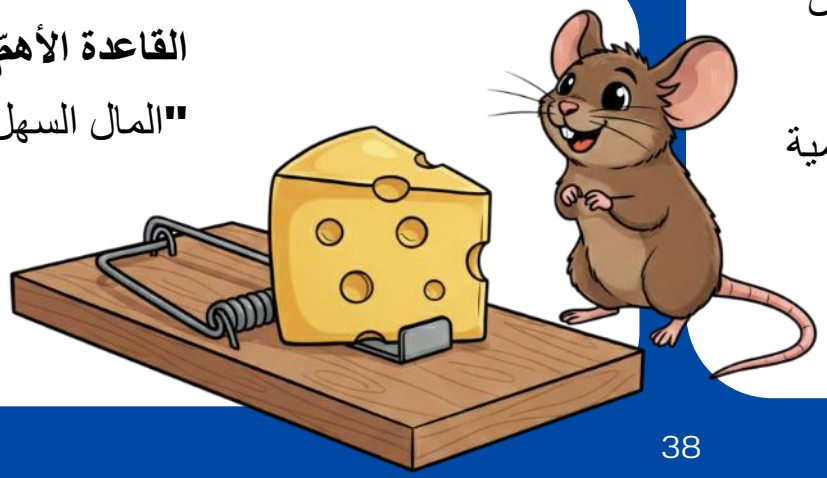
- وعود بعوائد غير واقعية تفوق معدلات السوق بأضعاف
- وجود برنامج إحالة قائم على جذب مشاركين جدد
- غياب الترخيص والمستندات القانونية
- إعلانات عدوانية وإلحاح زمني)مثل» :اليوم فقط(«!
- انعدام الشفافية :لا معلومات واضحة عن الإدارة أو التسجيل الرسمي
- قبول أموال نقدية أو عملات مشفَّرة من دون مستندات رسمية

تحقّق من الشرعية

- يجب أن تمتلك جميع المؤسسات المالية ترخيصًا من البنك المركزي لروسيا الاتحادية
- يمكن التحقّق عبر الدليل الرسمي على الموقع : cbr.ru/inside/warning-list

القاعدة الأهمّ

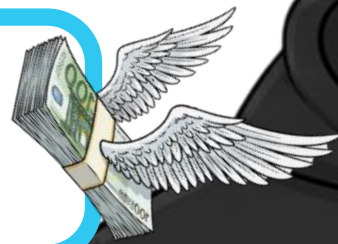
"المال السهل دائمًا له ثمن باهظ"



الهدف الرئيسي للمحتالين

خفض مستوى الوعي لدى الضحية وإيقاف التفكير النقدي لديها

تتغيّر الأساليب، فيما تظلّ الفكرة واحدة



متاجر ومواقع تصيّد احتيالي

مخطّط المحتالين

يعرضون سلعًا وتذاكر ورحلات بأسعار مخفَّضة لاستدراج الضحية

ينشئ المحتالون نسخًا مزيّفة لمواقع المتاجر وشركات الطيران والبنوك وغيرها

قواعد السلامة

تأكّد من أن الموقع يستخدم بروتوكول HTTPSوليس HTTP

لا تنتقل عبر الروابط الواردة في رسائل البريد الإلكتروني

اشترِ فقط عبر التطبيقات الرسمية

استخدم برنامجًا لمكافحة الفيروسات

تحقّق من وجود أخطاء في النصّ واسم الموقع

بطاقة منفصلة للمشتريات عبر الإنترنت

توصيل الزهور و»الخدمات الحكومية«

مخطّط المحتالين

مكالمة ثانية من «خدمة الأمن»

مع عرض المساعدة لاستعادة الوصول إلى منصّة «الخدمات الحكومية»

اتصال يُدّعي أنه من جهة رقابية حكومية «روسكومنادزور»

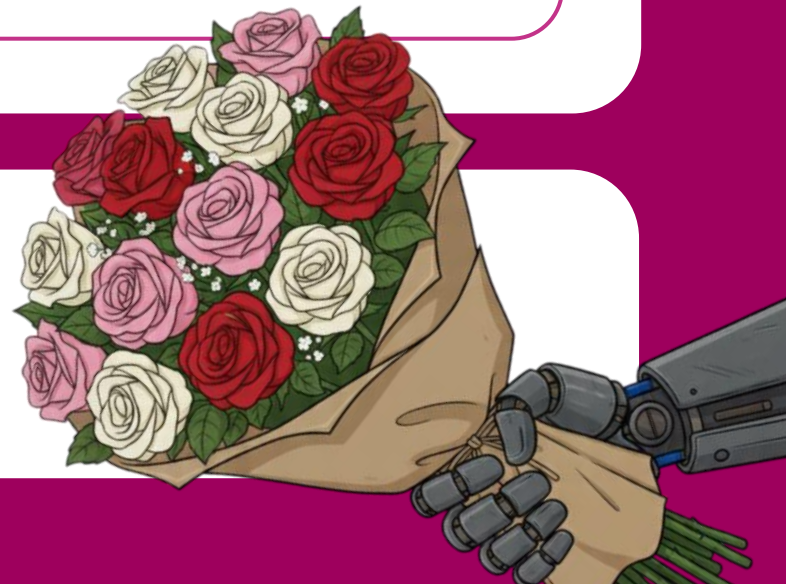
يُبلَّغ فيه عن وضع يُقال إنه غير آمن

اتصال يُزعم أنه من خدمة التوصيل

ويُطلب فيه الإفصاح عن رمز التحقّق المرسل عبر رسالة SMS

قواعد السلامة

- لا تفصح أبدًا عن رموز SMS — فهي قد تُستخدم للحصول على قروض صغيرة باسمك
- اسأل نفسك :هل كنت تنتظر توصيلًا فعلًا؟ إن لم يكن كذلك ←فالأمر على الأرجح عملية احتيال



حظر البطاقات باستخدام الذكاء الاصطناعي

مخطّط المحتالين

يهدّدون الضحية
ويطالبونها بدفع المال

يطلبون حظر البطاقة
يتحجّجون بفقدان البطاقة أو سرقتها

يُجرى اتصال بالبنك باسم «العميل»
يذكرون بياناته الشخصية ويُقلّدون صوته باستخدام الذكاء الاصطناعي

قواعد السلامة

أخبر جميع أقاربك بهذه الحيلة

لا تقم بأي تحويل مالي مهما كانت الظروف

لا تتصل بالبنك إلا من خلال الرقم الرسمي المُعلن

مشكلة عالمية

الآثار النفسية

14%
شهدت علاقاتهم الأسرية تدهورًا

69%
يعانون من ضغط نفسي شديد

17%
يفقدون الثقة بأنفسهم

نسبة البالغين عالميًا

54%
الذين تضرّروا من عمليات الشراء عبر الإنترنت

57%
الذين تعرّضوا للاحتيال

48%
الذين تضرّروا من الاحتيال الاستثماري

خطّ الدفاع الأوّل هو التفكير النقدي والوعي الرقمي

- يكاد يكون واحد من كل أربعة ممّن يعتبرون أنفسهم حذرين يفقدون أموالهم رغم ذلك
- يواصل المحتالون تطوير أساليبهم باستمرار، ولم تعد اليقظة الأساسية كافية

الأولمبياد الدولية في للأمن المالي

أُعِدَّت مهامّ الأولمبياد استنادًا إلى المناهج الدراسية

طلبة الجامعات

- العلاقات الدولية ودراسات المناطق الأجنبية
- الاقتصاد والتمويل والأمن الاقتصادي
- الرياضيات وأمن المعلومات
- القانون

طلاب المدارس

- الرياضيات
- علوم الحاسوب
- العلوم الاجتماعية

الجوائز والمزايا

فرصة الالتحاق بتدريب عملي في روسفينمونيتورينغ وغيرها من الجهات

امتيازات عند الالتحاق بجامعات المعهد الشبكي الدولي (البكالوريوس، الماجستير، الدكتوراه)

rosfinolymp.ru

الأولمبياد الدولية للأمن المالي

sodrujestvo.org

المدرسة الشتوية للأمن المالي

نوفمبر — ديسمبر

المرحلة التأهيلية

طلاب المدارس *2–3 سبتمبر*

طلبة الجامعات *1–19 يونيو*

المرحلة التمهيدية

الجولة الثانية *19–21 أبريل*

الجولة الأولى *14–17 مارس*

حصة تعليمية في موضوع «الأمن المالي»

10 فبراير - 30 أبريل

المرحلة النهائية

سبتمبر

المدرسة الصيفية للأمن المالي

يوليو

المرحلة الدعوية

02 فبراير - 10 مارس

الشركاء

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ФИНАНСОВОМУ
МОНИТОРИНГУ

МИНИСТЕРСТВО
ПРОСВЕЩЕНИЯ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

МИНИСТЕРСТВО
ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

РУДН

МИНИСТЕРСТВО НАУКИ
И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

МУМЦУМ

содружество

ПСБ

ЦЕНТР
МЕЖОЛИМПИАДНОЙ
ПОДГОТОВКИ