

دليل أمان محفظة الكريبتو

للمستثمرين وحاملي المبالغ الكبيرة — إصدار ٢٠٢٦

ملاحظات أمان الكريبتو · crypto-safety-notes.pages.dev

تنبيه: هذا الدليل تعليمي فقط، وليس نصيحة مالية أو استثمارية. لا نعد بأي أرباح، ولن نطلب منك أبداً عبارة الاسترداد أو أي مبلغ.

١. عبارة الاسترداد (Seed Phrase)

- عبارة الـ ١٢ أو ٢٤ كلمة هي أموالك نفسها. من يملكها يملك كل ما في المحفظة.
- اكتبها يدوياً على ورق، والأفضل نقشها على لوح معدني مقاوم للحريق والماء.
- لا تحفظها أبداً في صورة، أو لقطة شاشة، أو ملاحظات سحابية، أو بريد إلكتروني، أو واتساب.
- احتفظ بنسختين في مكانين آمنين منفصلين (مثلاً خزانة منزلية وصندوق أمانات بنكي).
- فكّر في استخدام «عبارة مرور إضافية» (Passphrase) كطبقة حماية، مع حفظها منفصلة عن الكلمات.

٢. المحافظ الباردة (Hardware Wallets)

- اشترِ الجهاز من الموقع الرسمي للشركة المصنّعة أو موزّع معتمد فقط، وليس من سوق مستعمل.
- إذا وصلك الجهاز ومعه عبارة استرداد مطبوعة مسبقاً، فهو احتيال؛ لا تستخدمه.
- تحقق من العنوان والمبلغ على شاشة الجهاز نفسه قبل التوقيع، لا على شاشة الكمبيوتر فقط.
- قسّم أموالك: محفظة «ساخنة» صغيرة للاستخدام اليومي، ومحفظة باردة للمدخرات.

ادعم المشروع crypto-safety-notes.pages.dev/tip

٣. المحافظ متعددة التوقيع (Multisig)

- تتطلب توقيع أكثر من مفتاح لتحريك الأموال، مثل ٢ من ٣. فقدان مفتاح واحد أو سرقة لا يكفي لسرقة الأموال.
- ورّع المفاتيح على أجهزة وأماكن مختلفة، ويمكن أن يحتفظ شخص موثوق أو جهة حفظ بأحدها.
- جرّب الاستلام والإرسال بمبلغ صغير أولاً، ووثّق إعدادات المحفظة (الملف الوصفي) واحفظها.

٤. التخطيط للورثة

- إذا لم يعرف أهلك كيف يصلون إلى أموالك، فقد تضيع إلى الأبد.
- اكتب «خطاب تعليمات» يشرح أين توجد الأصول وكيف يُستعاد الوصول إليها، دون كتابة العبارة نفسها فيه.
- استخدم multisig مع وارث أو محامٍ موثوق، أو قسّم المعلومات بحيث لا يملك أي طرف وحده الوصول الكامل.
- استشر مختصاً قانونياً في بلدك حول الوصية وتوافقها مع الأنظمة المحلية، وراجع الخطة سنوياً.

٥. تسميم العناوين (Address Poisoning)

يرسل المحتال مبلغاً صغيراً جداً (أو صفراً) من عنوان يشبه عنوانك أو عنوان من تتعامل معه في أول وآخر الأحرف، على أمل أن تنسخه من سجل المعاملات لاحقاً.

- لا تنسخ أي عنوان من سجل المعاملات أبداً. استخدم دفتر عناوين محفوظاً ومراجعاً.
- طابق العنوان كاملاً، لا الأحرف الأولى والأخيرة فقط، وأرسل مبلغ تجربة صغيراً قبل التحويلات الكبيرة.

٦. «المستشار» المزيف واحتيال واتساب وتيليجرام

- رسالة من رقم مجهول، أو «خبير» يضيفك إلى مجموعة توصيات، أو شخص تعرّفت عليه حديثاً يقترح منصة «مضمونة».
- تُعرض عليك أرباح وهمية في لوحة تحكم، ثم تُطلب «رسوم» أو «ضريبة» قبل السحب. هذا احتيال دائماً.
- لا يوجد عائد مضمون. لا تثبّت تطبيقات تحكم عن بعد، ولا تشارك شاشتك مع أحد.
- انتحال صفة البنوك أو الجهات الحكومية أو دعم المنصات أمر شائع؛ تواصل دائماً عبر القنوات الرسمية التي تبحث عنها بنفسك.

٧. احتيال الصفقات خارج المنصات (OTC)

- عروض شراء أو بيع كميات كبيرة بسعر أفضل من السوق، أو لقاءات نقدية، هي فخ شائع.
- لا ترسل أصولك قبل التأكد الفعلي من استلام المقابل، واحذر من إيصالات التحويل البنكي المزيفة.
- تعامل فقط مع مكاتب OTC مرخصة ومعروفة، واطلب عقداً وتحقق من الهوية.

٨. التصيد الاحتيالي (Phishing)

- روابط بنطاقات مشابهة، وإعلانات بحث ممولة، ورسائل «حسابك سيُغلق» أو «اطلب الإيديرروب خلال ١٠ دقائق».
- اقرأ ما توقع عليه: صلاحيات «غير محدودة» قد تسمح لعقد بسحب رموزك. راجع الصلاحيات القديمة وألغها دورياً.
- لن يطلب منك أي دعم فني حقيقي عبارة الاسترداد أبداً.

قائمة فحص سريعة

- ☐ العبارة على ورق/معدن، نسختان، لا شيء رقمي
- ☐ جهاز بارد من مصدر رسمي
- ☐ multisig للمبالغ الكبيرة
- ☐ خطاب تعليمات للورثة
- ☐ دفتر عناوين + تحويل تجريبي
- ☐ لا «مستشارين» من واتساب، لا أرباح مضمونة

إذا وجدت هذا الدليل مفيداً، يمكنك دعم المشروع اختياريًا عبر صفحة الدعم: crypto-safety-notes.pages.dev/tip.html — شكرًا لك، ومحتوانا سيبقى مجانياً دائماً.