



SCAM CHECK

Ti stanno truffando?

7 segnali da controllare prima di fidarti di chi ti contatta parlando di Bitcoin o crypto.



Un segnale isolato non prova una truffa. Più segnali insieme richiedono una verifica immediata.

1

CONTATTO NON RICHIESTO

Ti chiamano o scrivono senza che tu abbia chiesto assistenza.

2

FONDI O CONTO “BLOCCATO”

Parlano di Bitcoin, crypto o di un conto a tuo nome da recuperare.

3

SANNO GIÀ QUALCOSA DI TE

Usano nome, email o vecchi investimenti per sembrare credibili.

4

URGENZA E PRESSIONE

Devi agire subito, altrimenti perderai fondi o accesso al conto.

5

CONTROLLO REMOTO

Ti chiedono di installare software o condividere lo schermo.

6

CREDENZIALI E ACCESSI

Vogliono password, codici 2FA, seed phrase o accesso a wallet/exchange.

7

DENARO PER ‘SBLOCCARE’ O ‘RECUPERARE’

Ti chiedono commissioni, tasse o anticipi in euro o crypto per sbloccare o recuperare presunti fondi.



TI STANNO CHIAMANDO ADESSO?

Fermati. Non devi decidere nulla durante la chiamata.

1

RIAGGANCIA

Chiudi la chiamata. Un operatore reale accetterà una verifica autonoma.

2

NON CLICCARE E NON INSTALLARE

Ignora link, allegati e richieste di controllo remoto.

3

VERIFICA DA SOLO

Cerca l'azienda tramite sito, app o numero ufficiale. Non usare i recapiti ricevuti.

NON RICHIAMARE IL NUMERO CHE TI HANNO FORNITO LORO.

4

NON PAGARE

Non inviare euro o crypto mentre qualcuno ti mette fretta.

NON FARE MAI QUESTE 4 COSE

- ✗ Comunicare la seed phrase del wallet
- ✗ Dettare o inoltrare codici 2FA
- ✗ Concedere il controllo remoto del dispositivo
- ✗ Inviare crypto per "recuperare" altre crypto

Verifica sempre tramite canali ufficiali. Un singolo segnale, da solo, non dimostra necessariamente una truffa.

Conosci qualcuno che potrebbe cascarci?
Inviagli questa checklist.

Vuoi ricevere aggiornamenti gratuiti su
Bitcoin, crypto e mercati?

ENTRA NEL CANALE TELEGRAM →