CR1PTO

Davide Baraldi

Pillole di Sicurezza Informatica per cripto investitori

CR1PTO

Davide Baraldi

Pillole di sicurezza informatica per cripto investitori.

Prima edizione
Gennaio 2022

Sommario

Prefazione

Questo libro vuole essere uno strumento di spunto per aiutare i cripto investitori nell'arduo compito di tutelare i loro investimenti digitali.

I temi trattati necessitano di approfondimenti per essere esplicati in maniera completa.

I concetti e i punti di vista narrati vengono esposti in maniera semplificata per essere comprensibili anche ai non tecnici.

Dispositivi

Per ottenere un alto livello di sicurezza è importante operare da computer.

Smartphone e tablet non sono consigliati.

Sarebbe ideale dedicare un device solo per questa attività, non metterlo a disposizione di terzi e non lasciarlo mai incustodito.

Software

Il software open source è più sicuro di quello proprietario perchè il codice può essere visionato da chiunque e questa peculiarità lo rende meno incline a bug e problematiche di sicurezza.

Qualsiasi software dovrebbe essere scaricato solo dal sito ufficiale controllandone l'autenticità attraverso l'hash e la firma crittografica.

Installare software trovati a caso su internet, con programmi p2p o che sono stati passati dall'amico potrebbe compromettere la sicurezza del dispositivo.

Sistemi operativi

L'utilizzo di software libero come Linux o B.S.D. riduce notevolmente la superficie d'attacco e conferisce pieno potere sul sistema operativo e sul dispositivo.

Usare sistemi chiusi come Windows e macOS non è saggio a causa dei loro perpetui problemi di sicurezza e stabilità.

Lo stesso principio vale per iOS e Android.

Se si utilizza un sistema vulnerabile, è importante implementare un hardware wallet così che il seed e le chiavi private siano custodite fuori dal sistema.

Protezioni

Installare antivirus e firewall è fondamentale per difendersi.

Se per qualsivoglia motivo si ricade su un software commerciale bisogna rammentare che le versioni free non sono performanti come le versioni complete.

La configurazione standard non è sufficiente di questi tempi, perciò configurare tutto in maniera paranoica è un passo necessario.

Connessioni

Utilizzare T.O.R. aggiunge un layer crittografico alla connessione e non sarà possibile geolocalizzare il dispositivo.

La scelta di una V.P.N. è una buona prassi per cifrare ulteriormente il traffico e limitare la localizzazione della connessione.

Cambiare i D.N.S. è utile per evitare forme di censura e per aumentare la sicurezza della connessione.

Browser

Browser a codice pubblico come Firefox, Chromium o Brave aumentano la sicurezza della navigazione in rete.

È pericoloso l'utilizzo di browser closed source come Chrome, Opera, Edge e Safari perché questi programmi sono soggetti a un numero maggiore di problemi e bug di sicurezza.

Navigazione

Durante la navigazione è bene controllare che l'indirizzo del sito sia corretto e che appaia il lucchetto prima della barra dell'indirizzo.

Fretta o disattenzione possono far passare inosservato un sito malevolo confondendo una lettera come la l con la i.

Wallet

L'implementazione di wallet liberi come Metamask ed Electrum danno il pieno controllo sul portafoglio e la reale proprietà sulle cripto valute.

I wallet con codice proprietario sono da considerarsi più rischiosi e meno sicuri.

Lasciare i propri asset sugli exchange significa non esserne il proprietario.

Backup

I file importanti contenenti il seed e le chiavi private dovrebbero risiedere solo dentro a contenitori o dispositivi cifrati.

La ridondanza è importante, per cui creare copie dei backup e dislocarle in aree geografiche differenti è salutare.

Scrivere i codici su carta o archiviarli su una memoria di massa non crittografata crea delle vulnerabilità di sicurezza.

Password

Le password necessitano di un'alta entropia e non devono avere inerenze con la vita privata, il lavoro o le passioni.

Crea codici con una logaritmica mnemonica così che si possano ricordare come una poesia e non ci sia la necessità di scriverli.

Una buona password dovrebbe contenere almeno 10 caratteri tra cui lettere minuscole, maiuscole, numeri e caratteri speciali.

Attacchi

Esistono vari tipi di attacchi, ma uno di quelli più efficienti è l'ingegneria sociale.

Per contrastarla è bene non fidarsi di nessuno ed evitare la divulgazione di informazioni personali come le routine, i software, gli investimenti, i viaggi e tutti quei dati sensibili che potrebbero essere utilizzati per creare un attacco mirato col fine di compromettere i devices utilizzati.

Postfazione

Le impressioni e i giudizi riguardanti dispositivi, metodologie e software esposti in questo libro provengono dai test eseguiti nei laboratori CR1PT0 e dall'esperienza del suo C.E.O. nelle forze armate e dell'ordine.

La documentazione degli argomenti trattati è pubblica e a disposizione di chiunque.

CR1PT0.COM

Pillole di sicurezza informatica per cripto investitori

"Se possiedi le chiavi private,
possiedi le criptovalute."

C.E.O. CR1PT0