GUIDE

Travel and Physical Security Guide for Web3 Teams

Defending bodies, not just bytes: wrench attacks, doxxing, duress planning, and the first 30 minutes

Prepared for	Web3 teams	Classification	Public
Prepared by	Oak Security	Date	2026-06-17

Oak Security GmbH

1. What This Guide Is For

This guide is for Web3 team members, founders, and high-net-worth individuals whose association with crypto is public or discoverable. Everything else in an opsec program defends bytes. This one defends bodies.

The 2024-25 wave of crypto-linked kidnappings, home invasions, and coercion incidents moved physical security from a paranoid hobby into a first-class risk surface. The pattern is not hypothetical and not rare. The reason is structural: the industry produced, in fifteen years, a population of people who are simultaneously publicly identifiable, publicly known to control assets, and operating without the personal-security infrastructure that comparably wealthy people in other industries have. A founder whose name is on a token launch, whose face is on a podcast, and whose wallet is searchable on chain has the visibility of a celebrity and the protection budget of a software engineer. Attackers have noticed.

> **NOTE**
>
> **Baseline rule:** the weakest link in any cryptosystem is the person who holds the key, and that person can be found, followed, and coerced. Comply, survive, recover, in that order. Keys are replaceable. People are not.

This guide covers the wrench attack and why crypto holders are targeted, doxxing as the pre-attack, home and office hardening, duress planning and family preparedness, travel and event security, SIM-swap defence, signer device hygiene, and a runbook for the moment an incident is live. Read Section 9 before you need it.

2. The Anatomy of a Wrench Attack

The wrench attack takes its name from the XKCD comic in which a $5 wrench defeats whatever cryptography the victim was congratulating themselves about. The joke describes an operational attack. A wrench attack (also called a rubber-hose attack in older literature) bypasses the cryptographic stack by extracting keys, signatures, or transfer authority directly from the human who controls them.

It runs through five phases that mirror the digital kill chain.

Phase	What happens	Defensive seam
Reconnaissance	A target is identified from a public signal: a tweet about a trade, a LinkedIn role at a token-launching protocol, a conference panel, a chain-analysis report, a legal filing tying a name to a wallet. This is reading, not hacking.	Reduce public footprint (Section 3).
Surveillance	Escalation from a name to a location, a routine, and a security posture. Home address from data brokers or property registries. Family mapped through Instagram and school photos. Patterns from Strava and live-location shares.	Doxxing hygiene, family persona discipline.
Approach	Home invasion in the early-morning window (often around 06:00). Vehicle intercept during the school run. Forced entry at a conference hotel. Sometimes a family member is targeted first.	Home hardening, situational awareness.
Coercion	Physical violence, threats to family, captivity. The script every wrench attack converges on is "transfer the keys or we start." The attack is engineered so complying is the only survivable option.	Decoy wallets, timelocks, multisig elsewhere.

Extraction	Funds move through mixers, bridges, and exchanges within minutes of the forced transfer. By the time the victim is freed, assets are forty hops away.	Exchange relationships, rapid rotation.

Attackers want compliance, not heroism. The structural defences are the ones that make compliance not equivalent to total loss: a credible decoy, a timelock the attacker cannot beat from inside the captivity window, a multisig threshold sitting in other cities.

3. Doxxing: The Pre-Attack

Every wrench attack, every SIM-swap, every targeted home invasion begins with doxxing. In its operational sense, doxxing is the assembly of a full personal dossier from open-source signals: real name, home address, family members, daily patterns, financial visibility, security posture. The attacker does not need inside information. The attacker needs hours and the willingness to read.

Doxxing defence is public-persona hygiene.

- **Assume open-source recon.** Everything public (a project role, a conference photo, a podcast appearance, a GitHub commit under a real name, a regulatory filing) is discovery for an attacker. This is the attacker's literal first step.
- **Minimise the wealth signal.** No portfolio screenshots. No "we raised $X" photos with watches in frame. No supercar posts. The French kidnap-wave victims were, almost without exception, publicly visible as crypto-wealthy. Visible wealth attracts targeting in a way that visibility alone does not.
- **Scrub data brokers.** Spokeo, BeenVerified, Whitepages, Pipl in the US, and the European equivalents, republish home addresses, relatives, and phone numbers. Annual scrub via DeleteMe or Optery plus manual opt-out for the brokers they miss. Brokers re-list within months, so treat this as a renewable subscription, not a one-time exercise.
- **Split identities for different audiences.** A pseudonym for research contributions and on-chain activity. The real name reserved for legally required contexts (regulatory filings, contracts, employment). Work and personal social accounts separated, ideally on separate devices.
- **Family is part of the persona.** Attackers target the weakest reachable member of the household. Children's school locations not tagged in photos. No live-location shares to public audiences. No "we are away on holiday" posts until the family is home. The Vierzon kidnap involved Balland's partner. The May 2025 Paris incident targeted a crypto executive's father as the lever. The operational unit of physical-security planning is the household, not the individual.

4. Two Case Studies

French Kidnap Wave, 2024–25

The most documented cluster of crypto-linked physical attacks in any single jurisdiction to date. Reporting in *Le Monde*, Reuters, and Bloomberg catalogued at least half a dozen kidnappings or attempted kidnappings linked, by stated motive or financial demand, to cryptocurrency holdings. The cluster ran from mid-2024 through mid-2025 and involved multiple separate criminal groups, suggesting copy-cat dynamics rather than one coordinated campaign.

The pattern was consistent. Victims were publicly known (a founder, an executive, a commentator) or one social step removed from someone who was. Attackers used open-source research, not insider information. Demands were paid in cryptocurrency to attacker-controlled wallets. Methods escalated. Most victims survived. Some sustained lasting physical injury. The playbook is portable: nothing about it is France-specific. Anyone publicly visible in crypto, in any jurisdiction, is now part of the addressable target set.

Ledger Co-Founder Kidnapping, Vierzon, January 2025

On 21 January 2025, David Balland (co-founder of hardware-wallet manufacturer Ledger) and his partner were kidnapped from their home in Vierzon by a group of five to seven attackers. The attackers had conducted reconnaissance: they knew the location, the routine, and the household composition. The home was breached during the early-morning window.

The demand was a multi-million-euro cryptocurrency ransom, communicated to co-founder Éric Larchevêque while the victims were still captive. To apply pressure, the kidnappers severed one of Balland's fingers and sent it to Larchevêque as proof of intent. The attackers were willing to inflict permanent injury within the first 24 hours, before any ransom delay had compounded.

The response ran two parallel tracks. Larchevêque contacted French authorities immediately rather than attempting private negotiation as the primary strategy. The GIGN, France's elite gendarmerie counter-terrorism unit, conducted a rescue within roughly 24 hours, freeing both victims and arresting several suspects. A partial negotiation posture (engaging without committing) bought the hours the GIGN needed. No ransom was ultimately paid.

The lessons generalise:

- Every founder-level signer is a target, whether or not they think of themselves that way. Visibility is the criterion, not self-perception.
- Comply first, survive, rotate later is the correct doctrine under live coercion.
- Law enforcement is only as fast as the relationships you built before you needed them.
- Keys are replaceable. People are not.

5. Home and Office Physical Security

The home is the highest-value defensive surface because it is where the household is most predictable in time and place. The baseline controls are not exotic.

Control	What to do
Harden the entry point	Reinforced front door with a multi-point lock. Peephole or doorbell camera. A monitored alarm with a 24/7 response contract, not a self-monitoring app. Cameras at entrances with local recording.
Safe room	A room with a deadbolt, a charged phone, known reception, and a printed contact list (police, counsel, private security, a designated company contact). If the house is breached at 06:00, whichever adult is closest to the children needs a place to reach help without negotiating with intruders.
Keys and devices do not sleep in the nightstand	Hardware wallets, seed backups, and signing laptops live in a concealed safe rated for fire and force, bolted to structure. Not on a bedside table.
Decoy hardware in expected places	A Ledger box on the desk, an old wallet with a small balance in a drawer. These absorb the initial search and reduce pressure on the household during a breach.
Operational discipline	No high-value transactions performed visibly through windows. Close blinds before signing. No item in the home reveals the value at stake.
Office parity	Badge-in access, locked-device policy, clean-desk discipline, perimeter cameras, an unlisted office address. Where possible, the address on regulatory filings is a registered-agent address, not the working office.

6. Duress Planning and Family Preparedness

The doctrine under physical threat is comply, survive, recover. A key is replaceable. A multisig seat is replaceable. A wallet is replaceable. A person is not. Resistance under duress statistically ends worse, for the victim, the family, and the financial outcome, than compliance followed by rapid rotation. Every control here serves that doctrine.

- **Decoy wallets with credible balances.** A phone wallet with a believable amount, set up specifically to be the thing an attacker finds and drains. It satisfies the "give me access" demand without exposing the real multisig or long-term storage. Credibility matters: an attacker who believes they hit the floor stops escalating, and escalation is what causes lasting harm. Use a plausible-deniability cold tier (hand-over wallet for coercion, real value behind a BIP-39 passphrase).
- **Timelocks on large transfers.** If the multisig requires a six-hour or 24-hour delay above a threshold, a forced signing at 04:00 cannot complete before rescue or reset. This is the best structural defence against live coercion: it converts a problem the attacker thought solved (forcing a signature) into one they cannot solve inside the captivity window. A signer who can demonstrate the transfer will not clear in time has, in multiple incident reports, ended the coercion phase faster than any other intervention.
- **Multisig threshold too high for single-person coercion, and the attacker can see that.** A threshold that visibly requires signers in other cities removes the point of coercing any one person.
- **Family duress word.** A pre-agreed phrase, innocuous in normal conversation, that signals "I am being coerced, call for help" without alerting the attacker. Train family and close team on it. Default to coerced if the safe word is missing. The duress word is never used in normal conversation; the moment it appears, the receiver knows.
- **Pre-built family IR plan.** Who does the family call first: counsel, private security, local police, the company? Written down, in the safe room, in printed form, with numbers that work without internet. Rehearsed at least annually. Review kidnap-and-ransom insurance where the risk profile warrants it.

7. Travel and Event Security

Every trip doubles the attack surface for its duration. The household is unfamiliar with the environment, the hotel and transport baseline is outside the team's control, the device is exposed to networks the team does not own, and location is broadcast (sometimes deliberately, in conference programmes).

Pre-Trip Preparation

- **Assess the destination.** Jurisdiction risk (hostile state, crypto-restrictive, extradition treaty), physical-crime rate, conference profile, who else will be there, whether the trip is announced or discoverable. Some destinations are not worth the trip for some travellers. That is a defensible decision.
- **Travel with a clean device.** Wiped laptop, fresh OS image, minimum software, no wallet keys, no SSH keys to production, no password-manager vault cached locally. Travel laptop is not the daily driver. Travel phone is not the daily driver where stakes justify it. Re-image on return.
- **Decide whether keys travel at all.** The default is that signing devices do not travel. Hardware wallets, seed backups, and signing devices stay home or in a secure in-country facility. Backup MFA hardware key stored separately from the primary. Freeze banking, exchange, and treasury access for the trip where possible.
- **Itinerary is need-to-know.** Immediate family, one backstop colleague, security or executive assistant if applicable. Not "the team." Not Slack. Not Instagram stories. Do not post itineraries or boarding passes. Announce the trip after return, not before.
- **Duress plan rehearsed.** Who calls whom if the traveller misses a check-in? Agree the check-in cadence before departure.

Hotel and Ground Transport

- **Room discipline.** The in-room safe is not a security boundary against motivated staff, but it raises the cost. Door wedge or portable door alarm on top of the deadbolt. Room-service trays left outside the door. Switch rooms if anything feels off (staff asking about company affiliation, someone loitering, a knock that does not match a reservation pattern).
- **Do not broadcast the hotel.** No geotagged photos from the room or restaurant. No "drinks in the lobby" posts until you have moved on.
- **Pre-booked private driver** for the airport run and significant transfers. The cost premium over a ride-share is small; the difference between a vetted driver and an algorithm-allocated one is not. Use ride-hail apps over street taxis when the destination would reveal home or office.
- **Carry local-currency cash.** Pre-load enough for transport, tips, and a hotel night. The midnight convenience-store ATM is exactly the situation to avoid.
- **Situational awareness.** Phone charged, live location shared with one trusted person (not publicly), eyes up in lobbies and transit hubs, and the trained habit of noticing the same face twice.

Border Crossings and Hostile Jurisdictions

- **Assume the device will be inspected.** Most countries can legally compel a device unlock at the border (US Customs, UK Schedule 7, Chinese airport checks). Plan for that outcome before the queue, not from inside it.
- **Burner posture.** The travelling device contains nothing that would hurt you if copied. No photos of signing ceremonies. No chat logs with multisig signers. No project-internal documents. No wallet apps on high-risk crossings.
- **Nothing chains to the real stack.** Seized or copied credentials must not chain to production access. Separate accounts with their own MFA. No cached vaults, no SSH agent keys, no active production session tokens. The worst case of a seizure is losing the device, not losing production access.
- **Power-state hygiene.** Power off the device before customs. Disable biometric unlock; passcode only (biometrics can be compelled in some jurisdictions in ways PINs cannot). Power-cycle after the crossing too: a phone in the before-first-unlock (BFU) state is meaningfully more secure than after-first-unlock (AFU), and a reboot returns it to BFU.
- **Destination legal counsel.** Who to call if detained, questioned, or property is seized. Warm the relationship before the trip.

Conferences and Events

DevCon, Token2049, EthCC, ETHGlobal events: all documented targets. Conference weeks have produced laptop thefts, device swaps in lounges, coordinated drink-spike-and-snatch attempts on after-party routes, and pickpocket rings tuned to lanyard-wearing attendees.

- **No signing at conferences.** The hardware wallet does not travel to DevCon. If a transaction must go out during conference week, a non-travelling signer handles it.
- **Conference Wi-Fi is adversarial by default.** Never log in to anything of value over the event SSID. If connectivity is required, the phone's LTE tether under a VPN is the floor.
- **Charge only from your own brick.** Every public USB port, charging kiosk, and organiser cable is untrusted. Use a data-blocking cable for any connection to hardware you did not bring.
- **Badge and swag are signal.** The speaker lanyard, the project tee, the sticker-covered laptop tell strangers who you are and what you likely carry. Dress down. Cover the laptop lid. Take the badge off when leaving the venue. No company merch off-venue.
- **Bag discipline.** Laptop bag at the feet and in the hand, never slung over a chair. Do not leave a bag with anyone, even briefly. The five-second window is the entire window the snatch operation needs.

8. SIM-Swap Defence and Device Hygiene

SIM-Swap Defence

The SIM-swap is the textbook digital-physical crossover. The attacker social-engineers the carrier (by phone, in a retail store, or through a bribed employee) into porting the number to a SIM they control. Every SMS reset and SMS 2FA code then funnels to them: email recovery, exchange logins, banking 2FA, password-manager recovery. The Michael Terpin case is canonical: in 2018 he lost approximately $24 million through a SIM-swap that gave the attacker access to his exchange account.

- Set the carrier PIN and port-out lock on every line in the family. Re-check annually; carriers occasionally reset it during account migrations.
- Prefer eSIM where possible. Physical SIM slots are the most common swap channel (walk-in with fake ID). eSIMs require additional carrier verification.
- Nothing of value gated on SMS. Not exchange 2FA, email recovery, banking 2FA, or password-manager recovery. Hardware keys (YubiKey, Titan) or app authenticators only.
- Treat a dead number as an emergency. If SMS, calls, or data suddenly stop, assume a port-out is in progress and call the carrier from a different line immediately.
- Carrier choice is part of the threat model. MVNOs and prepaid tiers are historically weaker on port-out defence. Business lines with named account managers are stronger.

Signer Device Hygiene: Don’t Carry the Keys to the Treasury

- **Treat every signing device as a bearer instrument.** Possession of the device plus the PIN is possession of the funds. Never out of sight, tamper-evident packaging, chain-of-custody discipline.
- **No signing devices unattended in hotel rooms or checked luggage.** Cabin baggage only. Safe-in-safe in the hotel. If the device is not needed for the trip, it does not come.
- **Tamper-evident seals** during transit and between uses. Record the seal serial or pattern. Inspect before each use. Hours of unsupervised access lets an attacker implant compromised firmware that survives a normal inspection.
- **Never buy hardware wallets second-hand** or from unofficial resellers. The attacker-preloaded-seed scam has drained tens of millions over five years. Buy direct from the manufacturer, verify packaging, re-flash firmware before first use.
- **Rotate on any doubt.** Device out of sight for an hour. Luggage delayed. Seal inconsistent. The cost of a new seed is small; the cost of using a compromised device is total. The disposition is rotate, not investigate.
- **Backup geography.** Seed shards across geographically separated, physically secure locations (bank deposit box, fire-safe at a relative’s, trusted custodian), not all in one safe in one building. Do not travel with material that, combined, reaches the threshold.

9. If It Happens: The First 30 Minutes

This runbook is short by design. The first thirty minutes does not allow for a long checklist.

1. **If physical coercion is live, comply.** Keys are replaceable; people are not. Comply, survive, recover, in that order. Resistance during the coercion phase escalates violence statistically more often than it ends the coercion.
2. **Trigger the duress signal if possible.** The family duress word. A phone emergency-SOS that dispatches with location to a preset contact list. A trained silent alarm at home. These work only if rehearsed in advance.
3. **As soon as safe, call law enforcement first, counsel second.** Response time matters more than legal framing in the first thirty minutes. Give them the transaction hashes, wallet addresses, attacker description, and direction of travel. The first call gets a unit dispatched.
4. **Contact exchanges.** Coinbase, Binance, Kraken, OKX each have a law-enforcement and compliance hotline that can freeze incoming funds if reached within hours. A prior relationship turns hours into minutes. For a household at non-trivial risk, make those introductions before they are needed.
5. **Rotate everything.** All keys. All multisig seats. All password-manager vaults. Home door locks. Phone number. Social-media logins. Email passwords. The home address if feasible. If it was in the household's life when the incident started, rotate it. The attacker may have observed any of it.
6. **Plan post-incident care for the family.** Trauma is part of the loss, not a separate concern. Professional counselling, temporary relocation, a step back from public exposure. Plan this before it is needed: the next incident often comes from a burnt-out signer or a destabilised family unit.

10. Checklist

Use before any non-trivial travel, when adopting a higher public profile, and on a quarterly review of the physical attack surface.

Doxxing and Public Persona

Check	Done
Public bios do not tie full legal name to city to employer to asset class.	
Data-broker opt-outs current (DeleteMe / Optery plus manual); re-checked this period.	
No public posts about asset value, hardware-wallet model, or exchange relationships.	
Public photos hide home interior, street numbers, plates, school badges, landmarks.	
Family (children's school, partner's employer, parents' addresses) not in public footprint.	
Work and personal identities and accounts separated.	

Home, Office, and Duress

Check	Done
Reinforced door, deadbolt, doorbell camera, monitored 24/7 alarm.	
Safe room with deadbolt, charged phone, printed contact list, known reception.	
Seeds and cold-tier devices in a concealed, force/fire-rated, bolted safe. Decoys in expected places.	
Plausible-deniability cold tier: hand-over wallet; real value behind BIP-39 passphrase.	
Timelock on large transfers; multisig threshold structurally too high for single-person coercion.	
Family duress word agreed and trained; default to coerced if missing.	
Printed, rehearsed family IR plan in the safe room. K&R insurance reviewed where appropriate.	

Travel, Conferences, and Devices

Check	Done
Trip threat assessment done; itinerary need-to-know; announced only after return.	
Clean travel device: no seeds, no signing keys, nothing chaining to production.	
No signing devices in checked luggage; cabin only; safe-in-safe in hotel.	
Power off and disable biometrics before borders; passcode only; power-cycle after.	
Carrier PIN and port-out lock on every line; eSIM where possible; nothing of value on SMS.	
No signing at conferences; conference Wi-Fi treated as hostile; own charging brick only.	
Badge off outside the venue; no company merch off-venue; bag never out of hand.	
Tamper-evident seals on signing devices, recorded and inspected; rotate on any doubt.	

First 30 Minutes (Print and Store in the Safe Room)

NOTE

Comply. Trigger the duress signal. Law enforcement first, counsel second. Exchanges within the hour with hashes and addresses. Rotate everything. Care for the family.

11. References

- Reuters reporting on French crypto kidnappings, 2024–25: https://www.reuters.com/
- *Le Monde* coverage of the Vierzon (Balland) kidnapping, January 2025: https://www.lemonde.fr/en/
- US v. Terpin (SIM-swap, 2018, approximately $24M): https://www.courtlistener.com/
- DeleteMe data-broker removal: https://joindeleteme.com/
- Optery data-broker removal: https://www.optery.com/
- US CBP border device search policy: https://www.cbp.gov/travel/cbp-search-authority
- UK Terrorism Act Schedule 7: https://www.gov.uk/government/publications/code-of-practice-for-examining-officers-and-review-officers-under-schedule-7-to-the-terrorism-act-2000