Map My Risk: Methodology

Nov 13, 2026 · El the Freedom Fairy (@el_freedomfairy)

Map My Risk scores a cryptocurrency holder's exposure to wrench attacks across five areas, using questions, points and weights informed by my coding of Jameson Lopp's 2026 cases and by published research. Data last reviewed: 13 November 2026 (Dataset v2). Numbers in square brackets refer to the Notes at the end.

Purpose and scope

Map My Risk is a free self-assessment for anyone holding cryptocurrency, not only bitcoin. It shows where a person's exposure to wrench attacks comes from and which changes may reduce it. It gives a relative exposure score. It is an awareness tool, not a prediction, a probability of being attacked or a security audit, and should not be solely relied upon to build a security architecture.

- **Users:** individual holders and their families, from beginners to long-term holders.
- **Output:** a relative exposure band, a profile, scores for five areas, three suggested changes, live what-if switches, and real 2026 cases that may reflect the user's profile.
- **Formats:** an online tool, a downloadable offline copy, and a printable self-scoring checklist.
- **Asset scope:** Lopp's database and my coding cover attacks on holders of any cryptocurrency. Cases are not separated by asset, and many 2026 cases involved USDT rather than bitcoin. The tool therefore speaks to crypto holders generally.
- **Data period:** Lopp's entries dated 1 January to 31 October 2026, downloaded on 10 November 2026.[1] The year is not complete, so 2026 figures are partial.
- **Review:** data is reviewed at regular intervals, and the tool shows the date of the last review. This version uses Dataset v2 (13 November 2026).
- **Definition:** my definition of a wrench attack, set out in the companion methodology for the definition and codebook.[2]

Theoretical framework

The tool combines two victim-focused theories, and a third shapes its advice.

- **Routine activity theory:**[10] a crime occurs when a motivated offender meets a suitable target without a capable guardian. It explains why some holders are chosen and others are not.

- **Lifestyle-exposure theory:**[11] a person's lifestyle and routines set how often they come into contact with potential offenders. It underpins the Visibility, Wealth signals and Routines areas.
- **Situational crime prevention:**[12] crime falls when it is made harder, riskier or less rewarding in the moment. It shapes the suggested changes, such as multisig and time-delays.

Area	Question it asks	Theory element	Link to my codebook
Visibility	Can you be found?	Exposure; offender identifies a target	A: Classification; K: How they knew
Wealth signals	Do you look worth it?	Target suitability (perceived value)	A: Classification
Access speed	How fast could funds move under duress?	Target suitability (ease of removal)	E: Access method
Household	Who could be used as leverage?	Absent or vulnerable guardians	A-PX; D: Relational
Routines	Where are your weak moments?	Convergence in time and place	D-P; B: Planning

Why these and not others.

Theory	What it explains	How it is used
Rational choice theory[12]	Offenders weigh effort, risk and reward	Not the base, because it explains offender decisions users cannot control; reflected in the Access speed area
Crime pattern theory	Where offences cluster in space and time	Not the base, because it needs location detail users would have to reveal; reflected only in the location question
CRAVED[12]	Why some goods are stolen more (concealable, removable, available, valuable, enjoyable, disposable)	Explains why crypto is attractive as an asset, not differences between holders
Crime script analysis[3][12]	The stages of an attack	Used to check the five areas cover every stage, from finding a target to moving funds

Blind spot. These theories centre on the victim's situation. The tool does not score offender-side drivers that users cannot control, such as Bitcoin's price, organised crime recruitment, or personal data sold on darknet markets.

Evidence base

The tool draws on five sources and triangulates them, rather than averaging them or treating any one as the truth. My coding is the primary source for anything it can count. The others cross-check it and fill gaps it cannot measure. Where sources disagree, the tool uses the more cautious figure and says so. The sources cover different periods and use different definitions, so their figures are not directly comparable.

Dataset	Period covered	Definition used	Used in the tool for
My coding of Lopp's database[1][2]	1 Jan – 31 Oct 2026 (147 cases; 109 meet my definition; Dataset v2)	My definition	Most figures, the amount thresholds, the location question and all example cases

Dataset	Period covered	Definition used	Used in the tool for
Chainalysis[5]	1 Jan – late June 2026 (46 incidents)	Violent attacks including home invasions, kidnappings and hostage situations	A cross-check on family or acquaintance targeting only (a broader category than my proxy code)
CertiK[7]	1 Jan – 30 June 2026 (52 verified incidents)	Physical coercion to compel a transfer or disclosure, or to pressure a third party	Geographic concentration
Ordekian et al.[3] [4]	105 news-reported incidents (2014 – Oct 2023), forum posts and 10 interviews	Physical attacks to obtain crypto, including burglary	In-person trading risk; victim selection; family as a route to the holder; under-reporting
GART Research[6]	2014 – 10 Feb 2026 (305 cases)	Physical attacks on crypto holders, including attempts that failed; built on and expanded from Lopp's database	How victims are found (leaks, public records); attack types; per-holder country rates; foiled attacks; family targeting

How independent the sources are. Gart's database was built on Lopp's and then expanded (p. 12),[6] so it overlaps my coding and cannot confirm it independently. It works more like a second coder: a partial check on how the same cases read to someone else. Ordekian et al. are the most independent source, drawing on interviews, forum posts and news reports.[3] Gart, CertiK and Chainalysis are commercial firms, so their framing may reflect commercial interests. Chainalysis is now used only as a cross-check on family targeting, and Gart replaces it everywhere else because Gart gives page-numbered evidence.

How my coding was done. The 2026 cases were coded with AI assistance, applying my codebook and decision rules to Lopp's summaries, the sources he links and further reporting where available. Dataset v2 (13 November 2026) uses a revised codebook that records physical harm (C), loss of liberty (L), weapons (W) and how the attacker knew about the victim (K) as separate codes. I set the rules, have fully reviewed 11 cases so far and applied the patterns from my review to the rest, which remain provisional. The tool's figures use all cases, reviewed or not. Cases have not been independently verified, so some codes will change as reporting develops.

Which cases the tool uses. Figures from my coding use only the 109 cases that meet my definition, with one exception. The in-person trading question also draws on the 27 crypto-lure robberies that fall outside it. These are not wrench attacks by my definition, because the target was cash, but they are a real physical risk to anyone trading crypto in person, so they count as evidence for that question only.

Key figures from my coding (Dataset v2, n = 109):

- **Access:** where the method was reported, 31 of 39 cases involved forced transfers and 11 password or PIN coercion (some both); 46 attacks obtained nothing.
- **Physical harm and liberty:** injury or worse in 49 cases (32 injury, 12 grievous harm, 5 fatal); 29 victims abducted and 9 more held for an hour or longer. A weapon was reported in 56 cases, most often a gun (21).
- **Location:** France 48 cases; Russia and the United States 7 each.
- **Selection:** 96 coded as targeted; 35 involved a relative or household member as leverage (proxy targeting). How the attacker knew about the victim was clear in 43 cases: insider 18, leaked data 10, public profile 10, a trade 4, no prior knowledge 1.
- **Amounts:** completed forced transfers ranged from about US$1,000[49] to over US$1 million,[23][51] and one family was attacked over €100.[50]

Family targeting across sources. My first coding (Dataset v1) found proxy targeting in only 7 of 103 cases, because each case could take only one selection code. Dataset v2 records a relative or household member used as leverage alongside targeting (A-TG/PX as well as A-PX) and finds it in 35 of 109 cases (32%). This is close to, and slightly above, Chainalysis's estimate that family members or acquaintances were targeted in 25–30% of 2026 incidents,[5] which also counts acquaintances. Gart gives no percentage, but it documents partners, children and parents targeted in early-2026 French cases (p. 26) and an attempted abduction of an executive's daughter (p. 44).[6] The Household area now rests on my own figure, with Chainalysis as a cross-check.

Question design

An initial set of 18 questions was drafted with AI assistance. I then edited, cut and added questions to reach 20, and each was assigned to an area based on the evidence above. Answers run from 0 (safest) to 3 (riskiest). Where a question has three answers, the option that removes all protection scores the full 3 points. The weapons question comes last because it only tailors advice and carries no points.

#	Area	Question	Answers (points)	Rationale
1	Visibility	Do people know you hold crypto?	No one knows (0); A few trusted individuals (1); A wider circle: friends, extended family or a small social media following (2); I am publicly known in crypto (3)	96 of 109 cases coded as targeted[2]; public figures among news-reported victims (p. 24:11)[3]
2	Visibility	Have you given ID (KYC) to exchanges?	No (0); One service (1); Several services (2); Yes, and my data was in a leak (3)	Leaked exchange data used to find home addresses (p. 10)[6]; Ételfay (Waltio leak) [22] and Brétigny (hacked data)[52]
3	Visibility	Could a stranger find your home address from public sources?	Very unlikely (0); Possibly (1); Likely (2); Yes, easily (3)	Home invasions were 21.3% of 305 cases (p. 20); property and company registries used to locate homes (p. 10)[6]
4	Visibility	How visible are you at crypto events?	I don't go (0); Occasionally (1); Regularly (2); I speak or am recognisable (3)	Public figures targeted, some more than once (pp. 24:11, 24:17)[3]
5	Visibility	Do you live where tax or wealth records are public by law?	No (0); Yes, but limited (2); Yes, very transparent (3)	Tax and wealth records and property registers used to identify targets and estimate wealth (p. 10); a tax official accused of searching tax data for crypto holders (p. 11) [6]

#	Area	Question	Answers (points)	Rationale
6	Wealth signals	Do you talk about your specific holdings or gains?	Never (0); Close friends only (1); Group chats or forums (2); Publicly, or I show them off (3)	Boasting named as an opportunistic trigger[4]; privacy as first defence[8]
7	Wealth signals	Is crypto part of your work?	No (0); Behind the scenes (1); Founder, executive or known trader (2); Visible service: exchange, OTC, ATM (3)	Exchangers, executives and traders recur in 2026 cases, e.g. Andijan[32] and Hung Hom[40]
8	Wealth signals	Does your lifestyle signal wealth?	No (0); A little (1); Noticeably (2); Clearly: cars, watches, luxury (3)	Visible wealth draws attention[8]; Pattaya[24]
9	Access speed	How much could you send right now from the devices you carry?	Under US$1,000 (0); US$1,000–10,000 (1); US$10,000–100,000 (2); Over US$100,000, or most holdings (3)	Thresholds set from the range of completed forced transfers in 2026[49][23][51]; see Validity on Western bias
10	Access speed	How is your main stash secured?	Multisig, keys apart (0); Hardware wallet away from home (1); Hardware wallet or seed phrase at home (2); Exchange or phone app (3)	Geographic key separation stops forced transfers[8]
11	Access speed	Is there any delay before large amounts can move?	Time-locks or a vault (0); Withdrawal limits (1); No deliberate delay, but several devices (2); Instant (3)	Delays remove the payoff of coercion[8]
12	Access speed	Do you have a plan for what to do under duress?	Yes, practised (0); Yes, untested (1); No (3)	A Rome victim's emergency code blocked all transfers[14]

#	Area	Question	Answers (points)	Rationale
13	Household	Is anyone else able to access your crypto?	Only me (0); My partner (1); Immediate family (2); Wider family, staff or friends (3)	Reasoned: anyone who can move funds can be targeted instead
14	Household	Who lives with you or depends on you?	Alone (0); A partner (1); Children or elderly parents (2); Family and/or household staff (3)	Relative or household member used as leverage in 35 of 109 cases (32%)[2]; relatives or acquaintances in 25–30% (industry estimate)[5]; partners and families targeted in early-2026 cases (p. 26)[6]; Sallanches[34], Voiron[35]
15	Household	Would your family know what to do if someone used them to reach you?	Yes, we have a plan (0); Roughly (1); No (3)	Proxy targeting[5]; a security expert warned attackers may go through family as an easier route (p. 24:16)[3]; household plans recommended[9]
16	Routines	Do you buy or sell crypto in person (P2P, OTC, for cash)?	Never (0); Sometimes (2); Regularly (3)	About a quarter of news-reported incidents happened during P2P trades (pp. 24:10, 24:18)[3]; P2P trades 10.5% of 305 cases (p. 20)[6]; 27 crypto-lure robberies in 2026[2]
17	Routines	How predictable are your movements?	Unpredictable (0); Somewhat (1); Very predictable, or shared online in real time (3)	Street abductions and ambushes, e.g. Saint-Léger-sous-Cholet[46] and Saint-Paul[45]

#	Area	Question	Answers (points)	Rationale
18	Routines	How secure is your home?	Alarm, cameras, strong entry (0); Some measures (1); Basic locks (2); Nothing in particular (3)	Alarms drove off attackers in Loire-Atlantique[16] and Grivesnes[17]; 17 foiled attacks (5.6%) in Gart (pp. 20, 35)[6]
19	Routines	Do you live in or regularly travel to places with many reported wrench attacks?	No (0); Sometimes travel to them (1); Live in or regularly travel to them (3)	France 48 of 109 cases in my coding[2]; Europe 39 of 52 in CertiK[7]; Gart rates countries per million crypto holders (p. 28)[6]
20	Context (not scored)	Which of these do you keep in your main home? (tick all)	Firearms; Knives, swords or blades; Improvised weapons; None	No evidence that weapons lower risk; La Roche-sur-Yon[48]; used only to tailor advice

Short helper notes appear under questions 5, 9, 13, 15, 16 and 19, and cite their sources in plain words. Question 15's note gives my own figure (35 of 109) beside the industry estimate. Question 19 links to Lopp's interactive data.

Scoring model

Scores are calculated in four steps, all in the user's browser.

1. **Points.** Each answer carries 0 to 3 points, as listed above. Question 20 carries none.
2. **Area scores.** Each area's score is the points earned as a share of the most that area allows.
3. **Overall score.** A weighted average of the five area scores.
4. **Band and red flags.** The overall score sets the band; any red flag lifts a Lower result to Moderate. The result is a relative exposure score, not a probability: 65% does not mean a 65% chance of being attacked.

$$\text{Area score} = 100 \times \frac{\sum \text{points earned in the area}}{\sum \text{maximum points in the area}}$$

$$\text{Overall} = 0.25\,V + 0.20\,W + 0.20\,A + 0.20\,H + 0.15\,R$$

Weights. The weights are expert judgement, not empirical coefficients: they were not derived statistically or tested against who is actually attacked. The table sets each weight beside the closest figure the data offers.

Area	Questions	Max points	Weight	Closest measurable figure	What it shows
Visibility (V)	1–5	15	25%	96 of 109 cases targeted (88%); source of knowledge clear in 43, of which 20 were a public profile or leaked data[2]	Most victims were chosen, and being findable is what most directly decides who is chosen, so this area has the highest weight
Wealth signals (W)	6–8	9	20%	No direct measure	Supported by research,[4] [8] not counted in the data
Access speed (A)	9–12	12	20%	Forced transfers in 31 of 39 cases with a known access method[2]	How funds are taken, not who is chosen: attackers usually can't see how fast a victim can reach their keys, so this area mainly shapes how long an attack lasts and how much is lost
Household (H)	13–15	9	20%	35 of 109 cases (32%) in my coding;[2] 25–30% per Chainalysis[5]	The sources broadly agree
Routines (R)	16–19	12	15%	17 of 109 pseudo-stranger cases (16%),[2] plus 27 lure robberies outside the definition	In-person trading is also a red flag

These figures measure different things, and how often something appears in attacks is not the same as how much it raises the chance of being attacked, so they cannot be converted directly into weights. Equal weighting (20% each) is the main alternative. Over 20,000 random answer sets, equal weights changed the band in about 5% of cases, and the earlier weights (Visibility 20%, Access speed 25%) also in about 5%. This shows the result is not very sensitive to the exact weights; it does not show the weights are right. I also ran eight example personas, from a quiet long-term holder (7.7, Lower) to a young crypto influencer (62.6, Higher); all eight landed in the same band under equal weights. Results close to 25, 45 or 65 should be read as on the border between bands. Some questions about visibility may overlap across areas and count the same exposure twice; this will be tested once real answer data exists.

Bands. The cut-offs sit below even quarters (25, 45 and 65 rather than 25, 50 and 75) on purpose: for a safety tool, wrongly reassuring someone is worse than prompting a check, so moderate exposure is not labelled Lower. The band names describe relative exposure,

not calibrated levels of danger: someone in the Highest band is not shown to face more attacks than someone in the Higher band. They have not been calibrated against outcomes, because there is no data on holders who were never attacked.

Band	Overall score
Lower exposure	Under 25%
Moderate exposure	25% to 44%
Higher exposure	45% to 64%
Highest exposure	65% and above

Red flags. Each appears repeatedly before attacks in the 2026 data, so any one keeps the result at Moderate exposure or higher and is listed on the results page:

- publicly known in crypto (question 1), e.g. the influencers in Vitória[20] and Ribeirão Preto;[21]
- data exposed in a leak (question 2), e.g. Ételfay;[22]
- over US$100,000 or most holdings on carried devices (question 9), e.g. London;[23]
- trading crypto in person regularly (question 16), e.g. Krasnoyarsk[41] and the 27 lure robberies.[2]

Worked example. Access speed answers worth 2 + 3 + 3 + 1 give 9 of 12 points, an area score of 75%. That area then contributes 75 × 0.20 = 15 points to the overall score.

Results

Profiles. Each user receives one profile, named after their highest-scoring area so the result points to where to start.

Profile	Assigned when	Example cases shown (2026)
The Quiet Stacker	Overall under 25% with no red flags	Shown as "How others stayed safe": Rome (emergency code)[14], Saint-Juery (fought off)[15], Loire-Atlantique[16] and Grivesnes[17] (alarms), Winnetka (escaped)[18]
The Visible Holder	Visibility is the highest area	Sweden[19], Vitória[20], Ribeirão Preto[21], Ételfay[22], Saint-Juery[15], London[23]

Profile	Assigned when	Example cases shown (2026)
The Beacon	Wealth signals is the highest area	Pattaya[24], Bankya[25], Koh Samui[26], Bogdanlia[27], Pasay[28]
The Open Vault	Access speed is the highest area	Alanya[29], Coconut Creek[30], Ivanovo[31], Andijan[32], Malacca[33]
The Exposed Household	Household is the highest area	Sallanches[34], Voiron[35], Saint-Martin-le-Vinoux[36], Gandhidham[37], Seine-et-Marne[38], Bender[39]
The Street Trader	Routines is highest and the user trades in person sometimes or regularly	Hung Hom[40], Krasnoyarsk[41], Chennai[42], Indore[43], Karachi[44]
The Creature of Habit	Routines is highest without in-person trading	Saint-Paul[45], Loire-Atlantique[16], Saint-Léger-sous-Cholet[46], Karachi[44], Strasbourg[47]

Ties between areas go to the area with the larger weight. Example cases were selected with AI assistance from my coded dataset to illustrate each profile, all from cases meeting my definition; each links to its source. They illustrate a profile rather than prove a risk.

Three suggested changes. The tool offers two changes from the user's highest-scoring area and one from the second (Lower results get one from each of the top three areas), each tagged by effort (Free, Low cost, Choice, Bigger change):

- **Visibility:** remove crypto from public profiles; make your address harder to find (data-broker opt-outs, checking what property, company and tax records show, a PO box); use fewer ID-holding exchanges and watch for breach notices.
- **Wealth signals:** stop sharing amounts or gains; separate your crypto work identity from home life; avoid linking visible luxury to crypto.
- **Access speed:** carry less, keeping only an affordable-to-lose amount on devices; move savings to multisig with keys apart; add a time-delay or vault and rehearse a duress plan.
- **Household:** limit who knows and who can access; agree a family plan with a code word; make sure no family member can move funds alone.
- **Routines:** avoid in-person trades, or meet in public, start small and bring someone; vary routines and stop sharing live location; improve home security.

The changes follow situational crime prevention[12] and published guidance.[3][8][9]

What-if switches. Nine switches show the effect of a change by setting that answer to its safest option and recalculating: carry under US$1,000; move to multisig; add a time-delay; make and practise a duress plan; stop talking about holdings; fewer people know; agree a family plan; stop trading in person; upgrade home security. Only switches that would change the user's answers are shown.

Weapons note. If the user keeps any weapons, the results add a note: weapons do not lower the score; one 2026 victim who fired at attackers was himself convicted;[48] and weapons kept at home can be used against the household. It advises secure storage, knowing local law, and a plan focused on getting people out.

Privacy and delivery

The tool collects nothing: there is no log-in, KYC, form, analytics or cookie, and answers never leave the user's browser or appear in the web address. Like any website, the host (GitHub Pages) can see that the page was visited, and the page loads its font from Google Fonts, so users wanting the most privacy are directed to the offline copy.

- **Online:** a single page hosted on GitHub Pages, showing the date the data was last reviewed.
- **Offline:** a "Download for offline use" button saves a fresh copy of the page that runs without an internet connection; only the source links need one.
- **Paper:** a print view turns the tool into a self-scoring checklist with the same questions, the same points and the same red-flag rule, scored without area weights (see below).

Is the paper version weighted the same? No. The paper version adds raw points out of 57 with no weights, because a weighted sum is hard to calculate by hand. It is a simplified alternative, not an exact copy. Its band cut-offs are the same percentages applied to 57 points: 0–14 Lower, 15–25 Moderate, 26–37 Higher, 38 and above Highest exposure. Both versions compare the exact percentage with the cut-offs, so 14 points (24.6%) is Lower. Because Visibility is weighted more online, someone near a cut-off can land in a different band on paper. Its purpose is the same: a private record a family can fill in together without a device.

Validity and limitations

The percentages are exact arithmetic, but the points, weights and band cut-offs are researcher judgement informed by evidence, not a validated statistical model.

- **No comparison group.** There is no data on crypto holders who were never attacked, so the tool cannot estimate a true probability of attack. The figures describe reported attacks, not raised likelihood: 88% of victims being targeted does not tell us how much more likely a visible holder is to be attacked than an invisible one. This is why it leads with bands and a profile rather than a single number. An anonymous survey of holders who were never attacked would allow a comparison; this is future work.
- **AI-assisted coding from limited sources.** The underlying cases were coded with AI assistance from Lopp's summaries, the sources he links and further research where reporting allowed, under my rules and review. In Dataset v2 I have fully reviewed 11 of the 147 cases so far; the rest are provisional. Codes have not been independently verified and may change as fuller reporting emerges.
- **Single coder, no reliability test.** Inter-rater reliability testing means two or more people code the same cases independently and their agreement is measured, usually with Cohen's kappa,[13] where 1 is perfect agreement and 0 is chance. It shows a codebook is clear enough that results do not depend on one person's reading. This has not yet been done.
- **Mixed datasets.** Figures come from five sources with different periods and definitions (see Evidence base). Where they disagree, the tool uses the more cautious figure. On proxy targeting my Dataset v2 figure (32%) is now close to Chainalysis (25–30%).[2][5] Gart's database is built on Lopp's, so agreement between Gart and my coding is not independent confirmation.[6]
- **Partial year.** 2026 data runs only to 31 October 2026.[1]
- **Reported cases only.** All datasets miss unreported attacks, which researchers believe are many.[4]
- **Western and media bias.** Most reported cases come from Europe, North America and parts of Asia, and coverage favours violent, newsworthy and English- or French-language cases. The dollar thresholds in question 9 reflect these settings: under US$1,000 may be a small sum in Western Europe but a large one elsewhere, so users should judge amounts against local incomes.
- **All crypto, not only bitcoin.** Neither Lopp's database nor my coding separates assets, and many 2026 cases involved USDT. Findings apply to crypto holders generally, and bitcoin-specific defences such as multisig may not be available for every asset.
- **Self-report.** Results depend on honest, accurate answers, and people tend to underestimate how visible they are.
- **Hand-picked examples.** Profile case examples illustrate rather than prove risk.
- **Point in time.** Weights and figures reflect the data at the last review, and will be reviewed at regular intervals.

Notes

1. Lopp, J. Known Physical Bitcoin Attacks. Entries dated 1 January to 31 October 2026, downloaded 10 November 2026.
2. El the Freedom Fairy (2026). Wrench attack definition, codebook and coded 2026 case dataset, published in El's Wrench Attack Coding Tool 2026 and its companion methodology.
3. Ordekian, M., Atondo-Siu, G., Hutchings, A. and Vasek, M. (2024). Investigating Wrench Attacks: Physical Attacks Targeting Cryptocurrency Users. 6th Conference on Advances in Financial Technologies (AFT 2024), LIPIcs vol. 316, Article 24, pp. 24:1–24:24. DOI 10.4230/LIPIcs.AFT.2024.24.
4. Ordekian, M. et al. (2025). $5 Wrench Attacks: When Cryptocurrency Crime Get Physical. Bentham's Gaze. A plain-language summary of [3].
5. Chainalysis (2026), report on violent crypto attacks to late June 2026, as reported by The Block and CoinMarketCap. Reports family members or acquaintances targeted in about 25–30% of incidents, a broader category than my proxy code; used only as a cross-check for the Household area.
6. GART Research (2026). Kidnapping, Ransom, and Physical Attacks: Challenges in Cryptocurrency Security. Analysis of 305 Documented Attacks (2014–2026). February 2026. Built on and expanded from Lopp's database (p. 12); published by a commercial security firm.
7. CertiK (2026). Intel3D H1 2026 Wrench Attacks, 23 July 2026.
8. Casa. How to protect your bitcoin from $5 wrench attacks.
9. Casa. The bitcoiner's guide to physical security.
10. Cohen, L. E. and Felson, M. (1979). Social change and crime rate trends: a routine activity approach. *American Sociological Review*, 44(4). Citation from memory; check before publishing.
11. Hindelang, M. J., Gottfredson, M. R. and Garofalo, J. (1978). *Victims of Personal Crime*. Citation from memory; check before publishing.
12. Cornish, D. B. and Clarke, R. V. (1986). *The Reasoning Criminal*; Cornish, D. B. (1994), crime scripts, *Crime Prevention Studies* 3; Clarke, R. V. (1999), *Hot Products* (CRAVED). Citations from memory; check before publishing.
13. Cohen, J. (1960). A coefficient of agreement for nominal scales. *Educational and Psychological Measurement*, 20(1). Citation from memory; check before publishing.
14. 7 June 2026, Rome, Italy. Lopp line 760. Source
15. September 2026, Saint-Juery, France. Lopp line 795. Source
16. 16 March 2026, Loire-Atlantique, France. Lopp line 727. Source
17. 17 July 2026, Grivesnes, France. Lopp line 780. Source

18. 8 March 2026, Winnetka, United States. Lopp line 718. Source
19. 13 January 2026, Sweden. Lopp line 681. Source
20. 11 June 2026, Vitória, Brazil. Lopp line 763. Source
21. 3 July 2026, Ribeirão Preto, Brazil. Lopp line 775. Source
22. 5 June 2026, Ételfay, France. Lopp line 759. Source
23. 4 March 2026, London, England. Lopp line 714. Source
24. 6 October 2026, Pattaya, Thailand. Lopp line 810. Source
25. 25 July 2026, Bankya, Bulgaria. Lopp line 783. Source
26. 29 April 2026, Koh Samui, Thailand. Lopp line 747. Source
27. 10 March 2026, Bogdanlia, Bulgaria. Lopp line 724. Source
28. 16 January 2026, Pasay City, Philippines. Lopp line 684. Source
29. 12 February 2026, Alanya, Turkey. Lopp line 708. Source
30. 8 June 2026, Coconut Creek, United States. Lopp line 761. Source
31. 6 September 2026, Ivanovo, Russia. Lopp line 803. Source
32. January 2026, Andijan, Uzbekistan. Lopp line 671. Source
33. 17 April 2026, Malacca, Malaysia. Lopp line 742. Source
34. 14 January 2026, Sallanches, France. Lopp line 683. Source
35. 25 January 2026, Voiron, France. Lopp line 691. Source
36. 4 February 2026, Saint-Martin-le-Vinoux, France. Lopp line 700. Source
37. 21 July 2026, Gandhidham, India. Lopp line 782. Source
38. 20 May 2026, Seine-et-Marne, France. Lopp line 756. Source
39. 27 January 2026, Bender, Transnistria. Lopp line 692. Source
40. 6 March 2026, Hung Hom, Hong Kong. Lopp line 715. Source
41. May 2026, Krasnoyarsk, Russia. Lopp line 751. Source
42. 19 August 2026, Chennai, India. Lopp line 790. Source
43. 7 February 2026, Indore, India. Lopp line 703. Source
44. 17 June 2026, Karachi, Pakistan. Lopp line 766. Source
45. 27 March 2026, Saint-Paul, France. Lopp line 732. Source
46. 9 January 2026, Saint-Léger-sous-Cholet, France. Lopp line 678. Source
47. 31 March 2026, Strasbourg, France. Lopp line 734. Source
48. 31 October 2026, La Roche-sur-Yon, France. Lopp line 815. Source
49. July 2026, Moscow, Russia (about US$1,000 transferred). Lopp line 772. Source
50. 13 July 2026, Taverny, France (€100). Lopp line 777. Source
51. 2 July 2026, Bali, Indonesia (US$5 million). Lopp line 774. Source
52. 21 October 2026, Brétigny-sur-Orge, France. Lopp line 812. Source