

Nine Rules of Whale Safety

For large crypto wallet holders.

A short guide for you and the people around you.

01 **Keep your wealth and whereabouts private.**

02 **Don’t let one person unlock the reserves.**

03 **Don’t let your phone unlock everything.**

04 **Secure your home. Control who gets in.**

05 **Meet in public. Keep control of where you go next.**

06 **Vary your routine. Pay attention when arriving and leaving.**

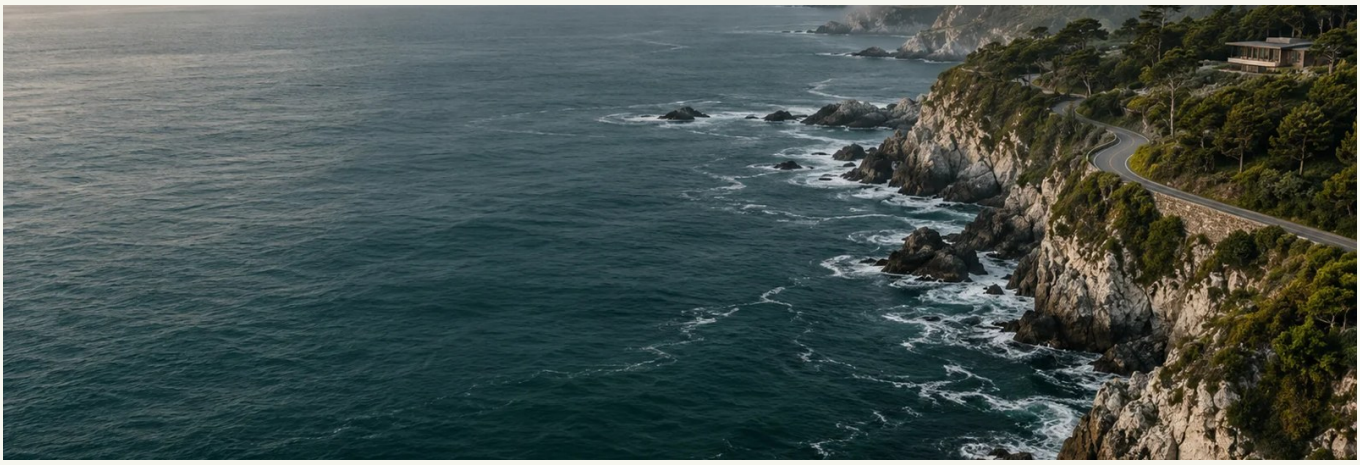
07 **Practise a plan with people you trust.**

08 **During an attack, put people before money.**

09 **Take threats seriously—even after an attack ends.**

Read more. Make a plan. Follow new cases.

01 Keep your wealth and whereabouts private.



Share less about what you own and where you will be.

Look at what others can see.

Review public wallet links, interviews, home photos and live travel posts. Agree privacy boundaries with family and staff; consider information held by service providers, too.

Share only what is needed.

Someone arranging your car needs a pickup time, not your balance or full itinerary. Post trips after you leave.

Plan for old leaks.

Deleting a post does not erase copied data. If an account is breached, check whether it exposed your home or movements.

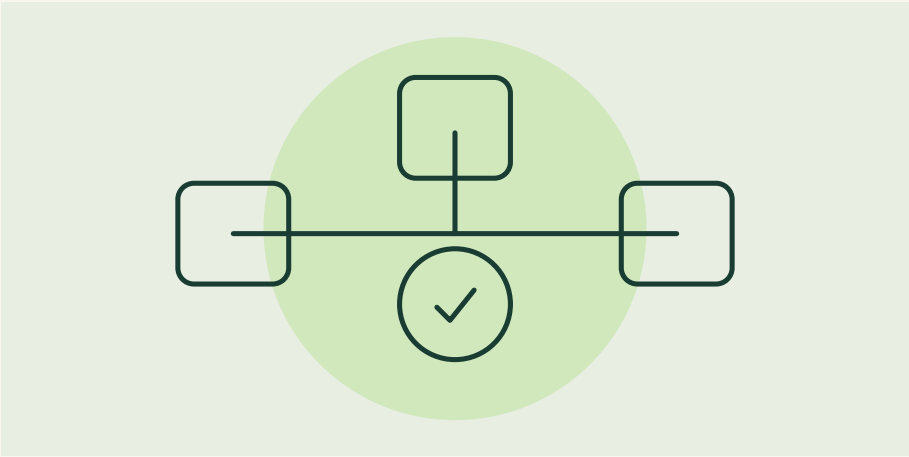
ONE THING TO DO

Check what your name, handle and recent posts reveal.

A US sentencing account describes attackers using a compromised iCloud account to track a victim before a home burglary.

Read the sources and supporting guidance online

02 Don’t let one person unlock the reserves.



Build in independent checks that you cannot simply bypass.

Separate spending from reserves.

Keep routine funds available. For substantial reserves, consider independent approval and withdrawal restrictions with qualified help.

Check the shortcuts.

Include recovery keys, account resets and instructions to assistants. Another device or property is not independent protection if you can retrieve it or order access.

Test recovery, too.

Choose an arrangement you can maintain and recover if a signer or device is lost. Practise independent approval; recognising your voice does not prove you are acting freely.

ONE THING TO DO

Ask: what could I transfer, reset or have released on my own?

In Minnesota, attackers forced a victim to another property for devices. Geographic separation alone did not prevent the theft. Transfer restrictions cannot guarantee personal safety.

Read the sources and supporting guidance online

03 Don’t let your phone unlock everything.



Carry only the access you need. Remember what the screen can reveal, too.

Limit what the phone can reach.

Keep everyday spending and unfamiliar apps away from reserves. Include your laptop, cloud backups and account recovery. Deleting a wallet app alone does not cut access.

Protect the recovery routes.

Secure email, cloud accounts and password recovery. Use passkeys or strong two-step verification where supported, with tested backups.

Verify before acting.

Check ordinary money requests through a separate, known contact route. Avoid showing balances or handing over an unlocked phone. A read-only portfolio can still reveal your wealth.

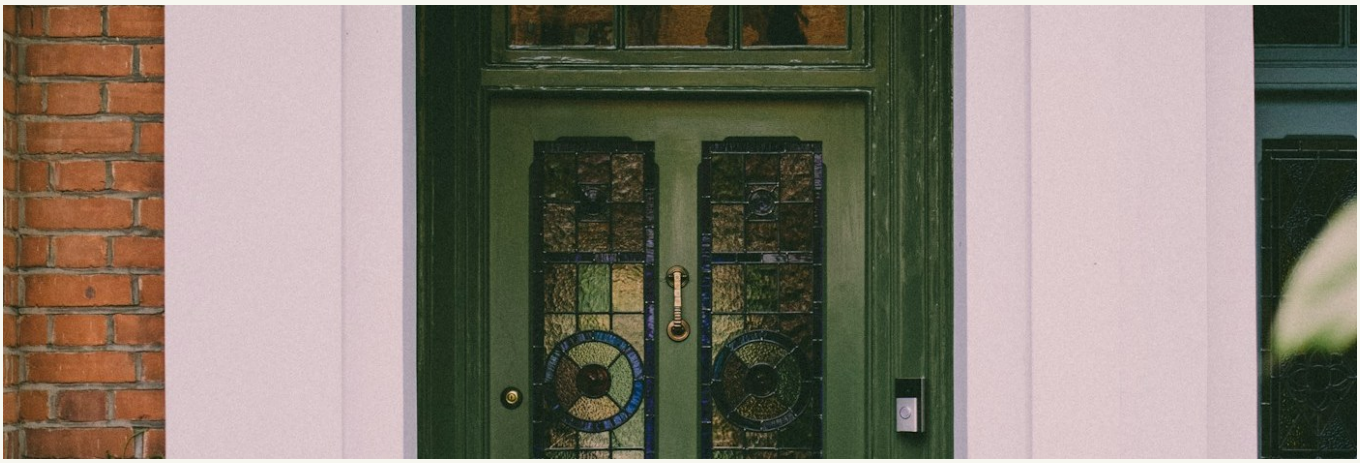
ONE THING TO DO

Imagine someone holding your unlocked phone. What could they see, spend or reset?

Taiwan reporting describes a seller’s phone being seized after an account demonstration and used to transfer bitcoin. The exact account controls were not established.

Read the sources and supporting guidance online

04 Secure your home. Control who gets in.



Strengthen the entrance. Agree what happens if it fails.

Review the whole entrance.

Have a qualified installer assess doors, frames, locks and reachable windows. Include garages and shared-building access; keep fire exits usable. Review your workplace and accommodation, too.

Verify before opening.

Use the intercom and an independently known contact. A uniform, your name or an expected delivery is not proof. Apply the same rule to hotel visitors.

Know who responds.

Lighting, cameras and alarms need a response. Practise where to seek safety, how to call for help and who acts on an alert—including when you are away.

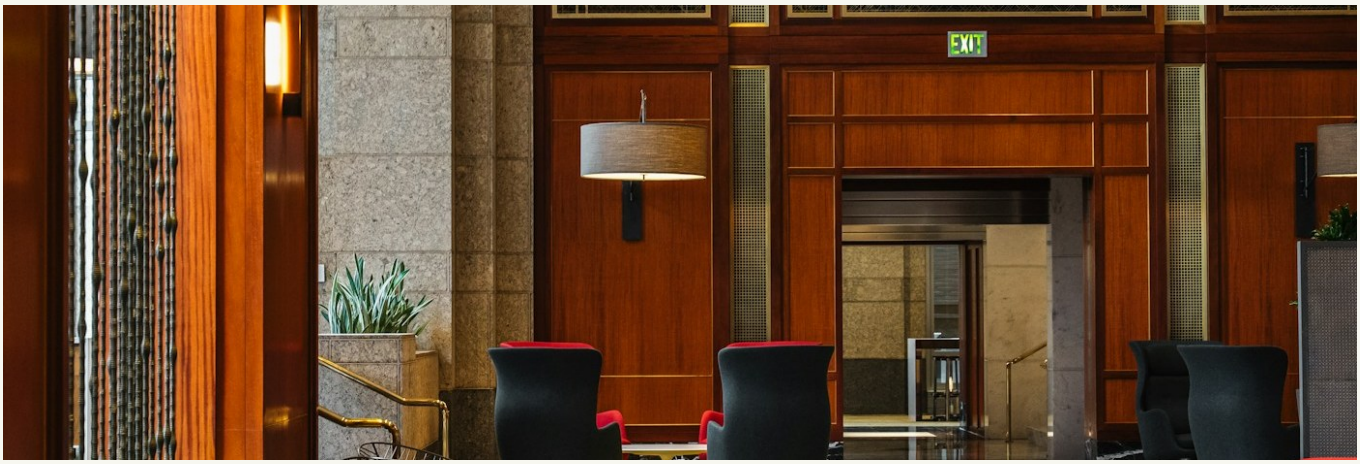
ONE THING TO DO

Walk through an unexpected visitor scenario with everyone at home.

A US indictment alleges that attackers posed as delivery workers to enter crypto holders' homes. These are allegations, not convictions.

Read the sources and supporting guidance online

05 Meet in public. Keep control of where you go next.



A lobby, a private room and a car are different decisions.

Choose a staffed public place.

For people you are unsure of, choose a busy, staffed venue and arrange your own way home. Apply the same care to dates, introductions and business meetings.

Treat a venue change as a new decision.

An invitation upstairs, into a car or to an afterparty is a fresh decision. A referral or previous successful meeting does not make the next setting safe.

Keep settlement separate.

Avoid large-cash handovers and wallet demonstrations at introductory meetings. Use lawful, independently verified services; a successful small trade proves little about a larger one.

ONE THING TO DO

Set the exact venue, your return journey and a check-in before you go.

The Tokyo hotel-room case and Singapore cash-meeting case show different problems: private access and cash exposure. A public location alone does not make a deal safe.

Read the sources and supporting guidance online

06 Vary your routine. Pay attention when arriving and leaving.



Vary familiar journeys. Pay attention at arrivals and departures.

Vary safely.

Where practical, vary familiar times and routes while staying on sensible, well-used roads. Avoid creating a more isolated journey just to be unpredictable.

Check the pickup.

Match the vehicle and driver to your booking; knowing your name is not enough. Check your surroundings before getting in or out. Plan the return before a night out.

Seek help if followed.

Avoid going home or confronting the person. Seek a staffed, busy place and assistance. Share travel details privately with someone trusted.

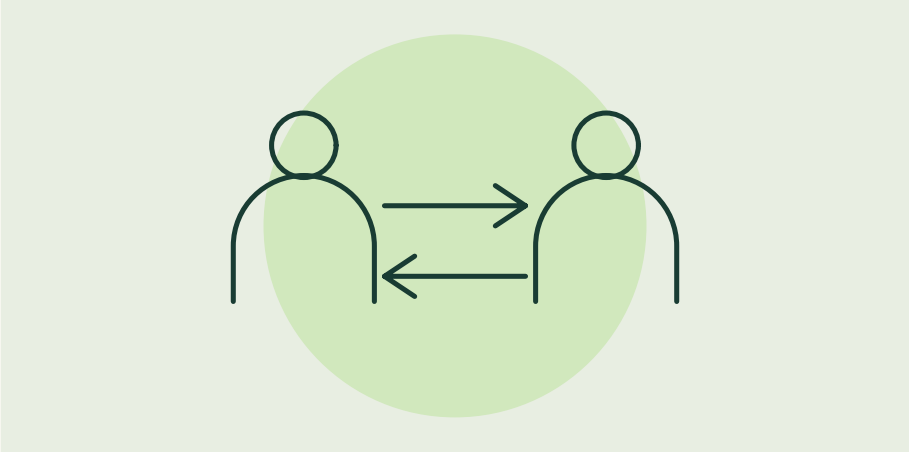
ONE THING TO DO

Review the journey after your next meeting, not just the meeting itself.

Personal-security guidance identifies arrivals, departures, vehicle entry and predictable journeys as moments to pay particular attention.

Read the sources and supporting guidance online

07 Practise a plan with people you trust.



Agree who notices, who acts and how to get help. Include someone outside the household.

Choose the right people.

Include trusted family, carers and staff as appropriate. If a partner, relative or business associate is threatening you, seek confidential support outside that relationship.

Agree when someone acts.

Agree visitor and child-pickup rules, check-ins and a backup contact. Rehearse what happens if you miss a check-in. Credible danger should not wait for a fixed deadline.

Practise an unusual money request.

A genuine voice can still be speaking under coercion. A code word is one possible signal, not proof of safety. Seek professional help when danger is credible.

ONE THING TO DO

Ask who would notice if you and your partner became unreachable together.

In a Wuhan prosecutor account, a relative was forced to send a genuine voice confirmation. The remote holder then transferred USDT. Identity did not establish safety.

Read the sources and supporting guidance online

08 During an attack, put people before money.



Survival comes first. No wallet can promise your release.

Protect life.

Do not fight over property or attempt to disarm someone. Avoid sudden movements and seek help as soon as it is safe.

Understand the duress-wallet limits.

A separate wallet intended for surrender may not satisfy an attacker who expects more or suspects hidden accounts. There is no reliable universal amount or promise of release.

Plan before a crisis.

Discuss any duress wallet or alert system with a qualified adviser beforehand. People helping you should seek crisis advice before blocking transfers while anyone remains captive.

ONE THING TO DO

Keep “protect people” separate from “prevent a transfer” in your plan.

The sources disagree on decoy wallets. Bankless questions their reliability; Hodlguard and SEAL discuss possible uses. None establishes a dependable way to make an attacker release someone.

Read the sources and supporting guidance online

09 Take threats seriously—even after an attack ends.



A payment, escape or release may not end the danger.

Take the warning seriously.

Act on threats, attempted entry or suspected following, including from people you know. Do not meet a threatening counterparty alone to settle a dispute.

Get support from safety.

From a safe place, seek medical care, police or specialist support as needed. Preserve evidence. Review where you stay and who can reach you; keep recovery arrangements private.

Secure access and keep checking.

When safe, review exposed devices, accounts, keys and recovery access with trusted help. Include psychological support. Be wary of unsolicited offers to recover stolen funds.

ONE THING TO DO

Choose a trusted contact and professional support before you need them.

Greater Manchester Police documented repeated extortion and abductions of the same victim. Payment and release did not end the targeting.

Read the sources and supporting guidance online

Before you rely on this guide

An educational guide.

Whale Safety helps you prepare. We do not provide emergency assistance or personal case support. Incident submissions are for editorial review, are not monitored in real time, and do not notify police.

Fit the plan to your life.

These are general suggestions, not a personal security assessment or legal, financial or medical advice. Check local law and get qualified advice for your home, custody setup and travel.

Duress wallets have limits.

An attacker may already know your holdings or keep demanding more. Hidden funds, time delays and extra signers may not end coercion. Plan these arrangements with qualified help before a crisis.

Evidence is uneven.

The guide draws on research, published reporting, talks and practitioner guidance, including the supplied partner material and Claude reference PDF. Cases illustrate risks, not proof that a precaution would have prevented an attack.

This is a living guide.

Independent security-expert review is pending. The wider incident register contains unverified leads; we have not closely reviewed every linked source. See the website for source labels and corrections.

Presented by DeGate.

This educational guide is not a security certification or a promise about any financial product. Reading it requires no account, wallet connection or proof of wealth.

Go deeper.

The website holds the full sources, cases and updates. Start with these readings.

Bankless: separate spending and reserves, 17:24

Bankless: custody and coercion, 61:06

Rigel Walshe: The Hodlguard, full talk and Q&A

The Hodlguard: presentation slides

Ordekian et al.: Investigating Wrench Attacks, AFT 2024

SEAL: defensive design principles; contributor guidance

SEAL: incident response; contributor guidance

Police.uk: personal safety

US DOJ: delivery impersonation allegations

The nine rules

Case studies & incident map

My safety plan

Submit an incident for editorial review

Whale Safety
Read. Save. Return.

Photographs illustrate settings, not incidents. Lobby: Josh Hild. Airport: Lennart Rudolph. Entrance: Edward Howell. Photos via Unsplash; source links are on the website. Coast: existing site artwork. Diagrams: Whale Safety.