Shopping, Marketplace, and Rental Scams

KB-AK011

1. Reduce discoverable personal context before an adversary can weaponize it. Audit public profiles, family posts, data-broker listings, school/activity rosters, old breach exposure, and household routines; remove or limit unnecessary details and teach family members to treat unexpected personalized contact as a verification trigger.
2. Reduce live routine signals such as travel posts, school schedules, caregiving patterns, check-ins, and repeated location cues. Share sensitive updates after the fact with limited audiences, and treat messages timed to your circumstances as suspicious until verified. Apply this rule consistently across channels so the decision is governed by verification, documented evidence, and trusted review instead of the adversary's framing.
3. Control the first contact instead of accepting the adversary's chosen channel. Use known phone numbers, official apps, bookmarked sites, and trusted intermediaries; do not click supplied links, scan unexpected codes, or continue a sensitive conversation inside a new channel chosen by the sender.
4. Break the secrecy instruction immediately by telling one trusted person and moving the decision into a shared review process. Legitimate helpers will not require isolation from family, caregivers, schools, banks, or advocates. Apply this rule consistently across channels so the decision is governed by verification, documented evidence, and trusted review instead of the adversary's framing.
5. Create a pause-and-verify rule for Marketplace and Search Placement. Before acting, confirm the claim through an independent source, involve a trusted reviewer, preserve evidence, and refuse secrecy, payment, credentials, data, or device access until the request is verified.
6. Separate claims from evidence. Verify identities, emergencies, brands, documents, and stories through independent sources before acting, and preserve screenshots or message headers when something seems staged or inconsistent.
7. End the call and restart through a trusted number from a bill, card, portal, school directory, or official website. Do not provide codes, payment, remote access, or personal details to anyone who reached you first. Apply this rule consistently across channels so the decision is governed by verification, documented evidence, and trusted review instead of the adversary's framing.
8. Pause all payment movement and use a second reviewer before sending funds. Never use gift cards, crypto, wire transfers, payment apps, or overpayment refunds for unexpected requests; call the bank or merchant through verified channels.
9. Check whether the proof can be verified outside the adversary-controlled page or thread. Search independently for the organization, person, complaints, registration, and original source of testimonials or images. Apply this rule consistently across channels so the decision is governed by verification, documented evidence, and trusted review instead of the adversary's framing.
10. Put waiting periods and outside review around offers that promise money, romance, recognition, comfort, or exclusive access. Require written terms, independent search, no upfront fees, and no sharing of intimate images, credentials, or financial details.

11. Use a pre-agreed family verification phrase, call the person directly, and contact local emergency or institutional channels yourself. Do not send money, codes, travel details, or documents while panic is driving the decision. Apply this rule consistently across channels so the decision is governed by verification, documented evidence, and trusted review instead of the adversary's framing.
12. Refuse to act on the imposed timeline. Capture the message, independently contact the court, agency, school, employer, or company, and require written documentation before any payment, disclosure, or account change.
13. Avoid revealing where you bank, invest, work, receive benefits, store crypto, or manage important accounts. Keep financial and account details out of public posts and casual chats, and use account alerts so unusual access or payment requests are caught quickly. Apply this rule consistently across channels so the decision is governed by verification, documented evidence, and trusted review instead of the adversary's framing.
14. Treat pressure as evidence that verification is needed. Refuse secrecy, deadlines, threats, and fear-based demands until the claim is checked through official channels and a trusted supporter has reviewed it.
15. Use a password manager, passkeys or MFA, and official account recovery pages only. Never share one-time codes, recovery links, passwords, session tokens, or screen access with someone who initiated contact.
16. Protect accounts, devices, and finances with layered safeguards. Use password managers, passkeys or MFA, device updates, account alerts, transaction limits, and a rule that no one receives codes, remote access, or payment instructions through an unsolicited conversation.
17. Make money, data, identity, labor, and access movement reversible, documented, and reviewable. Refuse gift cards, crypto, wire transfers, payment apps, check overpayment schemes, credential sharing, and secrecy; use official support or bank fraud channels before complying.