Identity Theft and Personal Data Misuse

KB-AK037

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. 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.
3. 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.
4. Confirm identity through an independent contact path and ask for a detail the real person or organization can verify outside the suspicious conversation. Treat refusal, urgency, or channel switching as a stop signal. 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. Share the minimum data necessary only through verified portals. Redact unneeded details, decline requests for full identity documents in chat, and confirm why each data element is required before submitting it.
6. Prevent the adversary from shaping the victim's choices, information flow, or access to help. Keep outside counsel involved, preserve independent communication channels, and reject demands that limit what the target can read, say, verify, or disclose.
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. 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.
9. 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.
10. 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.
11. Escalate when safety, dignity, identity, reputation, devices, or family stability are at risk. Preserve evidence, involve trusted supporters, contact platforms, schools, banks, legal aid, or

emergency services as appropriate, and prioritize the victim's physical and emotional safety over embarrassment.