



Impersonation and Authority Scams

KB-AK006

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. Notice questions or content that probes fear, loneliness, grief, money stress, health needs, desire for opportunity, or trusted beliefs. Slow the exchange, decline to share sensitive context, and ask a trusted person to review the interaction before the other party can personalize pressure. 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. 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.
5. 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.
6. 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.
7. 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.
8. 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. Apply this rule consistently across channels so the decision is governed by verification, documented evidence, and trusted review instead of the adversary's framing.
9. 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.





10. Break isolation early. Keep sensitive decisions inside a circle of trusted people, use family code words for emergencies, and make it normal to ask for help before sending money, data, photos, or access.
11. 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.
12. 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. Apply this rule consistently across channels so the decision is governed by verification, documented evidence, and trusted review instead of the adversary's framing.
13. 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.

