Inappropriate Content Exposure

KB-AK041

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 the public signals an adversary could use to select you or your household. Review privacy settings, remove unnecessary age, school, family, routine, role, and hardship details from public spaces, and treat personalized unexpected contact as a reason to verify independently. 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. 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. Apply this rule consistently across channels so the decision is governed by verification, documented evidence, and trusted review instead of the adversary's framing.
6. Do not tap the supplied link or code. Open the known app or bookmarked site yourself, inspect the sender and domain, and report suspicious messages before deleting them.
7. 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.
8. 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.
9. Name the emotional lever before responding. If a message creates flattery, confusion, obligation, sympathy, or urgency, pause the interaction, slow the decision, and ask a trusted person to review the request out loud.
10. Create a pause-and-verify rule for Emotional State Manipulation. 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. Apply this rule consistently across channels so the decision is governed by verification, documented evidence, and trusted review instead of the adversary's framing.

11. Create a pause-and-verify rule for Anger or Outrage Amplification. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.