Catfishing

KB-AK013

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. Limit visibility into family, caregiver, school, church, workplace, and friend connections. Ask close contacts not to confirm private details in unexpected conversations, and use a family verification phrase for requests that claim to involve someone you know. Apply this rule consistently across channels so the decision is governed by verification, documented evidence, and trusted review instead of the adversary's framing.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.

11. 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.
12. 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. 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. 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.
14. Keep the relationship on-platform until trust is independently established, refuse financial requests and intimate-image pressure, and ask a trusted person to review inconsistencies, secrecy, or rapid emotional escalation. Apply this rule consistently across channels so the decision is governed by verification, documented evidence, and trusted review instead of the adversary's framing.
15. 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.
16. 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.
17. 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.
18. 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.