DIGITAL DEFENSE ALLIANCE | AHEF DEFENSE LIST

Outing, Doxing, and Forced Disclosure

KB-AK020

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. Audit what can be learned about you from search results, people-search sites, social profiles, breach notices, and public records. Remove or restrict what you can, use opt-out processes where available, and avoid answering casual questions that reveal recovery answers, routines, assets, or family structure. 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. 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.
4. 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.
5. 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.
6. Create a pause-and-verify rule for Fear, Shame, and Reputation Leverage. 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.
7. 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.
8. 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.
9. 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.

10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.