# Hacked Email Account

*KB-AK025*

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. 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.
4. 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.
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. 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.
7. 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.
8. Create a pause-and-verify rule for Lookalike Portal or Domain. 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.
9. 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.
10. 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. 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 Approval or Security Prompt Capture. 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.
12. 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.
13. 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.
14. End recurring access and repeated pressure systematically. Block, report, rotate credentials, revoke sessions and app permissions, preserve evidence, and tell trusted contacts what happened so recontact attempts are easier to recognize.
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.
17. Verify the sender domain, hover links before opening, and use a separate official channel for any request involving money, credentials, forms, files, benefits, school accounts, or account recovery.