

Unknown or General Compromise

Something seems off. Start here when you're not sure what happened.

Questions? Email hello@ohanasec.io

PHASE 1 – IMMEDIATE

Change your email password right now

- 1 Change your email password right nowYour email is the master key. If only one thing got through, this is the one to secure first.Change your email password from a trusted deviceSign out of all other sessionsCheck for forwarding rules (Settings > Forwarding)
- 2 Check your most sensitive accounts for unauthorized activityBank and credit card — check recent transactionsInvestment / brokerage accountsPayPal, Venmo, Zelle — check recent paymentsSocial media — look for posts or DMs you didn't send
- 3 Run a breach checkFind out if your email and passwords have been exposed in known data breaches.ToolsHavelBeenPwned guide — OhanaSecureHavelBeenPwned.com↗

PHASE 2 – ASSESS

Common signals and what they suggest

- 1 Common signals and what they suggestUnusual bank charges or transfers→ switch to Financial AccountEmail password reset you didn't request→ switch to Email / Central AccountPosts or DMs you didn't send on social→ switch to Social MediaYou sent money to someone you met online→ switch to Crypto / InvestmentScamPop-up saying your computer is infected, then phone call→ Tech Support Scam (follow Crypto / Investment Scam steps)You clicked a link in a suspicious email or text→ change your email and any account matching that login
- 2 Check your devices for malwareIf you think a device was compromised (slow, strange behavior, or you allowed remote access), run a scan.Windows: Windows Defender is built-in and effective for most situationsMac: Malwarebytes free version catches the most common threatsIf in doubt — back up your data and reset the device to factory settings

PHASE 3 — REPORT

Change passwords on all high-value accounts

- 1 Change passwords on all high-value accountsPrioritize: email, banking, investment, healthcare, government portals. Use unique passwords for each — this is exactly when a password manager pays off.
- 2 Enable 2FA on your most important accountsSetup guidesAuthy — authenticator appBitwarden — password manager
- 3 Report the incidentReporting resourcesFTC ReportFraud.ftc.gov↗FBI IC3 — for financial losses or wire fraud↗IdentityTheft.gov — personalized recovery plan↗

PHASE 4 — PREVENT

Use a password manager — this changes everything

- 1 Use a password manager — this changes everythingBitwarden — free, open source1Password — great family plan
- 2 Add 2FA to email, banking, and social accountsAuthy setup guideYubiKey — hardware 2FA
- 3 Freeze your credit — it's free and permanent until you unfreeze itEquifax↗Experian↗TransUnion↗
- 4 Review your digital footprintHaveIBeenPwned — check for exposed credentialsDeleteMe — remove your data from broker sites
- 5 Talk to your family — make a plan before the next incidentWho should a family member call if they think they've been hacked? What's the first three things to do? Having a simple, shared plan matters more than any single security product.Download: OhanaSecure Family Starter Checklist (PDF)

Key Resources

Official links for reporting, recovery, and prevention.

FTC ReportFraud	https://reportfraud.ftc.gov
FBI IC3	https://ic3.gov
HaveIBeenPwned	https://haveibeenpwned.com
Equifax Freeze	https://equifax.com/personal/credit-report-services/free-credit-freeze/
Experian Freeze	https://experian.com/freeze/center.html
TransUnion Freeze	https://transunion.com/credit-freeze

Need hands-on help?

OhanaSecure provides remote digital security sessions for families across the US. Email hello@ohanasec.io or visit ohanasec.io.