Responding to a breach | Aman

Aman - Dark Web Monitoring · https://www.aeserver.com/support/responding-to-a-breach-aman/

A finding in your report is a prompt to secure one specific account. In most cases it takes only a few minutes. This guide walks through what to do, in order.

Start hereA finding means information matching one of your monitored assets appeared in a breach of some other service. It does **not** mean your AEserver hosting, website or email was hacked.

Step 1. See which asset was affected

On the finding, look at **Breached Assets**. This tells you exactly which of your monitored email addresses appeared in that breach. Everything that follows applies to that address and the accounts it is used for.

Then check **Breach data found**. If passwords are listed, treat the finding as urgent. If only a name or job title appeared, the risk is lower and the main concern is targeted phishing.

Step 2. Change the password

Change the password on the account tied to the breach source, and anywhere else that password has been used. Reused passwords are how a single leak turns into several compromised accounts.

Use a password managerA password manager creates a different strong password for every account, so a leak at one service can never unlock another. It also removes the need to remember them.

Step 3. Turn on multi factor authentication

Switch on multi factor authentication wherever the account offers it. With it enabled, a leaked password on its own is not enough for someone to get in, because they would also need the code from your phone. This single step stops the large majority of account takeovers.

Step 4. Check the account for unusual activity

Look for signs the account may already have been accessed:

- sign ins from unfamiliar places or devices
- mail forwarding rules or filters you did not create
- sent messages you do not recognise
- changes to the recovery phone number or backup email

If you find anything unexpected, remove it and sign out all other sessions.

Step 5. Tell the person whose address was found

Let the colleague know their address appeared in a breach. Ask them to watch for password reset emails they did not request, unexpected login prompts, and messages that use personal details to sound convincing. Leaked information is often used to make phishing more believable.

Step 6. Work through the actions on the finding

Every finding lists its own recommended actions, tailored to the data that was exposed. Follow those, then move on to the next finding. Your threat score reflects the exposure that remains, so working through findings is what brings it down.

Quick checklist

- Identified the affected address under Breached Assets
- Checked whether passwords were among the data found
- Changed the password, and anywhere else it was reused
- Turned on multi factor authentication
- Checked the account for unfamiliar activity
- Told the colleague whose address was found
- Completed the actions listed on the finding

When to ask for help straight away If several accounts are affected, if money or customer data may be involved, or if you think someone already has access to a system, use **Get support** on the finding or contact AEserver support without waiting.

Get Aman Not monitoring your business yet? See pricing and get started.