AreYouSecured.

CONFIDENTIAL

IDENTITY EXPOSURE ASSESSMENT

Account Takeover Risk Report

alex.demo@example.com



EXPOSURE RATING

Elevated risk

6	3	2	4
Service accounts	High-value profiles	Sensitive	Findings

PREPARED FOR	ASSESSMENT DATE	REPORT ID	PREPARED BY
@alexdemo	November 21, 2026	AYS-ATR-20261121-E270	AreYouSecured SecOps

CONTENTS

About this report

This report shows where the identity behind alex.demo@example.com is exposed online, how attackers could use that exposure to take over accounts, and the exact steps to close each gap.

01	Executive summary	Exposure score and top priorities
02	Email exposure	Services this address is registered on
03	Social footprint	Public profiles and impersonation risk
04	Findings & guidance	What each finding means and what to do
05	Hardening roadmap	Prioritised, phased action plan
A	Appendix — raw data	Evidence, scope limits and notices

DOCUMENT CONTROL

Report ID	AYS-ATR-20261121-E270
Subject	**alex.demo@example.com · @alexdemo**
Assessment performed	**November 21, 2026 at 5:27 AM**
Assessment type	**Passive, open-source (OSINT); no account access**
Version	**1.0 — Final**
Classification	**Confidential — intended for the subject only**
Prepared by	**AreYouSecured SecOps · areyousecured.tech**

01 — EXECUTIVE SUMMARY

Account takeover exposure

How much of this identity is visible to attackers, and where to act first.



EXPOSURE RATING

Elevated risk

FINDINGS BY SEVERITY (4)

2 High **1** Medium **1** Low **0** Info

The assessment of **alex.demo@example.com** found **6 registered services** and **3 high-value public profiles** linked to this identity, plus 1 lower-relevance username matches listed in the appendix. **2 sensitive-category accounts were** detected. The overall exposure score is **42/100**, rated **elevated risk**.

Every linked account is a possible entry point for credential stuffing, account takeover and impersonation. The single most effective step is to secure the primary email account with app-based two-factor authentication, because it controls password resets for everything else.

TOP PRIORITIES

F-01	**Email registered on 9+ consumer services increases password-reuse blast radius.** Credential Stuffing	High
F-02	**Identity linked to finance/crypto-category platforms — high-value takeover target.** Sensitive Accounts	High
F-03	**Consistent username across many public platforms simplifies targeted impersonation.** Impersonation	Medium

42 TODAY → **88** / 100 projected

AFTER COMPLETING PHASE 1 AND 2 OF THE ROADMAP