

Protect personal attack surfaces and reputations with identiqo

- ✓ Uncover gaps in personal cyber defences for people in key C-suite positions
- ✓ Personal threat intelligence conducted to the highest standards of accuracy and trust
- ✓ Reduce the risk of CEO / investor fraud

PERSONAL DATA DETECTED

CEO targeting pattern detected

91%
CONFIDENCE

IDENTIQO DIGITAL
FOOTPRINT

Business directors and owners are high value targets

Threat actors are looking online for personal or sensitive information on senior people every day. There are no rules. Nothing is off limits. They will not think twice about leveraging information on loved ones, medical details, or financial information to achieve their objectives.

Track a persons' entire digital presence and leaked data across social media, online platforms, and the dark web

- identiqo personal threat intelligence is conducted to the highest standards of accuracy and trust. Analysts follow strict protocols and only information critical to investigations are included.
- An identiqo search leaves zero trace behind, and all communication is backed by bullet proof confidentiality agreements.

Surface fake social and professional media profiles.

See what information searches on AI platforms like Grok or Chat GPT will return on you.

Help predict likely forms of future digital led personal attacks.

Provides you with an understanding of how threat actors obtain personal information.



Scan to see your
digital footprint



Coming soon



The identiqo team understand the unique challenges faced by public figures like myself and have provided a depth of insight and intelligence I have not seen before.

[Click here to start your journey.](#)

What identiqo tells you

Your true individual level of digital exposure

Including how many times your data has been exposed in major, publicly known data breaches including instances of:

- Plaintext password exposure
- Weak encryption on key accounts
- Your data being in active circulation on criminal databases

The implication of these exposures:

Plaintext exposure

Your password has been acquired with no protection and anyone who has this data has your actual password.

Weak encryption

Your details have been acquired with some protection, but it's outdated and likely to be broken.

Your data is in circulation

And is being bought, sold, and used by criminals to try and take over accounts and steal identities.

What triage actions to take including:

- Changing passwords on impacted accounts, prioritising those linked to your email and financial services.
- Enable 2FA on all critical accounts.
- Execute a security check up on the specific services you use that you now know are breached.
- Harden your email accounts.

FUTURE BREACH RISK

82% Confidence



Recommendation:
Implement credential rotation schedule

EXECUTIVE TARGET PATTERN DETECTED

94% Confidence



Recommendation:
Enable 2FA

SPEAR-PHISHING VULNERABILITY

87% Confidence



Recommendation:
Implement email filtering rules