

Shield Your Executives from External Threats: Secure Data and Cease Impersonation Attacks

Problem

Executives & VIPs wield sensitive information, have access to high-value assets, and their reputation and influence make them prime targets for scammers who engage in social media impersonations, account takeovers, and phishing attacks. The proliferation of their personal data online represents not only a matter of individual privacy but also a critical focal point for cyber threats. Such data is a magnet for sophisticated social engineering attacks, ransomware, or spear phishing, expanding your attack surface.

Solution

Axur's cutting-edge cybersecurity platform proactively monitors both the Surface Web and the Deep & Dark Web to detect, inspect, and respond to external threats targeting your high-value accounts. Rapidly remove exposed personal information from data broker websites and take down fake social media accounts, elevating your cyber posture. Prevent threat actors and scammers from exploiting executive reputation, credentials, personal information, financial assets or sensitive data for impersonation, or social engineering attacks.

Personal Information Exposure

Monitor your Executives & VIP's personally identifiable information that may be exposed on the internet, and act quickly to protect your high-value account data and reputation.

Credential Exposure

Your sensitive and privileged access account credentials may be exposed on the internet, including for sale on darknet websites and marketplaces. Discover leaked credentials and act quickly to protect your attack surface and prevent the exposure of confidential information that could lead to spear phishing attacks, social engineering, and more.

Credit Card Exposure

Stop losses from improper purchases on corporate debit or credit cards of your Executives & VIPs. Identify card exposures to mitigate risks.

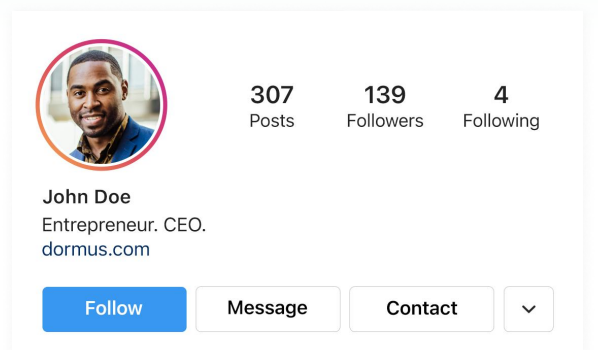
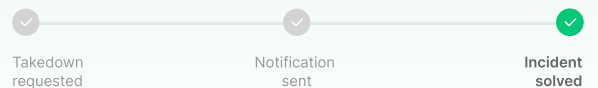
Fake Social Media Profile

Stop impersonation attacks targeting your Executives & VIPs all over social media platforms.

Experience ultra-precise detection with our exclusive FaceMatch technology, dramatically reducing false-positive rates.

Solved! Takedown in 40 minutes!

Tickets like this are usually removed in about 1 hour.



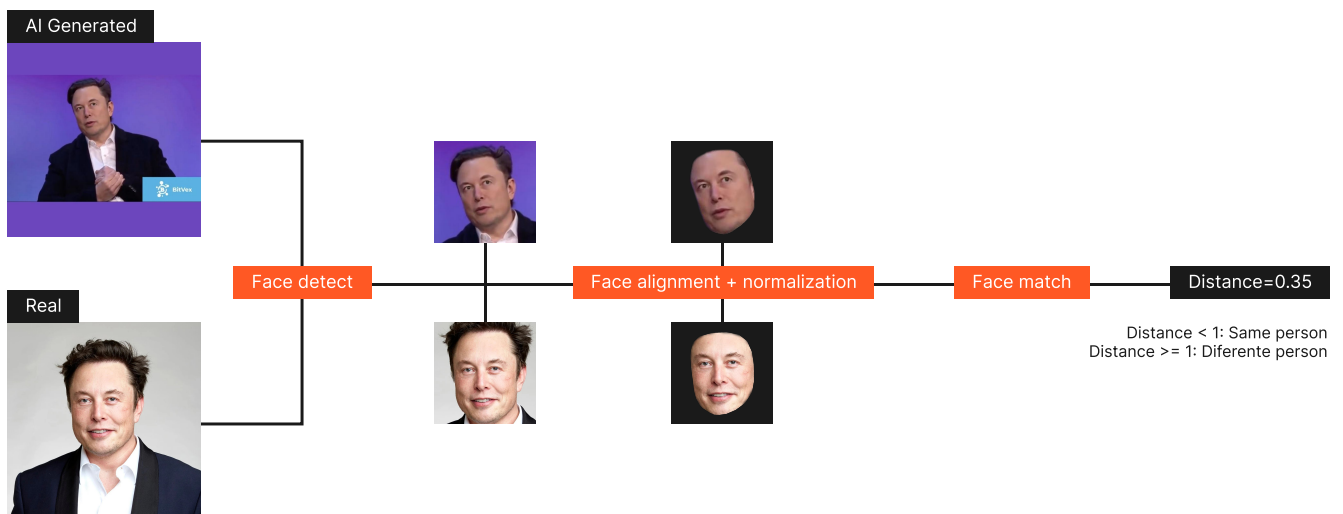
Events history

- Solved! Internal treatment finished.**
11/06/2022 at 10:50 AM
- Takedown requested**
11/06/2022 at 10:16 AM
- Threat detected**
11/06/2022 at 10:15 AM

Unlock Effortless Collaboration with Secure Data Sharing

Advanced FaceMatch Recognition System

Harness the power of Axur's FaceMatch, a facial recognition technology that meticulously analyzes the suspicious profile's picture, comparing it to the monitored profile's official one. Detect impersonation accounts with ultra-precise accuracy, including images manipulated with artificial intelligence, and request immediate takedowns on social platforms.



Axur SafeShare

Introducing SafeShare, a unique solution catering to the special data handling needs of Executives & VIPs. With the SafeShare link, executives can securely submit their sensitive information directly into the platform for monitoring, including uploading photos from their device's gallery or taking selfies in real time. This process, facilitated without intermediaries, significantly reduces exposure points and enhances confidentiality. Executives can complete this secure submission on any computer, mobile phone, or tablet.

Enhanced Data Encryption Protocol

Axur's platform seamlessly integrates the submission of Authorization Terms and photos, featuring enhanced privacy measures such as blurring and signature status to initiate automatic takedowns without further executive input. All the entered data undergoes a hashing process to ensure an encrypted shield, surpassing standard security measures and aligning with international data protection regulations.

Protect Your Executives & VIPs Now

Get a demo

Trusted by thousands of executives from top global corporations

