

How Is This Different Than Normal Identity Monitoring?

Cyber Crucible's digital identity theft capability is proactive and preventative. It is preventing access to the information needed to conduct blackmail, extortion, and modern identity theft operations.

Traditional identity theft protection deals with passwords and other data in fraudsters' hands, and monitoring for things like fraudulent credit card usage, taking out fraudulent loans, or passwords eventually being found in data breaches. This is very reactive, and is difficult for customers to manage in their daily lives. It also opens the opportunity, which Cyber Crucible has observed, to blackmail individuals, and even coerce employees and executives into assisting the attackers to helping attack their employers.

There is a concerted effort by attackers to go after cookies, logins, messaging platforms, and other forms of authentication and private data to enable their attacks.

Cyber Crucible's identity theft focused analytics prevent that, in a manner which provides authoritative behavioral decision making without user involvement, against modern extortion tactics and cybercriminal file-less attacks.

Revision #3

Created 2026-05-18 20:28:45 UTC by Dennis Underwood

Updated 2026-07-20 19:22:35 UTC by Dennis Underwood