Identity Theft Prevention

Do you collect any of identity data?

Created by Dennis Underwood, last modified on Feb 23, 2023

The short answer is no, we do not.

The longer answer, is, no we do not, but in two different ways:

First, we never transmit passwords, cookies, oauth tokens, or anything else that would be considered identity data to our Cyber Crucible servers. That is true whether the server is customer-hosted, or Cyber Crucible hosted.

Second, we learned to conduct behavioral analysis of identity information, without actually processing identity information. That means that our analytics are not actually processing or exposing sensitive data such as actual passwords, session tokens, etc.

How Is This Different Than Normal Identity Monitoring?

Created by Dennis Underwood on Feb 23, 2023

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.

What identity data is protected?

Created by Dennis Underwood, last modified on Feb 23, 2023

Core Windows Operating System

- NTDS (Active Directory)
- Incubating feature that will continue to improve

VPN client credentials

- usernames
- passwords
- key-based authentication

Web Browsers

- cookies
- refresh tokens (“remember me” authentication tokens)
- oAuth tokens (session tokens, access tokens)
- passwords
- usernames
- browser history

Collaboration & Messaging Applications

- contacts
- userrnames
- chat histories
- saved chat contents
- saved chat attachments
- private messaging encryption keys
- passwords
- oauth tokens (session tokens, access tokens, refresh tokens)

Crypto Wallets

- wallet contents
- transaction records

- passwords
- encryption keys

Gaming:

- Incubating - currently only Steam
- passwords
- purchases
- credentials
- usernames
- oAuth tokens (session tokens, access tokens, refresh tokens)

File Sharing:

- Incubating - currently only FileZilla
- passwords
- purchases
- credentials
- usernames
- key-based authentication
- servers & server settings

How is identity data protected?

Created by Dennis Underwood on Feb 23, 2023

What cryptocurrency wallets are protected?

Created by Noah Greenberg on Jan 05, 2026

- Coinomi
- Armory (“Bitcoin Armory”)
- Electrum
- Exodus
- Guarda