Wie unterscheidet sich dies von einer normalen Identitätsüberwachung?

Die Fähigkeit von Cyber Crucible zum Schutz vor digitalem Identitätsdiebstahl ist proaktiv und präventiv. Sie verhindert den Zugriff auf die Informationen, die für Erpressung, Nötigung und moderne Identitätsdiebstahl-Operationen benötigt werden.

Herkömmlicher Identitätsdiebstahlschutz befasst sich mit Passwörtern und anderen Daten, die in die Hände von Betrügern gelangt sind, sowie mit der Überwachung von Vorgängen wie betrügerischer Kreditkartennutzung, der Aufnahme betrügerischer Kredite oder dem letztendlichen Auffinden von Passwörtern in Datenlecks. Dies ist sehr reaktiv und für Kunden im Alltag nur schwer zu handhaben. Zudem eröffnet dies die Möglichkeit – die Cyber Crucible beobachtet hat –, Einzelpersonen zu erpressen und sogar Mitarbeiter und Führungskräfte dazu zu nötigen, den Angreifern bei Angriffen auf ihre Arbeitgeber zu helfen.

Angreifer bemühen sich gezielt darum, an Cookies, Anmeldedaten, Nachrichtenplattformen und andere Formen der Authentifizierung sowie private Daten zu gelangen, um ihre Angriffe zu ermöglichen.

Die auf Identitätsdiebstahl fokussierten Analysen von Cyber Crucible verhindern dies auf eine Weise, die eine maßgebliche verhaltensbasierte Entscheidungsfindung ohne Nutzerbeteiligung ermöglicht – gegen moderne Erpressungstaktiken und dateilose Cyberangriffe.

Revision #1
Created 2026-07-24 04:27:38 UTC by Dennis Underwood
Updated 2026-07-24 04:27:38 UTC by Dennis Underwood