

Advancing Fraud Investigation & Disruption

Safely Investigating Fraud Infrastructure at Scale

Understanding Modern Fraud Operations

The Cyber Defence Alliance (CDA) supports financial institutions across EMEA in investigating fraud campaigns including phishing, smishing, vishing, and investment scams. Their role sits at the intersection of intelligence sharing and active investigation, helping member organizations understand emerging threats and respond more effectively.

A critical part of this work requires interacting directly with malicious websites, services, and social platforms to understand how fraud campaigns operate in real time. However, traditional approaches made this difficult to execute quickly, safely, and at scale.

The Challenge: Investigating Fraud Without Exposure

Before adopting Replica, CDA relied on a variety of research environments and manual workflows to conduct investigations. Analysts often could not safely access suspicious links or attacker infrastructure from corporate systems, creating delays and limiting visibility.

Research laptops provided a workaround, but they introduced operational overhead and slowed investigations. Moving findings back into corporate environments required manual effort, and much of the context was lost in the process. At the same time, fraud infrastructure was becoming more short-lived and harder to access, with attackers increasingly using targeting and fingerprinting techniques to evade detection.

The result was a fragmented and inconsistent process that made it difficult to investigate quickly, capture complete intelligence, or keep pace with modern fraud activity.



CYBER
DEFENCE
ALLIANCE

Industry:
Financial Services
Consortium

“ *Replica has completely changed the way we work. It's become synonymous with how we investigate.* ”

Barry Steel

Fraud & Cybercrime
Investigations
Cyber Defence Alliance

Investigating Fraud with Replica

Replica provides CDA with secure, isolated environments where analysts can safely interact with fraud infrastructure in real time. Instead of relying on disconnected tools and environments, investigators can now access malicious domains, follow scam workflows, and analyze attacker behavior from a single platform.

This has enabled CDA to move beyond surface-level analysis. Analysts can walk through phishing and scam sites end-to-end, follow malicious advertisements into attacker-controlled environments, and observe fraud activity on platforms like Telegram as it happens. They are also able to investigate the services and tooling that support fraud operations, from impersonation templates to payment flows, while capturing content that would otherwise disappear.

As fraud increasingly shifts toward mobile and highly targeted delivery, Replica also gives CDA a foundation to expand into more advanced investigative workflows, including mobile-focused fraud analysis.

The Impact

Replica has fundamentally changed how CDA conducts fraud investigations. Analysts can now access malicious content immediately, without delays or environment switching, and operate safely without relying on research laptops or risky workarounds.

This shift has led to deeper, more actionable intelligence, with full visibility into how fraud campaigns operate in practice. CDA is able to access more targeted and evasive content, increasing the success rate of investigations, while also improving how quickly insights can be shared across member organizations.

By consolidating investigation workflows into a single secure environments platform, Replica has enabled CDA to move from reactive analysis toward a more proactive approach to fraud disruption.

How it works

1

Fraud indicators such as suspicious domains, advertisements, or social activity are identified through member reporting or internal analysis

2

CDA analysts use Replica to safely interact with the infrastructure in real time, following the same paths a victim would take

3

Intelligence is captured and shared with member institutions to support mitigation and disruption efforts

“

CDA is doing the work most organizations can't, investigating live fraud infrastructure without putting their own systems at risk. With Replica, they don't face the false choice between access and safety. When you need to follow the attacker's path in real time, containment isn't optional.

”

Kris Schroeder

Founder and CEO

Replica Cyber