Fraud Shutdown Service for Digital Banking

Digital Insight's Fraud Shutdown for Digital Banking is an end-to-end Anti-Phishing, Anti-Trojan and Anti-Rogue Mobile App external threat management service, infused with cyber intelligence threat feeds – powered in partnership with RSA Security.

This turnkey service proactively detects and shuts down fraudulent phishing sites, blocks access to phishing sites prior to shutdown, extracts compromised user information, provides access to secure real-time reports and phishing alerts, and includes technical counter measures to dilute effectiveness of fraudulent attacks; one of the many ways that Digital Insight helps protect your financial institution's reputation, while giving your users peace of mind and reducing your liability exposure stemming from online fraud attacks.

Financial Institution Benefits

- Give Peace of Mind – The detection, monitoring and shutdown services identify online fraud attacks in the early stages, before they can proliferate - in turn - protecting your financial institution's brand and overall digital presence.
- Deter Future Attacks – Countermeasures weaken the ability for criminals to obtain end-user information – increasing the chance of catching the fraudsters and helping deter future attacks.
- Minimize Data Exposure – Fast, fraudulent site and rogue mobile app shut down minimizes end-user data exposure and damages of an attack.
- Save Time and Resources – Leverage this external threat management service to work on behalf of your clients and outsource the headache of dealing with phishing, Trojans and rogue mobile apps. Specifically designed by anti-fraud, financial institution experts for financial institutions – making implementation a seamless experience.

Features

Detection and Prevention

- Real-time Alert and Detection Services – Provides detection and real-time alerts of phishing attacks – identifying them as they take place and taking immediate action. Combines multiple technologies, such as email probes, spam filtering and chat-room monitoring.
- Anti-Fraud Cyber Intelligence – in the form of both feeds and reports, cyber intelligence provides insight into cybercrime trends and in-depth investigations into fraud methods and operations with the global cyber-criminal underground.

- Reporting – This service will give you access to a secure web portal dashboard that shows a single, comprehensive, real-time view of the status-of-attack shutdown.

Shutdown

- Severity Assessment Services – Immediately upon detection, the experienced 24/7 Anti-Fraud Command Center performs an evaluation of the attack – estimating its severity and collecting additional information, like the account-holder data, which might be compromised.

- Site Shutdown – The 24/7 Anti-Fraud Command Center (AFCC) works on your behalf to stop attacks within hours and reduce the resources typically required to fend off these attacks. The AFCC contacts ISPs to help shut down the fraudulent websites, sends cease and desist letters to ISPs and supports over 15 languages.

- Rogue Mobile App Shutdown – Reduce fraud losses by taking action against malicious or unauthorized 'rogue' mobile apps. The Anti-Rogue App Service monitors all major app stores, detects apps targeting your organization's customer base and shuts down unauthorized apps – reducing threats to organization's reputation and financial losses due to mobile app fraud.

- Forensic Work – The AFCC conducts forensic work during and following attacks to, when possible, extract additional valuable information.

Support

- RSA Security provides direct client support for detection, prevention and shutdown features.