SHIELD | ZIGI

Case Study

SHIELD Protege la Aplicación de Servicios Financieros Zigi y a Sus Usuarios Contra el Fraude

"La tecnología de SHIELD nos permite estar siempre un paso adelante de las actividades fraudulentas, garantizando los más altos estándares de seguridad para nuestro ecosistema y nuestros clientes."

Brenda Menjívar
Chief Data Officer, Zigi

Key Takeaways

Eliminó cuentas falsas creadas con la intención de abusar de promociones

Evitó ataques de toma de cuentas, resguardando las cuentas de los usuarios

Garantizó un ecosistema seguro y confiable

Facilitando a los usuarios manejar sus finanzas de manera sencilla y segura

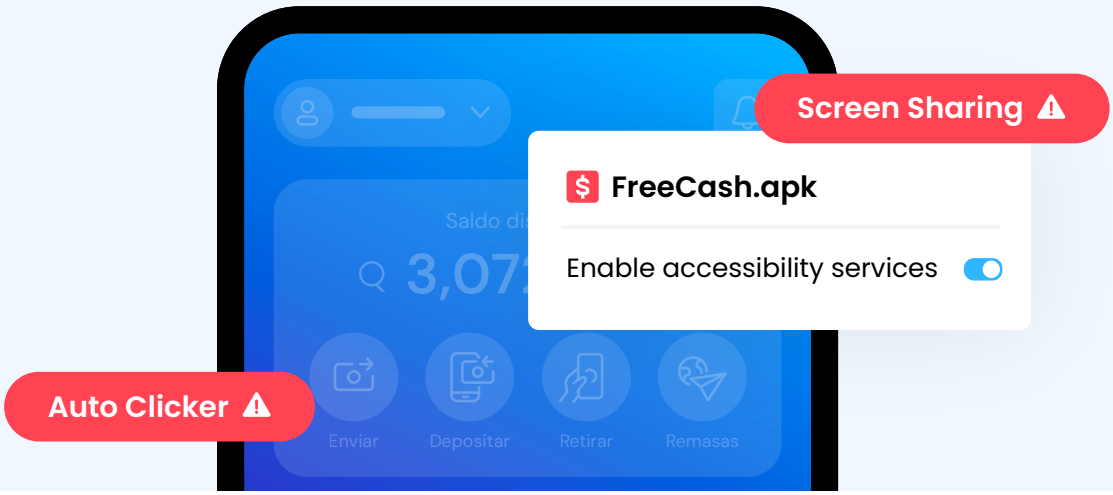
La plataforma Zigi ayuda a los guatemaltecos a administrar sus finanzas permitiéndoles recibir remesas, enviar dinero, pagar a través de un código QR, y mucho más. La misión de Zigi es desarrollar comunidades que impulsen y potencien la riqueza en Centro América, acelerando la inclusión financiera en la región.

La seguridad es su principal prioridad. A pesar de la presencia común del fraude en las soluciones fintech, lo cual podría minar la confianza del usuario, Zigi está solucionando de manera proactiva los riesgos planteados por los ciberdelincuentes. Ha elegido la **solución de inteligencia de riesgos basada en dispositivos de SHIELD** para detectar y frenar el fraude desde su origen, resguardando así a sus clientes y al ecosistema.

Customer Profile
Zigi es una aplicación de servicios financieros 100% digital con sede en Guatemala. La plataforma atiende a las necesidades financieras esenciales de los guatemaltecos, permitiendo a los usuarios manejar su dinero de manera sencilla, transparente, segura y accesible.

Industry
Servicios Financieros

Region
LATAM



Los ataques de toma de cuentas están en aumento

Los ataques de Toma de Cuentas (ATO) están incrementándose, siendo la industria financiera un blanco principal para los ciberdelincuentes. Este término se refiere a la acción de los estafadores de acceder de manera ilícita y tomar el control de las cuentas bancarias de los usuarios para realizar transacciones no autorizadas, transferir fondos o llevar a cabo otras actividades maliciosas.

Por lo general, los estafadores recurren a tácticas de **ingeniería social** para llevar a cabo ataques de ATO, manipulando a los usuarios para que revelen datos de inicio de sesión o descarguen malware. **El phishing** o **spear-phishing** es un ejemplo de este tipo de amenaza. En tales ataques, los defraudadores envían mensajes o correos electrónicos que aparentan ser de fuentes legítimas, como bancos u organizaciones de confianza. Estos mensajes suelen contener enlaces a sitios web o aplicaciones falsas diseñadas para recopilar información confidencial o engañar al usuario para que instale malware.

Los estafadores también se valen de los **permisos de accesibilidad** para llevar a cabo ataques de ATO. Los defraudadores pueden manipular a los usuarios para que descarguen aplicaciones maliciosas y luego otorguen permisos de accesibilidad a esas aplicaciones. Por ejemplo, los estafadores podrían activar la **función compartir pantalla** y **autoclics** sin que la víctima lo sepa. Esto facilita que los estafadores manipulen a los clientes, tomen el control de sus cuentas y extraigan su dinero.

Mitigando el Fraude de Abuso Promocional en la industria fintech

Zigi busca ofrecer descuentos a los usuarios cuando pagan utilizando la aplicación y también ofrece un programa de referidos que premia a los clientes existentes al recomendar la plataforma a amigos y familiares.

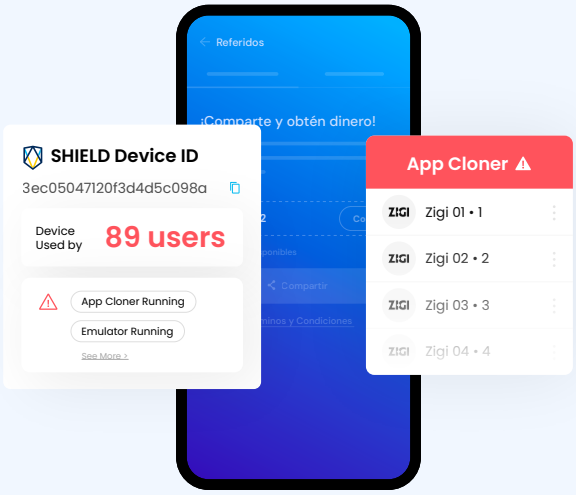
Estas promociones suelen atraer a estafadores que utilizan aplicaciones y herramientas maliciosas, como **clonadores de aplicaciones** y **emuladores**, para crear miles de cuentas falsas. Estas cuentas se pueden utilizar luego para aprovecharse de los incentivos y promociones de la plataforma.

Una posible consecuencia de estas prácticas resulta en un desvío de parte del presupuesto destinado al marketing de la plataforma, a casos de posible fraude.

Cómo SHIELD Refuerza la Defensa de Zigi Contra el Fraude

El equipo de Zigi comprendía que proteger la aplicación bancaria del abuso promocional y las cuentas de sus clientes contra los ataques de toma de cuentas era crucial. Por esta razón, optaron por utilizar la tecnología de SHIELD como la primera línea de defensa de la plataforma contra el fraude.

La solución de inteligencia de riesgos basada en dispositivos de SHIELD se impulsa mediante una avanzada tecnología de huella digital de dispositivos y los últimos algoritmos de inteligencia artificial y



aprendizaje automático. Identifica el fraude en su origen y analiza miles de puntos de dispositivos, red y datos de comportamiento para proporcionar insights accionables en tiempo real.

SHIELD Device ID, el estándar global para la identificación de dispositivos, les permitió identificar los dispositivos fraudulentos utilizados para crear cuentas falsas, previniendo así el **abuso promocional** y la **toma de cuentas**.

El equipo también aprovechó el **SHIELD Risk Intelligence**, identificando malware y herramientas maliciosas asociadas con el fraude, como **clonadores de aplicaciones**, **autoclicadores** y **emuladores**.

El **SHIELD Risk Intelligence** también garantiza que la plataforma se mantenga un paso adelante de los estafadores con el Global Intelligence Network: una biblioteca continuamente actualizada que contiene todos los patrones de fraude encontrados, así como las últimas técnicas maliciosas. Con más de 7.000 millones de dispositivos y más de mil millones de cuentas de usuario analizadas en todo el mundo, SHIELD aprovecha esta inteligencia para sincronizar patrones de ataque en tiempo real.

La solución proporciona al equipo de Zigi inteligencia de dispositivos accionable en tiempo real y un enfoque proactivo para la prevención del fraude, garantizando un ecosistema seguro y confiable.

Brenda Menjívar, Chief Data Officer de Zigi, comentó: “La tecnología de SHIELD nos permite estar siempre un paso adelante de las actividades fraudulentas, garantizando los más altos estándares de seguridad para nuestro ecosistema y nuestros clientes”.

SHIELD is a device-first risk intelligence company. We are dedicated to helping organizations worldwide eliminate fake accounts and all malicious activity with the global standard for identification and intelligence.

Leveraging AI, we identify the root of fraud and provide actionable risk signals in real time, helping all online businesses stop fraud, build trust, and drive growth.

With offices in San Francisco, Miami, London, Berlin, Jakarta, Bengaluru, Beijing, and Singapore, we are rapidly achieving our mission - eliminating unfairness to enable trust for the world.

For more information, visit **shield.com**.

/shieldfraud

/shieldfraud

/company/shield

shield.com