Arkose Labs

Microsoft Outlook.com Tackles Fraud and Abuse Globally Using Arkose Labs

CASE STUDY

Microsoft

Business Problem

- Large-scale fake account registrations
- Email accounts used for malicious and fraudulent purposes
- Fraud mitigation disrupted good user experience

Solution

- Unified authentication for new users
- Innovative challenges stop bots and fraudsters
- Malicious emails detected and challenged downstream

Results

- 33% improvement in good customer throughput
- 98% reduction in fraud and abuse
- Stopped customer complaints about SMS verification

“As well as protecting our own customers, we needed to protect the wider ecosystem from fraud and abuse originating from Microsoft Outlook.com accounts”

Overview

Outlook.com has hundreds of millions of active users, offering an integrated solution of email, calendar, task management, and more. It is trusted to provide secure communication; however, its popularity makes it a prime target for fraudsters looking to abuse new accounts to extort money or obtain sensitive information using malicious emails.

The Business Problem

Cloud-based email platforms are under constant attack from fraudsters looking to create fake email accounts to commit downstream fraud. Attackers use bogus accounts to attempt to blackmail individuals with unfounded threats of revealing compromising information to their contacts.

As legacy controls were unable to stop this abuse, Microsoft turned to SMS tokens to stamp out fake new accounts and abuse. Unfortunately, this was an expensive solution that failed to address the problem. While fraudsters found ways to circumvent this control, true users were required to do out-of-band authentication which damaged throughput rates. Often this was because good customers were blocked since they had a number with an area code where fraudsters were operating; they used a VOIP as their primary number; or they were delayed in receiving the SMS tokens.

Outlook.com needed a new way to stop fraudulent new account creations, reduce abuse, while improving customer experience - all in a cost-effective manner. This was important not only to protect their own users but to create a safer environment for the wider ecosystem.

The Arkose Labs Solution

Microsoft deployed the Arkose Labs platform to differentiate between good users, bots, and malicious humans in order to eliminate abuse. New users were shown enforcement challenges when sending their first email. The team implemented custom rules and policies to detect anomalous and suspicious behavior, with challenges being presented whenever there was evidence of downstream large-scale abuse. This has been implemented across the global Outlook.com solution.

Adaptive enforcement challenges are made using 3D visuals rendered in real time, with countless possible variations. These ensure that all automated attacks fail, and extensive testing ensures that they are resilient to being solved en masse. Incrementally complex challenges are presented to bad actors attempting to disseminate malicious content, to sap their time and efficiency and erode the potential profitability of attacks.

Good customers, on the other hand, enjoyed a far superior user experience. Authentication occurred within the email application for minimal disruption and while challenges were nigh-on-impossible for automated attacks to solve, they were quick, simple, and even fun, for true users to complete.

Key Advantages

Microsoft recognized that the Arkose Labs solution had a number of key advantages over alternative solutions - such as asking users to identify characters and basic images or completing SMS verification.

- Authentication puzzles generated by Arkose Labs had proven resilience to being solved through automation
- Good users were never blocked, but asked to complete a simple authentication challenge
- In-band authentication did not disrupt the users' flow and improved good customer throughput
- Protection against malicious humans as well as automated attacks
- Major cost savings compared to SMS verification

Demonstrated Results

When Arkose Labs was deployed, Microsoft Outlook.com saw a 33% improvement in good customer throughput. There was a 98% reduction in fraud and abuse, with malicious users being prevented from carrying out large-scale attacks after setting up new accounts. Moving away from SMS verification led to major cost savings. Each check cost significantly less and customer complaints about the SMS verification stopped, relieving the burden on in-house teams dealing with these issues. Microsoft was able to roll this out globally, with Arkose Labs supporting over 100 languages.

"Fraudsters' mindsets ultimately come down to money and how much they can get out of an attack. We recognized that the cost of circumventing the Arkose Labs solution was prohibitively high, whereas the cost-benefit analysis was in the fraudsters' favor for alternative fraud controls."

Arkose Labs bankrupts the business model of fraud. Its patented platform combines Arkose Detect, a sophisticated risk engine, with Arkose Enforce, which uses targeted step-up challenges to wear fraudsters down and diminish their ROI. The world's largest brands trust Arkose Labs to protect their customer journey while delivering and unrivaled user experience.

Schedule Demo

demo@arkoselabs.com
(800) 604-3319
arkoselabs.com