
Arkose Labs
Technology Sector
Q3 2020 Fraud and Abuse Report

Introduction

At the beginning of 2020, no one could have foreseen the critical role tech platforms would play in connecting society. Since the onset of the COVID-19 pandemic and related lockdowns, the world has relied on video conferencing platforms, remote collaboration tools and shared storage services to conduct business, education and leisure activities.

It's no surprise then that there was an uptick in fraud activity targeting this industry in Q2. Fraudsters used the increased traffic flocking to these platforms in an attempt to blend in with good customers and carry out attacks.

In particular, there was a major trend towards human-driven attacks in Q2, with 57% of attacks now coming from sweatshops. This can partially be explained by the pandemic; as lockdowns decimated economies and people lost their jobs, more and more are willing to do whatever it takes to put food on the table, including fraud. In fact our data shows that some of the highest countries of origin for human-based attacks were in those that were among the earliest to impose lockdowns.

As the world begins to return to something resembling normalcy through the rest of 2020, it will be interesting to monitor whether these fraud trends continue for tech platforms.

By better understanding the evolving digital landscape, businesses can ensure they are well-equipped to tackle the rising tide of fraud and ensure long-term protection against attacks.

1H 2020: Key Fraud and Abuse Trends

As COVID-19 forces commerce online, the Arkose Labs network records double the volume of attacks over 6 months.

1.1 billion
attacks detected and stopped

2x attack volume
since 2H 2019

25% attack rate
on all transactions

Elevated Attack Levels in 2020

Attack patterns have been evolving rapidly in the first 6 months of 2020

21.2% mobile
attack mix

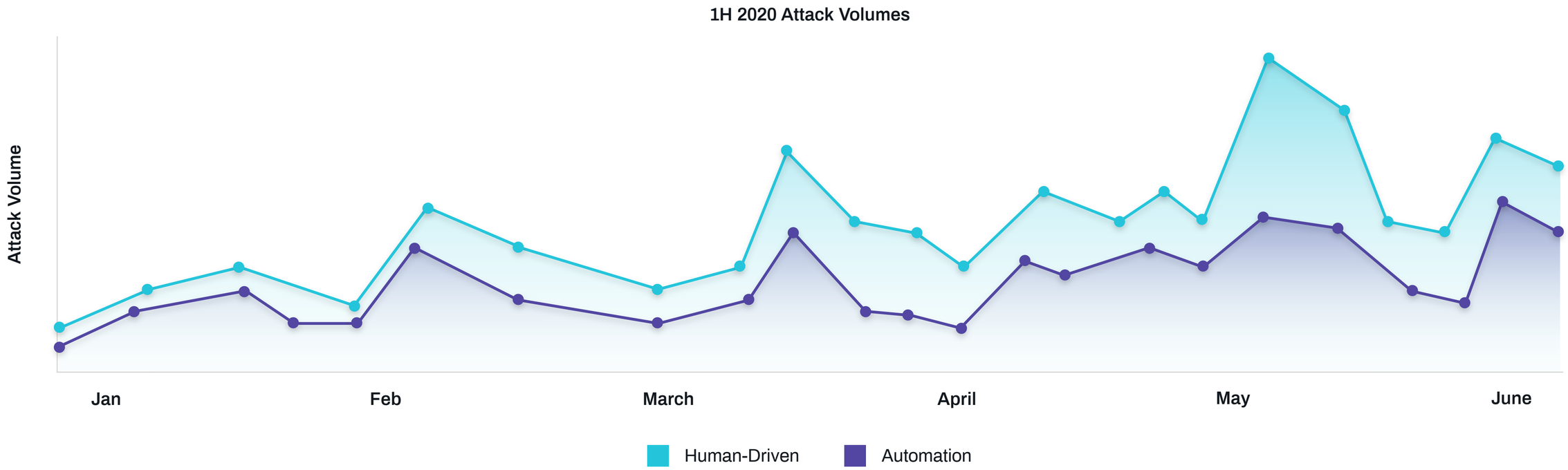
33.5% human
vs 66.5% bot attacks

Most attacked
use case is logins

Heightened Attack Volumes in 2020

Businesses are facing an increasingly hostile threat landscape in 2020. Major spikes in attacks can be seen across the first six months of the year,and Arkose Labs has observed a general upwards trend in the intensity of attacks. Normal consumer behavior has been in flux, due to the upheaval caused by COVID-19. It is harder to user historical benchmarks of transaction habits when assessing traffic.

Therefore, organizations relying purely on data-driven fraud defenses run the risk of more traffic falling into a "gray area" when differentiating between trusted and fraudulent behavior. They therefore require robust defenses that provide hard evidence of a user's true underlying intent.



Human-Driven Attack Spike on the Technology Sector

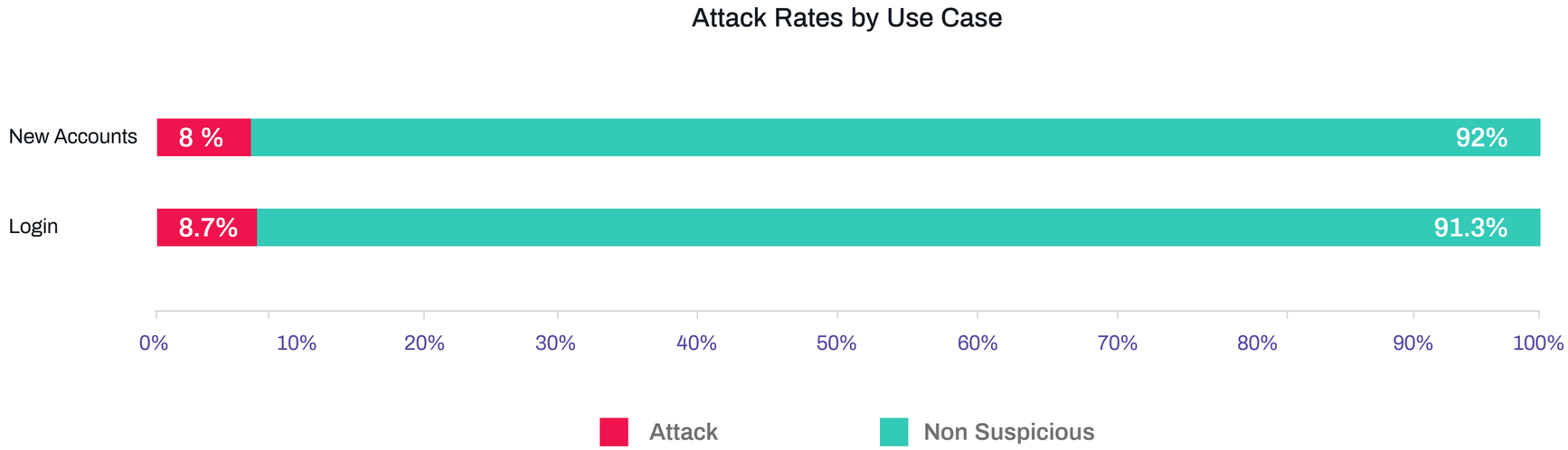
8.5%
attack rate

57% of attacks
from sweatshops

27%
of attacks
on mobile

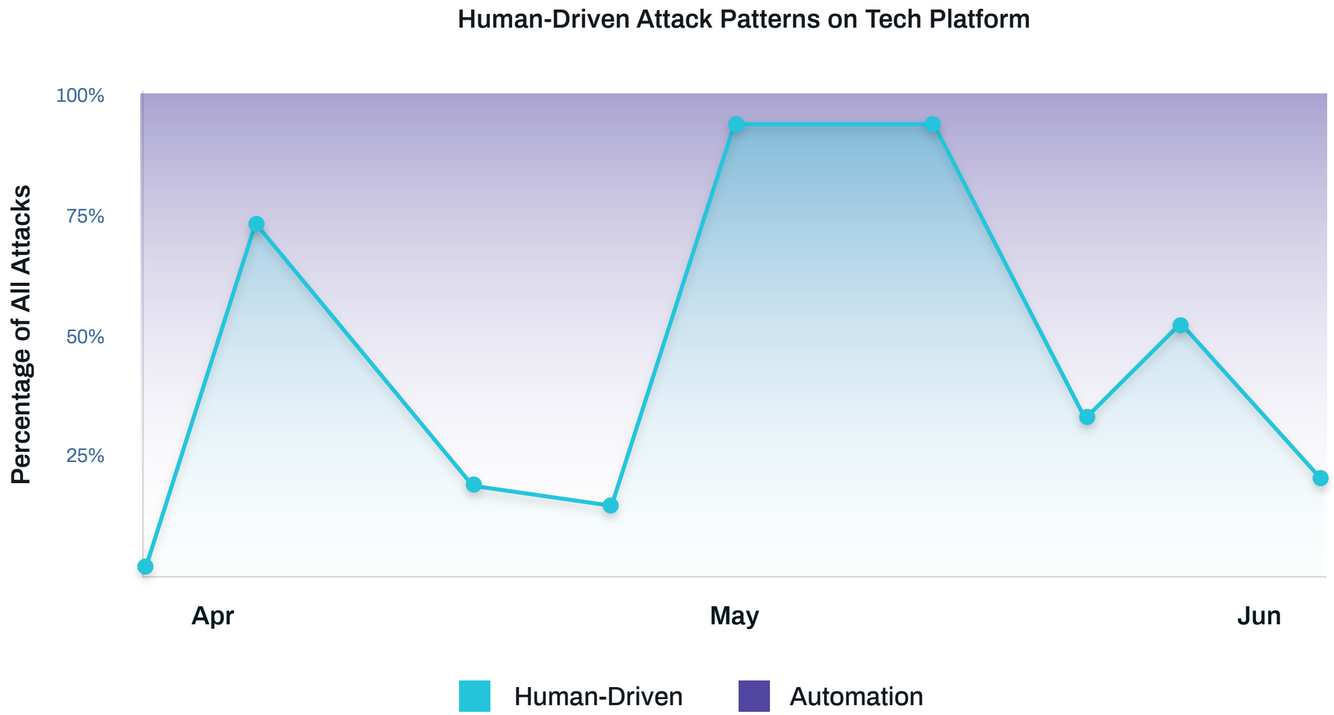
The ability for users to communicate and collaborate digitally has never been more important. Alongside “lockdown”, “social distancing” and “isolation”, the word “zoom” has entered people’s day-to-day vocabulary - regardless of an individual’s preference on video calling platform.

As a result, the technology industry is witnessing an uptick in targeted attacks. There was a major swing towards human-driven attacks in Q2, with 57% of attacks now coming from sweatshops. Tech also had an elevated mobile attack mix, with 27% of attacks targeting mobile traffic.



Tech Case Study: Battling Human Fraud Operations

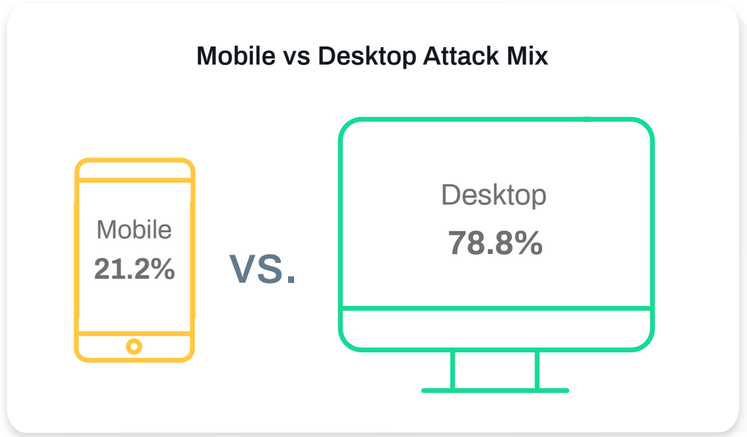
A global technology company was experiencing peaks in attacks, which the Arkose Labs team ascertained to be human-driven activity originating from a known solving solution. These operations use cheap human labor to bypass authentication challenges at scale. Whereas automated attacks can be addressed using simple interactive challenges, and regularly changing the nature of the challenge, the key to rooting out mass human-driven attacks is to increase the complexity of a challenge. These operations run on such small margins that any delay in their ability to complete challenges will deter click farm attacks long term. Using this strategy, Arkose Labs was able to effectively defend the tech platform from pernicious sweatshop-driven attacks.

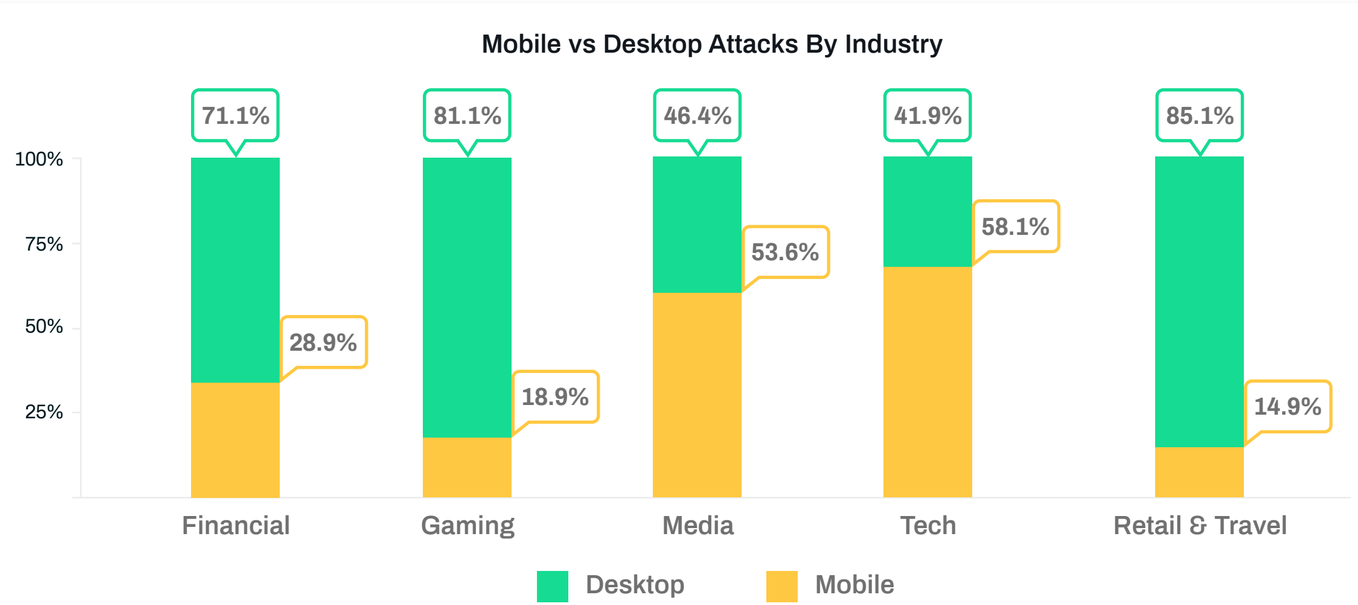


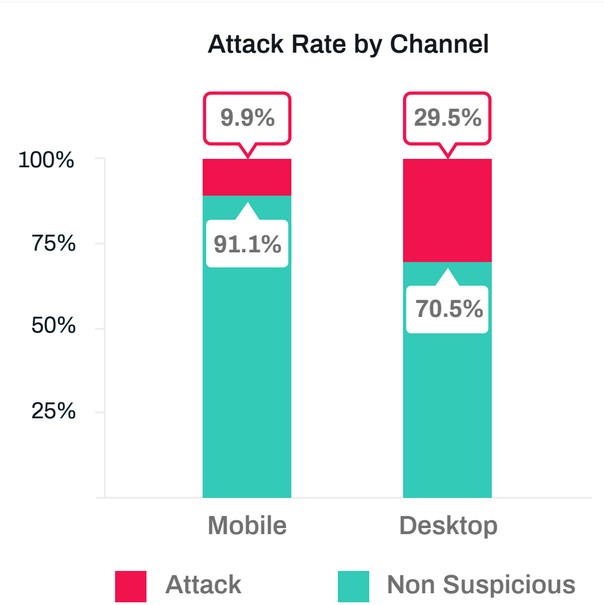
Mobile Powers Sweatshop Attacks

While mobile attack rates vary greatly by industry, overall they are lagging behind desktop attacks on the Arkose Labs network. 37% of all transactions originated from mobile, but only 21% of all attacks were on mobile transactions. Of those mobile attacks, 38% were human-driven which is higher than the overall human-driven attack mix. Click farm workers will line up multiple mobile devices to execute attacks at scale.

There is a great deal of variation in the mobile versus desktop attack mix when parsing this by industry. Technology platforms saw the highest mobile attack rate compared to any other industry in the first half of 2020.

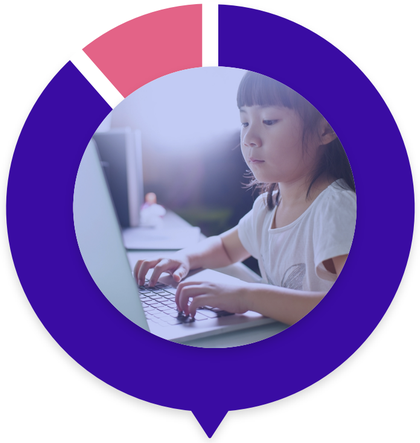






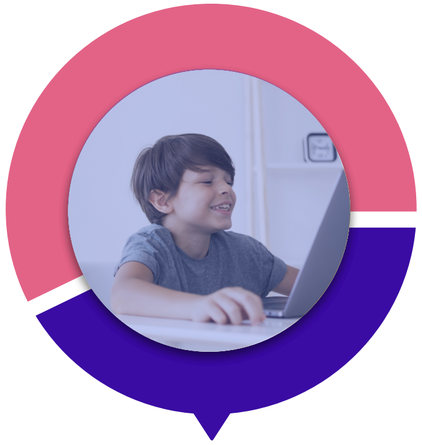
COVID-19 Lockdowns Accelerate Digital Adoption Among Kids

COVID-19 lockdowns across countries have forced closures of schools, daycare and other institutions. A lot of teaching activity is now being done through digital means, either using video conferencing tools or videos that teachers create and upload to an online repository. Furthermore, social nteractions are also happening more frequently online for children. These can take the form of the “zoom playdates” that have become commonplace during lockdowns. Additionally, children are spending increasing hours on digital entertainment platforms.



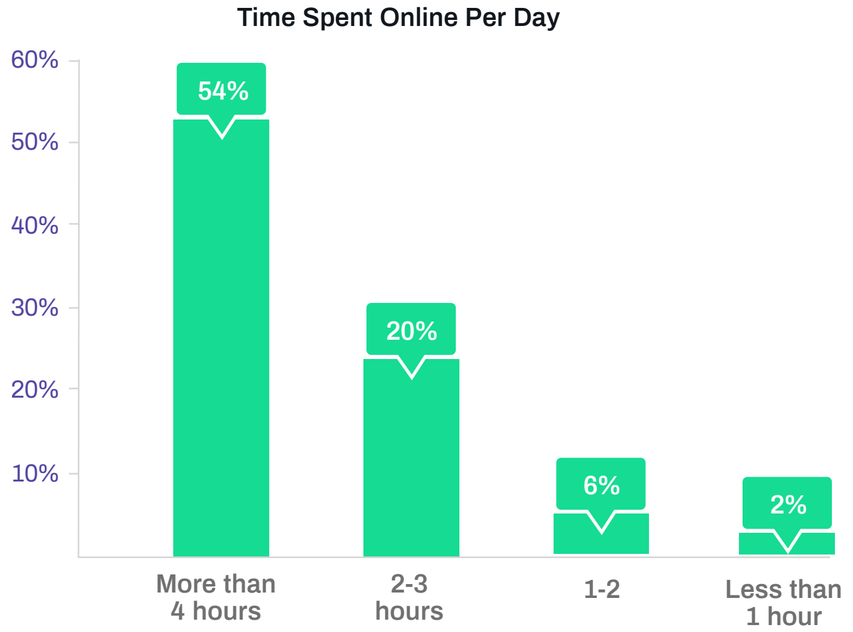
95%

of children spend more time online due to COVID-19



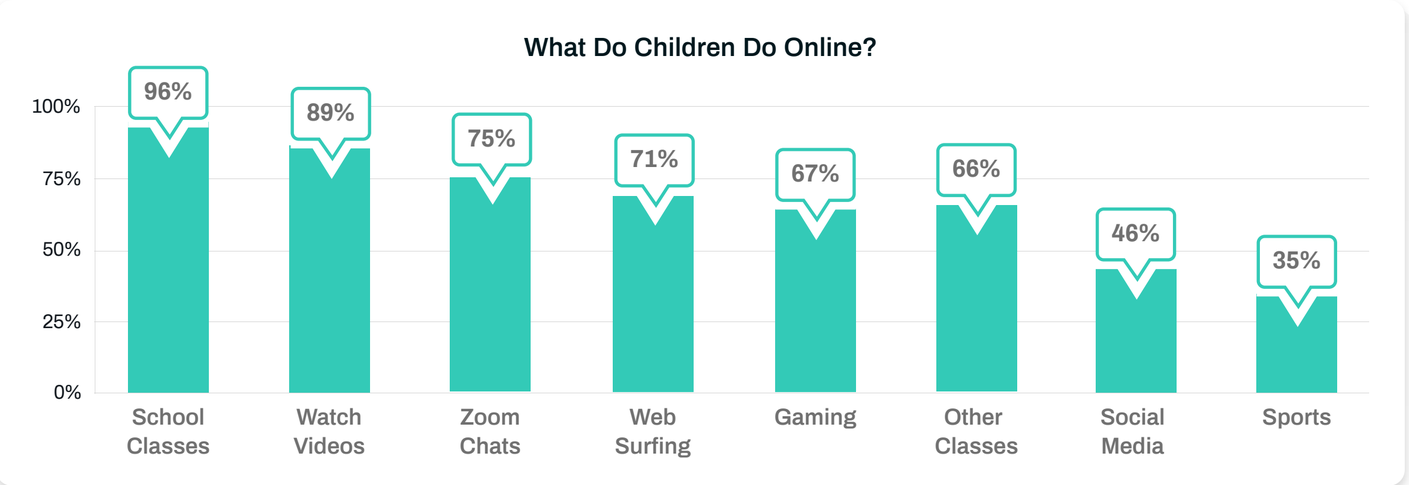
44%

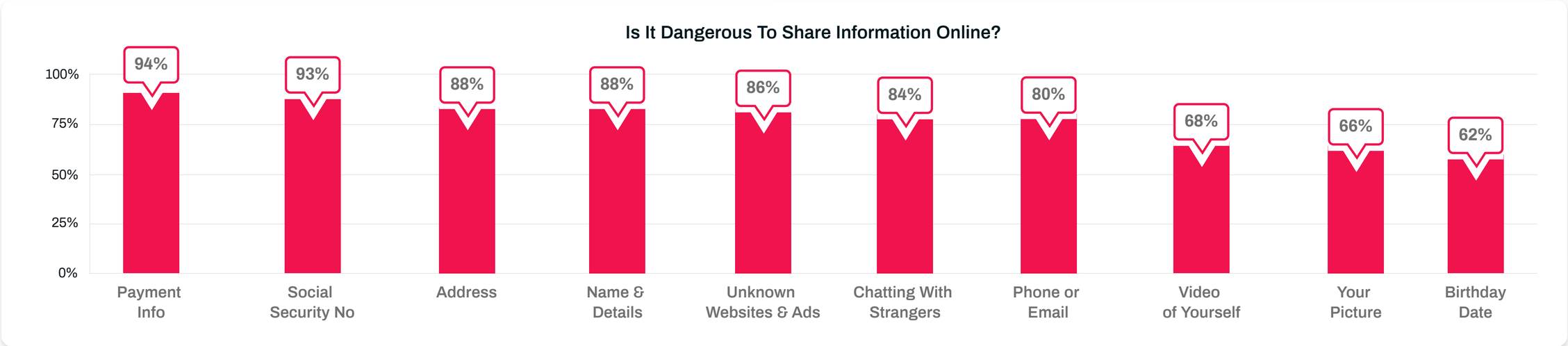
of children careful sharing information online



Today’s Users; Tomorrow’s Spenders

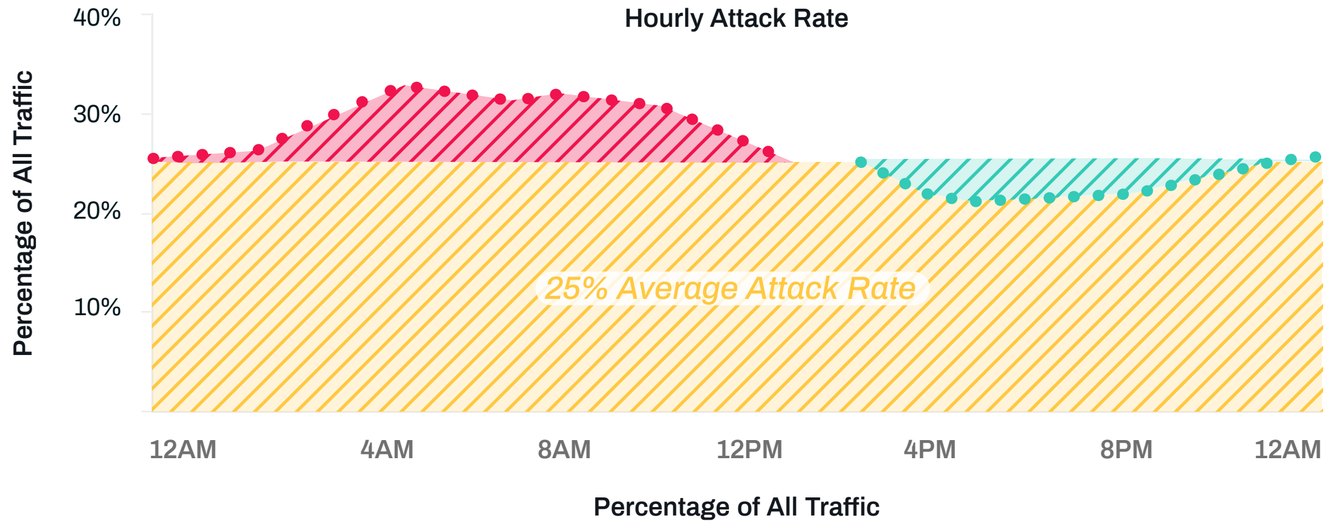
Arkose Labs surveyed children across the globe on their digital habits in 2020. The effect of COVID-19 was very much apparent, with classes for school being the top online activity. There was a high awareness of the dangers of sharing payment information online, however the dangers of sharing personal data such as birthdate was much lower ranked by the children in the survey.





The Most Dangerous Hour of the Day

When comparing attack levels with legitimate traffic patterns, it is clear that the morning is most dangerous period of the day. Businesses are facing cross-border attacks from fraudsters operating across timezones and using automated scripts that can run through the night. Therefore, attacks do not always tie in with the peak hours of legitimate consumers. 5am is the time of the day that has the highest attack rate across all traffic, with attacks 10% higher than in the afternoon. Traffic coming between the hours of 4am and 10am is generally higher risk than other times during the day.



Highest attack rate at 5am

Elevated attack rates between 4am and 10am

Microsoft Outlook.com Tackles Fraud and Abuse Globally

Microsoft

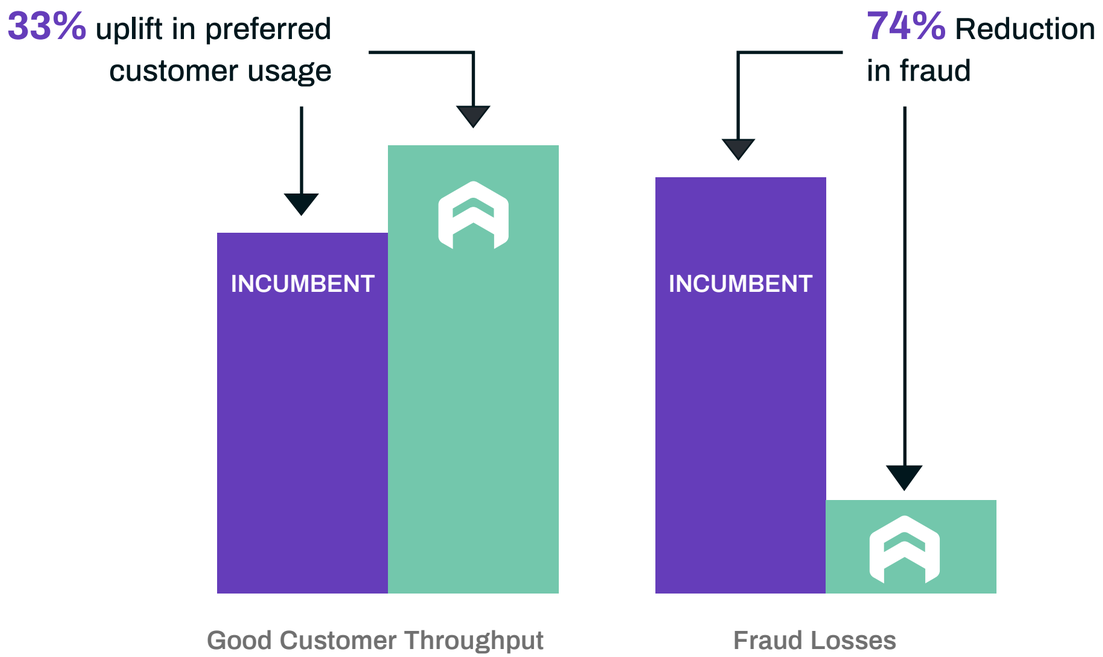
Outlook.com has hundreds of millions of active users, however, its popularity makes it a prime target for fraudsters looking to abuse new accounts to extort money or obtain sensitive information using malicious emails.

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



Trend Spotting: Beyond Mitigation Focused Strategies

Gartner's Cool Vendor report this quarter flagged that in the current threat landscape, businesses need to go beyond mitigation-focused strategies that rely on threat scores and behavioral analysis. More robust fraud detection capabilities are required, in a way that still delivers great user experience. Arkose Labs' ability to combine risk assessments with targeted enforcement challenges in a user-friendly way, puts it in a unique position address this issue.

Arkose Labs was featured as a Gartner 2020 Cool Vendor in the report which highlights "interesting, new and innovative vendors, products and services" in the IAM and fraud space.

Cool Vendors in IAM and Fraud Detection

Highlights from the report:

"The balance between detecting and mitigating fraud and creating low-friction and seamless UX has never been as important."

The limitations of mitigation-focused strategies in defeating fraud and automated abuse.

Traditional CAPTCHAs are being beaten by automation.

Download the full report at arkoselabs.com/gartner

Report Methodology

The Q2 Arkose Labs Fraud and Abuse Report is based on actual user sessions and attack patterns that were analyzed by the Arkose Labs Fraud and Abuse Prevention Platform from January to June 2020. These sessions, spanning account registrations, logins and payments from financial services, ecommerce, travel, social media, gaming and entertainment were analyzed in real-time to provide insights into the evolving fraud and risk landscape.

Unsophisticated bot attacks don't result in a user session and thus have not been included in this report. The report focuses on attacks from fraud outlets that combine state-of-the-art technology with stolen identity credentials and human efforts.

The attack patterns have been analyzed across parameters and closely investigate the mechanics of inauthentic attacks as they range from automated bots to human 'sweatshop' driven attacks. These attacks focus on defrauding the businesses and their users through fraudulent account registrations, account takeovers or payments using stolen credentials.

Arkose Labs uses a bilateral approach that combines global telemetry with a patent-pending enforcement challenge to profile user activity in detail and act upon data in real time. This provides unique insights into attacker identification and classification, enabling the platform to deploy appropriate responses and countermeasures. Suspect sessions are identified when they show characteristics that have been classified as abusive or malicious by Arkose Labs, based on previous activity on other customers' digital properties.

While Arkose Labs supports multiple use cases across the customer journey, these have been broadly grouped under account registrations, logins and payments for the purposes of this report.

About Arkose Labs

Arkose Labs

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a 2020 Cool Vendor, its innovative approach determines true user intent and remediates attacks in real time. Risk assessments combined with interactive authentication challenges undermine the ROI behind attacks, providing long-term protection while improving good customer throughput.

Sales: (800) 604-3319

Offices

San Francisco
250 Montgomery St 10th Floor, San Francisco, CA 94104, USA

Brisbane
315 Brunswick St, Brisbane, Queensland AU