



CASE STUDY

2019 Challenge: Grow traffic & limit complaints



STC Kuwait Case Study

January 2019 –
September 2022

mcpinsight.com

ABOUT STC



Saudi Telecom Company (STC) is the Saudi digital enabler of telecom services in the Kingdom of Saudi Arabia, and among the operators in the Middle East.

The company offers landline and fixed infrastructure, mobile and data services. STC offers mobile, broadband and cloud computing services.

90% of logged consumer complaints are categorised as ‘transaction unknown’

The cause of unknown transactions are split – Analyses Mason 2020 survey of consumers shows the reasons as:

50% Payment Fraud and 50% Misleading Consumers

In 2019 MCP agreed on new advertising standards with STC, and implemented the MCP SCANNER ad monitoring and compliance enforcement system. This was followed by MCP SHIELD to block payment fraud.

The following key compliance issues were drastically reduced:

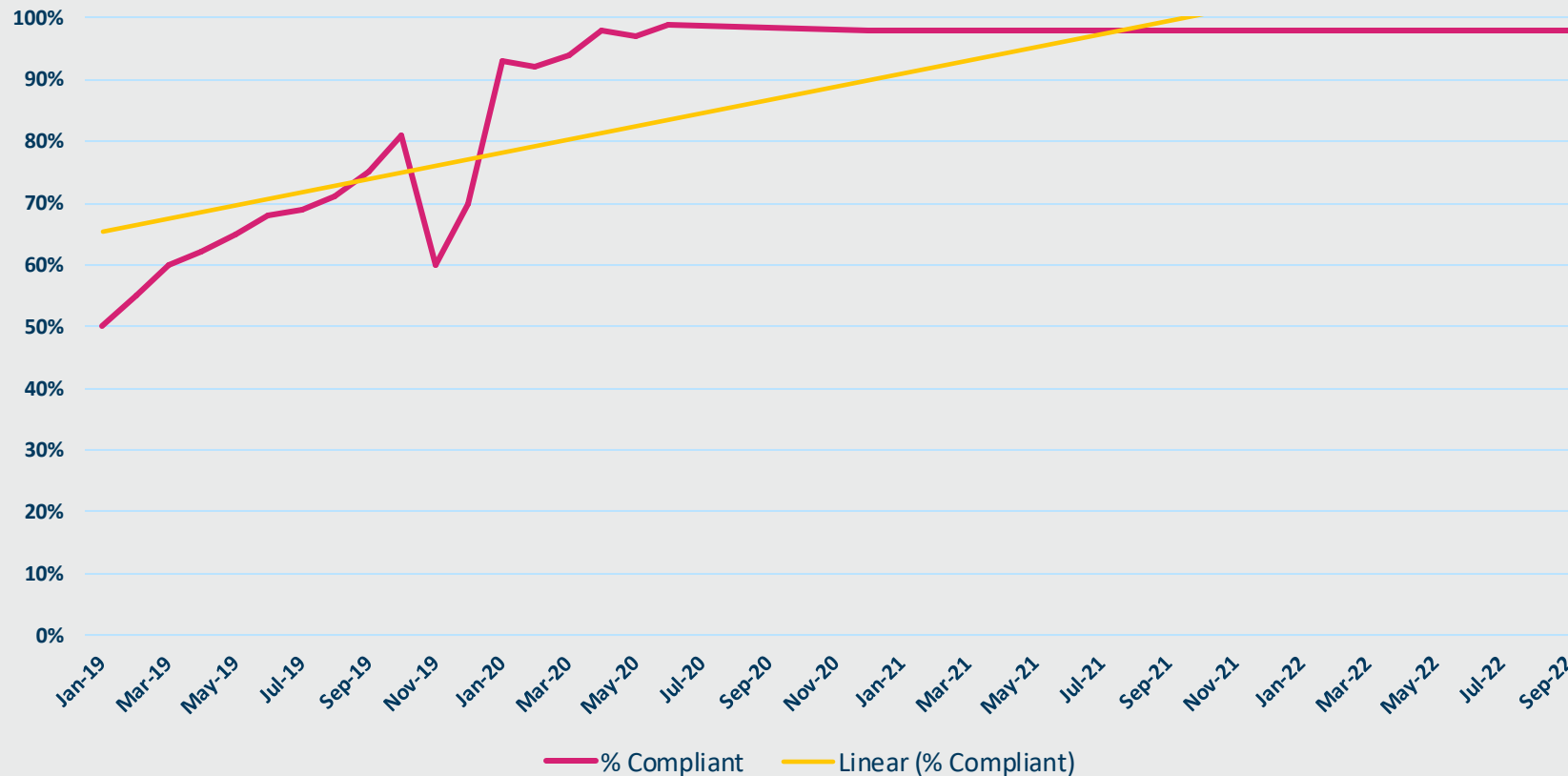
- Adult Ads & Ads on Adult Sites;
- Content Locking;
- Misleading (including false win money promotions);
- Promotion Branding (including Brand passing off e.g. Royal Family and large brands like MNOs, WhatsApp..)

Advertising compliance increased to 93%+ within 6 months of deploying MCP SCANNER.

GROW TRAFFIC & LIMIT COMPLAINTS



Advertising compliance trend of onboarded services on STC



Within the first 12 Months of using MCP SCANNER, advertising compliance increased from **50% to 98%** on STC (while other Network Operators, Ooredoo averaged 32% and Zain averaged 71% over the same period) and STC compliance has remained high at 98%+.



RESULTS

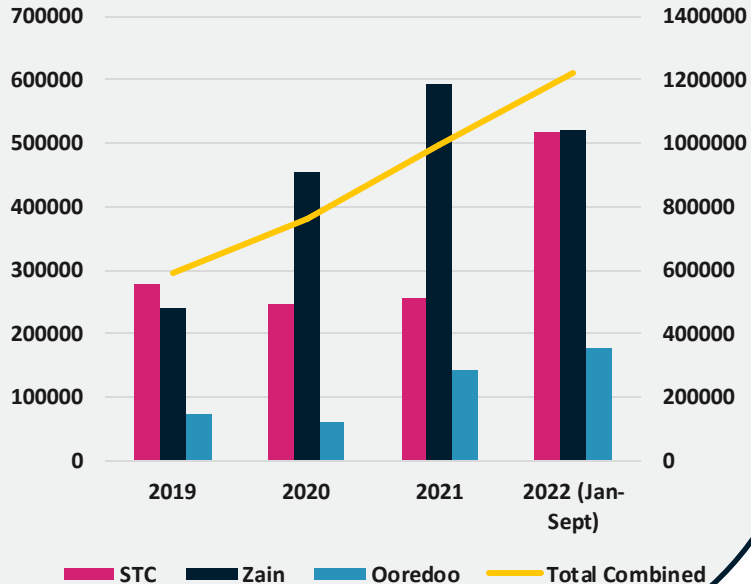


MNO Ad Market Share as seen on MCP Scanner



Since 2019 MCP Insight's support has helped STC maintain a strong position in Kuwait's DCB market. A secure framework has seen significant merchant and advertising growth on STC between 2021 and 2022.

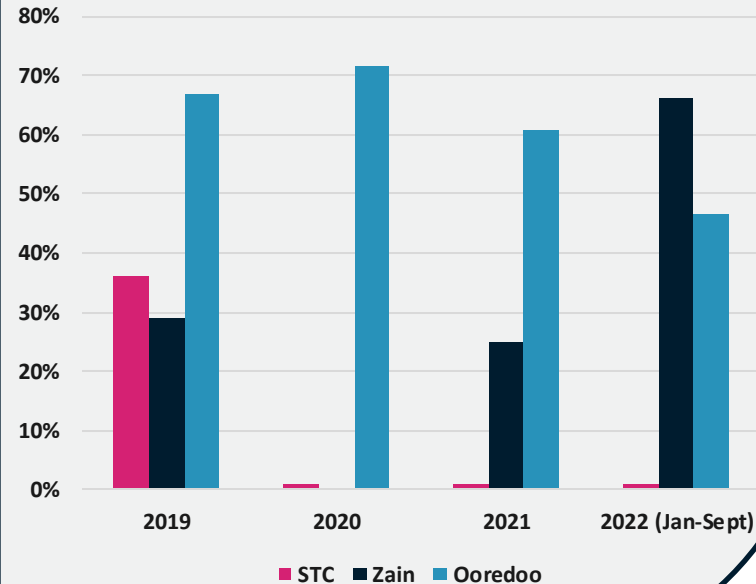
MCP Scale Up Tests: 1.2m+ Ad Flows in 2022



Non-Compliant Traffic as a % of Total Traffic on Each MNO



STC's % non-compliant traffic found on MCP Scanner has remained at around 2% since 2020 while the % non-compliant traffic has remained high on Ooredoo and increased on Zain.

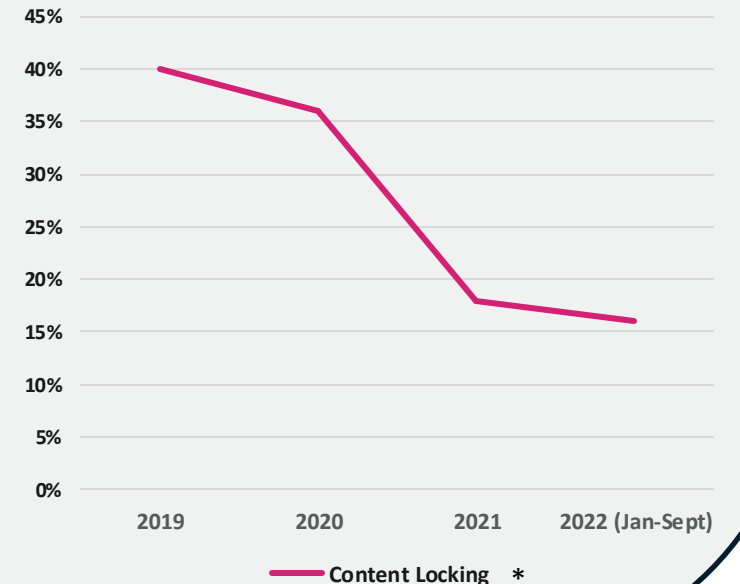


Decrease Trend of STC's share of Ad Fraud* issues



Supported by MCP Insight's automated MCP SCANNER and manual search, STC has significantly lowered their share of Kuwait's Ad Fraud (Content Locking) cases in comparison to its competitors.

Between 2019 and 2021 total Content Locking on STC Kuwait decreased by 23% and has continued to decline in 2022.



THE FRAUD CHALLENGE

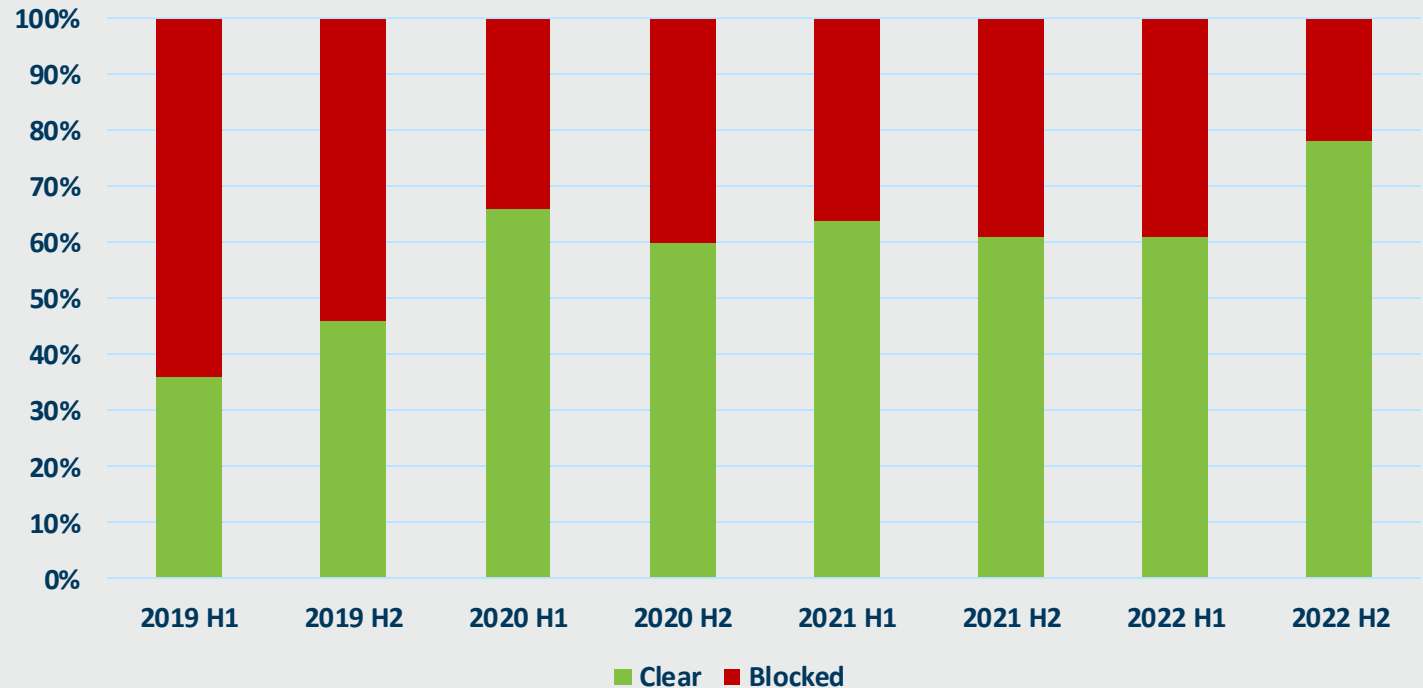


In mid-2019 60%+ of the traffic on STC were fraudulent attempts.

The implementation of MCP's antifraud system MCP SHIELD started to block all fraudulent activity, forcing an improvement in the quality of affiliate traffic (e.g. less buying of blind traffic; preferred partners..).

The graph shows the trend of clear traffic on MCP SHIELD between 2019 and 2022. By 2020 a stable pattern of 60-70% legitimate traffic emerged. There has been an increasing emphasis on Google traffic and this has helped contribute to an improving picture of 75%+ legitimate traffic by H2 2020.

% of Clear and Blocked Traffic on STC between the 1st and 2nd Half of each Year



The implementation of MCP SHIELD on STC traffic not only blocked all fraudulent activity but also created a secure environment which has led to significant growth in legitimate transactions.



SHIELD - 1 YEAR ANALYSIS



Key Statistics (Oct 2021 – Sept 2022)

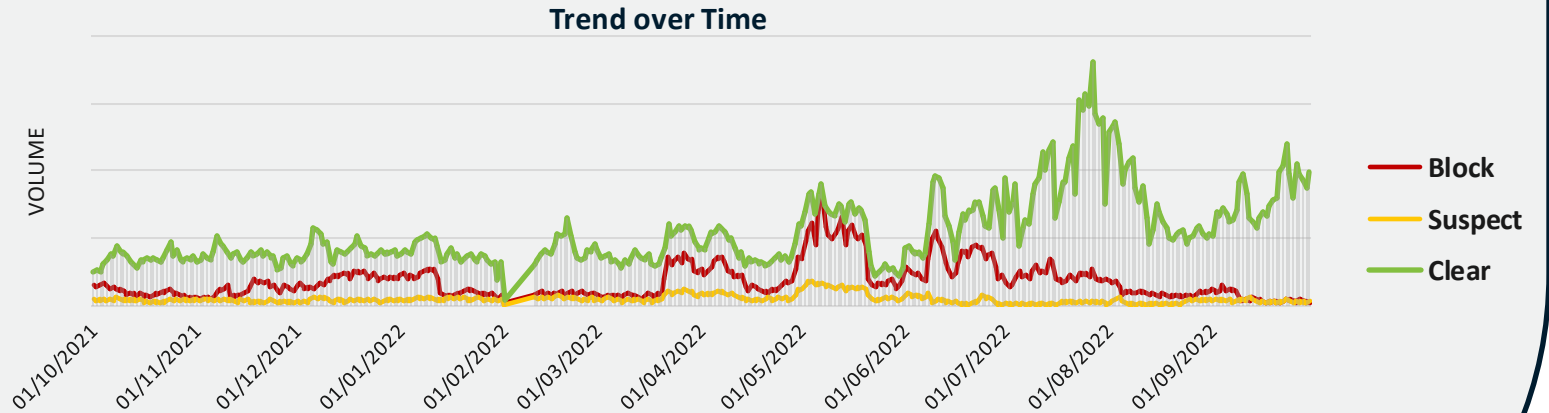
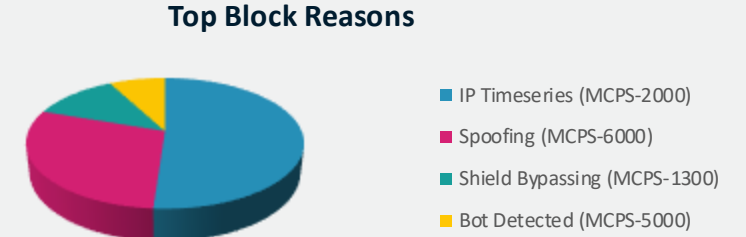
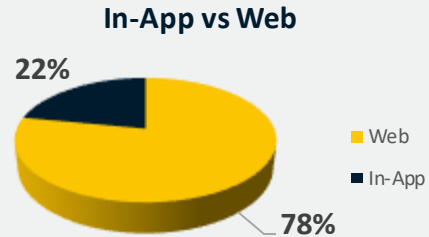
Block **23%**

Suspect **6%**

Clear **70%**

- In 2019/20 In-App traffic represented 50% of all traffic and 70%+ was attempted fraud
- With the implementation of MCP SHIELD, this fraud traffic is blocked and In-App traffic now averages 22%
- Throughout the 1yr period, there is an increasing clear rate and growing volume of transactions, peaking in July

STC SHIELD Trend Analysis (Oct 2021 – Sept 2022)



- By August '22 the Clear rate for traffic has risen to 90%
- This is supported by a high percentage of Google web and in-app traffic

SHIELD - 1 YEAR ANALYSIS



Key Statistics (Oct 2021 – Sept 2022)

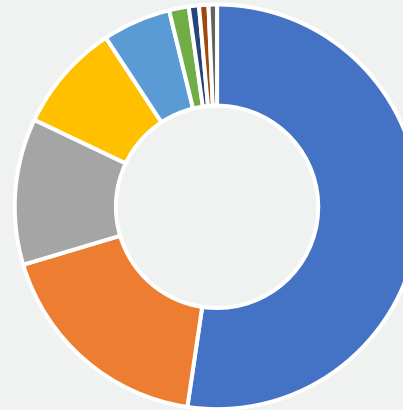
Block **26%**

Suspect **6%**

Clear **68%**

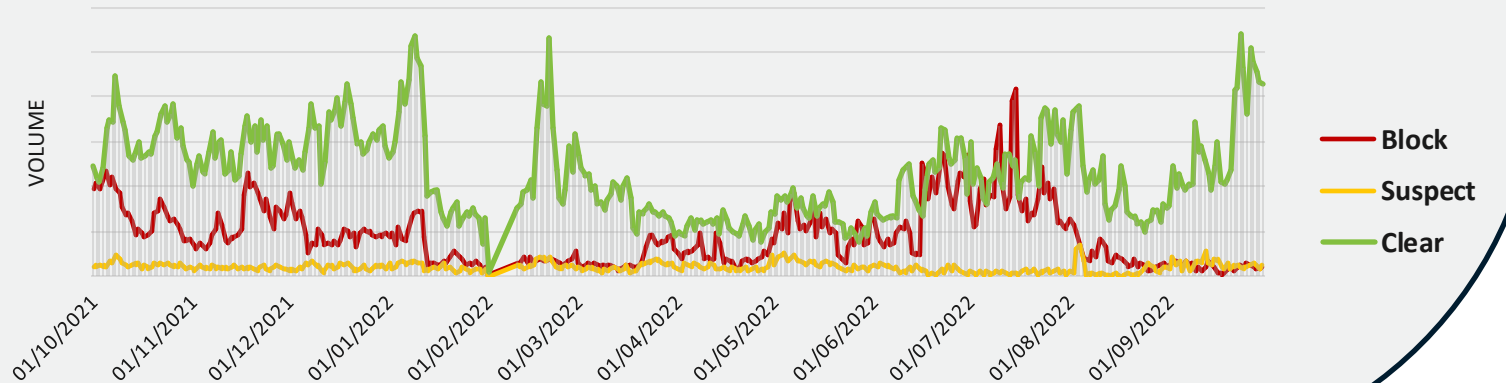
- Although 2022 has witnessed a period of good in-app traffic, July-August period saw a peak of In-App malware attacks which were blocked
- Reasons for blocking In-App fraud are the generally the same as reasons for blocking web traffic.
- Additional reasons for blocking In-App fraud are **APK Fraud** and **Remotely Controlled Fraud**

In-App (APK) Traffic Trend



- Failed Interaction (MCPS-9000)
- Spoofing (MCPS-6000)
- Bot Detected (MCPS-5000)
- IP Timeseries (MCPS-2000)
- Shield Bypassing (MCPS-1300)
- APK Fraud (MCPS-4000)
- IP / Network Block (MCPS-1000)
- Failed Input Verification (MCPS-1100)
- Remotely Controlled Fraud (MCPS-8000)

Trend over Time



FRAUD SPECIALIST TEAM



Manual Testing for App Malware

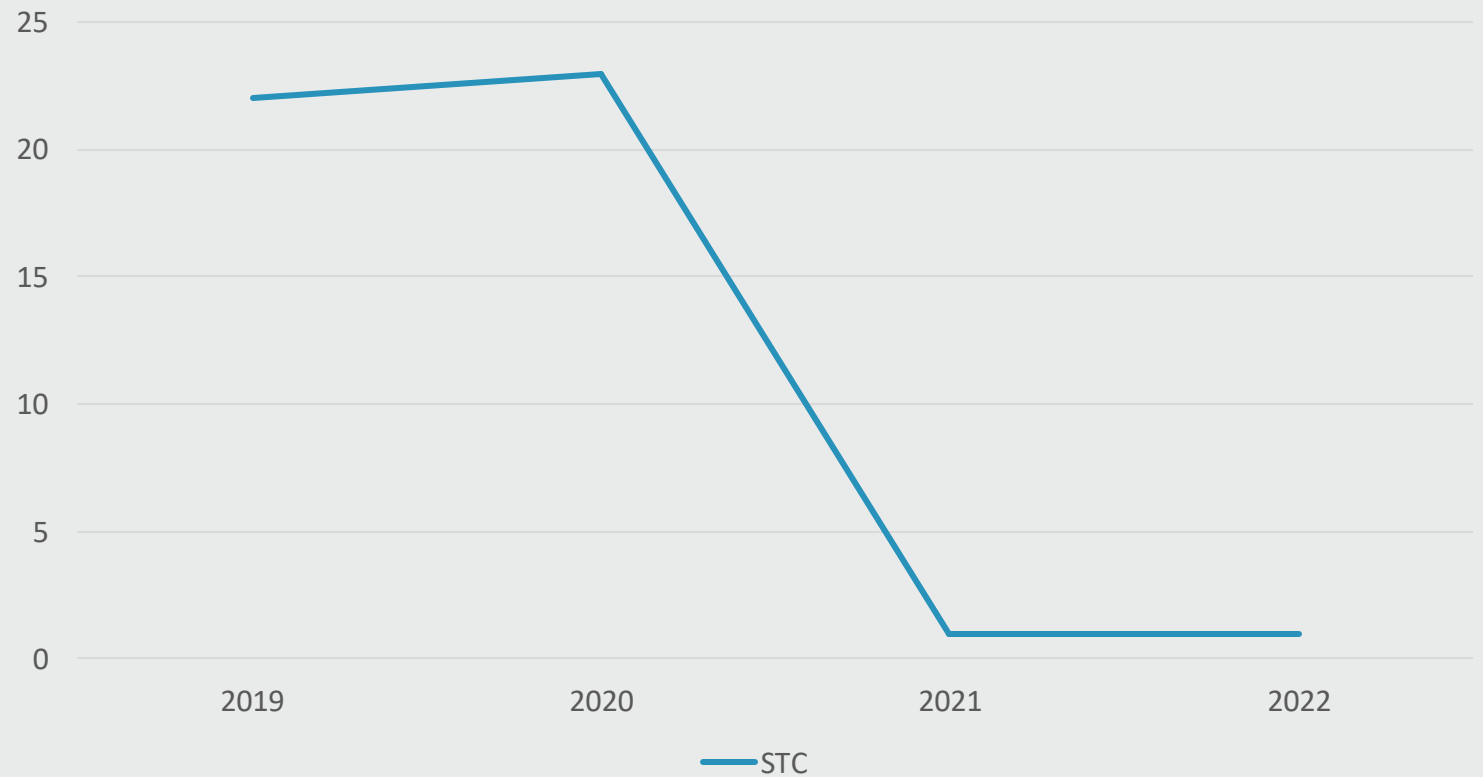
Since 2019, using MCP SHIELD targeted data, 4,500 suspect apps were manually installed on Kuwait devices. We attempt to replicate the consumer experience with malware and use intel to improve MCP SHIELD detection.

The successful roll out of MCP SHIELD across all services in Kuwait since 2020 is demonstrated by the significant drop in app malware seen in our consumer test devices

In 2021 and 2022 there have been only 2 cases per year

The 2022 cases aligned with the huge increase in app malware attacks seen July-Aug 2022.

App Malware Manual Finds on STC



FRAUD SPECIALIST TEAM



Manual Testing of Suspected Apps

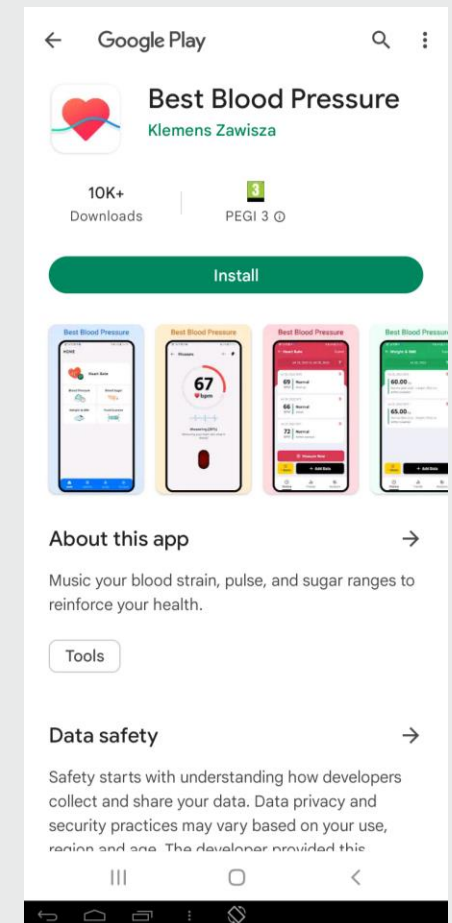
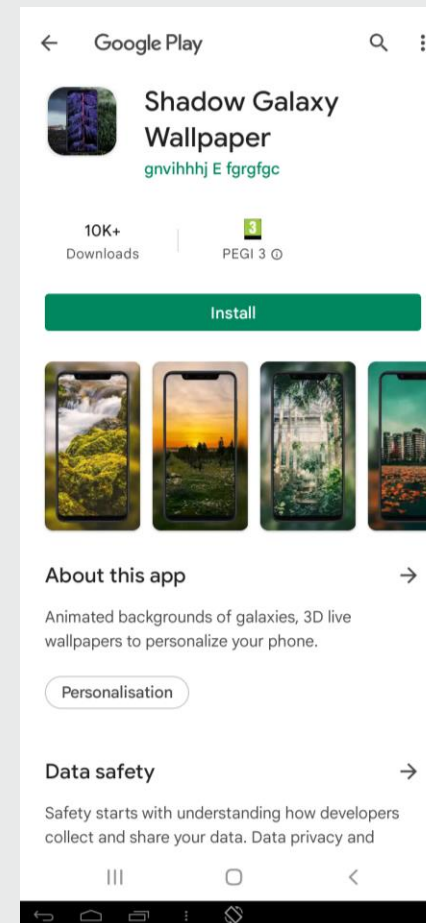
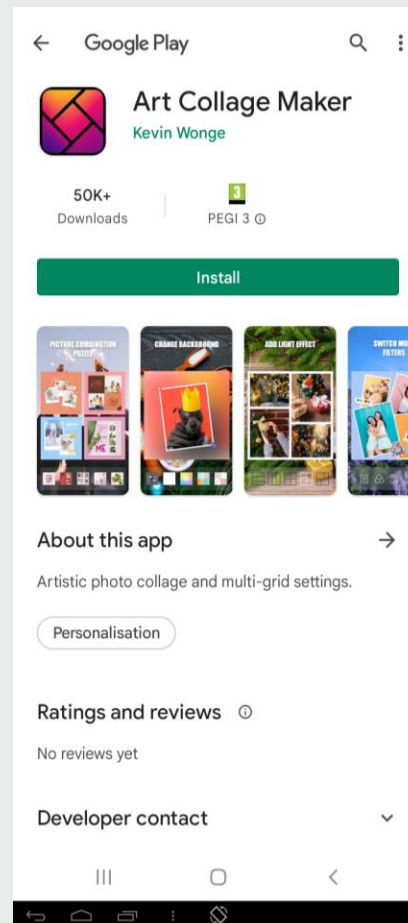
- 90% app-malware found in 3rd party stores
- Tools and Personalisation app categories have the highest amount of fraud

Although 90% of app-malware is found in 3rd Party Stores, some of the Malware Apps which we identified through MCP SHIELD, were live on the Google Play store.

In Google, the top malware categories were Personalization and Health

These apps were also sending traffic in KSA, France, United Kingdom, Germany, South Africa, Nepal, Malaysia, Japan, Australia, USA and Canada.

App Malware Manual Finds on STC



FRAUD SPECIALIST TEAM



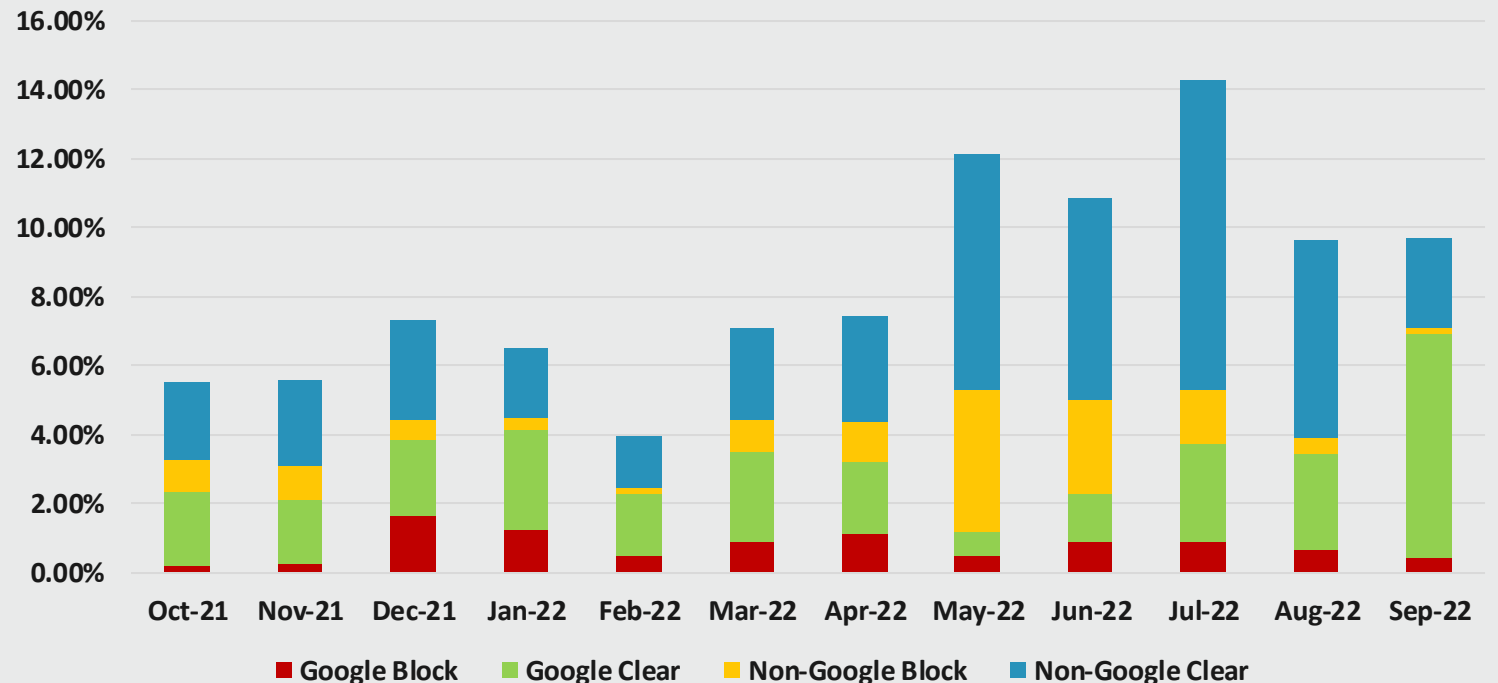
Trend of Google and Non-Google Traffic

With a secure anti-fraud framework in place, the market has opened up to more brands. New services with new ad traffic partners creates a cycle of attempted fraud (which continues to be blocked) followed by improving good traffic.


This cycle can best be seen in May 2022, where Google traffic decreased by 62%, and there was a corresponding 61% rise in Non-Google traffic, but also a surge in blocked Non-Google traffic.

The higher volumes of traffic have persisted since May, peaking in July. The shake out of bad Affiliate traffic (June to August) has decreased the volume of Non-Google traffic but increased the clear rate, with an increasing return of focus to good Google traffic.

Google vs Non-Google Block/Clear | October 2021 – September 2022



By August 2022 the Google block rate began to decrease again and September has seen Google Traffic volumes overtake Non-Google traffic, which presents very clear traffic overall at 93%.



“We are happy to recommend MCP to anyone who is seriously interested in eradicating misleading and fraudulent online flows.”

DIGITAL PRODUCTS & PARTNERSHIPS • STC





**MAKING THE MOBILE
PAYMENTS INDUSTRY
A SAFER SPACE TO
GROW YOUR BRAND**

mcpinsight.com

info@mcpinsight.com

[@mcp_alerts](#)