

openmind

SHAPING THE FUTURE OF MESSAGING



Openmind Networks & Swisscom

Making SMS Safer than Ever

Making SMS Safer than Ever

- How Swisscom protects its subscribers

During the summer of 2020, as the world came to terms with pandemic life, customer care staff at Swisscom were alerted to unfamiliar and suspicious messaging activity on their network. Like operators everywhere, Swisscom were on guard against fraudsters using the cover of the Covid-19 emergency to target vulnerable subscribers. Swisscom proactively engaged Openmind networks to conduct an audit on their network to discover the extent of the problem.

Openmind reaffirmed that Swisscom subscribers were indeed being targeted by fraudsters with 'Smishing' messages. These Smishing messages were spoofed to look like a parcel delivery notifications, but containing a URL that if clicked could download malware to an Android phone. If clicked on an iPhone, the same URL would throw up a faked iTunes login page designed to capture usernames and passwords from Apple users. Indeed Apple users were the primary target of this attack. The intent of the fraudsters was to get access to the iTunes store to buy Netflix vouchers that could be sold online.



Instances of similar attacks were reported by operators across Europe. Not unlike Covid-19, Smishing hit in wave after wave, moving from one operator to another. One particular Smishing fraud hit primetime - 'Flubot' - a cunning banking Trojan hosted on a botnet of infected handsets, capable of emptying the bank accounts of unwary subscribers. Faced with these attacks, and knowing that a solution was available from Openmind Networks, Swisscom determined to take immediate action to protect their subscribers.

‘Flubot’ - a cunning banking Trojan hosted on a botnet of infected handsets, capable of emptying the bank accounts of unwary subscribers.



Finding a solution

Openmind had spent several years on research & development in using machine learning techniques to identify fraudulent messages from within the mass of legitimate messages delivered on a mobile network.

Openmind had created a services team dedicated to uncovering and blocking fraudulent messaging traffic. Working together with Swisscom's Fraud Team, they designed a service that could detect incoming Smishing messages and block them before they were delivered to subscribers.



Crucially, this also had to be done while adhering to strict subscriber privacy regulations in Switzerland. Even though technology was used to identify Smishing frauds, this technology could only be applied to messages that were first stripped of any details that could uniquely identify the targeted subscriber.

This was achieved using Message-anonymization software delivered by Openmind and was essential to securing approval by Swisscom's Data Protection Officer for implementation of the new service.



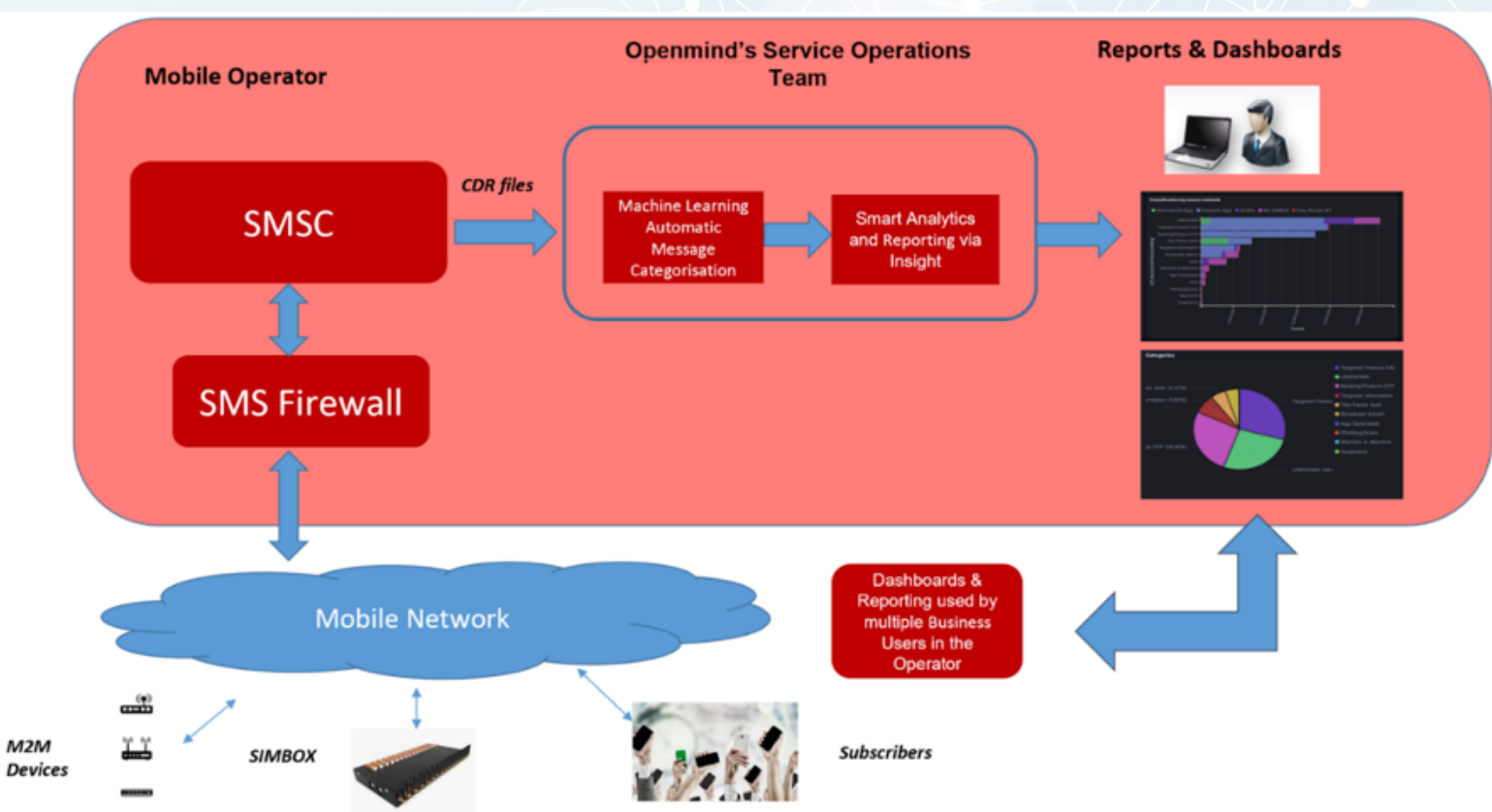
How Smishing Messages are detected and blocked at Swisscom





Openmind's Smishing Detection service is built on the Smart Control Platform. The Smart Control consists of a central Machine Learning engine coupled with different analytical tools that support the real-time, pro-active detection and blocking of different types of messaging fraud.

The new software is overseen, maintained and updated using a DevOps CI/CD process by Openmind's Managed Services team, and is integrated into Swisscom's network allowing for real-time instructions on what messages to block. Openmind's Managed Services team works closely with Swisscom's Fraud teams to ensure that the new and emerging threats are recognised and tackled quickly and effectively.



Smishing Solution



Once activated, the Smishing Detection Solution immediately proved its worth, preventing fraudulent messages from being delivered to Swisscom Subscribers. Thomas Martinson, Product Manager of Communications Services is enthusiastic about the success of the new service.

“Openmind has been very reactive in developing, deploying and supporting a smart Smishing detection solution to protect Swisscom customers.



The Openmind solution, together with Swisscom's proven Cyber Defense underlines once again Swisscom's best network-best services promise towards its customers and partners”, he said.



Securing Messaging Networks from Fraud

About Openmind:

Openmind Networks, coming from deep experience in core messaging infrastructure, has a mission to help our customers protect their subscribers from fraud and to help our customers protect their networks from fraud and cyber attacks. Our customers include some of the world's largest Mobile Operators, Wholesale Operators, Aggregators and Social Media providers.

About Swisscom

Swisscom, Switzerland's leading telecoms company and one of its leading IT companies, is headquartered in Ittigen, close to the capital city Berne. Outside Switzerland, Swisscom has a presence on the Italian market in the guise of Fastweb. 2021 around 18,900 employees generated sales of CHF 11,183 million. It is 51% Confederation-owned and is one of Switzerland's most sustainable and innovative companies.

