

Robocall Mitigation Plan



Business Information

VOIPSV

San Salvador

Contact Information

Julio Valladares

CTO +50323825000

support@voipsv.com

Introduction

In the ever-evolving landscape of telecommunications, the rise of automated and fraudulent calls has posed significant challenges for service providers, resellers, and users alike. As a reseller in the telecommunications industry, leveraging the robust call prevention systems of our esteemed providers, we are committed to safeguarding our service against these threats. Despite the sophisticated prevention measures already in place, the dynamic nature of telecom fraud necessitates a vigilant and proactive approach to detection, response, and user education. This document outlines a comprehensive mitigation plan aimed at fortifying our defenses against unwanted calls, ensuring the integrity of our service, and maintaining the trust of our valued users.

Objective

The primary objective of this mitigation plan is to enhance our capabilities in detecting and responding to automated and fraudulent calls, while also empowering our users with the knowledge and tools to protect themselves. By building on the prevention frameworks provided we aim to implement a layered security approach that includes rigorous monitoring, swift incident response, robust legal cooperation, and extensive user education. This plan is designed to be adaptable, ensuring it remains effective against evolving threats and maintains compliance with federal and international regulations. Through these efforts, we strive to provide a secure and reliable telecommunications service that meets the needs of our diverse user base, from Latin America to the United States, and everywhere in between.

Detection

Continuous Monitoring: Despite and Voxbeam implementing their own prevention measures, we will conduct constant monitoring of call traffic to identify unusual patterns that may indicate fraudulent behavior, using statistical methods and pattern analysis.

Reporting and Alerts: Develop an alert system based on thresholds to notify the security team of abnormal call volumes or suspicious patterns, facilitating rapid detection and action.

Regular Security Audits: Perform regular security audits to assess and enhance the capability to detect suspicious or fraudulent activities.

Response

Escalation Procedures: Implement clear escalation procedures for quickly responding to detected incidents, including the immediate suspension of involved accounts and communication with providers about the actions taken.

Incident Response Team: Maintain a dedicated incident response team prepared to act 24/7 on reports of fraudulent activity or unauthorized automated calls.

Policy Review and Adjustment: Continuously review the effectiveness of response policies and adjust as needed to improve the response capability against emerging threats.

Legal Cooperation

Collaboration with Authorities: Establish protocols for effective collaboration with legal authorities and regulators, including the preparation and provision of evidence in compliance with applicable laws.

Transparency and Regulatory Compliance: Ensure operational transparency and compliance with relevant federal and international regulations, adapting business practices to facilitate legal and regulatory cooperation.

User Education

Training and Awareness: Develop education programs for users about the risks of fraudulent calls and how to identify and report suspicious activities.

Active Communication: Maintain active and open communication with users regarding the security measures implemented and the procedures for reporting suspicious or fraudulent calls.

Online Resources: Provide accessible online resources, such as guides, frequently asked questions (FAQs), and best security practices, to empower users in protecting their own accounts.

Conclusion

In conclusion, the telecommunications landscape demands constant vigilance and adaptation to combat the persistent threat of automated and fraudulent calls. Our comprehensive mitigation plan, built on the foundations of detection, response, legal cooperation, and user education, represents a holistic approach to safeguarding our services and users. By effectively leveraging the prevention systems, and enhancing them with our own robust measures, we are positioned to tackle these challenges head-on. Our commitment to security, transparency, and user empowerment will not only help mitigate the risks associated with unwanted calls but also strengthen the trust and reliability that our users place in our service. As we move forward, we will continue to evaluate and refine our strategies, ensuring that we remain at the forefront of telecommunications security and service excellence.