AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

Securing the Digital Presence of a Leading Telecom Provider

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

Overview:

A leading telecom provider faced a growing wave of digital fraud campaigns that exploited its trusted brand name. Cybercriminals launched fake promotional offers, SIM upgrade scams, phishing messages, and impersonation schemes designed to mislead customers into sharing sensitive personal and financial information.

These fraudulent activities not only created financial risk for customers, but also damaged brand reputation, increased customer support complaints, and weakened trust in legitimate digital campaigns. With telecom brands being highly visible and frequently targeted, the organization needed an immediate and proactive solution to monitor, detect, and dismantle online abuse at scale.

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

Challenges:

01 Fake Promotions and Scam Campaigns:

Threat actors created fraudulent websites, sponsored ads, and promotional pages using the telecom provider's branding, colors, and messaging style. These campaigns falsely promised discounted recharge plans, free data bundles, and special loyalty rewards to lure customers.

02 Brand Impersonation Across Channels:

Unauthorized third-party vendors and scammers misused the company's logo, trade name, and digital identity across websites, social media pages, and messaging platforms. Customers often struggled to distinguish between legitimate communication and fraudulent activity.

03 SIM Swap and Identity Fraud Risks:

Certain scams promoted fake SIM replacement or KYC update links, tricking users into submitting personal data that could later be used for SIM fraud or identity theft.

04 Misinformation on Pricing and Services:

Fraudulent social media campaigns spread false information regarding plan pricing, service outages, and telecom offers. This created confusion among customers and generated unnecessary pressure on customer support teams.

05 Rapidly Evolving Threat Landscape:

Scam content was being created and reposted quickly across multiple channels, making manual detection and takedown efforts inefficient and slow.

Solution:

Ampcus Cyber was engaged to deploy a rapid-response digital risk protection program with an implementation timeline of just 1 week. The solution included:

Real-Time Digital Monitoring

Continuous surveillance across websites, social media platforms, app stores, ad networks, marketplaces, and messaging ecosystems to identify misuse of the telecom brand in real time.

Automated Fraud Detection

Advanced detection mechanisms were implemented to identify fake advertisements, phishing domains, impersonation pages, counterfeit promotions, and unauthorized resellers using brand assets.

Threat Prioritization and Incident Response

Detected threats were categorized based on severity, reach, and customer impact, allowing high-risk scams to be addressed immediately.

Takedown and Legal Enforcement

Ampcus Cyber coordinated takedown requests, abuse reports, and enforcement actions with hosting providers, registrars, platforms, and relevant authorities to remove malicious content quickly.

Brand Trust Protection Strategy

Recommendations were provided to improve customer awareness, strengthen official communication channels, and reduce future impersonation risks.

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

Outcome:

01 **Dismantled Fraudulent Campaigns:** Multiple fake promotions, phishing sites, and impersonation campaigns were identified and removed before causing wider damage.

02 **Reduced Brand Abuse:** Unauthorized use of the telecom provider's brand identity across digital channels was significantly reduced.

03 **Strengthened Customer Trust:** Customers regained confidence in official offers and communication channels.

04 **Lower Customer Complaints:** The reduction in scam exposure led to fewer fraud-related complaints and less strain on support teams.

05 **Reduced Financial Losses:** By stopping phishing and scam campaigns early, potential customer losses and reputational damage were minimized.

Conclusion:

For telecom providers, brand trust is a critical asset. In a fast-moving digital environment, fraudsters continuously exploit recognizable brands to target customers. Through rapid deployment, continuous monitoring, and swift takedown actions, Ampcus Cyber helped this telecom provider secure its digital presence and protect both its customers and reputation.

India
601-609A, 6th Floor, Beta Block, Sigma Soft Tech Park, Varthur Kodi, Whitefield, Bangalore, Karnataka - 560066.

USA
14900 Conference Center Dr, Suite # 500, Chantilly, VA 20151.

UAE
Office 306, Building A6, Dubai Digital Park, Dubai Silicon Oasis, Dubai.

Philippines
19th floor Exxa Tower, Bridgetowne, E.Rodriguez Jr. Ave cor C5 Road, Ugong Norte, Quezon City.

www.ampcuscyber.com

letsconnect@ampcuscyber.com