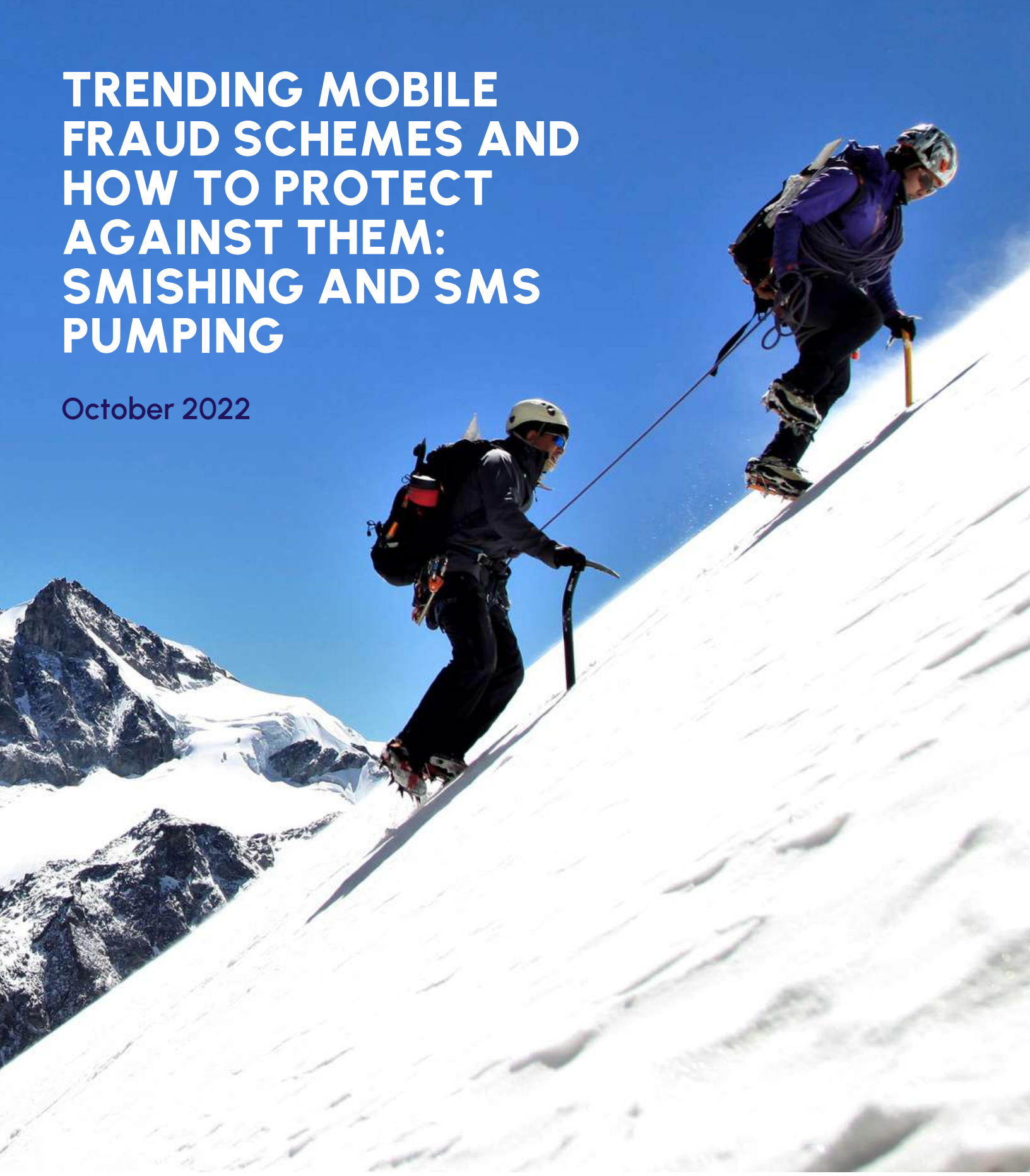
TRENDING MOBILE FRAUD SCHEMES AND HOW TO PROTECT AGAINST THEM: SMISHING AND SMS PUMPING

October 2022

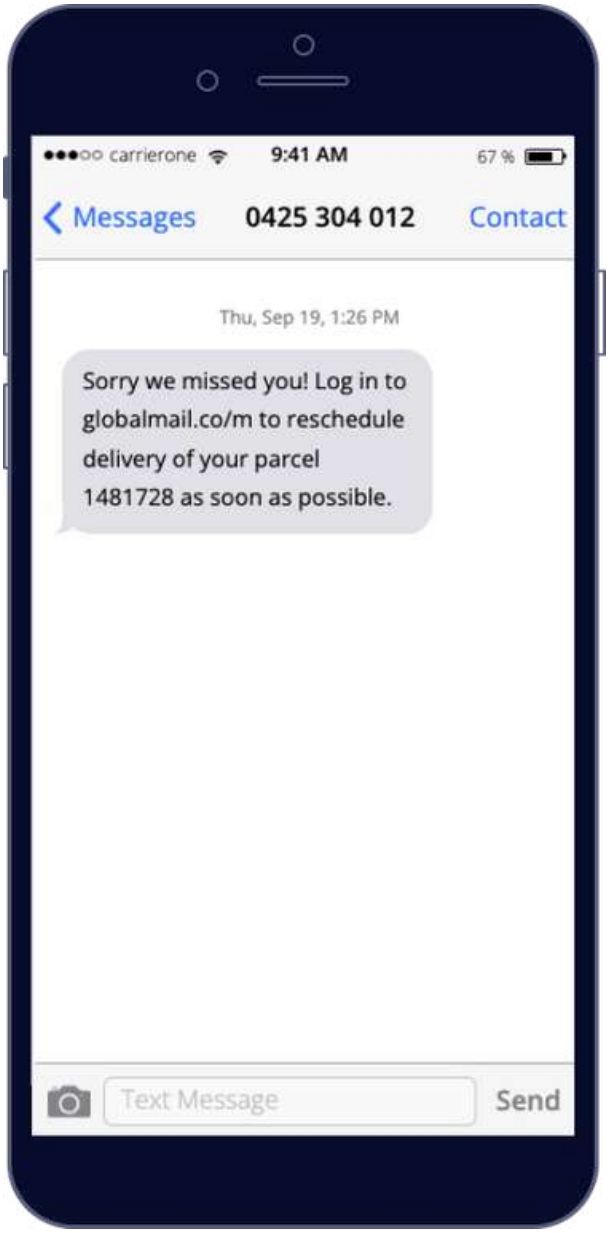


soprano

IN THIS BRIEFING

- Fraud Alert: Smishing
- Tools to Protect Your Audience From Smishing
- Fraud Alert: SMS Pumping
- How to Prevent an SMS Pumping Attack
- Soprano Connect Security Features Summary

Fraud Alert: Smishing



Overview

Smishing is characterised by the same three steps:

1. A message claiming to be from a legitimate source is sent to targets with a link,.
2. The link leads the victims to a branded web page where the victim will submit personal information.
3. The fraudster uses that information for criminal gain.

One of the most successful smishing schemes which has massively gained in popularity follows a very simple choreography: a victim will be sent a message from a supposed mail carrier e.g., "AusPost scheduled delivery for parcel number 2374619381 is delayed. Sign in to https://auspost-rescheduleasap.com to reschedule delivery." When the victim follows the link, they will see a website that looks very much like they would expect an Australia Post official web page to look, where they will be presented with a form for their personal data.

Smishing is a huge risk for firms and individuals alike. Regardless of who might be burdened with the consequences, senders, providers, authorities, and end recipients all need to work together to proactively prevent and defend against smishing.

Solutions

Increase Awareness

Teach users and partners on how to recognise a smishing attack (with real-world examples) and how to report it.

Simulate Attacks to Inform Training

Simulated smishing attacks are one of the best ways to test your internal teams' mobile security readiness. Work with IT and security to review the results and make improvements.

Implement Multi-Factor Authentication (MFA)

MFA will make it harder for cybercriminals to gain access to your systems even if they succeed in collecting usernames and passwords from internal staff.

Restrict IP Access

Restricting your application access based on IP address controls can boost protection from outside attacks.

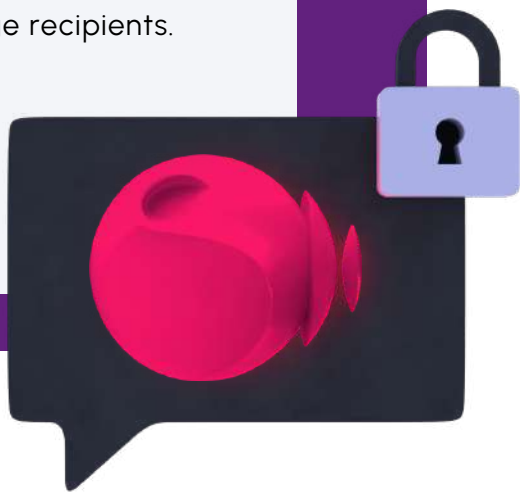
TOOLS TO PROTECT YOUR AUDIENCE FROM SMISHING

FRAUD DETECTION AND PREVENTION SERVICE

Soprano Design has delivered messaging for financial institutions, hospitals, governments, airports, and other security-forward industries for 28 years. Our customers' needs require a higher level of service and delivery because their messages serve critical purposes such as saving lives, elevating citizens' health, and responding to emergencies.

In addition to rigorous organisational security, Soprano Connect offers a suite of features which help protect our customers, and in turn protect their end message recipients. One such feature is the newly released Fraud Detection and Prevention Service (API) which is a stand-alone API dedicated to detecting and indicating possible fraudulent mobile numbers in the platform. Users can start filtering for fraudulent numbers by setting configurable parameters in Soprano Connect which assigns values to three indicators of risk: SIM Swapping, Trusted Network, and Call Forwarding. These fraud checks may be assigned a "weightage" value where the sum of all three values must add to 100. Users can choose to check for all three, two, or a single fraud type. When this license is purchased, users can (in conjunction with the HTTP API and Connect API SMS) decide whether to send SMS or not based on a predetermined risk threshold. With this feature in place, users who send sensitive messages (like one-time passwords) can withhold messages from numbers or devices which are indicating that they might be part of or targets of fraud.

Fraud is an increasingly pervasive issue in mobile communications, and firms have a responsibility to protect not only themselves, but also their audiences whenever possible. With the Fraud Detection and Prevention Service API, Soprano offers protection for customers and a proactive defense for their message recipients.



FRAUD ALERT: SMS PUMPING

OVERVIEW

SMS pumping, also known as artificial traffic inflation, is when cyber criminals (usually coordinating as a sophisticated group) obtain a large volume of numbers whose traffic is delivered by a single provider and send high volumes of traffic to an online form or web app which sends an SMS automatically when a number is submitted to the form. Depending on the capability of the fraudster and their complicit partner, these large SMS volumes are sent to premium-rate destinations which further inflates the cost of the attack. When the targeted business pays their inflated SMS bill, the provider will give a share of the profits to the cyber criminals.

This kind of activity is too risky for large providers to take part—they would not knowingly partake in this kind of scheme. Unfortunately, very few people realize that the organisation they buy their mobile traffic from is rarely the only entity to handle their traffic. Networks purchase traffic from one another in a layered set of routes which results in better connectivity for everyone—but also obscures bad actors that might be mishandling traffic and working with fraudsters.

HOW TO SPOT IT

- Monitor for high volumes of incomplete login attempts (for OTP SMS pumping attacks).
- Look for adjacent number inputs (+99999999990, +9999999999, (+99999999992 etc.) in rapid succession and alert your traffic provider. Often victims will see a block of sequential mobile numbers that were provided by the SMS pump service and are controlled by the rouge operator.
- Set alerts to notify of unexpected spikes in traffic.

HOW TO PREVENT AN SMS PUMPING ATTACK

01 Report any unexpected spikes in traffic as early as possible and investigate the source

02 Set a volume cap and alerts on all mobile number gathering forms or logins

03 Set rate limits on your OTP webform input box so that it will not send more than 1 message per X seconds to the same number or country prefix. This may not prevent the fraud, but it might discourage them from targeting your app in the first place

04 Implement rates by API user or IP address

05 Build an allow or block list based on the country code. See here for a list of Country Codes

06 Modify your OTP user experience by using CAPTCHAS or other services to detect and deter bots

Soprano Connect Security Features

Content Masking (Full or Partial)

This module secures the content of your messages by immediately masking the contents to anyone viewing the details of the message in the portal, in reports, or reports exports. It will also mask the content within the database during a customised timeframe, leaving only the metadata to show the message was sent. This ensures that your data is:

- Secure data at rest
- Maintained to superior data protection standards
- At a lower risk of theft or fraud

This product allows users to choose between full content masking or partial content masking. In full content masking mode, all message content will be masked whereas in partial content masking mode, users can define which part of the message content will be masked using redact identifiers.

IP Access Control

IP Access Control allows Soprano Connect administrators to restrict access to IP addresses that are pre-approved and pre-defined in the platform. Login requests from any other IP address is denied, even if the login credentials are valid.

Single Sign On (SSO)

With SSO users can integrate Soprano Connect with their Identity (IDP) Servers to authenticate their corporate users when logging in to Soprano using their corporate credentials. Soprano's SSO supports SAML2.0, OAuth2.0/Open ID protocols and IDP servers such as Microsoft Azure Active Directory (Azure AD) and OKTA. The SSO integration gives organisations a centralised control system of access and reduces password fatigue for users which enhances the security, lowers the burden of IT help desks, and increases organisational efficiency.

Soprano Connect Security Features (Cont.)

2FA for Soprano Connect

Two-Factor Authentication (2FA) for the Soprano portal is the second layer of added security which a user can select to protect the account or system. If it is enabled by the Customer Administrator, the messaging portal user must go through an additional layer of security after entering the password by receiving and providing a OTP before being granted access to the messaging portal. The 2FA is applicable for several processes on messaging portal including the Login, Change Password, Forgot Password and Reset Password.

Simple Template Messaging

This feature allows customer administrators to define standard templates to be used across their organisation to send messages. It restricts access to the advanced functionality of managing message templates. Only users with Simple Template Messaging admin privilege (which is typically assigned to customer admins) are allowed to manage templates while standard users must use the pre-defined templates (with allowed customisations) to send messages. For standard users, it provides an easy-to-use message sending experience equipped with pre-defined templates. Users can customise inputs as needed and design a unique SMS for each recipient.

Authenticator

This module offers a two-factor authentication (2FA) solution to enable employees, customers, and suppliers secure access to online services. It creates and delivers one time passwords (soft token) via SMS to authorise online virtual private network (VPN) access or financial transactions to reduce fraud and improve network security.

Soprano Connect Security Features (Cont.)

User Content Visibility

The Soprano Connect platform is set by default to enable both administrators and standard users to select user data in an enterprise account for any selected company or sub company, orders, dashboards, user or all users. The 'User Content Visibility' provides a restricted view for standard users in any function that enables the selection of company, orders, dashboards or users to be selected. The restriction is not applicable for customer administrators.

Consent Management

Customers can use Consent Management to set preferences of target audiences for messages sent out in the portal and monitor/control the level to which messages get sent to recipients. Recipients (when allowed) can choose to opt-out of messages they receive. Such opt-in or opt-out details are captured as part of Backlist and Whitelists and can be managed within Soprano Connect. This is a critical feature that enables customers to meet legal and regulatory compliances.

Legacy Blacklist or Whitelist

This is the legacy filtering feature that allows users to filter destinations where messages are sent as part of standard OPT-OUT or OPT-IN management for broadcast messaging for all messages sent via all channels from the platform.

soprano

Let's work together

(02) 9900 2200

sales@sopranodesign.com