Messaging Security Best Practices

June 2022

Table of Contents

1 Background

The messaging ecosystem is constantly evolving to keep pace with messaging's popularity among Consumers.[1] Messaging's popularity is largely attributable to its status as a trusted and convenient communications environment among Consumers. That popularity, however, also makes it attractive for bad actors, who may seek to employ a variety of techniques to exploit Consumers and undermine trust in the messaging ecosystem.

These Messaging Security Best Practices are intended to reflect the wireless industry's ongoing efforts to protect Consumers against Unwanted Messages and preserve the trust in and security of messaging services.

In developing this initial version of the Messaging Security Best Practices, CTIA consulted a variety of experts from across the messaging ecosystem to identify a number of activities that could threaten messaging security, as well as the steps that stakeholders should take to protect against and address those threats. By implementing these best practices and securing their respective messaging platforms, stakeholders can play an important role in helping to protect Consumers further from Unwanted Messages and supporting continued trust in the messaging ecosystem.

2 Purpose

The messaging security best practices described below are intended to help preserve trust in the wireless messaging ecosystem[2] and prevent the delivery of Unwanted Messages to Consumers. Section 3 outlines general messaging security best practices that stakeholders may employ to help protect Consumers from Unwanted Messages. Sections 4 through 6 identify messaging security best practices that stakeholders may employ to help address a particular security concern.

[1] The definitions for certain capitalized terms that appear throughout these Messaging Security Best Practices are included in the CTIA Messaging Principles and Best Practices. *See* CTIA, *Messaging Principles and Best Practices*, https://www.ctia.org/the-wireless-industry/industry-commitments/messaging-interoperability-sms-mms.

[2] The messaging ecosystem includes cloud-based services that require the use of a separate messaging client (*e.g.*, an app) that is distinct from and may not interoperate with Wireless Providers' messaging networks. These best practices are intended to apply to messaging services that only interoperate between cloud-based platforms and Wireless Providers' messaging networks using the applicable services, such as SMS and MMS.

3 General Messaging Security Best Practices

3.1 Monitoring and Blocking

Service Providers may block a message where a risk assessment: (1) complies with applicable information security standards;[3] and (2) reasonably suggests the message is an Unwanted Message.[4]

A risk assessment may include, but is not limited to, network monitoring and evidence of the following activities associated with the sending of Unwanted Messages:

- Fraud or other malfeasance, including fraud or malfeasance associated with compromised API credentials;
- Utilization of grey routes;
- Lack of authentication; or
- A pattern of abuse of industry best practices, including the Messaging Principles and Best Practices.

3.2 Forensic Analysis Cooperation

Service Providers, Inter-Carrier Vendors, Connection Aggregators, Registrars, Network Security Vendors, and other stakeholders in the messaging ecosystem should cooperate to prevent Message Senders from sending Unwanted Messages.

3.2.1 Requesting Information

To facilitate cooperation without unduly burdening other parties, stakeholders should request only information that is reasonably necessary to identify Message Senders that are sending Unwanted Messages. Such information may include:

- The message origination point (*e.g.*, IP address, telephone number, or other information associated with the Message Sender);
- Message destination (*e.g.*, IP address, telephone number, or other information associated with the recipient);
- The date and time of the message;

---

[3] *See, e.g.*, National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity* (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf; NIST, *Guide for Conducting Risk Assessments* (Sept. 2012), https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf.

[4] While applicable information security standards may help stakeholders determine whether a message is an Unwanted Message, the definition of "Unwanted Message" is identical in the Messaging Security Best Practices and the Messaging Principles and Best Practices.

- Session Initiation Protocol (SIP) header anomalies;
- Evidence that the message was an Unwanted Message (*e.g.*, evidence that the message was abusive, harmful, malicious, unlawful, SHAFT content,[5] or otherwise inappropriate); or
- The volume of messages.

3.2.2 Responding to Information Requests

To timely address security concerns, parties should respond within a reasonable timeframe to lawful inquiries from other stakeholders regarding the sending of Unwanted Messages or other potential abuses.

Responses to lawful inquiries should be reasonable and sufficiently substantive so that the requesting stakeholder has sufficient information to continue its investigation and eliminate the sending of Unwanted Messages.

3.2.3 Notifying Cooperative Stakeholders of Mitigation Steps

Stakeholders should notify cooperating parties of the steps taken to mitigate the existing threat and how similar, future threats will be addressed.

3.2.4 Know Your Customer

To assist with potential forensic analysis efforts and identify a Message Sender sending Unwanted Messages, Communications Platform as a Service (CPaaS) providers, Connection Aggregators, and other parties should undertake reasonable efforts to "know their customer" by obtaining sufficient identifying information to verify or authenticate a Message Sender's identity before the Message Sender sends a message.

3.3 Consumer Education

To protect Consumers and other end users from phishing, smishing, and other behavior that results in the sending of Unwanted Messages, Service Providers, Connection Aggregators, Network Security Vendors, and other stakeholders that interact with Consumers and other end users should consider creating and sending educational materials that inform Consumers and other end users how they may protect themselves from behavior before such behavior occurs.

To reduce the negative impact of behavior associated with the sending of Unwanted Messages, Service Providers, Connection Aggregators, Network Security Vendors, and other stakeholders that interact with Consumers and other end users should send advisories that:

- Provide notice of the behavior that led to the sending of Unwanted Messages;

[5] "SHAFT" refers to content related to sex, hate, alcohol, firearms, or tobacco.

- Discuss how the recipient of the notice can identify and/or protect themselves from the behavior; and
- Explain how the recipient can assist the Service Provider, Connection Aggregator, Network Security Vendor, or other stakeholder sending the advisory to combat the behavior.

For example, a CPaaS provider may email its customer about regularly rotating API credentials or a data breach that compromised the customer's API credentials and explain next steps for minimizing the negative consequences of the compromised API credentials.

4 Email Origination (Email-to-SMS)

4.1 Email Authentication

Email authentication technologies protect Consumers by allowing Service Providers and other stakeholders to perform forensic analysis and, thus, more easily identify the actual sending domain, identify the bad actor, and take appropriate action.

Accordingly, Message Senders should ensure that all messages utilize common or standardized email authentication technology (*e.g.*, DomainKeys Identified Mail (DKIM), Sender Policy Framework (SPF)).

4.2 Obtaining Consumer Consent and Honoring Consumer Opt-Out Requests

Section 5.1 of the Messaging Principles and Best Practices (Consumer Consent) states that a Message Sender should obtain the appropriate level of consent from a Consumer before sending a message to that Consumer.

Section 5.1.1 of the Messaging Principles and Best Practices (Message Senders Should Provide Clear and Conspicuous Calls-to-Action) states that, to obtain the appropriate level of consent, the Message Sender should display a clear and conspicuous Call-to-Action that contains appropriate disclosures to Consumers about the type and purpose of messaging that Consumers will receive. Calls-to-Action and subsequent messages should not contain any deceptive language, and opt-in details should not be obscured in terms and conditions.

Section 5.1.3 of the Messaging Principles and Best Practices (Consumer Opt-Out) states that Message Senders should, among other things:

- Ensure Consumers have the ability to opt-out of receiving messages at any time; and
- Acknowledge and respect Consumers' opt-out requests.

These Consumer consent principles apply to email-to-SMS messages. A Message Sender's failure to abide by such principles may increase the risk that a Message

Sender's messages are blocked in accordance with Section 3.1 of the Messaging Security Best Practices (Monitoring and Blocking).

5 Disposable Telephone Numbers and Free Text-Enabled Telephone Numbers

5.1 Snowshoe Messaging

Snowshoe Messaging is a technique in which the Message Sender spreads messages across many different telephone numbers. Snowshoe Messaging is closely tied to the use of disposable or temporary telephone numbers, which are affordable or free telephone numbers that are generally obtained through a web-based service or pre-paid SIM card purchases and are used for a temporary purpose.

Consistent with Section 5.5.2 of the Messaging Principles and Best Practices (Snowshoe Messaging), Message Senders should not engage in Snowshoe Messaging.

To prevent Message Senders from engaging in Snowshoe Messaging, CPaaS providers, Cloud-Based Providers, and other Service Providers in the messaging ecosystem should:

- Monitor volumetric thresholds and patterns;
- Use reasonable analytics to identify Message Senders sending Unwanted Messages (*e.g.*, Message Senders engaged in Snowshoe Messaging); and
- Employ other reasonable efforts, as outlined in these Messaging Security Best Practices, to prevent Unwanted Messages from being sent to Consumers.

6 CPaaS Providers and Compromised API Credentials or Systems

6.1 Dynamic Access to Credentials and Passwords

Message Senders, CPaaS providers, and other relevant stakeholders in the messaging ecosystem that use (or require the use of) API credentials should comply with recognized industry security best practices regarding the management of API credentials and passwords (*e.g.*, Federal Information Processing Standard (FIPS), NIST).

6.2 Maintaining Contractual Privity with Third Parties

CPaaS providers and Connection Aggregators should only provide API credentials and permissions to third parties with whom they have a written agreement describing the appropriate use, protection, or sharing of such API credentials and permissions.

6.3 Compromised Account Shutdown

CPaaS providers and Message Senders should monitor the use of API credentials for evidence that such API credentials have been compromised by either internal or external threats. Where evidence exists that API credentials have been compromised, CPaaS providers and Message Senders should take action to remedy the problem.

If a CPaaS provider initially discovers that a Message Sender's API credentials have been compromised, the CPaaS provider should notify the Message Sender and shut down the Message Sender's compromised account as soon as reasonably possible.

If a Message Sender initially discovers that its API credentials have been compromised, the Message Sender should notify its CPaaS provider so that the compromised account may be shut down as soon as reasonably possible.

6.4 Compromised System Remediation

CPaaS providers, Message Senders, and other stakeholders in the messaging ecosystem should monitor their respective systems and take appropriate action to address activity that suggests the system has been compromised in such a way that increases the risk of sending Unwanted Messages.

Examples of a compromised system may include, but are not limited to:

- Situations in which the Message Sender does not have a business relationship with the CPaaS provider or Wireless Provider through which the Message Sender sends the message;
- Spoofing (*i.e.*, when the Message Sender alters the phone number or name associated with the message to mislead a Consumer); and
- Other cases where a Message Sender intends to harm, abuse, or exploit a Consumer by sending an Unwanted Message.