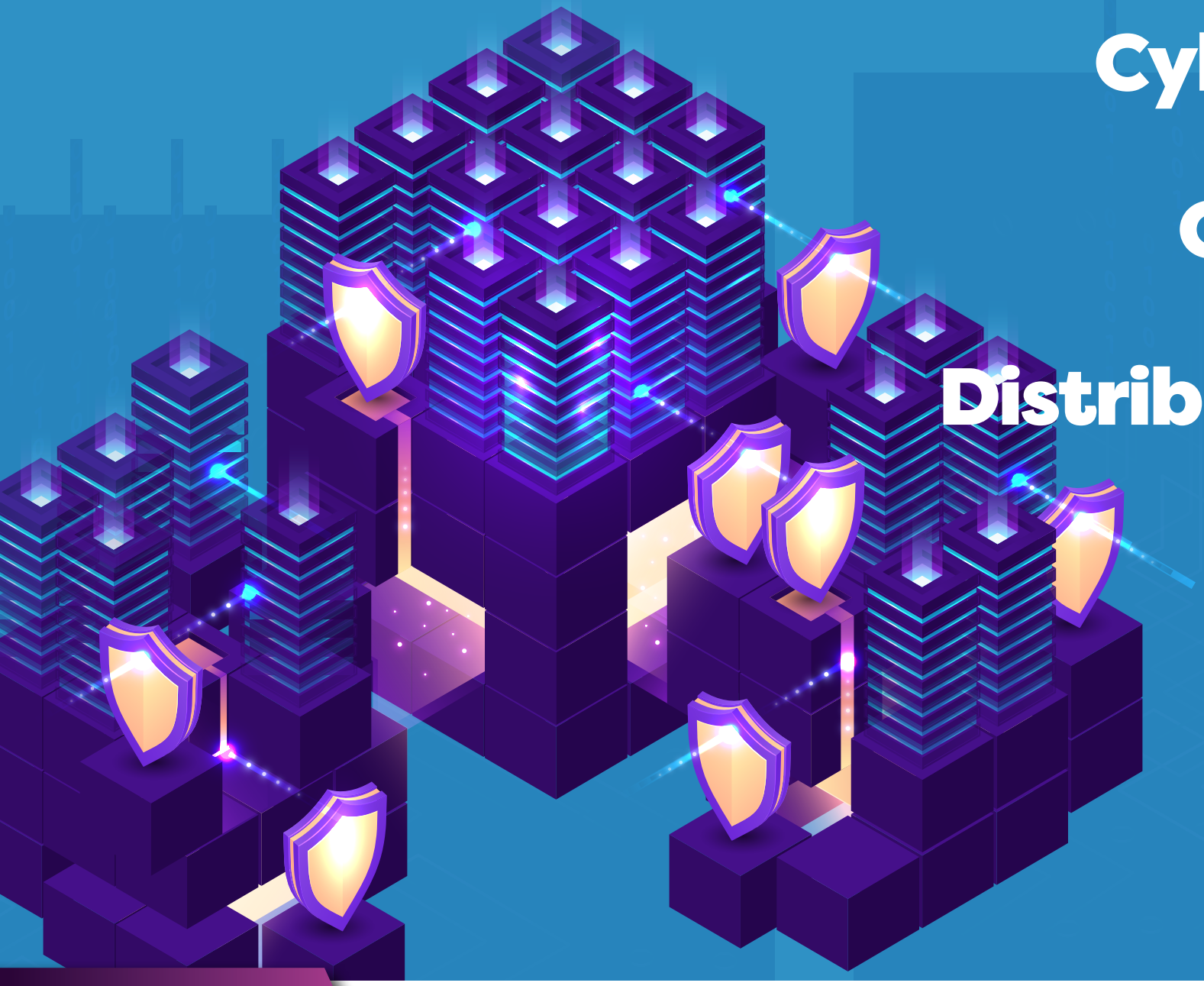


Cybersecurity Aspects of Commercial Message Distribution (SMS)

Cybersecurity Best Practices

B.18

Volume B:
A technical approach

IDB

INCD
Israel National
Cyber Directorate

Originally published by the Israel National Cyber Directorate in Hebrew under the title *Recommendations for Implementation: Distribution of Publications via Text Message (SMS).* © (2021) Israel National Cyber Directorate.

© (2024) Inter-American Development Bank for this translation.

This document was originally published by the Israel National Cyber Directorate (INCD) in Hebrew. Its translation into English was carried out by the cybersecurity team of the Innovation in Citizen Services (IFD/ICS) division of the Inter-American Development Bank (IDB), and it is included as a chapter of the "Cybersecurity Best Practices" collection.

The reader should keep in mind that cybersecurity is a rapidly evolving field. Although these documents reflect established principles, they may be periodically updated as necessary to reflect developments in this field. Additionally, while every effort has been made to present the recommendations and resources in a way that is universally applicable to organizations around the world, the reader may find references that are specific to Israel's cyberecosystem and context (such as the amounts indicated in New Israeli Shekels [NIS], or references to Israeli law or government agencies).

This publication may be downloaded, copied, and distributed, provided that proper attribution is given to the National Cyber Directorate for the original version in Hebrew and to the IDB for the English translation and that the publication is not changed. The opinions expressed in this publication are those of the authors and do not necessarily reflect the point of view of the IDB, its Board of Directors, or the countries it represents.

The original document is available at: **https://www.gov.il/he/pages/smsbp**. Please note that it includes the following disclaimer:

"This document has been prepared by the National Cyber Directorate in order to promote cybersecurity in the Israeli economy. All rights reserved to the State of Israel - National Cyber Directorate. The document has been prepared for the benefit of the public. Duplication of the document or its incorporation in other documents will be subject to the following conditions: the acknowledgment of authorship of the National Cyber Directorate in the format that appears below; the use of the latest version of the document; not making changes to the document. The document contains information of a professional nature, the implementation of which will require knowledge of the systems and adaptation to their characteristics by a professional in the field of cybersecurity. Any comments or references can be sent by email to: tora@cyber.gov.il."

Contents

Foreword

Digital Transformation and the Challenges of Cybersecurity

As digital transformation continues to expand throughout the world, governments, organizations, individuals, and even objects are increasingly connected to the internet. Although digitalization offers undeniable benefits, such as efficient public service delivery, economic growth, and essential connectivity, it also contributes to our growing collective exposure to cybersecurity risks. Recently, the global COVID-19 pandemic has been an important driver of this phenomenon. As a result of widespread social distancing policies, the number of e-commerce transactions and online personal communications grew sharply in a short period of time, along with the number of employees who began teleworking for the first time. In this unprecedented situation, many internet users undertook novel online interactions without enough awareness of the security risks involved. Organizations had to quickly adapt to these challenges by setting up fully remote workflows, often without all of the necessary security measures in place or appropriate guidance to employees.

Cybercriminals are quick to exploit the uncertainty and vulnerability of unsuspecting individuals. Phishing and other social engineering scams proliferated, taking advantage of the global need for information related to the pandemic and the massive use of videoconference applications. In April 2020, Google reported more than 18 million daily malware and phishing emails related to COVID-19 in only a week. Hackers posing as the World Health Organization sent phishing emails and massively spread malicious links to fake videoconference meetings and attachments containing malware. According to the Check Point Research 2021 Security Report, in the first few months of 2020, almost a million attack attempts against Remote Desktop Protocol (RDP) connections, widely used among organizations for employees' remote connections, were observed every day. In fact, RDP attacks were the most popular form of cyberattack, surpassing even phishing emails. In the second half of the year, as more organizations strengthened the security of their remote platforms, hackers focused their efforts on exploiting vulnerabilities in employees' private assets and remote access devices to penetrate their organizations. Although such threats were maximized by this global context, they are not novel and will not go away; we continue to live in an environment of heightened risk, which is particularly serious in regions of the world where cybersecurity policies and technology are less developed and where citizen education and awareness around this issue are lacking. In other words, although the shifts due to the COVID-19 pandemic may revert to what they were before the pandemic, they have brought to light the urgent need to strengthen individual and collective protections against cyberrisks.

Strengthening cybersecurity is essential to safeguard citizens' rights to privacy and property in the digital sphere, promote citizens' trust in digital technologies, and support economic growth through safe digital transformation. In particular, citizens must be assured that the digital systems they use for their personal or professional activities, as well as those that involve their personal data, possess adequate security measures to guarantee the integrity, confidentiality, and availability of their information and the services that they need. Moreover, security breaches have a significant negative economic impact. A recent report by McAfee estimated that cybercrime costs the world economy around US$6 trillion annually, or 0.8 percent of global GDP.

Israel: A Global Leader in Cybersecurity

Israel's innovation and entrepreneurship ecosystem is globally recognized as one of the most vibrant in the world, earning it the name Startup Nation. According to the March 2021 OECD Science and Technology Indicators, Israel is the country that invests the highest percentage of its GDP (4.9 percent) in research and development (R&D). The country is host to more than 300 research and development and innovation (R&D&I) centers of multinational companies. Of these, dozens are dedicated to cybersecurity.

It is no surprise that 40 percent of all private investment in cybersecurity worldwide takes place in Israel, which also has one of the world's largest private ecosystems in this area, second only to that of the United States. According to 2021 data, in that year US$8.8 billion were invested in around 131 Israeli companies from this sector, and more than 40 were acquired for a total of US$3.5 billion. Israel has more than 500 cybersecurity startups, and by 2021, 33 percent of the world's "unicorns" were Israeli. Overall, Israel's export of cybersecurity products was estimated in 2020 at US$6.85 billion.

The Israel National Cyber Directorate (INCD) is responsible for securing Israel's national cyberspace and for establishing and advancing its cyberresilience. The INCD operates at the national level to constantly raise the level of security of organizations and citizens, to prevent and manage cyberattacks, and to strengthen cyberemergency response capabilities. Its positioning as part of the Prime Minister's Office clearly demonstrates the centrality and importance of its responsibilities. Its goals include to prepare and enable the Israeli private sector and general public to protect themselves from cyberthreats by adopting cybersecure technologies, publishing best practices, training personnel, and raising awareness. Furthermore, it aims to establish and strengthen the cyberscience and -technology base by developing highly qualified human capital, supporting advanced academic research, engaging in deep technological R&D, and fostering the cyberindustry. The INCD strives to maintain a protected, safe, and open cyberspace for all of the State of Israel's population and businesses and to facilitate the country's growth and its scientific and industrial base.

The State of Cybersecurity in the Latin American and Caribbean Region

The Inter-American Development Bank (IDB) carries out periodic assessments to capture the evolving capacities of its member states to defend themselves against the growing threats in cyberspace. The 2020 Cybersecurity Report, "Risks, Progress, and the Way Forward in Latin America and the Caribbean," developed in partnership with the Organization of American States (OAS), showed that countries were at varying stages of development in their preparedness to face cybersecurity challenges, but generally still had ample room for improvement.

While in 2016, the year of the report's first edition, 80 percent of the countries in the region did not have a national cybersecurity strategy in place, this number had only fallen to 60 percent by 2020. Furthermore, only a few countries manage the exposure of their critical infrastructure, such as their energy, healthcare, telecommunications, transportation, water supply, and financial sectors, to cyberattacks. As revealed by the 2020 report, only 7 countries of the 32 assessed had a critical infrastructure protection plan in place. This is one of the most worrisome findings of all, considering the catastrophic impact that attacks on these sectors could have not only on national economies, but on the lives of all their citizens.

In terms of countries' capacity to manage and respond to cybersecurity incidents, the same study found that 63 percent of countries had security incident response teams in place, such as computer emergency response teams (CERTs) or cybersecurity incident response teams (CSIRTs). However, of the 20 countries that did, only 3 had reached advanced maturity in their ability to coordinate such responses. In fact, 23 out of the 32 countries were still in an initial stage of maturity in this respect. This finding underscored the general need for countries to strengthen the capacity of their teams to effectively coordinate their responses to cyberincidents. Moreover, the report examined the availability of educational and training opportunities in cybersecurity and found that fewer than half of the countries in the region offered formal education in cybersecurity, such as postgraduate, master's, or technical degrees. Needless to say, having sufficient trained professionals is essential to design and implement the cybersecurity policies and measures that are necessary to ensure a country's resilience in the face of increasingly sophisticated and complex cyberattacks.

The Inter-American Development Bank's Support to Strengthen Cybersecurity Capacity in the Region

For the past few years, the IDB has actively supported the region in the development of cybersecurity capacity, the design and implementation of national-level cybersecurity policies, and the strengthening of cybersecurity capabilities in the sectors it helps develop. This support takes a number of forms. The IDB has provided financial assistance amounting to tens of millions of dollars to develop national cybersecurity capabilities through more than 15 public sector investment loan operations, as well as significant additional funding to ensure the cybersecurity of digital transformation investment projects.

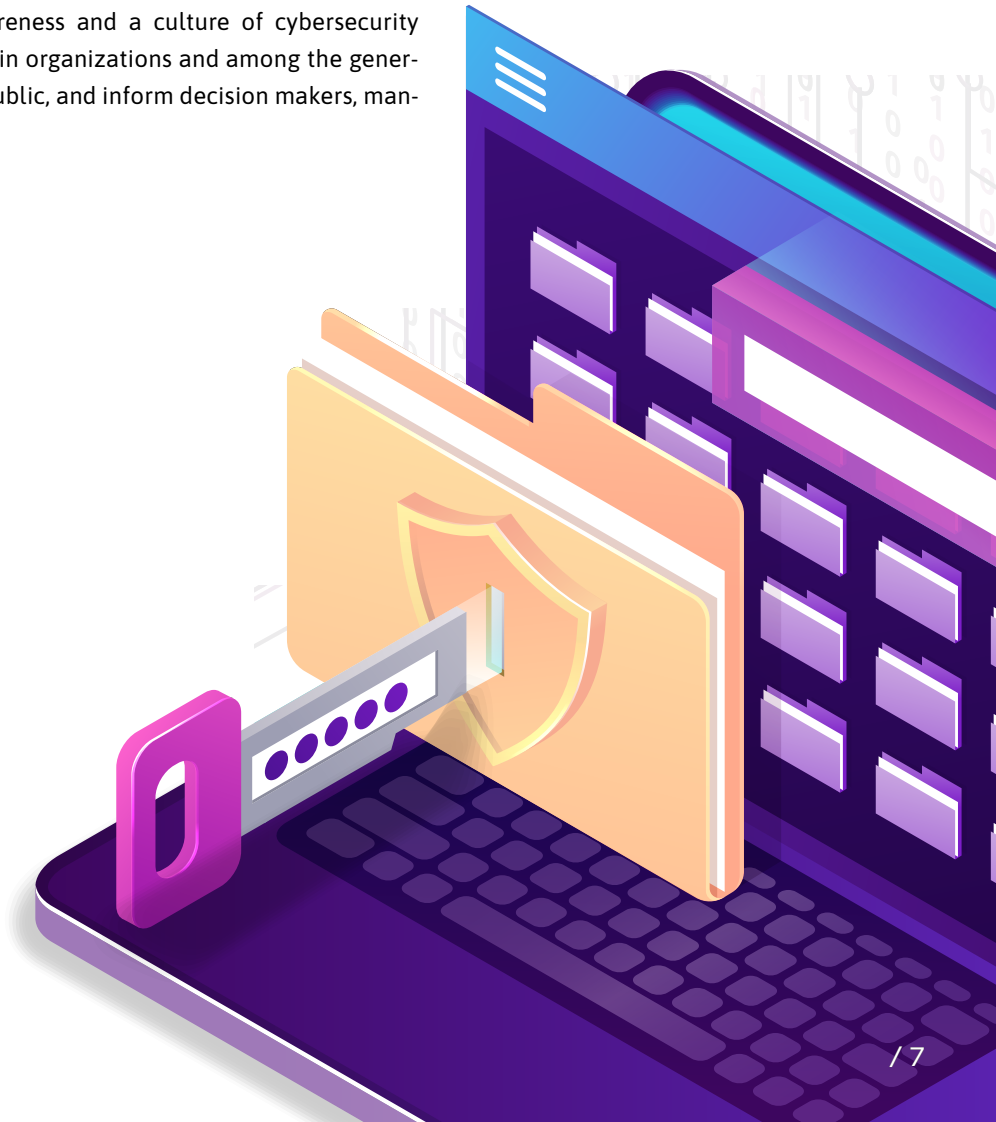
It also provides technical guidance and conducts cybersecurity projects across the region through consultancies, assessments, and tailor-made cybersecurity-strengthening projects on topics that include critical infrastructure protection, cybercrime and forensic analysis, design and strengthening of CSIRTs and security operations centers (SOCs), and national and sectoral cybersecurity strategies. In addition, the IDB has made substantial efforts to provide opportunities for Latin American and Caribbean professionals to strengthen and update their skills in this field by regularly offering workshops and training opportunities. These have included two-week cybersecurity executive courses, offered jointly with the Hebrew University of Jerusalem, as well as tailor-made courses on critical infrastructure protection and others targeted for specific sectors. Finally, the IDB has produced several high-impact publications dealing with national and sectoral cybersecurity issues, and continues to update and add to this body of knowledge regularly.[1]

1. See the website of the Data and Digital Government Cluster (DDG) of the IDB's Innovation in Citizen Services (ICS) division: **https://www.iadb.org/en/who-we-are/topics/modernization-state/data-and-digital-government**.

The IDB and the INCD: Joining Forces

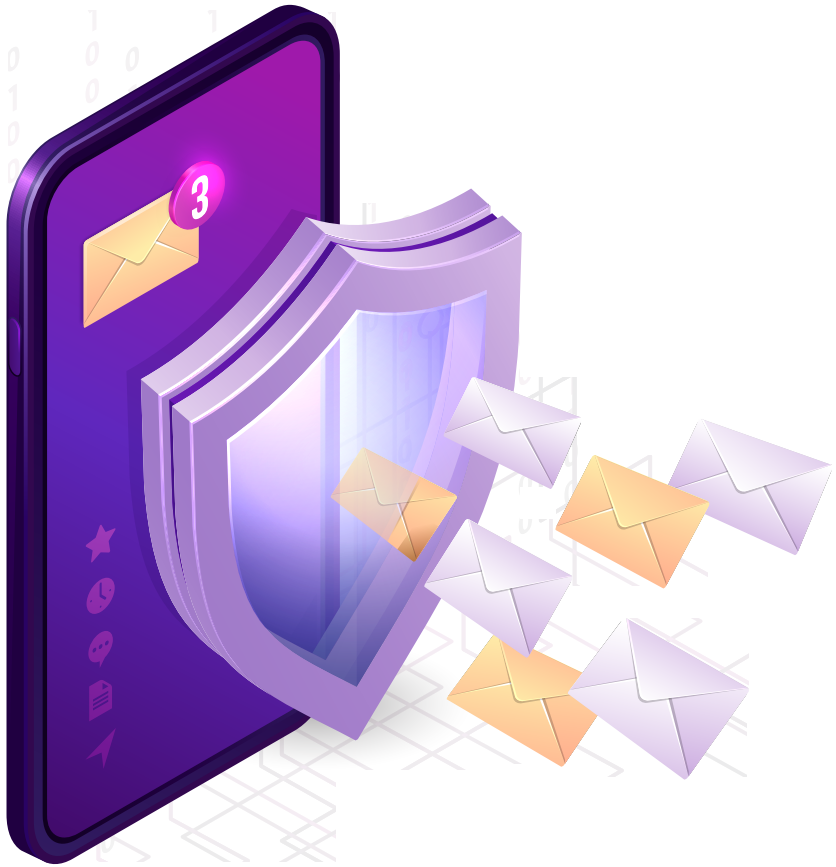
The challenges of cybersecurity, like those of the internet itself, are global. Thus, sharing the knowledge and tools to meet these challenges benefits everyone. In recognition of this reality, the INCD and the IDB have partnered to make Israel's expertise in this area accessible to LAC countries. This collaboration has supported the LAC region in the form of executive and technical trainings on advanced cybersecurity topics, cutting-edge conferences for LAC public officials and professionals in the field, and innovative technical assistance projects. This publication is a product of this collaboration. It consists of a series of cybersecurity methodological guides for organizations, developed by the INCD in light of its analysis of risks, attack methods, cyberincidents, and globally accepted standards. These guides have been translated into Spanish and English as a joint activity of both organizations. They are being made available in these languages with the aim of providing access to this body of knowledge to audiences throughout the LAC region and contributing to strengthening cyberresilience in the region.

The challenge of protecting the digital space will continue to grow, along with the need for proven expertise to confront it. The insights contained in these guides are a resource to promote much-needed professional training in cybersecurity in the LAC region. These guides will contribute to raise organizational standards, promote greater awareness and a culture of cybersecurity within organizations and among the general public, and inform decision makers, managers, and leaders in their cybersecurity initiatives. It is our hope that these guidelines will serve as a roadmap for professionals and leaders throughout the LAC region, working together to build a more secure and prosperous future.



/01. Goal

This document contains best practices for the distribution of commercial messages via SMS.



/02. Review of Major Threats

Distributing text messages to customers can expose both the sending organization and the recipient to a number of cyberrisks. These risks include the following:

01

Damage to the image of the sending organization as a result of an impersonation campaign that rides on the coattails of the legitimate sending organization to glean information or inject malware into end users.

02

Legal exposure of the sending organization as a result of actions that contravene legal and regulatory requirements such as the Spam Act, transfer of information between public bodies, privacy protection regulations, and others.

03

If the activity is carried out through a third-party SMS distribution service provider, the sending organization is exposed to cyberrisks that originate in the supply chain.[2]

2. For more information, see the document ***Supply Chain*** available within this "Cybersecurity Best Practices" collection through the following link: **https://www.gov.il/BlobFolder/generalpage/expsupplychain/en/Supply%20chain.pdf**.

04

Additional threats regarding means of identification. For more information, see the document ***Advanced Multi-Factor Authentication against Cybersecurity Threats***.[3]

Table 1 describes the main threats derived from distribution of commercial messages via SMS.

Table 1. Main Threats in the Distribution of Commercial Messages via SMS

No.	Type of Threat	Description
1	Sending an SMS impersonating a legitimate message from the organization (SMS phishing, aka "smishing")	Redirecting the user to a malicious site (watering hole attack) from which an attack tool is downloaded (drive-by attack) and activated on the user's mobile device.
2		Redirecting the user to a malicious site (watering hole attack) that impersonates the organization's legitimate website and requesting identification information or other sensitive/confidential information.
3		Asking the user to reply with an SMS containing sensitive/confidential information such as identification information for accessing an online service.
4		The link in the message contains malicious software/code that operates on the user's mobile device (sometimes even without the need for action on the part of the user).
5	Malicious takeover of the distribution system	A malicious entity takes over the distribution system, allowing it to spread malicious software/code transversely.
6		Sending an SMS containing malicious software/code to the distribution system interface, which may compromise the availability, confidentiality, or reliability of the information, including sending malicious messages out of the official distribution system.
7	Customer database leakage	Due to negligence in cybersecurity and/or protection of privacy on the part of the service provider that sends the message.
8		Due to malicious action on the part of the service provider that sends the message.
9		Due to malicious action by an employee (insider threat) of the service provider who sends the message.
10		Sending sensitive/confidential information to the wrong recipient due to a malfunction or human error.
11		Sending information in violation of the Spam Act/Communications Law/Privacy Protection Law or other law.

3. The document ***Advanced Multi-Factor Authentication against Cybersecurity Threats*** will be available in the future within this "Cybersecurity Best Practices" collection.

/03. Best Practices

First, a risk assessment process must be performed and a distinction must be made between the type and risk level of information that can be sent via a messaging distribution system that is considered unsecured as opposed to cases where it is required to act through a different distribution channel.

As part of the considerations, it is possible to examine, among other things, the information flow channel (whether it is one-way information from the distributor to the end customer, or two-way); whether the message is informative (such as an update on visiting hours or opening hours) as opposed to messages in which personal and customized information is sent to the customer; and whether the message includes a link to the site the user is required to enter and whether this site requires identification information or is open to everyone equally and does not require identification.

In general, distributing commercial messages via SMS is not a recommended practice in light of the risks to the organization and its customers arising from this implementation. However, in cases where the organization decides to use this technology, there are a number of protective measures that can be implemented to help reduce the risks. These include the following:

01

While distributing the message, present details on the subject on your organization's website. Update the website about a contact campaign running, add contact details and a way to ask questions, set up a call center, and ensure that it will be accessible to the public in terms of language, visibility, and awareness. Consider posting on social media about the existence of a customer contact campaign and how to check the authenticity of the sender.

02

Define an organizational policy of allowed and forbidden actions regarding text messages. Publish this policy on the organization's website. Such a policy can include short and clear sentences such as "Our representative will never ask you for your password, either by phone or by SMS" or "We never ask customers to provide credit information via SMS."

03

If the messaging system is intended to deliver sensitive/personal information, examine solutions for digitally signing the messages as well as provide end-to-end encryption of the information. Give preference to keeping the sensitive information on the server under your control, and to sending a link to the customer rather than sending a sensitive file to the customer's end device.

04

Consider having customers indicate their acknowledgement of the risks involved in receiving text messages and provide protection recommendations when signing (i.e., deleting sensitive information provided in text messages after being read, setting a password on the device to which the text messages are sent, using unique passwords for your organization, etc.).

05

Post contact information for the cybersecurity agent on the company's website in a clearly visible place so that customers can ask questions or report incidents or suspicious activity.

/04. Extended Recommendations

Table 2. List of Extended Recommendations

No.	Recommendation
	Characteristics of SMS Messages
1	Include informative information only in the SMS and do not include sensitive/ confidential data, links, multimedia messages (MMS), or attachments.
2	Attach a random ID to each message, valid for 72 hours after sending the SMS, which will allow the user to test the authenticity of the message on the organization's website. Do not direct the user to the organization's website via a hyperlink.
3	Verify that the telephone number used to send the SMS is fixed, fully owned by the organization, registered as an operator authorized by the Ministry of Communications, is only used to distribute text messages, and that it appears in the "sender" field.
4	Ensure that the contact details of the third-party SMS distribution service provider appear in each message, including the name and phone number of the service provider.
	Considerations when Choosing an SMS Distribution Service Provider
5	Prior to contracting, verify that the service provider (including its infrastructure and systems) meets the requirements of the ***Cyberdefense Methodology for an Organization*** (in its latest version).[4]
6	Prior to contracting, verify that the application programming interface (API) of the service provider meets the following requirements: • The development is done in accordance with accepted principles for secure development. • The identification process includes mutual authentication based on digital certificates (mutual transport layer security [mTLS]). Use of username and password, or pre-shared password, etc. does not meet this requirement. • API access is possible from internet protocol (IP) addresses defined according to the list of authorized users. • A security device is used to protect against cyberattacks (e.g., web application firewall [WAF]/runtime application self-protection [RASP]).

4. The document ***Cyberdefense Methodology for an Organization 2.0*** is available within this "Cybersecurity Best Practices" collection through the following link: **https://www.gov.il/BlobFolder/generalpage/cyber_security_methodology_2/en/ICDM%20V2.pdf**.

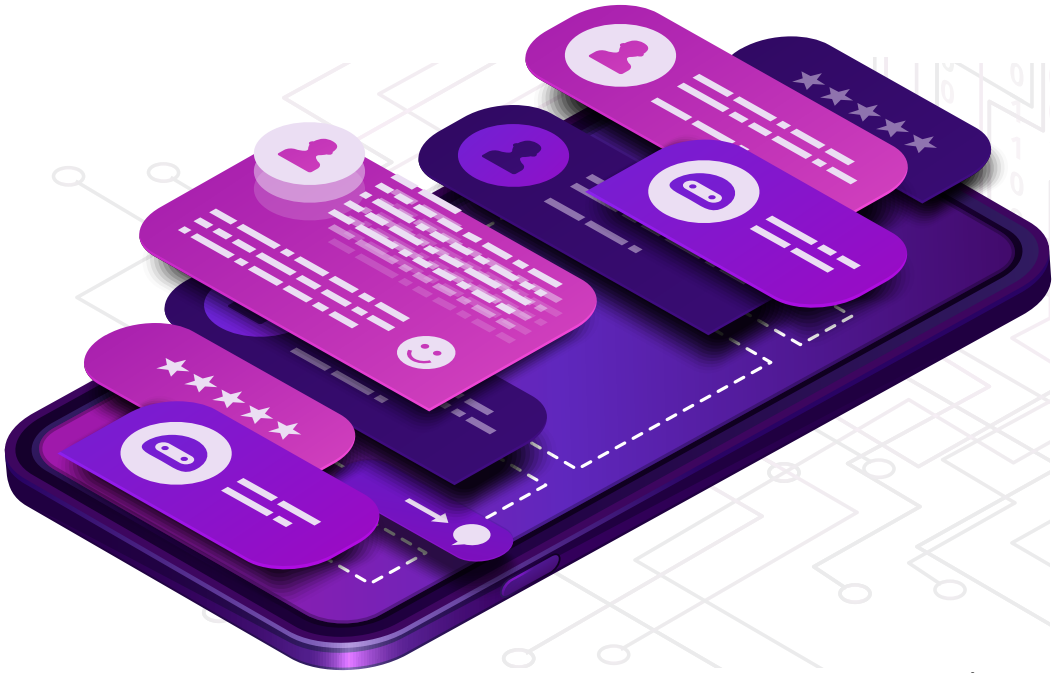
No.	Recommendation
	Considerations when Choosing an SMS Distribution Service Provider (cont.)
7	Prior to contracting, verify that the service provider complies with the following requirements: • All development is done in accordance with accepted principles for secure development. • The identification process of its employees includes the use of multi-factor authentication (MFA). This could be achieved by implementing/acquiring an enterprise MFA solution from a reputable organization such as Microsoft, Cisco, or similar. Using a temporary/fixed password plus an SMS password does not meet this requirement. • A security device is used to protect against cyberattacks (e.g., WAF/RASP).
8	Prior to contracting, verify that the service provider has not experienced a cyberincident and/or privacy protection incident in the last seven years.
9	Prior to contracting, verify that the service provider has an information and cybersecurity officer who is subordinate to the Chief Executive Officer (CEO) of the organization and has the experience, knowledge, and resources required to carry out their responsibilities.
10	Prior to contracting, perform resilience tests to examine the durability of the service provider's infrastructure and systems. If faults of medium grade or higher are found, do not engage with the supplier.
11	Sign a legal agreement with the service provider, approved by the organization's legal counsel, which will include reference to common issues such as: • Confidentiality agreement • Conflict of interest prevention • The supplier's obligation to meet the requirements of information protection and cybersecurity • The supplier's obligation not to misuse the information received from the organization • Proffering of compensation without the obligation to prove damage • The obligation to irreversibly delete the information immediately after distribution • The supplier's obligation to comply with legal and regulatory requirements

No.	Recommendation
	Securing the File Transfer Process between the Organization and the Service Provider
12	Ensure that the file transfer process between the organization and the provider meets the requirements of the document ***Securing Managed File Transfer (MFT)***.[5]
	Intra-Organizational Activities
13	Conduct a risk assessment at least once a year regarding the consequences of distributing commercial messages via SMS, including an examination of the effectiveness of protection controls.
14	Perform periodic resilience tests to examine the level of durability of the service provider's infrastructure and systems. If faults of medium grade or higher are found, cease engagement with the supplier.
15	Ensure that the information passed to the service provider is as limited as possible. For example, do not include information that is not required, such as residential address, last name, ID number, etc.
16	Perform random checks at the service provider's premises to ensure that the provider deleted the organization's information after distribution.

5. The document ***Securing Managed File Transfer (MFT)*** will be available in the future within this "Cybersecurity Best Practices" collection.

No.	Recommendation
Intra-Organizational Activities (cont.)	
17	Ensure that the cyberassets involved in the distribution process are not directly accessible on the internet. Alternatively, use virtual desktop infrastructure (VDI) or another solution for browsing.
18	Use accepted services for brand protection (digital risk protection, or DRP) to detect, identify, and thwart phishing activities in cyberspace.
19	Ensure that the organization itself meets the requirements of the ***Cyberdefense Methodology for an Organization*** (in its latest version, see link on p. 15 of this document).
20	Continuously monitor message distribution to the users, including failure rates, etc.
21	Require users to occasionally reconfirm the phone number used to receive text messages.
Support for Users/Customers	
22	To respond to user inquiries, the organization will maintain a 24/7 human support center, 365 days a year, subordinate to the organization's information and cybersecurity officer. Note that using the regular service center or a mechanized response is not an appropriate alternative.
23	Ensure that the support center operates in accordance with a work procedure that includes incidents and responses. At least once a year, examine the procedure to ensure that it is up to date and approved by the organization's management.
24	Publish, through the various service channels, instructions for users on how to address threats resulting from receiving malicious messages, including contact information for the support center.

No.	Recommendation
Support for Users/Customers (cont.)	
25	Issue a publication periodically to reinforce users' awareness of the type of information being sent and the nature of the service, including information on how to contact the support center.
26	Offer compensation without proof of damage to a user who was directly and/or indirectly harmed as a result of receiving a message from the organization.
27	Ensure that the user has access to a copy of the content of the SMS via an alternative service channel (such as an online site accessible after logging in), which includes sufficient parameters to demonstrate the authenticity of the SMS initially received, such as date, time, sender identity, and copy of the message.



Distributing commercial messages to customers via SMS can expose both the sending organization and the recipient to a number of cyberrisks. Among these risks, it is worth highlighting the damage to the image of the organization as a result of an impersonation campaign (phishing), the legal exposure as a result of actions that contravene legal and regulatory requirements for information transfer and privacy protection, and risks that originate in the supply chain.

As a result, the distribution of commercial messages via SMS is not a recommended practice in light of the risks to the organization and its customers. However, in cases where the organization decides to use this technology, there are a number of protective measures that can be implemented to help reduce the risks.

This document describes the main threats derived from distribution of commercial messages via SMS and, based on these, offers a series of implementation recommendations and best practices to help organizations improve their internal processes associated with the transmission of informative material via text messages and minimize the risks related to this practice.

Cyberspace is a field of opportunities in terms of technological progress, connectivity, integration, and global connection to the internet. But it is also a field of threats and risks. Cyberattacks can harm organizations and inflict significant financial and image damage. To be prepared to defend against cyberthreats, an organization must master a large number of specializations, whether they are technological, organizational, or process centered. The list of documents presented below reflects the state of the collection at the time of publication of this document.

Volume A: A methodological approach

Volume B: A technical approach

- **B.01** Securing Internet of Medical Things (IoMT) Components
- **B.02** Securing Access Point Name (APN) Infrastructure
- **B.03** Hardening Computer Systems
- **B.04** Reducing Cybersecurity Risks in Video Surveillance Cameras
- **B.05** Reducing Cybersecurity Risks at the Organization's Endpoints
- **B.06** Securing Enterprise Resource Planning (ERP) Systems
- **B.07** Preparation for and Response to a Ransomware Attack in the Organization
- **B.08** Reducing Cybersecurity Risks for Industrial Control Systems (ICS)
- **B.09** Cybersecurity Risk Survey Template for Industrial Control Systems (ICS)
- **B.10** Securing Voice over Internet Protocol (VoIP) Infrastructure
- **B.11** Advanced Multi-Factor Authentication against Cybersecurity Threats
- **B.12** Major Cybersecurity Threats of Remote User Support Platforms
- **B.13** Prevention of and Response to Border Gateway Protocol (BGP) Hijacking
- **B.14** Preparation for Distributed Denial-of-Service (DDoS) Attacks
- **B.15** Reducing Cybersecurity Risks in Building Management Systems (BMS)
- **B.16** Cybersecurity through Mobile Device Management (MDM/EMM) Systems
- **B.17** Securing Managed File Transfer (MFT)
- **B.18** Cybersecurity Aspects of Commercial Message Distribution (SMS)
- **B.19** The Israeli Cyber Emergency Response Team (CERT) Principles of Operation
- **B.20** Securing Multimedia Systems
- **B.21** Integrating Principles of Cybersecurity in the Backup and Recovery Processes

Volume C: Secure software development