Which?

SMS and Protecting Your Customers

1 Check SMS is right

2 Protect your SMS Sender ID

3 Be clear and consistent

4 Consider security in procurement

5 Avoid links if you can

6 Don’t use generic URL shorteners

7 Don’t include phone numbers

8 Consider tone and language

9 Be careful with personal information

10 Ask why you are messaging

SMS is a useful and effective business tool: 99% of SMS messages are read and 90% within three minutes[1], and SMS can be used to reach people who don't have a smartphone. However, ubiquity means scammers also favour SMS.

Which? has created this guide to help you protect your customers from scams. Build trust with your customers by creating a distinction between your genuine messages and fraudulent ones.

This guide assumes you are complying with data protection and privacy laws and already have express and continuing consent from your customers to send them marketing and functional SMS messages.

Here are our top 10 tips for using SMS

1 Make sure SMS is the right medium

SMS is not secure: genuine numbers can be spoofed, and the messages are not encrypted, so it's worth asking the following questions before you send a text:

. Can customers be sure it is from us?
. Do the messages include personal information?
. Will this message come as a surprise to a customer?
. Is there another way we could share this message, such as an email or a push notification from an app?

2 Protect your SMS Sender ID where possible

Large businesses and well-known brands should protect their SMS Sender IDs from being spoofed. You can do this by registering with the SMS SenderID Protection Registry run by the Mobile Ecosystem Forum.

Scammers will try to impersonate legitimate companies in smishing texts, but this scheme can help prevent scam messages landing in existing message threads. To help your customers recognise and trust your messages, clearly communicate which protected header you will use. This information should be easy for your customers to find and verify if they're uncertain about a message that has come through. Contact MEF to enquire about protecting your Sender ID through their SMS SenderID Protection Registry.

3 Be clear and consistent

Your customers should know what to expect from you. Consistency is key!

Limit how many SMS Sender IDs you use (ideally only one). Use clear language and be consistent in tone. Address your customers the same way in every message – this could be first name or title and last name, but be consistent.

4 Consider security in your SMS procurement processes

It's important to consider security as well as cost when procuring SMS services. Ask providers if they're signed up to MEF's Business SMS Code of Conduct and ask them what they're doing to protect your customers from scams and spam.

5 Avoid hyperlinks unless absolutely necessary

Scammers rely on people clicking on hyperlinks. If you can't avoid sending links in a text, make sure your customers know what you use links for - tell them you will only ever send a hyperlink to a delivery tracking page, for example.

An alternative to hyperlinks is directing customers to make their own way to the content on your website if that's where the link would lead. While some businesses can't avoid hyperlinks, others can and should avoid them - for example, banks. Tell your customers clearly what you do use links for, or be clear that you will never send a hyperlink in a text.

6 Use consistent and verifiable domain names, and don't use generic URL shorteners

There are some circumstances where businesses include links to improve the customer experience.

If you must include a link, it's important your customers can recognise it as a legitimate link associated with your brand. Avoid generic URL shorteners, like Bitly and TinyURL. If you need to shorten a link to fit it in the message, use a customised shortened URL (Bitly and TinyURL offer these too) and communicate what this will look like to your customers. Make it easy for customers to find and verify your domain names, so they can check the link is legitimate if they are uncertain.

7 Don’t include phone numbers

Scammers will sometimes include a phone number to encourage your customers to call them directly, so don’t include phone numbers.

Instead, if you need your customer to call you back, tell them to use a verified number. For example, banks could say ‘call back the number on the back of your card’. Other businesses could direct customers to their websites.

Do not invite customers to use a search engine - they could be at risk of fake helpline numbers and expensive referral services.

8 Consider the tone and language you use

Are you creating a sense of urgency or panic? Scammers rely on panicking their victims into responding quickly: your message should not scare your customers.

Is your message professional-sounding? Make sure your message is clearly written and consider building in a copy check before sending it.

9 Be careful with personal information

Scammers rarely address recipients by name, so where possible, you should do so, and tell your customers to be wary of any messages that don’t.

If you must include any other personal information, partially redact it so the customer will recognise it, but it will be of no use to anyone else who sees it or intercepts the message. For example, only include part of a postcode, or part of an account or card number.

10 Consider why you are messaging your customer

Is your message in response to customer activity (e.g. logging in online, or making a payment) or is it unsolicited?

If the message will come as a surprise, consider how the customer will recognise it as legitimate. Are you meeting all the other points in the guide to help with this?

Text messages should be sent within business hours where possible. Those sent outside of business hours should be driven by customer activity.

Glossary

. **Mobile Ecosystem Forum (MEF)** – a global trade body that acts as an impartial and authoritative champion for addressing issues affecting the broadening mobile ecosystem. Its goal is to accelerate the growth of a sustainable mobile ecosystem that drives inclusion for all and delivers trusted services that enrich the lives of consumers worldwide. MEF runs the SMS SenderID Protection Registry in the UK and has created the Trust in Enterprise Messaging programme, its cornerstone being the Business SMS Code of Conduct.

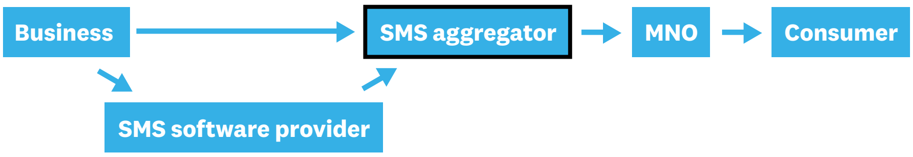
. **Push notifications** – a short, web-based, pop-up message or notification sent by an application to a user. These can be sent when the application is not open to get the user to engage with the app / the message.

. **Sender ID** – the name or number that a SMS text message appears to come from, also known as a message header. When a Sender ID is a name, rather than a number, it can also be known as an ‘Alpha Tag’ or an ‘Alphanumeric SenderID’.

. **Smishing** – a portmanteau of SMS and phishing. This is the fraudulent practice sending text messages pretending to be from well-known companies in order to get individuals to reveal personal information.

. **SMS** – stands for “Short Message Service”, which is the service used to send text messages to mobile phones.

. **SMS aggregators** – intermediary companies that sit between the businesses sending SMS messages [or the software provider they use] and the mobile network operators (MNOs). Text messages pass through the aggregators before reaching the MNOs’ networks and then the receiving consumer.



Business

SMS aggregator

MNO

Consumer

SMS software provider

. **SMS SenderID Protection Registry** - established as a blocking system for spoofed smishing text messages. Large businesses and well-known brands can register the Sender IDs or headers they use when sending text messages to their customers and the system limits the ability of fraudsters to impersonate a brand by checking whether the sender is the genuine registered party.

. **Spoofed /spoofing** - disguising a communication from an unknown source as being from a known, trusted source. In phone calls, scammers might spoof the number of a known company or organisation which is the number that then appears on your caller ID. In SMS, scammers try to spoof Sender IDs to look like the messages are coming from trusted companies.

[1] Mobilesquared (2010), Conversational Advertising, p.8: https://mobilesquared.co.uk/wp-content/uploads/2017/12/Conversational-Advertising.pdf

Which?

Organisations supporting this guide

Thanks to the organisations and businesses that have collaborated on the development of the guide, and to the following organisations for supporting this initiative:

CONSUMERS INTERNATIONAL

AICES International Express

Home towork

Mobile UK

MEF MOBILE ECOSYSTEM FORUM

proofpoint.

The Cyber Helpline
Supporting victims of cybercrime

TUFF Telecommunications UK Fraud Forum

Friends Against SCAMS

For more information on which businesses have agreed to adopt this guide or for information on adopting it yourself, go to which.co.uk/sms-guide