National Cyber Security Centre
a part of GCHQ

Business communications – SMS and telephone best practice

How to ensure your organisation's SMS and telephone messages are effective and trustworthy.

In this guidance:

This guidance will help you protect your customers from fraud by ensuring that your SMS and telephone messages are consistent, trustworthy, and reach your target audience without being blocked or deleted as suspicious.

Implementing this guidance will also make it harder for criminals to exploit telecoms channels. By minimising the complexity of any given service, it will help authorities to be more focussed and efficient in detecting and preventing fraud across telecoms networks.

> Note
>
> This guidance covers SMS and telephone messaging only. System administrators who want to secure their organisation's email systems should refer to the NCSC's guidance on email security and anti-spoofing. Information for consumers about spotting fraudlent messages can be found on the NCSC's report a scam call page.

The problem with telecoms

For many organisations, and particularly those that deal directly with the general public, SMS and telephone messages represent an extremely effective means of mass communication.

Unfortunately, the technology and systems that underpin mass communications cannot reliably tell the recipient who originated a phone call or SMS message. This means that cyber criminals are able to pose as legitimate organisations, mimicking their communications or concealing malicious links to enable fraudulent activity.

For these reasons, you should implement the guidance in this document, to make it easier for consumers to distinguish your official communications from attempted deception.

Creating trustworthy content

To be recognised as legitimate, it's crucial that all your content meets the standards expected of your organisation. Poor formatting, spelling mistakes and other inconsistencies not only damage your reputation, but are frequently associated with fake messaging.

You should also carefully consider the contact method you use for each communication.

When creating content, keep the following in mind:

- don't ask for personal details
- don't include links, if possible
- where it is absolutely necessary to include links, make sure they are human readable and easy to remember
- avoid language that induces panic or implies urgency (these are tactics often used by phishing attacks)
- be clear on how you will/won't communicate with your customers

Speak with a single voice

As a general rule, you should keep telephone numbers, email addresses, and SenderIDs to an absolute minimum and ensure your messaging is consistent. It is particularly important in larger organisations that all communications teams (including those involved in advertising) are aware of the emails and telephone numbers already in use.

Consistency has a number of benefits:

- if your messages come from a single source, it's easier for recipients to distinguish between legitimate and fraudulent messages
- fewer communication channels can be better protected, making them harder for criminals to abuse
- official sources can list these contact details definitively, so that they become well known
- your messages explaining the communications process will be more readily accepted (for example, describing the kind of information your organisation would never ask for)

Contact by SMS

SMS is a great way to communicate with people for the following reasons:

- **ubiquity** – the vast majority of mobile phones globally support the SMS protocol making it easy and cheap to develop services
- **familiarity** – people understand SMS messages
- **timely** – SMS messages generally get delivered, globally, within a few seconds
- **inexpensive** – relatively low cost to use
- **reliability** – the inherent reliability of SMS means people can 'send and forget'

  Careful consideration needs to be given to the purpose of your message, and the details that you present as the originator of your message, such as:

- **SenderIDs** (the text address that appears in place of the sending telephone number) are aimed at building trust in messaging, but are not supported globally. They are case sensitive and are only designed for one-way communication.
- **Shortcodes** are generally five-digit numbers that need to be provisioned on the individual mobile networks, but support two-way messaging.
- **Long dial/mobile numbers** can look like a message that's sent from one person to another (rather than from one organisation to thousands of people).

Due diligence regarding SMS suppliers

You should familiarise yourself with the NCSC's guidance on Protecting SMS messages used in critical business processes.

Before you start putting SMS services in place, ensure you know the answers to the following questions:

1. Do you plan to use SMS at all? If so, who is the SMS supplier, and what other organisations are in their supply chain?
2. Does the service need two-way communication?
3. What SenderID, if any, do you propose to use? **Note**: SenderID does not support two-way SMS, and is **not** supported in every country.
4. Are you planning to include links? **Note**: some countries are now preventing the use of links in messages.
5. Are you planning a bulk SMS campaign?
6. **Finally, is the message price lower than market rates or too low to be true**? If it is, the supplier may be using 'grey routes' or other routing techniques which can result in a customer data compromise and/or poor customer experience.

You should ensure your suppliers:

- are signed up to the A2P Code of Conduct
- are transparent and willing to share all of their downstream providers
- take an active part in the MEF Registry (a cross-sector trade body initiative that combats smishing and spoofing)
- provide data on the routing of the SMS (without this it is impossible to distinguish between legitimate and fraudulent SMS)

You should also make sure that suppliers are required to tell you when they change provider and give you adequate notice of this change. When using a shortcode, you should make sure that it is only used for your messaging purposes, and that you can port that number to another operator.

You should try to find a service provider who is as close to the mobile operators as possible. The more suppliers between you and the mobile operator, the more that can go wrong, including the loss or manipulation of customer data. It also becomes harder to investigate any problems.

If you cannot find details on the supplier's website which answer these questions, ask them directly. If they won't answer, these are grounds for concern.

SenderID considerations

Take care when selecting your SenderID. Ideally you should choose a SenderID that reflects your brand and avoid generic SenderIDs such as 'Alert' or 'NoReply'.

Note that it's difficult to differentiate between certain characters (for example the letter 'o' can look like the number zero '0'), especially on a small screen. This is often exploited by criminals who use 'similar looking' SenderIDs. It is worth noting that special characters (ie non-alphanumeric characters such as ! and *) can often result in strange behaviours, so you should avoid using them.

Unicode can be useful if you are communicating in other languages or when using emojis, but it can inflate the number of messages being sent.

SMS guidance

To summarise the key messages from this section:

- Understand your communications supply chain. Using fewer providers makes the whole process easier to manage.
- Audit your messages. Validate that the messages are received exactly as you sent them. Any changes to the content or message sender are indicators that your message provider is using grey routes, putting your messages at risk of fraud, delay, or even regulatory breach. The MEF Registry can also help you with auditing your supply chain.
- Include clauses in your contracts to cover full transparency of the supply chain and clauses enabling you to withhold money if fraud is suspected.
- Avoid using links in messages. Where this is absolutely necessary, we recommend using simple, human-readable links, such as gov.uk/coronavirus. You should not use URL shortening services. Note that some countries are now blocking links in messages.

- Ensure links are consistent in ALL messaging, making it easier for people to check them independently.
- Be careful when choosing a SenderID. Keep the number of SenderIDs to a minimum. Avoid special characters, and ensure the SenderID is added to the MEF Registry.

SMS and one time passcodes (OTP)

SMS is frequently used as part of multi-factor authentication (MFA) on websites. Criminals are using techniques to Artificially Inflate Traffic (AIT) leaving the website owner out of pocket. The NCSC has already published guidance on choosing the right type of authentication. Ideally you should offer different MFA options so the user can choose the one that best suits their needs.

You should:

- Establish whether SMS is the right solution. If it is, refer to section 3 above (Contact by SMS).
- Ensure your APIs for triggering SMS are **not** internet-facing (or publicly accessible) as these are often exploited by fraudsters.
- Ensure your website has input validation so that only a telephone number of the correct length and format is accepted.
- Restrict the number of retries a user/identifier can initiate in a given time. This can help protect against denial of service attacks and limit your fraud exposure.
- Consider whether you need to send messages internationally. If not, then do not send them. If you do, consider blocking high-rate countries and/or doing further non-SMS checks before registering the number.
- Do **not** send to unallocated numbers or virtual numbers. These are numbers that don't have a person at the other end, and are used by criminals to artificially inflate traffic. Your messaging provider should be able to help with this.
- Consider implementing business rules such as blocking multiple requests from the same IP address (or multiple requests for the same phone number from different IP addresses) and introduce rate limiting to help protect against attacks. Where possible, try to understand your historical message patterns for comparison. If there is a sudden spike, then it's likely to be an attack.
- Consider introducing technology to identify bots. This will help reduce your exposure to fraud or denial of service attacks.
- Monitor your conversion rates. If the messages you send do not result in an input by the user, work with your provider to understand why.
- Include fraud clauses in your contracts so that you can hold your message provider to account.

Contact by telephone

Spoofing a phone number is easy for criminals. They can make a call that began in New Zealand (and reached you via Fiji) look like a local call from a number you trust.

To detect this deception, phone companies rely on underlying data about the call, known as 'signalling details.' Unfortunately, these details are not always applied accurately by call centres. This makes detecting spoof calls very difficult.

In light of this, it is essential that official numbers:

- be kept to a minimum
- do not vary
- are well publicised

The work of preventing spoof calls can then be much more focussed and efficient.

You should also try to ensure that providers are not routing your UK-to-UK calls overseas. Fraudsters will often originate UK calls from outside the UK. Because of this, calls that have been routed overseas could be blocked, even if they are legitimate.

Due diligence regarding telephone services

Before you start putting services in place, ensure you know the answers to the following questions:

1. What type of number(s) are you looking to use? For example, shortcode, mobile, geographic, non-geographic, freephone?
2. Are all of the calls outbound-only, or do you want to accept some inbound calls?
3. Are you expecting to send or receive SMS? SenderIDs and some numbers cannot receive messages.
4. Who is/are the provider(s) of the Interactive Voice Response systems and/or call centres?
5. Which phone provider assigned the telephone number?

Telephone guidance

You should:

- Provide mechanisms for customers to establish contact. It's **always** better to allow the customer to initiate contact when providing personal information, as this significantly inhibits fraudsters. This could be achieved through a number of channels, including email, online, or inbound calls.

- Understand **who** is providing your telephony services and the call routes they are using. Having fewer providers makes it easier (for example) to ensure that your calls are **not** being routed overseas.

- Maintain consistency on numbers used for services.

- Any service that only receives calls should be added to the **Do Not Originate** list. This helps prevent the number from being used to make outbound calls. In order to deal with the limitations of this protective measure, you should also make it clear that your customers will never receive a legitimate call from this number. Please contact Ofcom about this at DNO@ofcom.org.uk.

- Check your provider is correctly identifying, or 'signalling' the numbers they use to make calls on your behalf. Ensure they are following the General Conditions.
- Request that your provider prevents your numbers from being moved (ported) to a different operator. In the UK, porting of numbers between operators (such as EE, Vodafone, BT and Three) is both quick and easy.
- Confirm that the routing does not go offshore. Many fraudulent calls originate outside the UK. Routing legitimate calls outside the UK and back (for a cost saving) makes it harder to protect your customer.

Help your customers (and authorities)

Implementing the following top tips will go a long way to help your customers identify legitimate messages. They also make it easier for the authorities to track and stop fraud on telecoms networks.

1. Keep messages simple and consistent.
2. Use minimal phone numbers, SenderIDs and email addresses.
3. Publicise your contact details (the numbers and email addresses, websites and SenderIDs).
4. Do **not** ask for personal details.
5. Use links sparingly and make them human readable.
6. Apply this guidance to your supply chain due-diligence.
7. Provide a way for your customers to independently check your communications.
8. Provide a means for your customers to contact you independently.
9. Provide guidance on how customers can report scams. If necessary, refer them to the NCSC's guidance on How to report a scam phone call.

Useful resources

OFCOM advice on tackling nuisance calls

NICC Requirements on Communications Providers in relation to Customer Line Identification

NICC Guidance on blocking of inbound international calls with UK Network Number as CLI (pdf file)

NCSC guidance on protecting SMS messages used in critical business processes

A2P Code Of Conduct (MEF)

Discussing SIM Farms and the data breach risk (MEF YouTube channel)

Business SMS, SIM Farms and the Data Protection Risk (MEF)

what is short codes.com?

SMS Best Practice: our guide for businesses (which?.co.uk)