FACT SHEET: SMS Scams

FACT SHEET

SMS Scams (text message/smishing) often appear legitimate, sometimes even showing in the same message stream as the real organisation as scammers can 'spoof' phone numbers. Banks, parcel deliveries, telcos or internet providers, Commonwealth government agencies, online retailers, streaming services, or gas and electricity providers are some of the favourite organisations that scammers impersonate in SMS scams. Their goal is to get you to click on a link and/or call a number in order to do any or all of the following:

1. Acquire your login details, such as username and password
2. Access you accounts
3. Take over your accounts
4. Steal your money
5. Download malicious applications and viruses to your device
6. Gain remote access to your device

Quick Facts

- Individuals are more likely to respond to a scam SMS if they have recently interacted with the legitimate organisation, are customers of that organisation, or are experiencing a difficulty with that service.
- IDCARE clients report a loss of around $2 million per year as a result of responding to SMS scams.
- For those clients who lost money, the average amount was $9854.

Prevention – How can I avoid SMS scams

- Don't click links within texts. Instead, contact the organisation directly using details you find independently of the text message, such as on their legitimate website.
- Download the legitimate app for the organisation – this will allow you to check and make communications, track parcels, and contact them securely.

Detection – Is this a scam?

It is always safest to assume that an SMS is a scam, and contact the legitimate organisation by phone, through their app, or in person. If the organisation asks you to login to your account, don't use the link provided in the message. Instead, open the app you have already downloaded or type in the web address that you know is correct for that organisation.

SMS scams are becoming increasingly sophisticated, with many using the exact wording that the real organisation uses in their text messages. You can no longer rely on spotting a fake SMS through spelling errors, grammar mistakes, or because they come from different phone numbers than usual.

Response – What do I do now?

I didn't click on the link, but I replied with a text message or called the number. What can someone do with the personal information I have provided?

Information such as name, address, and email address are credentials that alone would be considered low risk of direct financial fraud, however they will invite more phishing communication if obtained by a scammer. In most cases what is of real value to identity thieves is your credit or other payment card details, account username and password, and multi-factor authentication (MFA) codes. Identity thieves also target government issued credential information, such as driver licences, passports, myGov or RealMe login details, tax information, or Medicare card details.

What about my debit or credit card details?

If you have provided your debit or credit card details, contact your financial institution/s straight away to let them know that your personal details have been compromised and request additional security be placed on your accounts.

FACT SHEET: SMS Scams

FACT SHEET

Response – What do I do now?

I clicked the link but I didn't fill in any details

In some cases, clicking on the link has become enough for malware to be installed on some devices. Run your antivirus software on the affected device, and then disconnect your phone from the internet.

If you feel confident, you can try the following. Otherwise, ask your local IT service provider for help.

- Review your browser's privacy and security settings to make sure you're comfortable with what's checked or unchecked. For example, look to see if your browser is blocking third-party cookies, which can enable advertisers to track your online activities.
- Clear your browsers cache and cookies.
- Download the latest updates for your browser.
- Check plug-ins and extensions. If you find anything unusual, remove it straight away.
- Change all passwords that you have intentionally or perhaps unintentionally saved to the browser.
- Check for any recent downloads to your device that you do not recognise and remove.
- If you have backed-up your phone, install a backed-up version from before you received the SMS.

I clicked the link and filled in the details

- Disconnect your phone from the internet.
- Using a different phone, contact your banks to advise them and request additional security on your account.
- Contact the legitimate organisation and request additional security on your account and assistance with changing your login details and setting up multi-factor authentication.
- Run your antivirus software on your phone.
- Review your browser's privacy and security settings, as described above.

What else can I do to increase my phone's security?

Go through all applications on the device to detect any unknown programs. Remove them immediately.

- **Apple:** Using a different device, log into your Apple account/ID through the official Apple website. Check all personal information including the phone numbers and email addresses associated with the account are correct. Check all devices you are currently logged into and log out any unknown devices. We recommend periodically updating your Apple ID password and do not use the same password as other accounts. If you would like further support with your Apple devices, you can contact Apple on 1300 321 456.
- **Android/other:** Run antivirus software then update any relevant passwords (eg. Google Play/Gmail password). If your antivirus application allows, set it to update and run automatically.

My email account is receiving a lot of spam now

Some people affected by these types of scams have received emails indicating that they have been signed up to online marketing, such as from dating sites and movie sites. If you do receive an email suggesting this, it is best not to click 'Unsubscribe' and rather block the sender. You may choose to do your own research and contact the relevant company directly to request removal from their marketing communications.

*__Please note:__ This information is generalised to support individuals in most situations. However, depending upon your experience, capabilities and the device(s) you use, seeking professional support may be advisable. IDCARE's recommended steps for an individual concerned about their identification is based upon the information provided by you. A generic template is not able to appropriately address every individual's situation and some events may require additional steps.

****If at any time during the scam you were asked to provide your driver licence, Medicare, passport, tax file number, IRD number, banking or other online account details, or to give remote access to your device, contact IDCARE through our Get Help form.**