Education information about Scam Calls, SMS and other communications

Scammers use numerous methods to impersonate legitimate businesses to obtain personal and private information. They will often claim to be from the Government or organisations you're likely to know. The purpose of this document is to provide our customers information on:

- The types of scam calls and scam SMS related fraud risks to which you may be exposed:
- How to identify scam calls
- How to identify scam SMS and emails
- How to identify Scam Websites
- The steps to take to mitigate fraud risks from scam communications.
- Products or services to assist in blocking suspicious or unwanted scam communications.
- What to do if you have received scam communications

What are the types of scam communication related fraud risks

- Financial loss
- Identity take-over

How to identify scam calls

Here are some signs that a call may be fraudulent:

- Calls from people impersonating employees from well-known organisations, such as the Government, or familiar companies asking for your information
- Calls seeking financial details, such as your credit card or banking details, in order to process a refund or other 'overpayment' which you are not aware of or have not requested
- Calls seeking to access your computer remotely
- Some guidelines to follow:
- Do not give out any personal details if you are unsure of the caller and hang-up.
- Don't respond to missed calls that come from numbers you don't recognise. Calling back may result in instant charges in excess of $20.
- Be careful of phone numbers beginning with "19". These are charged at a premium rate and can be expensive.
- Be careful of being tricked into calling expensive international phone numbers.

How to identify scam SMS or email:

Here are some signs that a SMS or email may be fraudulent:

- It is from an unknown, unidentifiable or unverified sender
- An unexpected SMS messages asking for your personal or financial details
- SMS and MMS numbers that start with 19xx. These are charged at a premium rate and can be expensive. Also look out for numbers that start with an international country code other than +61, which is Australia’s country code
- Messages promising unexpected prizes that require you to send money to claim them
- Texts that encourage you to click a link or which may then ask you to install a piece of software on your mobile phone or tablet. Just like computers, malicious software can put your phone and personal information at risk.
- Unaddressed or generically addressed emails, such as “Dear Customer”.
- Badly written emails with broken sentences, spelling mistakes, grammatical errors and words in a foreign language
- Suspicious looking URLs
- Emails that include a zip file, an .exe or other suspicious attachment
- Emails that display account information that doesn't match your account details
- Requests for your credit card, passwords, account details or personal information either by replying to the email, or by asking you to ‘click a link’ and fill in a web form.

Some guidelines to follow:

- Don’t reply to the SMS or email
- Don’t provide any personal details
- Don’t click on any links
- Don’t open any attachments
- Don’t call any numbers associated with the SMS or email

How to identify Scam Websites:

Scam websites can be difficult to spot. If you come across a website that you suspect is fraudulent, here are some guidelines to assist in detecting if it could be a scam and what to do:

- Look out for incorrect spelling and grammar, and poor layout, imagery and styling
- If you accidentally click on a link which opens a website, don't enter any information into the website
- Don’t call any numbers associated with the website
- Don’t click on any links
- Products or services to assist in Blocking suspicious or unwanted Scam Calls and Scam SMS

- Use ad blockers, spam protection and other content filters to help block potentially malicious items.
- Consider enabling call screening and protection software which may be available in your mobile phone's operating system.
- The steps to take to mitigate fraud risks from scam communications
- The best way to protect yourself is through awareness and education. You can find out more information at https://www.accc.gov.au/publications/the-little-black-book-of-scams .

What to do if you have received scam calls and scam SMS

If you suspect it’s a scam call, SMS, email or website, please don't give away any personal details or access direct links . Block the suspected spam number and report to Scamwatch:
https://www.scamwatch.gov.au/report-a-scam

If you’ve shared other personally sensitive information, such as your driver’s licence number, Medicare, passport or contact details (e.g. your phone number or address), then you may want to visit IDCare at https://www.idcare.org – they can help you formulate a response plan to address potential identity theft.

Consider filing a report at https://www.acorn.gov.au . This will assist law enforcement become better resourced to provide assistance to victims. Additionally,

Stay calm. As frustrating as it is to learn that you may be at risk, keeping focussed and calm will help you manage your response properly.

Think carefully about what information, or access, you may have provided to criminals. Take an inventory and write down what you remember sharing or entering into the fraudulent website.

If you provided any banking or other financial details such as a credit card number, contact your financial institution immediately. Be sure to monitor your accounts closely in the future as well.

If you provided any usernames or passwords, immediately change your passwords to a new and secure version.

To report a suspected scam to GSIM, please contact us at support@gsim.au .