Scam Calls and SMS and Staying Safe Online

(Last updated July 2022)

With so much of your personal information contained online, and so many daily transactions being conducted online, it is important to take steps to protect your information. At Cmobile, we are committed to ensuring that your information is protected and secure, and we are likewise committed to assisting you to defend yourself against cyber threats and attacks and scam calls and SMS.

According to data from Scamwatch, Australians lost more than $205 million to scams between 1 January and 1 May 2022. This represents an increase of 166% compared to the same period in 2021. The unfortunate reality is that if you own a mobile phone and you send or receive SMS, you are at risk, and the risk is increasing. The ever-increasing sophistication of scammers is therefore a key issue faced by Cmobile and other telecommunications providers.

Types of scams

Scams can take many forms from dating and romance scams where scammers pretend to be looking for love to elicit the sending of money, to links seemingly from Australian Post about the delivery of a parcel, to unexpected money scams. For more details on scams, please visit Types of scams | Scamwatch.

Scammers will attempt to contact you via many different means including calling you or sending you an SMS or email. It is almost impossible to say how scammers acquire your number or email address given the amount of transactions conducted online, however there are a number of steps you can take to protect yourself online.

- ***Use strong passwords and PINs*** for all of your accounts and devices. Never use a password or PIN that could be easy to guess such as your date of birth, 1234 or 0000, your child or pet's name of even a combination of these, and do not use the same password or PIN for all accounts. Consider using a password manager (such as 1Password) where complex passwords can be easily created and securely stored so you won't have to remember them all.
- ***Lock your device with a secure PIN*** and update it regularly.
- ***Be suspicious*** of all communications from parties you do not recognise. Do not click on links or open attachments in an SMS or email unless you trust the sender and are expecting the communication. Even where you know the sender, check the email address looks correct. Do not respond to missed calls or SMS from numbers you do not recognise.
- ***Allow unknown calls go to voicemail.*** Generally, scammers will not leave a voicemail. If a voicemail is left, you can ascertain then if it's a genuine call.
- ***Block suspicious or unknown numbers***. Most devices will allow you to easily block a number. Please contact us if you need assistance with this.
- ***Do not provide information*** to people calling you unless you are sure they are who they say they are. If someone calls you and claims to be from your bank, Cmobile, your energy provider or any other organisation and they request information, consider calling that provider back on their main customer service number so you can be sure the call originated from them.

- ***Do not allow remote access to your device.*** This is a very common scam. Providing a scammer with access to your device is like providing a thief with the keys to your house. Never allow this no matter what the person calling says to you.
- ***Install security software on all your devices and apply the latest updates.*** Protect your devices by using security software (such as McAfee) and ensure latest iOS and Android updates are applied to your device.
- ***Limit the sharing of information online.*** Unless your social media accounts are set to private, everyone can see everything you post online. Strongly consider how much information you share online, particularly your date of birth, the area you live in, when you are away on holidays and what information can be gleaned from photographs (for example, a photo of your child in their school uniform can tell someone where your children go to school and therefore the area in which you live).
- ***Be mindful that your friends and family could have their social media accounts hacked.*** Be careful clicking on links seemingly from friends or family members sent via social media. Scammers who have hacked a social media account will often contact people on the friends' list and send out malicious links with messages urging you to click (such as "hey, I think this is you on this video"). Do not click the link.
- ***Never provide codes to anyone.*** If you are sent a code via sms or email to access your accounts, never share that code with anyone.
- ***Use secure Wi-Fi.*** Always be careful about what information you share over a public wi-fi network as hackers can easily intercept this information.

What you can do if you have received scam calls or SMS

There are a number of actions you can take to report scam calls or SMS:

1. Report the call to us at scamreport@cmobile.com.au or on 1300 545 000. Provide details of the number(s) that called you and the date and time and any information that was provided to you by the caller.
2. Report the scam to www.scamwatch.gov.au.
3. Block the number on your device.

What to do if you have lost money or personal information to a scammer

Contact your financial institution immediately. They may be able to assist you in retrieving the funds. They will also be able to assist you to further protect your accounts. Also consider a fraud monitoring service where your personal information has been stolen.

Cyber Threats

Like scams, cyber threats take a number of different forms and below we explain the most common ones.

- ***Phishing***. Phishing is the practice of sending emails which appear to come from reputable companies you trust in order to induce you to reveal personal information such as passwords or credit card information, or to open a malicious attachment.
- ***Malware***. Malware is usually delivered to you via a link or in a file that is sent to you via email and is activated once you click on the link or open the file. Malware is malicious software used by hackers to gain unauthorised access to your computer where they can then gain access to passwords, bank and service provider logins.

- ***Identity theft***. Identity theft occurs when a hacker obtains your personal information and uses it to create identity documents, either fake ones or by applying for real ones. Once they have done this, they can use your identity to apply for loans and make expensive purchases online in your name.
- ***Hacking and data breaches***. All apps and websites are at risk of hacking as cyber criminals are always trying to exploit vulnerabilities. If you have ever had your credit card details stolen, it is very likely it is the result of cyber hacking. When a website is hacked, the goal is generally to harvest customer credit card numbers and personal information. Regularly check your credit and debit card statements for any unusual charges and report them to your bank immediately.

Where you can find more information about consumer scams

The following sites all provide awareness training materials on consumer scams:

Home | Scamwatch

ACSC Homepage | Cyber.gov.au

Scams and online misinformation | ACMA

The little black book of scams | ACCC