



## ระวางการหลอกหลวงหรือสแกม

คนหลอกหลวงหรือสแกมเมอร์มักจะเสแสร้งว่ามาจากองค์กรที่ไวใจได้ เช่น Services Australia

พวกเขาอาจหลอกคุณให้ให้เงินหรือข้อมูลเป็นค่าตอบแทนการจ่ายเงิน บริการและความช่วยเหลือ

หากสแกมเมอร์ได้รับข้อมูลของคุณไปแล้ว พวกเขาจะสามารถ:

- เข้าถึงบัญชีธนาคารของคุณและโอนเงินไปจากบัญชี
- ใช้ชื่อคุณทำสัญญาติดตั้งโทรศัพท์หรือสัญญาอื่น ๆ
- ขโมยเงินบำนาญบ้านของคุณ
- เข้าถึงบัญชีอีเมลและโซเชียลมีเดียของคุณ
- เสแสร้งว่าเป็นคุณ

หากคุณสูญเสียเงินเนื่องจากการหลอกหลวง คุณอาจไม่ได้เงินนั้นคืน

## ข้อมูลที่สแกมเมอร์ต้องการ

สแกมเมอร์อาจพยายามที่จะได้ข้อมูลต่อไปนี้ของคุณ:

- ชื่อและนามสกุล
- วันเดือนปีเกิด
- ที่อยู่
- รายละเอียดบัตร Medicare
- Centrelink Customer Reference Number (CRN)
- เอกสารยืนยันตัวตน
- รายละเอียดการลงชื่อเข้าใช้ myGov หรือรหัสเชื่อมต่อ
- รายละเอียดบัญชีธนาคาร
- รหัสผ่านต่าง ๆ

## วิธีป้องกันตัวเอง

เพื่อป้องกันข้อมูลของคุณ:

- รู้วิธีระงับการหลอกหลวง
- ระวังตัวเมื่อมีคนติดต่อคุณมาโดยที่คุณไม่คาดหวัง โดยเฉพาะอย่างยิ่ง หากพวกเขามีกำหนดเวลาเร่งด่วน
- อย่าบอกรหัสเชื่อมต่อ รหัสผ่านหรือคำตอบของคุณสำหรับคำถามลับเด็ดขาด
- อย่าให้ผู้อื่นใช้หรือเห็น myGov ของคุณหรือบัญชีออนไลน์อื่น ๆ
- ใช้รหัสผ่านที่คุณจดจำได้ง่าย แต่ยากสำหรับคนอื่นที่จะเดา
- ป้องกันอุปกรณ์มือถือของคุณด้วยการปิดล็อกมันเมื่อคุณไม่ได้กำลังใช้มันอยู่
- ป้องกันจดหมายทางไปรษณีย์ของคุณด้วยการติดกุญแจตู้จดหมาย และส่งต่อจดหมายของคุณไปที่อื่นหากย้ายที่อยู่

## วิธีบอกว่ำนั่นคือสแกมหรือไม่

คุณสามารถระบุสแกมด้วยการทราบว่าเราทำอะไรและเราไม่ทำอะไร

### สิ่งที่เราทำ

เราอาจส่งอีเมลหรือข้อความสั้น ๆ ถึงคุณ ข้อความของเราจะไม่มีชื่อหรือรายละเอียดสำหรับการติดต่อของคุณ แต่อาจจะ:

- ขอให้คุณจองหรือเตือนคุณเกี่ยวกับการนัดของคุณ
- บอกให้คุณทราบเกี่ยวกับการจ่ายเงินของคุณ
- ยืนยันเมื่อคุณเปลี่ยนแปลงรายละเอียดเกี่ยวกับตัวคุณแล้ว
- บอกคุณว่าคุณมีข้อความใหม่ในกล่องจดหมาย myGov ของคุณ

หากคุณเป็นหนี้เงินเรา เราจะส่งจดหมายถึงคุณ

เราอาจจะโทรศัพท์หาคุณ แต่ต้องระวังหากคุณไม่ได้กำลังคาดหวังโทรศัพท์จากเรา คุณควรขอชื่อและรายละเอียดสำหรับการติดต่อของผู้ที่โทรมา หาก你不คิดว่าผู้ที่โทรมาคือเรา ให้วางสายแล้วโทรกลับไปที่หนึ่งในหมายเลขการจ่ายเงินของเรา

### สิ่งที่เราไม่ทำ

เราจะไม่มีวันขอให้คุณ:

- บอกรหัสของคุณหรือ Personal Identification Number (PIN) แก่เรา
- จ่ายเงินเราให้ช่วยเหลือคุณ
- ส่งหรือโอนเงินให้เราเพื่อให้คุณได้รับการจ่ายเงิน
- ชื่อบัตรของชวีญหรือบัตรกำนัล
- คลิกหรือเชื่อมต่อหรือเปิดเอกสารแนบในอีเมลหรือข้อความ
- ให้รายละเอียดส่วนตัวบนโซเชียลมีเดียของคุณ เช่น Facebook หรือ Twitter
- ให้เราเข้าถึงคอมพิวเตอร์หรืออุปกรณ์ส่วนตัวของคุณ

นอกจากนั้น เราไม่ทำงานร่วมกับบริษัทอื่น ๆ ที่จะให้ข้อเสนอพิเศษแก่คุณด้วย

## จะอย่างไรหากคุณถูกสแกม

หากคุณสูญเสียเงินหรือให้ข้อมูลส่วนตัวของคุณไปแล้ว คุณควร:

- เก็บบันทึกรายการที่ได้เกิดขึ้น
- โทรศัพท์ถึง Scams and Identity Theft Helpdesk ของเราทันทีที่หมายเลข **1800 941 126** แจ้งให้เราทราบหากคุณต้องการล่ามและเราจะจัดล่ามให้คุณโดยไม่เสียค่าใช้จ่าย
- รายงานเหตุการณ์เป็นภาษาอังกฤษ [scamwatch.gov.au](http://scamwatch.gov.au)

## จะหาข้อมูลเพิ่มเติมได้ที่ไหน

- โทร **131 202** เพื่อพูดคุยกับเราเป็นภาษาของคุณเกี่ยวกับการจ่ายเงินอุดหนุนรายได้และบริการต่าง ๆ จาก Centrelink

- โทรถึง Translating and Interpreting Service (TIS National) ที่หมายเลข **131 450** เพื่อที่จะพูดกับเรา เป็นภาษาของคุณเกี่ยวกับการรับเงินจาก Medicare และ Child Support และบริการต่าง ๆ
- ไปที่ **servicesaustralia.gov.au/yourlanguage** เพื่ออ่าน ฟังหรือดูข้อมูลเป็นภาษาของคุณ
- ไปที่ **servicesaustralia.gov.au/scams** สำหรับข้อมูลเป็นภาษาอังกฤษ
- มาที่ศูนย์บริการของเรา

หมายเหตุ: การโทรศัพท์จากโทรศัพท์บ้านของคุณไปหมายเลข '13' จากที่ไหน ๆ ในออสเตรเลีย มีค่าโทรในอัตราคงที่ ซึ่งอาจแตกต่างจากค่าโทรศัพท์ส่วนท้องถิ่น และอาจแตกต่างกันระหว่างผู้ให้บริการโทรศัพท์ ไม่มีค่าใช้จ่ายสำหรับการโทรศัพท์ถึงหมายเลข '1800' จากโทรศัพท์บ้านของคุณ ส่วนการโทรศัพท์จากตู้สาธารณะ และจากมือถืออาจจะถูกจับเวลาและมีค่าใช้จ่ายในอัตราสูงกว่า

### คำสงวนสิทธิ์

ข้อมูลที่อยู่ในสิ่งพิมพ์ฉบับนี้ตั้งใจจะใช้เป็นเพียงคู่มือการจ่ายเงินและบริการต่าง ๆ เท่านั้น เป็นความรับผิดชอบของคุณที่จะตัดสินใจว่าคุณต้องการยื่นคำร้องขอรับเงินและยื่นคำร้องเกี่ยวกับสถานการณ์เฉพาะของคุณหรือไม่



## Beware of scams

Scammers often pretend to be from trusted organisations, like Services Australia.

They may trick you into giving away money or information in return for payments, services and help.

If a scammer gets your information, they can:

- access your bank account and transfer money from it
- use your name to set up a phone plan and other contracts
- steal your superannuation
- access your email and social media accounts
- pretend to be you.

**If you lose money because of a scam, you may not get it back.**

## Information scammers want

Scammers may try to get your:

- full name
- date of birth
- address
- Medicare card details
- Centrelink Customer Reference Number (CRN)
- identity documents
- myGov sign in details or linking codes
- bank details
- passwords.

## How to protect yourself

To protect your information:

- know how to identify a scam
- be careful when someone unexpectedly contacts you, especially if they have an urgent deadline
- never tell anyone your linking codes, passwords or answers to your secret questions
- do not let others use or see your myGov, or other online accounts
- use a password that is easy for you to remember, but hard for others to guess
- protect your mobile device by locking it when you are not using it
- secure your mail by having a lock on your letterbox and redirecting your mail if you move.

## How to tell if it is a scam

You can identify a scam by knowing what we do and what we do not do.

### Things we do

We may send you an email or text message. Our messages will not include your name or contact details, but may:

- ask you to book, or remind you about, an appointment
- tell you about your payments
- confirm when you have changed your details
- tell you if you have a new message in your myGov Inbox.

If you owe us money, we will send you a letter.

We may call you, but be careful if you are not expecting a phone call from us. You should ask for the caller's name and contact details. If you do not think the caller is us, hang up and call back on one of our payment lines.

### Things we do not do

We will **never** ask you to:

- tell us your password or Personal Identification Number (PIN)
- pay us to help you
- send or transfer money to us to get a payment
- buy gift cards or vouchers
- click on links or open attachments in emails or text messages
- give us your personal details on social media, like Facebook or Twitter
- give us access to your computer or personal devices.

We also do not work with other companies to give you special deals.

## What to do if you have been scammed

If you have lost money or given away personal information, you should:

- keep a record of what happened
- call our Scams and Identity Theft Helpdesk straight away on **1800 941 126**. Let us know if you need an interpreter and we will arrange one for free.
- report the incident in English at [scamwatch.gov.au](https://www.scamwatch.gov.au)

## Where to get more information

- call **131 202** to speak with us in your language about Centrelink payments and services
- call the Translating and Interpreting Service (TIS National) on **131 450** to speak with us in your language about Medicare and Child Support payments and services

- go to [servicesaustralia.gov.au/yourlanguage](https://servicesaustralia.gov.au/yourlanguage) where you can read, listen to or watch information in your language
- go to [servicesaustralia.gov.au/scams](https://servicesaustralia.gov.au/scams) for more information in English
- visit a service centre.

Note: calls from your home phone to '13' numbers from anywhere in Australia are charged at a fixed rate. That rate may vary from the price of a local call and may also vary between telephone service providers. Calls to '1800' numbers from your home phone are free. Calls from public and mobile phones may be timed and charged at a higher rate.

## **Disclaimer**

The information contained in this publication is intended only as a guide to payments and services. It's your responsibility to decide if you wish to apply for a payment and to make an application with regard to your particular circumstances.