Australian Government
Services Australia

ARABIC

حذار من الاحتيال

غالباً ما يتظاهر المحتالون بأنهم من مؤسسات موثوق بها، مثل Services Australia.

قد يخدعونك للتبرع بالمال أو لمعلومات مقابل مدفوعات وخدمات و مساعدة.

إذا حصل المحتال على معلوماتك، فيمكنه:

- الدخول إلى حسابك المصرفي وتحويل الأموال منه
- استخدام اسمك لإعداد خطة للهاتف وعقود أخرى
- سرقة معاشك التقاعدي
- الوصول إلى البريد الإلكتروني وحسابات وسائل التواصل الاجتماعي
- التظاهر بأنك أنت.

إذا خسرت المال بسبب عملية احتيال، فقد لا تسترده.

يريد محتالو المعلومات

قد يحاول المحتالون الحصول على معلومات تخصك:

- الاسم الكامل
- تاريخ الولادة
- العنوان
- تفاصيل بطاقة Medicare
- Centrelink Customer Reference Number (CRN)
- وثائق اثبات الهوية
- تفاصيل تسجيل الدخول إلى myGov أو رموز الربط
- تفاصيل البنك
- كلمات السر.

كيف تحمي نفسك

لحماية معلوماتك:

- إعرف كيف تتعرف على عملية احتيال
- كن حذراً عندما يتصل بك شخص ما بشكل غير متوقع، خاصة إذا كان استعجلوا مدة التحدث معك
- لا تخبر أي شخص مطلقاً برموز الربط أو كلمات المرور أو الإجابات على أسئلتك السرية
- لا تدع الآخرين أن يستخدموا أو يطلعوا على حسابات myGov أو حسابات أخرى على الإنترنت
- استخدم كلمة مرور من السهل عليك تذكرها، ولكن يصعب على الآخرين تخمينها
- احمي جهازك المحمول بقفله عند عدم استخدامه
- قم بتأمين بريدك عن طريق وضع قفل على صندوق الرسائل الخاص بك وإعادة توجيه بريدك إذا قمت بالانتقال الى بيت آخر.

كيف تتحقق مما إذا كان هناك عملية احتيال

يمكنك تحديد عملية الاحتيال من خلال معرفة ما الذي نقوم به وما الذي لا نفعله.

أشياء نفعلها

قد نرسل لك بريداً إلكترونياً أو رسالة نصية. لن تتضمن رسائلنا اسمك أو تفاصيل الاتصال بك، ولكن قد:

- نطلب منك حجز موعد أو تذكيرك به
- نخبرك عن مدفوعاتك
- نؤكد متى قمت بتغيير التفاصيل الخاصة بك
- نخبرك إذا كان لديك رسالة جديدة في صندوق الوارد الخاص بك في myGov.

إذا كنت مديناً لنا بالمال، فسنرسل لك خطاباً.

قد نتصل بك، ولكن كن حذراً إذا كنت لا تتوقع مكالمة هاتفية منا. يجب أن تسأل عن اسم المتصل وتفاصيل الاتصال. إذا كنت لا تعتقد أن المتصل هو نحن، فقم بإنهاء المكالمة ومعاودة الاتصال بأحد خطوط الدفعات الخاصة بنا.

أشياء لا نفعلها

لن نطلب منك أبداً:

- إخبارنا بكلمة المرور أو Personal Identification Number (PIN)
- أن تدفع لنا لمساعدتك
- إرسال أو تحويل الأموال إلينا للحصول على دفعة
- شراء بطاقات الهدايا أو القسائم
- أن تنقر على الروابط أو تفتح المرفقات في رسائل البريد الإلكتروني أو الرسائل النصية
- تقديم بياناتك الشخصية لنا على وسائل التواصل الاجتماعي مثل Facebook أوTwitter
- تعطينا الاذن باستعمال جهاز الكمبيوتر الخاص بك أو أجهزتك الشخصية.

كما أننا لا نعمل مع شركات أخرى لنعطيك صفقات خاصة.

ماذا تفعل إذا تم خداعك

إذا فقدت أموالاً أو قدمت معلومات شخصية، يجب عليك:

- الاحتفاظ بسجل لما حدث
- الاتصال رأساً بمكتبنا Scams and Identity Theft Helpdesk على الرقم **1800 941 126**. أخبرنا إذا كنت بحاجة إلى مترجم فوري وسنقوم بترتيب ذلك مجاناً.
- الابلاغ عن الحادث باللغة الإنجليزية على **scamwatch.gov.au**

أين يمكنك الحصول على مزيد من المعلومات

- اتصل بالرقم **131 202** للتحدث معنا بلغتك حول مدفوعات وخدمات Centrelink
- اتصل بخدمة Translating and Interpreting Service (TIS National) على الرقم **131 450** للتحدث معنا بلغتك حول مدفوعات وخدمات Medicare وChild Support

- اذهب إلى **servicesaustralia.gov.au/yourlanguage** حيث يمكنك قراءة المعلومات بلغتك أو الاستماع إليها أو مشاهدتها
- اذهب إلى **servicesaustralia.gov.au/scams** للحصول على مزيد من المعلومات باللغة الإنجليزية
- قم بزيارة مركز خدمة السنترلنك.

ملاحظة: يتم تحصيل رسوم المكالمات من هاتفك المنزلي إلى رقم "13" من أي مكان في أستراليا بسعر ثابت. قد يختلف هذا السعر عن سعر المكالمة المحلية وقد يختلف أيضاً بين مزودي خدمة الهاتف. المكالمات إلى رقم "1800" من هاتف منزلك مجانية. قد يتم تحديد وقت المكالمات من الهواتف العامة والهواتف المحمولة وتحصيلها بسعر أعلى.

اخلاء المسؤولية

المعلومات الواردة في هذا المنشور مخصصة فقط كدليل للمدفوعات والخدمات. تقع على عاتقك مسؤولية تحديد ما إذا كنت ترغب في التقدم بطلب للحصول على دفعة وتقديم طلب فيما يتعلق بظروفك الخاصة.

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**

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** where you can read, listen to or watch information in your language
- go to **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.