Australian Government
Department of Human Services

# 谨防骗局

骗局旨在骗取你的钱财或让你泄露你的个人信息。

无论你的背景、年龄和收入水平如何，在澳大利亚都可能成为诈骗犯的目标。他们通常会索要钱财，或主动提出给你提供钱财或服务以换取钱财或你的个人信息。

诈骗犯可能会谎称来自 Department of Human Services，以骗取你的钱财或让你泄露你的个人信息。他们可能会：

- 提供奖金
- 提供免费礼品
- 告诉你政府欠你的钱，或
- 威胁你给他们钱，否则将取消你的政府福利金。

如果你遇到骗局，损失了钱财，通常无法要回。

**常见骗局种类**

最常见的骗局是退还费用和 **phishing**。

退还费用

诈骗犯会试图让你相信政府、银行或其他大型机构应退还你某些费用。遇到以下情况，你就应该警惕，你可能已成为了退还费用骗局的目标：

- 你意外收到电子邮件、短信或电话，声称你将收到某种退还的费用。
- 来电者或发件人伪装成政府部门、银行或大型机构的工作人员。
- 对方要求你在得到退还费用前，预支一笔费用，作为行政费用或税费。

Phishing

诈骗犯会试图诱骗你泄露个人信息，如银行账号、密码或信用卡号等。遇到以下情况，你就应该警惕，你可能已成为了 phishing 的目标：

- 你收到电子邮件、短信或电话，对方声称是政府工作人员或其他与你有业务往来的人员，要求你更新或验证你的个人信息。
- 电子邮件或短信未正确拼出你的名字，并可能有拼写和语法错误。
- 你被引导到一个网站，更新你的详细资料，而该网站的地址看起来不像你平常用的那个，并且要求你提供通常不会泄露的个人信息。

警惕！如果仿佛天上掉馅饼——可能就是骗局。

请记住，我们绝不会：

- 询问你的密码或 Personal Identification Numbers (PINs)
- 致电或发信息给你，让你在领取福利或欠款前付款
- 通过电子邮件或 Facebook 或 Twitter 等社交媒体网站与你联系，要求你提供个人信息，或
- 在未事先告知的情况下，登门拜访。

**如果你认为你已经被骗了，应该怎么做？**

- 如果你认为你将自己的银行账户信息给了诈骗犯，请立即与你的银行或金融机构联系。
- 如果你被诈骗了钱财，立即报告当地警方。
- 向 Australian Competition and Consumer Commission (ACCC)报告遭受的骗局。ACCC 提供骗局报告警示人们当前骗局的形式，监控骗局变化趋势，并在可能的情况下制止骗局。你可以前往 **scamwatch.gov.au** 通过 Scamwatch 的“报告骗局（Report a scam）”网页在网上向 ACCC 报告骗局。

如果你不说英语，请拨打 **131 450** 使用翻译与口译服务（TIS National），请他们致电 Scamwatch。

**欲了解更多信息：**

- 访问 **humanservices.gov.au** 搜索“scams”
- 访问 **humanservices.gov.au/yourlanguage** 获取其他语言版本的文字、音频、视频资料
- 请拨打 **131 202** 使用你自己的语言咨询，或
- 前往你当地的服务中心。

注意：在澳大利亚境内用家庭电话拨打“13”开头的号码均按照固定费率收费。该费率可能与本地通话费率不同，并且不同电话服务供应商收取的费率也可能不同。使用家庭电话可免费拨打“1800”开头的号码。使用公共电话和移动电话拨打“1800”开头的号码可能会按较高费率计时收费。

Australian Government
Department of Human Services

# Beware of scams

A scam is designed to trick you into giving away your money or personal information.

Scammers target people of all backgrounds, ages and income levels across Australia. They'll usually ask for money, or they'll offer you payments and services in return for money or your personal information.

Scammers might pretend to be from the Department of Human Services so they can trick you into giving away your money or details. They might:

- offer bonus payments
- offer free gifts
- tell you the government owes you money, or
- threaten to cancel your government payment unless you give them money.

If you lose money because of a scam, you probably won't get it back.

**Common scams**

Some of the most common scams are **reclaim scams** and **phishing**.

Reclaim scams

Scammers will try to convince you that you can get money from the government,a bank, or another trusted organisation. These are some warning signs you might be a target of a reclaim scam:

- You get an unexpected email, text message or phone call that says you can reclaim money.
- The caller or sender pretends to be from a government department, bank, or trusted organisation.
- You**'**re asked to pay an upfront fee**,** to cover administration fees or taxes**,** before you get the money.

Phishing

Scammers will try to trick you into giving out personal information such as your bank account numbers, passwords or credit card numbers. These are some warning signs you might be a target of phishing:

- You get an email, text message or phone call from someoneclaiming to be from the government or other business you deal with, asking you to update or verify your details.
- The email or text message doesn**'**t use your proper name and may have typing and grammar mistakes.
- If you're directed to a website to update your details, the website URL doesn't look like the usual one you use, and you're asked for details you don't normally give.

Be wary! If it sounds too good to be true—it probably is.

Remember, we'll never:

- ask you for passwords or Personal Identification Numbers (PINs)
- call or message to ask you to send money for a benefit or something you're owed
- contact you through email or social media sites like Facebook or Twitter asking for your personal information, or
- visit your home without letting you know first.

**What should you do if you think you've been scammed?**

- If you think you've given your bank details to a scammer, contact your bank or financial institution immediately.
- If you've lost money because of a scam, report it to the local police immediately.
- Report the scam to the Australian Competition and Consumer Commission (ACCC). The ACCC uses reports about scams to warn people about current scams, watch trends and stop scams where possible. You can report scams online to the ACCC through Scamwatch's 'Report a scam' page at **scamwatch.gov.au**

If you speak a language other than English, call the Translating and Interpreting Service (TIS National) on **131 450,** and ask them to call Scamwatch.

**For more information:**

- go to **humanservices.gov.au** and search 'scams'
- go to **humanservices.gov.au/yourlanguage** where you can read, listen to or watch information in other languages
- call us on **131 202** to speak to someone in your language, or
- visit your local 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.