Australian Government
Department of Human Services

安全上网要诀

我们致力保障你个人信息安全，且重视你的网上安全。上网之时，你对保护自己个人信息有举足轻重的作用。

以下是一些可以保障你上网之时个人信息不外泄的方法。

- 退出账户
  - 使用网上账户时，每次用完都要退出，并关闭浏览器会话。
  - 使用 Express Plus app 时，用完后点击退出按钮。
- 保护密码
  - 自己的密码、登录资料、PIN，以及密保问题和答案都不要写下来，也不要告诉他人。
  - 使用字母、数字、大写字母、特殊字符的组合，设定高强度密码。
- 慎用公共电脑
  - 在网吧、图书馆之类的场所慎用网上账户。隐私浏览模式可用则用；每次浏览完毕，都要删掉浏览历史、cookies、cache，并关闭浏览器。
- 保护电脑和设备
  - 使用防护软件；来路不明的链接审慎点击；来路不明的文件或附件审慎下载。
  - 为手机和平板电脑设定密码，为 SIM 卡设定 PIN ，并启用手机锁，以此来保护自己的设备。
  - 使用手机防护软件、声誉良好的网站和手机应用程序。
- 一旦发现任何可疑或未经授权的网上行为，立刻向 SCAMwatch 或 Department of Human Services 举报。

我们非常重视你个人信息的安全和隐私。我们不会：

- 给你发送电子邮件或 SMS ，向你索要银行账户资料或网上账户的登录资料
- 要你告诉我们你的密码或 PIN （但你登录网上账户时须键入此二码）
- 通过社交网站（如 Facebook 或 Twitter）联系你，向你索要个人信息
- 给你发送带链接（URL）的 SMS 或电子邮件。本部门所发的链接只会在你登录自己的安全账户后方可收到
- 未经你同意，把你的信息传给他人，除非法律允许。

欲获得更多信息，请访问：**humanservices.gov.au/onlinesecurity**

Australian Government
Department of Human Services

Top tips for keeping safe online

We are committed to keeping your personal information safe and value your online security. You play an important role in keeping your information safe when you are online. Here are some ways you can ensure your information stays private when you are online.

- Log off
  - Always log off and close down your internet browser session when using your online account.
  - When using your Express Plus app hit the log off button when you are finished.
- Protect your passwords
  - Don't write down or tell people your passwords, log on details, PINs or secret questions and answers.
  - Create strong passwords using letters, numbers, capitals and special characters.
- Be careful when using public computers
  - Be safe when using your online account in places like internet cafés and libraries. Use private browsing mode if available, and always delete your history, cookies, cache and close your internet browser when you are finished.
- Protect your computer and devices
  - Use security software and be careful when clicking links, downloading files, or attachments from unknown sources.
  - Protect your devices by putting a password on your phone and tablet, a PIN on your SIM card and set your phone to lock after a short period.
  - Use mobile security software and reputable websites and mobile apps.
- Report any suspicious or unauthorised online activity to SCAMwatch or the Department of Human Services.

We take the security and privacy of your information very seriously. We won't:

- send you an email or SMS asking for your bank account details or your online account log on details
- ask you to tell us your password or your PIN (but you will need to type them in to access your online account)
- contact you via online social media sites (e.g. Facebook or Twitter) asking for your personal information
- send you an SMS containing a link (URL) or an email containing a link. The only links you will receive from the department will be when you are logged in to and using your secure account
- pass on your information to anyone without your consent, unless the law permits us to do so.

For more information go to **humanservices.gov.au/onlinesecurity**