



## 온라인 보안을 위한 도움말

본 기관은 개인 정보를 안전하게 보호하는 데 전념하고 있으며 온라인 보안을 중시합니다. 온라인 활동 시 개인 정보를 안전하게 보호하기 위해서는 본인의 역할이 중요합니다. 온라인 활동 시 개인 정보가 유출되지 않도록 하는 방법을 몇 가지 알려드리겠습니다.

- 로그오프하세요
  - 온라인 계정 사용 시 항상 로그오프하고 인터넷 브라우저를 종료하세요.
  - Express Plus app을 쓰실 때에는 사용 후 로그오프 버튼을 누르세요.
- 비밀번호를 보호하세요
  - 비밀번호, 로그인 정보, PINs, 비밀 질문 및 답변을 적거나 사람들에게 말하지 마세요.
  - 문자, 숫자, 대문자, 특수문자를 사용하여 보안 수준이 높은 비밀번호를 만드세요.
- 공용 컴퓨터를 사용할 때 조심하세요
  - 인터넷 카페나 도서관과 같은 장소에서 온라인 계정을 사용할 때 조심하세요. 가능한 경우에는 사생활 보호 모드를 사용하고 사용을 마친 후에는 항상 열어본 페이지 목록, 쿠키, 캐시를 삭제하고 인터넷 브라우저를 닫으세요.
- 컴퓨터 및 디지털 기기를 보호하세요
  - 보안 소프트웨어를 사용하고 출처가 불명인 링크를 클릭할 때, 파일을 내려 받을 때, 첨부 파일을 내려 받을 때 주의하세요.
  - 전화기 및 태블릿에는 암호를, SIM 카드에는 PIN을 설정하고 전화기는 시간이 조금 지나면 잠금 모드가 되도록 설정하여 디지털 기기를 보호하세요.
  - 핸드폰 보안 소프트웨어를 사용하고 믿을 수 있는 웹사이트 및 핸드폰 앱을 사용하세요.
- 의심스럽거나 불법적인 온라인 활동은 SCAMwatch 또는 Department of Human Services에 신고하세요.

본 기관은 개인 정보 보호 및 사생활 보호를 매우 중요하게 생각합니다. 본 기관은:

- 이메일이나 SMS를 보내 은행 계좌 정보 또는 온라인 계정 로그인 정보를 달라고 요청하지 않습니다
- 비밀번호나 PIN을 말해달라고 요청하지 않습니다 (온라인 계정을 사용하려면 본인이 타이핑을 통해 입력해야 합니다)
- 온라인 소셜 미디어 사이트(예를 들면 Facebook이나 Twitter)로 연락해서 개인 정보를 달라고 요청하지 않습니다
- 링크(URL)가 포함된 SMS를 보내거나 링크가 포함된 이메일을 보내지 않습니다. 본 기관으로부터 링크를 받으시는 경우는 본인이 로그인하여 본인의 안전한 계정을 사용할 때 뿐입니다
- 법에 의해 허용된 경우가 아닌 이상 고객의 동의 없이 개인 정보를 타인에게 넘겨주지 않습니다.

더 많은 정보를 원하시면 [humanservices.gov.au/onlinesecurity](https://humanservices.gov.au/onlinesecurity)를 방문하세요.



## 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](https://humanservices.gov.au/onlinesecurity)