Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

如何安全使用互联网

老年人指南

cyber.gov.au

序言

上网能让你同朋友和家人保持联络，了解一些话题，甚至能玩游戏。

就像开车前系好安全带一样，在使用互联网之前你也应该采取几个步骤保证安全。

澳大利亚网络安全中心 (ACSC) 希望确保所有人都能安全上网。本手册包含一些基本的网络安全措施，你可以在上网时用这些措施保护自己。

作为Australian Signals Directorate（ASD）的下属机构，澳大利亚网络安全中心（ACSC）提供网络安全建议、协助和操作响应措施，以防止、检测和补救对澳大利亚的网络威胁。ACSC的目标是帮助澳大利亚成为网络安全度最高的地方。

访问cyber.gov.au获取更多网络安全资讯、指南和建议

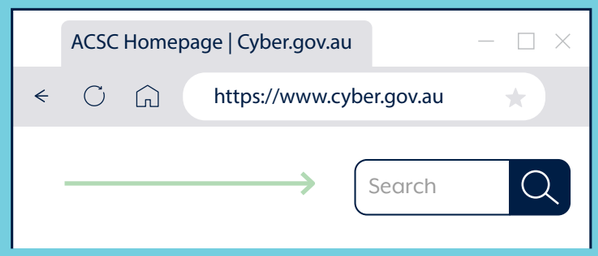
老年人网络安全

提示1：更新你的设备

更新你的软件就像保养你的 车辆一样。它能提高你的设备性能，令其更加安全。

网络罪犯总是在寻找新方法入侵他人的设备。在设备上设置自动安装更新能够弥补软件的任何弱点，让黑客们无从下手。

如需了解更多信息，请在cyber.gov.au上搜索“Updates”。



你知道吗：

更新还可能为您的设备添加新功能并使其运行更快。

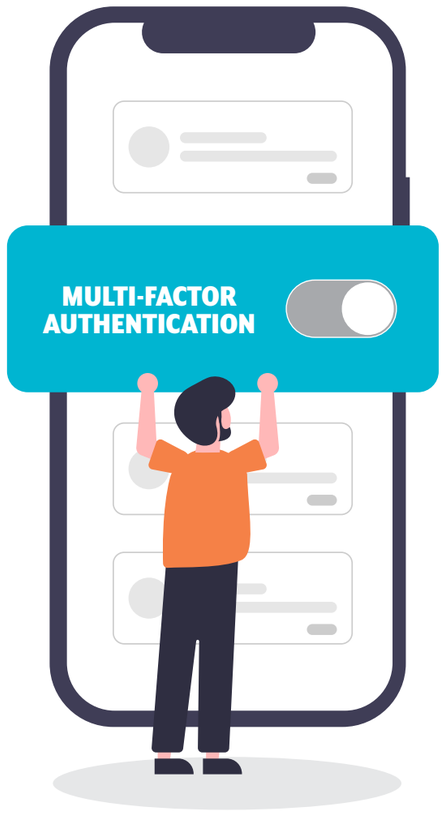
提示2：开启多重身份验证

你账户的多重身份验证就像是你家里的防盗网一样。它阻止试图闯入的罪犯从而给你保护。

多重身份验证开启后，你需要提供多种资讯才能登入你的账户。例如，你可能需要一个短讯密码和你自己的密码来登入你的社交媒体账户。

多重保护增加了罪犯入侵的难度。他们也许能破解一部分，例如你的密码，但他们仍然需要获得拼图的其他部分才能进入你的账户。

如需了解更多信息，请在cyber.gov.au上搜索“Multi-factor authentication”或“MFA”



请记住：

如果你需要帮助来开启多重身份认证，向家人或朋友求助。

提示3：备份你的设备

执行‘备份’是制作重要文件的副本并将其存放在安全的地方。这就像是复印珍贵照片后将其存放在保险箱里，以免日后原件丢失。

当你备份电脑、手机或平板设备时，你的文件副本会被存放在网上或另一个设备上。备份重要文件和珍贵照片后你会感到高枕无忧。

如果你的设备出现问题或被黑客入侵，你能够轻松地从备份中恢复文件。

如需了解更多信息，请在cyber.gov.au上搜索“Backups”

你知道吗：

定期备份你的设备 意味着你始终可以使用你最新的文件。

提示4：设置短语密码

如果说密码是给你的账户加了一把锁，那么短语密码就是给你一套防盗系统！这是更牢固更安全的升级版密码。

无法开启MFA时，使用短语密码保护你的账户。
短语密码使用4个或更长的随机词汇作为你的密码。
这让网络罪犯更难猜测而你更容易记住。

你创建的短语密码应该是：

- **长度足够** 越长越好。长度最好在14个字节以上。
  4个或更多你能够记住的随机词汇最好。
  例如，'purple duck potato boat'。
- **不可预测** 短语密码可预测程度越低越好。
  句子或许是很好的短语密码，但太容易被猜到。
  混合的4个或更多随机词汇是保密性高的短语密码。
- **独特** 的密码词组。不要重复使用密码词组。对不同的帐户使用不同的密码词组。如果您难以记住所有密码词组，请考虑使用密码管理器。通过密码管理器，您只需记住一个密码，密码管理器会帮您记住其它密码。在cyber.gov.au上搜索“password manager”以获取更多建议。

在cyber.gov.au上搜索“Passphrases”了解更多有关创建安全密码词组的信息

提示5：发现并举报骗局

你举报骗局越早，我们就能越早行动。

如果你相信有人在试图使用互联网欺骗你，你最好提前行动保持警惕，以免被人利用。

如果事情听起来好得令人难以置信，那就很可能不能相信。一条短讯可能说你赢得大奖或你的电脑有病毒，此类短讯并非只有你收到。

它可能来自骗子，他们想利用你。

请记住，骗子通常会冒充您信任的人或组织。如果您收到一条看似来自自己信任的人的消息，但他们使用了新的电话号码、电子邮箱或社交媒体档案，请保持警惕。在回复之前，请通过可以信赖的渠道与他们联系，以验证发送消息的是否确实是他们自称的人或组织。例如，如果您收到一条看似来自儿女的短信，但这条消息来自一个新号码，请不要回复。在社交媒体上向儿女发送消息，先确认他们是否真的更改了电话号码。

你知道吗：

狡猾的网络罪犯可能使用你知道的名字或电邮地址。以下情况要小心：

- **你被要求立即支付账单**
- **你被要求更改个人资讯或密码**
- **你被要求点击一个链接或打开一个附件。**

总结

现在你已经了解了安全使用互联网的知识，你可以更自信地享受网上时光了。

记住，网络罪犯总是能想出新方法来攻击网络用户。

定期更新你的网络安全知识，了解最新安全措施总是有好处。

奖励性提示

想要了解更多网络安全的知识吗？请阅读以下提示。

考虑你发布的内容。

慎重考虑你在网络上共享的资讯以及谁会看到。只接受你在生活中认识的人加好友的请求。

获取新威胁警示。

订阅我们的免费警示服务。这样当我们发现新的网络威胁时你会及时知道。

这样当攻击发生时你也会得到应对建议。

同亲友讨论网络安全。

现在你已经提高了网络安全知识，和家人朋友分享你所学到的。你的知识有可能帮助他们避免日后陷入骗局！

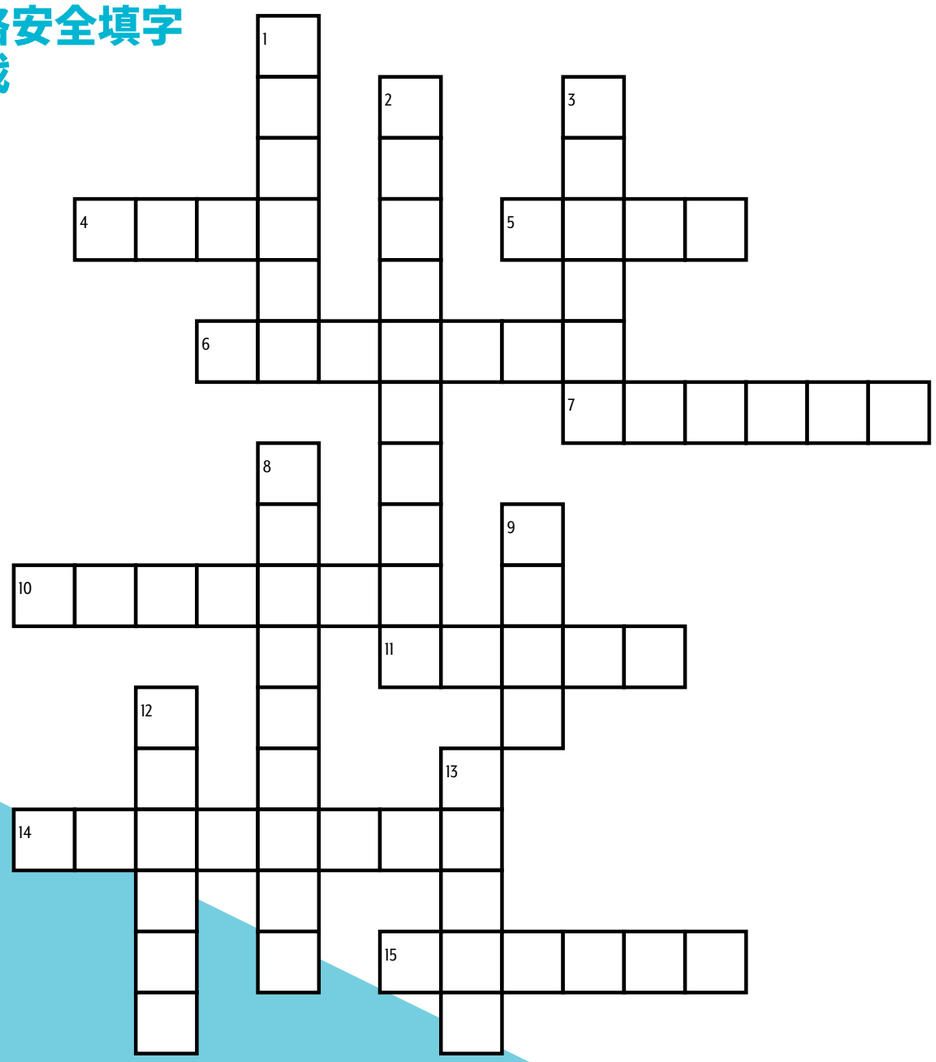
进行银行业务或网上购物时避免使用公共Wi-Fi。

公共Wi-Fi在看视频和网页时很便利，但只使用自己家里的网络进行任何涉及资金的操作。公共Wi-Fi可能有风险。

举报网络攻击事件，保护澳大利亚的安全。

如果你认为自己是网络犯罪的受害者，立刻采取行动。cyber.gov.au有更多建议

网络安全填字游戏



向下

1. Connected to the internet
2. A strong password
3. A person who uses computers to steal data
8. Software that destroys viruses
9. A deceptive scheme or trick
12. A copy of your computer's files
13. Relating to, or involving computers

横向

4. Wireless networking technology
5. Australia's lead agency for cyber security
6. A document on the World Wide Web
7. To give information about something
10. New, improved or more secure versions of software
11. Electronic mail
14. The state of being free from danger or threat
15. A tool that can connect to the internet

补充指南

获取更多资讯，请阅读我们的 *个人网络安全* 丛书：
3册指南旨在帮助澳洲澳大利亚民众了解基本网络安全知识以及如何采取行动保护自己免受常见网络威胁的攻击。

你可以在 cyber.gov.au 上阅读这3册指南

填字游戏答案

1. online, 2. passphrase, 3. hacker, 4. Wi-Fi, 5. ACSC, 6. webpage, 7. report, 8. antivirus, 9. scam, 10. updates, 11. email, 12. backup, 13. cyber, 14. security, 15. device

注

欲了解更多信息，或报告网络安全事件，请联系我们。

cyber.gov.au | 1300 CYBER1 (1300 292 371)

该号码仅可在澳大利亚境内使用。

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre