



Australian Government
Australian Signals Directorate

ASD AUSTRALIAN
SIGNALS
DIRECTORATE
ACSC Australian
Cyber Security
Centre



CÁCH SỬ DỤNG INTERNET AN TOÀN

HƯỚNG DẪN CHO NGƯỜI CAO NIÊN

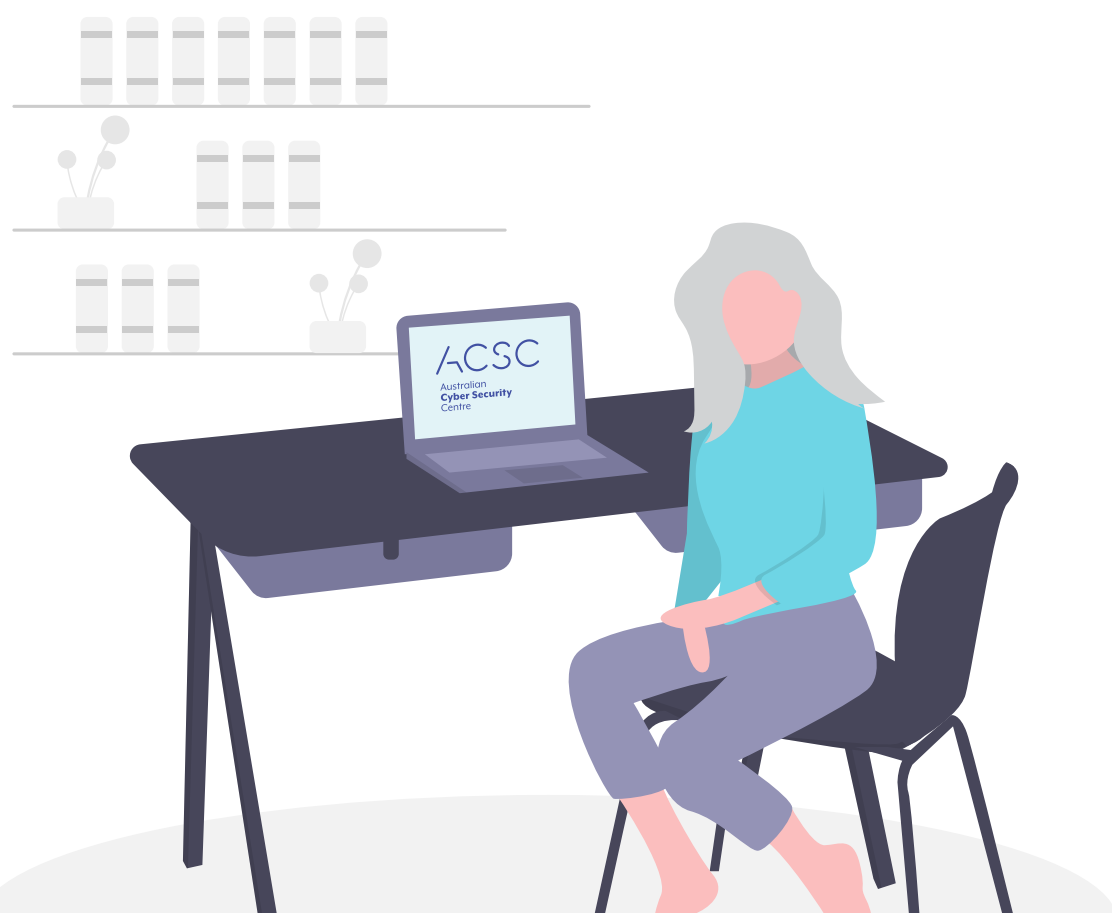
cyber.gov.au

Mở đầu

Việc lên mạng giúp quý vị giữ liên lạc với bạn bè và gia đình, học hỏi về các đề tài và cả chơi game.

Cũng giống như việc phải cài dây an toàn trước khi lái xe, quý vị nên thực hiện các bước trước khi dùng internet để được an toàn hơn.

Trung tâm An ninh Mạng Úc (Australian Cyber Security Centre - ACSC) muốn đảm bảo mọi người đều được an toàn khi lên mạng. Tài liệu này đề cập một số thông lệ cơ bản về an ninh mạng mà quý vị có thể thực hiện nhằm bảo vệ bản thân khi dùng internet.



Trung tâm An ninh Mạng Úc (ACSC), trực thuộc Tổng cục Tín hiệu Úc (Australian Signals Directorate - ASD), cung cấp hướng dẫn, hỗ trợ và cách ứng phó vận hành nhằm phòng tránh, phát hiện và xử lý các mối đe dọa trên mạng đối với Úc. Công việc của Trung tâm ACSC là giúp làm cho nước Úc trở thành nơi an toàn nhất khi kết nối trên mạng.

Muốn biết thêm chi tiết về an ninh mạng, về các hướng dẫn và lời khuyên, hãy vào trang [cyber.gov.au](https://www.cyber.gov.au)

An ninh mạng cho người cao niên

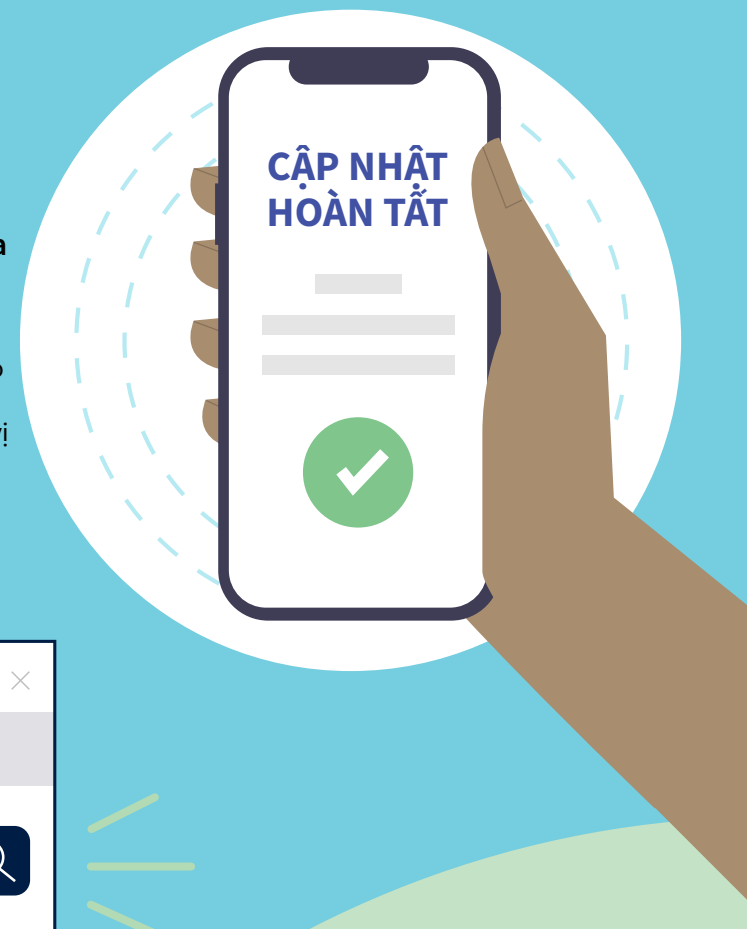


Chỉ dẫn 1: Cập nhật thiết bị của quý vị

Cập nhật phần mềm của quý vị giống như là đưa xe hơi đi bảo dưỡng. Nó cải thiện hiệu suất của thiết bị và làm cho thiết bị được an toàn hơn.

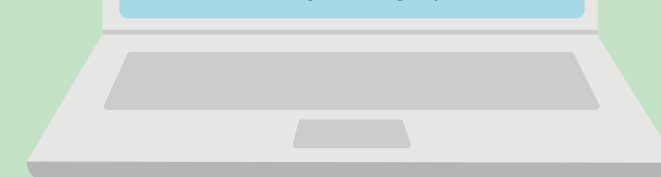
Tội phạm mạng luôn tìm những cách mới để xâm nhập vào thiết bị. Cài đặt thiết bị để tự động cập nhật có thể khắc phục được bất cứ điểm yếu nào trong phần mềm của quý vị và để tránh tin tặc.

Để biết thêm thông tin, hãy tìm kiếm 'Updates' (Cập nhật) trên trang mạng [cyber.gov.au](https://www.cyber.gov.au).



QUÝ VỊ CÓ BIẾT:

Các bản cập nhật cũng có thể bổ sung các tính năng mới cho thiết bị của bạn và giúp thiết bị chạy nhanh hơn.





Chỉ dẫn 2: Bật chức năng xác thực đa yếu tố

Chức năng xác thực đa yếu tố cho tài khoản của quý vị giống như có cửa lưới an toàn cho nhà quý vị.

Cửa lưới bảo vệ quý vị không để tội phạm tìm cách đột nhập vào nhà.

Khi bật chức năng xác thực đa yếu tố, quý vị cần phải cho nhiều chi tiết thì mới tiếp cận được tài khoản của mình. Ví dụ, quý vị có thể cần ghi mật khẩu và mã số ở tin nhắn điện thoại thì mới đăng nhập được vào tài khoản mạng xã hội của mình.

Nhiều lớp xác thực làm cho việc xâm nhập của tin tặc khó hơn. Chúng có thể xoay xở để đoán được một phần chẳng hạn như một phần mật khẩu của quý vị, nhưng chúng vẫn cần phải có các mảnh ghép khác nữa của hình ghép thì mới tiếp cận được vào tài khoản của quý vị.

Để biết thêm thông tin, hãy tìm 'Multi-factor authentication' (Xác thực đa yếu tố) hoặc 'MFA' trên trang mạng [cyber.gov.au](https://www.cyber.gov.au)



GHI NHỚ:

Nếu quý vị cần trợ giúp để bật chức năng xác thực đa yếu tố, hãy nhờ bạn hoặc người nhà giúp quý vị.



Chỉ dẫn 3: Sao lưu thiết bị

Thực hiện 'sao lưu' là khi quý vị sao một bản các hồ sơ quan trọng của mình và đưa vào nơi an toàn. Giống như sao chụp các ảnh quý để cất vào nơi an toàn phòng khi bị mất bản gốc.

Khi quý vị sao lưu máy tính, điện thoại hoặc máy tính bảng, các bản sao của hồ sơ của quý vị được lưu trực tuyến hoặc được lưu ở một thiết bị khác. Có bản sao lưu các hồ sơ quan trọng và các hình ảnh được quý vị yêu quý sẽ làm cho quý vị yên tâm.

Nếu có điều gì không hay xảy ra đối với thiết bị hoặc nếu quý vị bị tin tặc tấn công thì quý vị có thể dễ dàng khôi phục hồ sơ từ sao lưu.

Để biết thêm thông tin, hãy tìm 'Backups' (Sao lưu) trên trang mạng [cyber.gov.au](https://www.cyber.gov.au)



QUÝ VỊ CÓ BIẾT:

Thường xuyên sao lưu thiết bị của mình nghĩa là quý vị luôn luôn tiếp cận được các hồ sơ mới nhất của mình.



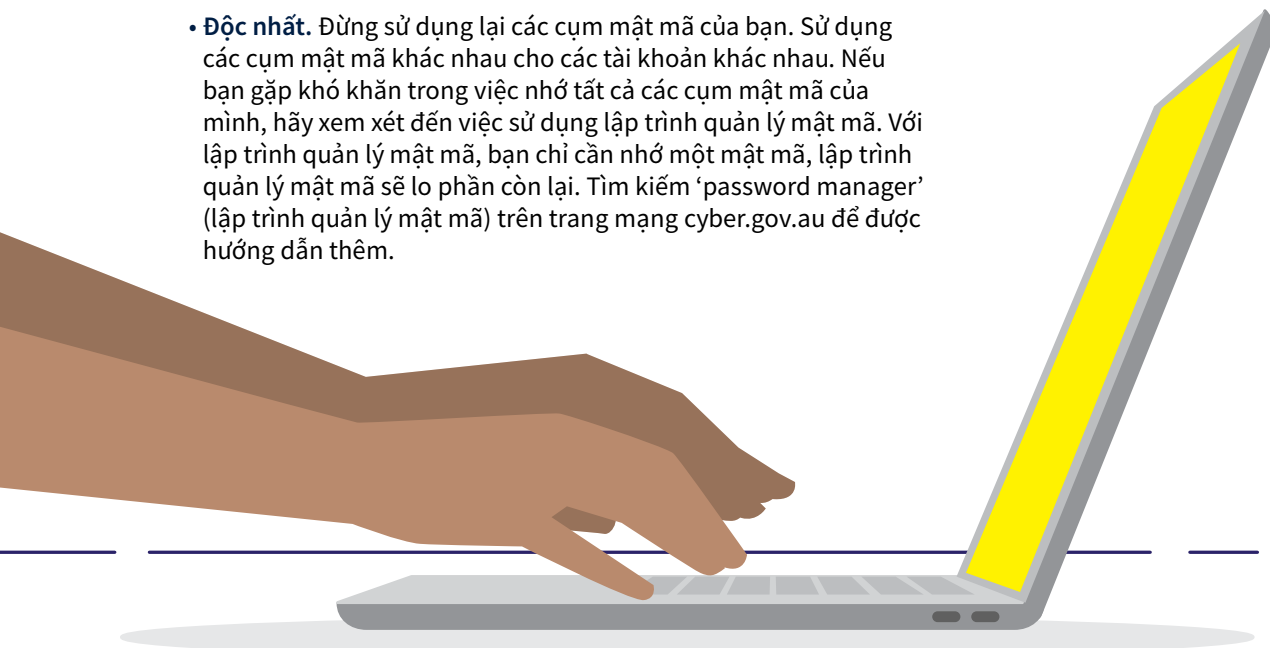
Chỉ dẫn 4: Dùng cụm mật khẩu

Khi có mật khẩu là quý vị có khóa cho tài khoản, nhưng có cụm mật khẩu là quý vị có cả hệ thống bảo vệ an toàn! Cụm mật khẩu mạnh hơn và là phiên bản an toàn hơn của mật khẩu.

Nếu quý vị không thể bật MFA được, hãy dùng cụm mật khẩu để bảo vệ tài khoản của mình. Cụm mật khẩu sử dụng bốn từ bất kỳ trở lên làm mật khẩu. Như vậy sẽ rất khó cho tin tặc đoán ra nhưng lại dễ nhớ đối với quý vị.

Khi quý vị tạo cụm mật khẩu, hãy làm cho nó:

- **Dài.** Càng dài càng tốt. Nhắm tới độ dài tối thiểu là 14 chữ. Bốn từ bất kỳ trở lên mà quý vị nhớ được thì thật là tuyệt. Chẳng hạn như 'màu tím con vịt khoai tây cái thuyền'.
- **Khó đoán.** Cụm từ càng khó đoán bao nhiêu càng tốt bấy nhiêu. Các câu có thể tạo thành cụm mật khẩu rất hay nhưng chúng lại dễ đoán hơn. Một hỗn hợp bốn từ bất kỳ trở lên sẽ làm cho cụm mật khẩu được mạnh hơn.
- **Độc nhất.** Đừng sử dụng lại các cụm mật mã của bạn. Sử dụng các cụm mật mã khác nhau cho các tài khoản khác nhau. Nếu bạn gặp khó khăn trong việc nhớ tất cả các cụm mật mã của mình, hãy xem xét đến việc sử dụng lập trình quản lý mật mã. Với lập trình quản lý mật mã, bạn chỉ cần nhớ một mật mã, lập trình quản lý mật mã sẽ lo phần còn lại. Tìm kiếm 'password manager' (lập trình quản lý mật mã) trên trang mạng cyber.gov.au để được hướng dẫn thêm.



Hãy tìm hiểu thêm về cách tạo các cụm mật mã an toàn bằng cách tìm kiếm 'Passphrases' (Cụm mật mã) trên trang mạng cyber.gov.au



Chỉ dẫn 5: Phát hiện và trình báo lừa đảo

Quý vị trình báo lừa đảo càng nhanh bao nhiêu, thì chúng tôi càng hành động được kịp thời bấy nhiêu.

Nếu quý vị tin rằng ai đó đang dùng internet để lừa đảo quý vị, tốt nhất là hãy chủ động và thận trọng thay vì mạo hiểm để bị lợi dụng.

Nếu điều đó nghe hay đến mức không thể có thật, thì chắc là vậy đó. Trong khi một tin nhắn có thể báo là quý vị vừa được trúng giải hoặc máy tính của quý vị bị vi rút, thì tin nhắn đó không phải là độc nhất cho quý vị đâu.

Tin nhắn đó có thể bắt nguồn từ kẻ lừa đảo và chúng muốn lợi dụng quý vị.

Hãy nhớ rằng, những kẻ lừa đảo thường giả danh một người hoặc tổ chức mà bạn tin tưởng. Hãy hồ nghi nếu bạn nhận được tin nhắn có vẻ như là từ ai đó mà bạn tin tưởng nhưng họ lại sử dụng số điện thoại, địa chỉ email hoặc hồ sơ mạng xã hội mới. Trước khi bạn trả lời, hãy xác minh xem người hoặc tổ chức đang nhắn tin cho bạn có thực sự đúng là người họ nói không, bằng cách liên lạc với họ qua một phương thức khác mà bạn có thể tin tưởng. Ví dụ: nếu bạn nhận được một tin nhắn có vẻ như là từ một trong những đứa con của bạn, nhưng lại đến từ một số mới, đừng vội trả lời. Trước tiên hãy gọi cho họ một tin nhắn trên mạng xã hội để kiểm tra xem có phải họ đã thực sự thay đổi số điện thoại không.



QUÝ VỊ CÓ BIẾT:

Tin tặc rất quý quý vị và có thể dùng một cái tên và địa chỉ email nghe quen quen. Hãy thận trọng nếu:

- người ta bảo quý vị hãy khẩn trương thanh toán một hoá đơn
- người ta bảo quý vị hãy đổi chi tiết hoặc mật khẩu của quý vị
- người ta bảo quý vị hãy nhấp chuột để vào đường dẫn hoặc để mở tài liệu đính kèm



Kết luận

Bây giờ, sau khi đã được trang bị kiến thức để sử dụng internet an toàn hơn, quý vị có thể tự tin lướt mạng và tiếp tục tận hưởng thời gian lên mạng.

Hãy nhớ là, tội phạm mạng luôn luôn nghĩ ra các kiểu mới để tấn công mọi người.

Không bao giờ uống phí khi thỉnh thoảng nâng cao kiến thức của mình về an ninh mạng và học hỏi những cách mới để giữ an toàn.

Tặng thêm chỉ dẫn

Quý vị muốn biết thêm cách giữ an toàn trên mạng?
Hãy thử xem các chỉ dẫn dưới đây.

Hãy nghĩ về những gì quý vị đăng lên.

Hãy nghĩ kỹ về thông tin quý vị chia sẻ trên mạng và những ai sẽ thấy bài đăng đó. Chỉ nhận yêu cầu kết bạn từ những người mà quý vị biết trong đời sống thực.

Nhận cảnh báo về các mối đe dọa mới.

Hãy đăng ký vào dịch vụ cảnh báo miễn phí của chúng tôi. Dịch vụ sẽ báo cho quý vị biết mỗi khi chúng tôi phát hiện ra một mối đe dọa mới trên mạng.

Dịch vụ cũng sẽ hướng dẫn quý vị nên làm gì nếu xảy ra cuộc tấn công.

Hãy nói chuyện về vấn đề an ninh mạng với gia đình và bạn bè.

Giờ đây quý vị đã có nhiều kỹ năng về an toàn trên mạng, hãy chia sẻ những điều quý vị đã học được

với gia đình và bạn bè. Kiến thức của quý vị có thể giúp họ tránh được các tình huống rắc rối sau này!

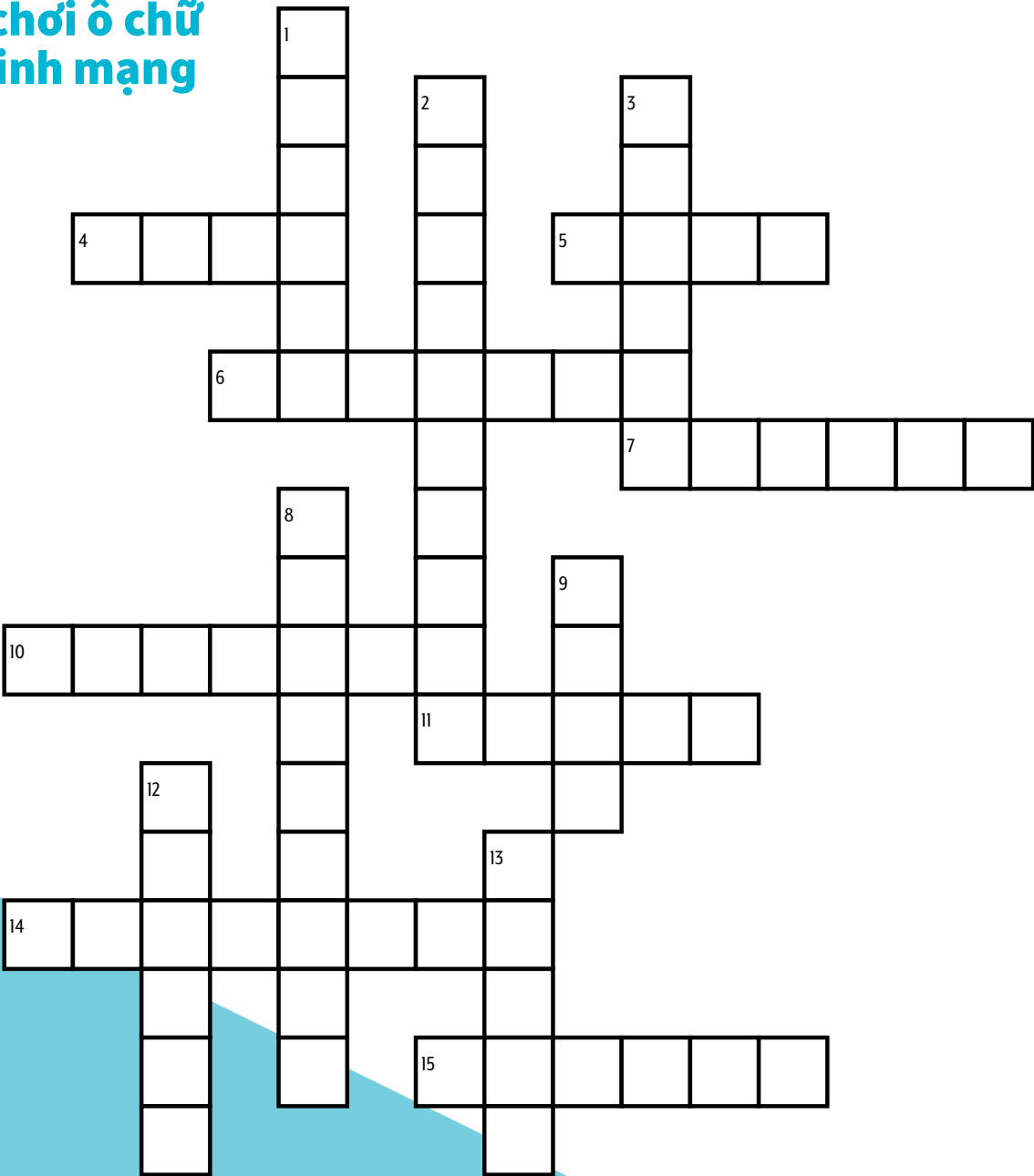
Hãy tránh sử dụng Wi-Fi công cộng khi quý vị giao dịch ngân hàng hoặc mua sắm trên mạng.

Wi-Fi công cộng rất tốt để coi video hoặc đọc các trang mạng nhưng hãy chỉ làm các việc liên quan đến tiền trên mạng khi quý vị dùng kết nối internet ở nhà. Wi-Fi công cộng có thể nguy hiểm.

Trình báo tội phạm mạng và các sự cố trên mạng để giữ cho nước Úc được an toàn.

Nếu quý vị cho rằng mình là nạn nhân của tội phạm mạng, hãy hành động thật nhanh. Có thêm hướng dẫn tại cyber.gov.au

Trò chơi ô chữ an ninh mạng



XUỐNG

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

NGANG

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

Các hướng dẫn bổ sung

Để có thêm chi tiết, vui lòng kiểm tra loạt bài An toàn Mạng Cá nhân: ba bản hướng dẫn được soạn thảo nhằm giúp người Úc bình thường hiểu được các vấn đề cơ bản về an ninh mạng và cách quý vị có thể hành động để tự bảo vệ chống lại các mối đe dọa phổ biến trên mạng.



Quý vị có thể tiếp cận tất cả ba bản hướng dẫn này tại **cyber.gov.au**

Các câu trả lời chơi ô chữ

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

Lưu ý

Tuyên bố miễn trừ trách nhiệm

Tài liệu trong tập hướng dẫn này chỉ mang tính chất tổng quát và không nên được coi là lời khuyên pháp lý hoặc dựa vào để được hỗ trợ trong bất kỳ hoàn cảnh hay tình huống khẩn cấp cụ thể nào. Đối với bất kỳ vấn đề quan trọng nào, quý vị nên tìm kiếm lời khuyên chuyên môn, độc lập, và thích hợp liên quan đến hoàn cảnh của mình.

Chính phủ Liên bang không chịu trách nhiệm hay trách nhiệm pháp lý nào đối với bất kỳ thiệt hại, mất mát hoặc phí tổn nào phát sinh do việc dựa vào thông tin trong tập hướng dẫn này.

Bản quyền

© Chính phủ Liên bang Úc Năm 2023

Ngoại trừ Quốc huy và nếu có quy định khác, tất cả tài liệu trình bày trong ấn phẩm này được cung cấp theo giấy phép Quốc tế Creative Commons Attribution4.0 (Thừa nhận sự Sáng tạo Chung4.0) (www.creativecommons.org/licenses).

Để tránh hồ nghi, điều này có nghĩa là giấy phép này chỉ áp dụng với các tài liệu như được nêu trong tập hướng dẫn này mà thôi.



Chi tiết về các điều kiện giấy phép liên quan có sẵn trên trang mạng Creative Commons, cũng như mã pháp lý đầy đủ cho giấy phép CC BY 4.0 (www.creativecommons.org/licenses).

Sử dụng Quốc huy

Các điều khoản mà theo đó Quốc huy có thể được sử dụng, được trình bày chi tiết trên trang mạng của Bộ Thủ tướng và Nội các (www.pmc.gov.au/government/commonwealth-coat-arms).

Muốn biết thêm thông tin hoặc trình báo sự cố an ninh mạng, hãy liên lạc với chúng tôi tại:

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

Số điện thoại này chỉ để sử dụng trong nước Úc mà thôi.



Australian Government
Australian Signals Directorate

ASD AUSTRALIAN
SIGNALS
DIRECTORATE
ACSC Australian
Cyber Security
Centre