

Giới thiệu về an toàn trên mạng Internet

Chúng ta hãy cùng giúp đỡ nhau để đảm bảo rằng chúng ta sử dụng Internet một cách an toàn.

Bảo mật máy tính và email

Rủi ro trực tuyến chủ yếu bao gồm:

- **Vi-rút**, lây lan từ máy tính này sang máy tính khác qua mạng Internet. Một số vi-rút chỉ làm quý vị khó chịu, một số khác có thể xóa dữ liệu của quý vị.
- **Trojan**, là những chương trình trông có vẻ như vô hại nhưng lại cố ý lừa để quý vị cài đặt chúng.
- **Phần mềm gián điệp (spyware)**, là các chương trình ăn cắp thông tin như mật khẩu hoặc các chi tiết tài khoản ngân hàng.

Quý vị có thể thực hiện các bước sau để bảo vệ bản thân và máy tính của mình khỏi các mối đe dọa trên trực tuyến.

1. Sử dụng **phần mềm chống vi-rút**, giúp tìm kiếm, ngăn chặn và loại bỏ vi-rút.
2. Sử dụng **phần mềm chống phần mềm gián điệp**, giúp ngăn chặn việc đánh cắp dữ liệu của quý vị.
3. Sử dụng tường lửa (firewall), giúp bảo vệ máy tính của quý vị không bị truy cập trái phép từ mạng internet.
4. Luôn cập nhật phần mềm bảo vệ internet của quý vị.
5. Nếu quý vị có phần mềm chống vi-rút đi kèm với máy tính mới, hãy gia hạn nó khi bản dùng thử hết hạn hoặc cài phần mềm miễn phí như AVG. Lưu ý rằng Windows 10 đi kèm với phần mềm chống vi-rút hiệu quả gọi là Windows Defender. Windows sẽ luôn tự cập nhật cho quý vị.
6. Nếu không chắc chắn, quý vị hãy tham khảo lời khuyên từ trang <https://www.staysmartonline.gov.au/>.

Giới thiệu về an toàn trên mạng Internet

Quý vị phải hết sức cẩn thận không để máy tính của quý vị tiếp xúc với phần mềm độc hại.

1. Suy nghĩ kỹ trước khi mở email và đặc biệt là các tệp đính kèm email từ những người quý vị không biết.
2. Chỉ giao dịch trên trực tuyến với các doanh nghiệp mà quý vị biết có danh tiếng tốt. Tìm kiếm thông tin về công ty trước khi mua hàng.
3. Định kỳ sao lưu tất cả thông tin trên máy tính của quý vị. Nếu máy tính của quý vị bị nhiễm vi-rút, quý vị sẽ vẫn truy cập được tất cả dữ liệu quan trọng của mình.



Bảo vệ bản thân và máy tính của mình khỏi các mối đe dọa trên trực tuyến

Sử dụng dữ liệu cá nhân trên mạng internet

Đôi khi ta cần phải cung cấp thông tin cá nhân trên mạng, nhưng cần giới hạn số lượng thông tin quý vị có thể chia sẻ, và luôn biết các quyền của mình.

- Chỉ cung cấp thông tin cho các công ty trung thực, nếu cần để xác minh danh tính của quý vị.
- Tránh đăng thông tin cá nhân (ngày sinh, địa chỉ nhà riêng, v.v.) lên các diễn đàn công cộng như Facebook. Thông tin cá nhân có thể bị bọn tội phạm sử dụng để trộm cắp danh tính.
- Pháp luật quy định việc sử dụng thông tin cá nhân bởi các công ty tư nhân. Ở Úc, đó là Luật Quyền Riêng Tư 1988.
- Luật Tự do Thông tin có thể áp dụng cho thông tin quý vị cung cấp cho các cơ quan chính phủ.
- Các công ty có uy tín có các chính sách bảo mật thông tin cá nhân. Hãy đọc các chính sách bảo mật thông tin cá nhân này trên các trang mạng của họ.
- Để biết thêm thông tin về quyền lợi của người tiêu dùng hoặc để cập nhật thông tin về việc bảo vệ quý vị khỏi những trò lừa đảo, vui lòng truy cập ACCC: <https://www.accc.gov.au/consumers>.



Pháp luật quy định việc sử dụng thông tin cá nhân bởi các công ty tư nhân ở Úc

Giới thiệu về an toàn trên mạng Internet

Thanh toán trực tuyến và các khu vực an toàn

Mua hàng trực tuyến có thể thuận tiện và có một số cách kiểm tra nhanh để giúp đảm bảo quý vị thanh toán an toàn.

1. Công ty mà quý vị đang giao dịch có danh tiếng tốt không? Kiểm tra các chính sách bảo mật thông tin cá nhân và chính sách hoàn trả trên trang mạng của họ. Sử dụng công cụ tìm kiếm để tìm hiểu thêm về công ty.
2. Mua hàng bằng thẻ tín dụng hoặc PayPal. Cả hai cách này đều có hình thức bảo vệ người mua hàng.
3. Ngay trước khi nhập thông tin thẻ tín dụng của quý vị, hãy kiểm tra **thanh Địa chỉ** trên trình duyệt máy tính của quý vị. Một trang mạng an toàn phải được đánh dấu bằng biểu tượng ổ khóa và trang mạng đó phải bắt đầu bằng **https:** (không phải là **http:**).



Cẩn thận với thông tin mà quý vị chia sẻ trên trực tuyến

An toàn trên trực tuyến cho trẻ em

Trẻ em có ít kinh nghiệm cuộc sống hơn và do đó sẽ có nhiều khả năng rủi ro hơn từ việc:

- Xem các tài liệu hình ảnh dành cho người lớn.
- Tiết lộ thông tin cá nhân.
- Bị ăn hiếp và quấy rối.

Các phòng chat (chatroom) trên Internet và mạng xã hội là những nơi dễ tiếp cận. Không bao giờ để con của quý vị gặp gỡ bất cứ ai mà các em đã 'gặp' trên trực tuyến trừ khi có người lớn đi kèm.

Quý vị có thể giúp bảo vệ trẻ em được an toàn khi tham gia trực tuyến.

1. Tạo tài khoản sử dụng riêng cho con mình trên máy tính.
2. Bật chế độ kiểm soát của cha mẹ đối với tài khoản đó.
3. Đối với Google, bật **Safe Search (Tìm kiếm An toàn)**, và đối với Bing hoặc Yahoo, chuyển Safe Search sang chế độ 'strict' (ng nghiêm ngặt)
4. Đặt YouTube thành 'restricted' (bị hạn chế), cùng với bất cứ trang mạng video nào khác.
5. Nói chuyện với con quý vị về những mối nguy hiểm mà các em có thể đối mặt trên trực tuyến.

Nếu một trẻ vô tình gặp phải một tình huống nguy hiểm trên trực tuyến, quý vị hãy báo cáo cho Văn phòng của Ủy viên An toàn Điện tử tại <https://www.esafety.gov.au/complaints-and-reporting>.