Cuộc sống trực tuyến

Bài 15: Công dân kỷ nguyên số

Mục tiêu bài học

- Các tiêu chuẩn truyền thông chuyên nghiệp
- Cách thức để tránh các hành vi không phù hợp khi trực tuyến
- Sở hữu trí tuệ, bản quyền và các quy định cấp phép
- Công thái học và cách thiết lập máy tính của bạn
- Bảo vệ máy tính khỏi các mối đe dọa phần mềm
- Vi rút là gì và cách ngăn ngừa chúng gây tổn hại máy tính của bạn
- Cách thức tự bảo vệ khi giao dịch thương mại điện tử hoặc mua hàng

Xác định các vấn đề về đạo đức

- Việc đưa thông tin lên Internet ngày càng trở nên dễ dàng hơn, với cảm giác được ẩn danh làm cho một vài người thực hiện những điều khi họ trực tuyến mà có thể họ sẽ không làm những điều đó khi không trực tuyến, hoặc dễ dàng bỏ qua các vấn đề liên quan đến quyền tác giả hoặc các vấn đề riêng tư
- Nhận thức rằng việc đang ẩn danh không thể bào chữa cho trách nhiệm đối với hành vi trực tuyến
- Tự bảo vệ mình và luyện tập cách ứng xử, ý thức được sự tôn trọng đến những vấn đề liên quan đến bản quyền, riêng tư giống như khi bạn đang giao tiếp trực tiếp.

Xác định các vấn đề về đạo đức

- **Tìm hiểu về sở hữu trí tuệ, bản quyền và cấp phép**
  - Thông tin trên Internet hoàn toàn miễn phí để bạn đọc, nghe, hoặc giải trí
  - Mọi người tạo ra các trang Web với rất nhiều lý do
  - Mặc dù các thông tin hiện hữu trên Web site giúp bạn dễ dàng truy cập miễn phí nhưng không ngầm định rằng các thông tin đó hoàn toàn miễn phí khi bạn sao chép, sử dụng, phân phối hoặc biểu diễn giống như bạn là người tạo ra các thông tin đó

Xác định các vấn đề về đạo đức

- **Sở hữu trí tuệ**
  - Bất kỳ sản phẩm hoặc sáng tạo nào được tạo ra đều được coi là *sở hữu trí tuệ* của cá nhân (hoặc tổ chức) tạo ra nó
    - bất kỳ thứ gì được tạo ra bởi các nhân hoặc nhóm đều được coi là sở hữu của các nhân hay nhóm đó
    - bất kỳ thứ gì được tạo ra bởi các nhân hoặc tổ chức dưới dạng hợp đồng với tổ chức thuộc quyền sở hữu của tổ chức khi họ chi trả "phí dịch vụ"
  - Việc ước lượng giá trị chính xác của sở hữu trí tuệ không phải là một nhiệm vụ dễ dàng hoặc đơn giản
    - Dường như có vẻ việc cố tính "mượn" tất cả hoặc một phần sở hữu trí tuệ của ai đó là một điều nhỏ, thì từ đó có thể gây thất thoát một số tiền nhất định từ việc đánh cắp bản quyền hay vi phạm bản quyền, và trong một vài trường hợp thậm chí là cả gián điệp công nghiệp

Xác định các vấn đề về đạo đức

- **Bản quyền**
  - Luật bản quyền được tạo ra để bảo vệ sở hữu trí tuệ
  - Bảo vệ bất kỳ tài liệu nào, đã xuất bản hay chưa xuất bản, được tạo ra bởi cá nhân hay tổ chức
    - Bản quyền là luật cho phép bạn sở hữu tài sản trí tuệ của mình
    - Không ai có thể tạo các bản sao bức tranh bạn vẽ, sử dụng mã nguồn trang Web trên trang Web của họ, hoặc trình bày bài hát do bạn sáng tác, trừ khi bạn đồng ý
  - Quyền tác giả cũng cung cấp cho bạn quyền được bán sản phẩm do sản phẩm bạn bỏ ra
    - đảm bảo cho duy nhất một mình bạn có thể bán, cho thuê, hoặc yêu cầu bồi thường với sản phẩm bạn đã bỏ ra.

Xác định các vấn đề về đạo đức

- **Đăng ký bản quyền**
  - Ngay khi sản phẩm của bạn đã hình thành nên dạng sản phẩm, nó đã được bảo vệ bởi quyền tác giả
    - Nói chung, bản quyền bảo vệ sản phẩm làm việc của bạn ngay từ khi bạn bắt đầu thực hiện công việc, bản quyền được áp dụng cho cả quãng thời gian sống của tác giả, và kéo dài năm mươi năm sau khi tác giả qua đời
  - Khi bạn đã tạo ra một sản phẩm, đặt một thông báo về bản quyền ở phía bên dưới
    - thông báo này bao gồm một ký hiệu bản quyền ©, tiếp đến là ngày tạo ra sản phẩm, và sau đó là tên bạn
    - Điều này là đủ để khẳng định bạn có thể yêu cầu bồi thường nếu ai đó xâm phạm quyền của bạn
  - nếu bạn muốn kiện một bên nào đó phải bồi thường thiệt hại vì vi phạm bản quyền, bạn cần phải đăng ký bản quyền với văn phòng bản quyền ở khu vực sở tại

Xác định các vấn đề về đạo đức

- **Các tài liệu đã có bản quyền trên các Web site**
  - Các tài liệu hiển thị trên một Web site có cùng các quy tắc bản quyền giống với bất kỳ loại phương tiện nào khác
  - Bạn có thể sử dụng tài liệu đã đăng ký bản quyền chỉ khi bạn được tác giả gán quyền sử dụnng
    - có thể phải trả phí bản quyền, hoặc bạn thừa nhận tác giả khi truyền tải lại nội dung trong công việc riêng của mình.
    - Trách nhiệm của bạn là cần xác định những gì cần yêu cầu trước khi sử dụng bất kỳ phần nào của tài liệu có bản quyền.
  - quy tắc “sử dụng hợp lý”, nghĩa là bạn có thể sử dụng các phần của thông tin có bản quyền với mục đích chỉ trích hoặc bình luận mà không cần có sự cho phép từ chủ sở hữu

Xác định các vấn đề về đạo đức

- Quyền tác giả mặc định thuộc về người sở hữu Web site hoặc người tạo ra tài liệu đã xuất bản, thậm chí không có ký hiệu bản quyền (©) hoặc văn bản xuất hiện trên sản phẩm
  - Người tạo ra sản phẩm có thể có bằng sáng chế trên sản phẩm hoặc công nghệ đó, nghĩa là họ có độc quyền trong việc tạo ra, sử dụng, hoặc bán sản phẩm hay dịch vụ
  - Họ có thể lựa chọn cách cấp phép hoặc gán cho bạn những quyền hạn cụ thể, nhưng bạn không thể quảng bá bạn là người sở hữu sản phẩm hay công nghệ đó
- Một vài Web site cho phép bạn sử dụng thông tin họ cung cấp khi bạn trích dẫn chính xác và trả phí cho họ
  - Tuy nhiên, bạn cần phải cẩn thận vì chủ sở hữu của các Web site đó chưa hẳn đã là người tạo ra thông tin, hoặc họ không được gán quyền hạn hợp pháp

Xác định các vấn đề về đạo đức

- **Hậu quả pháp lý của vi phạm bản quyền**
  - Sẽ nhận được một bức thư từ những nguồn hợp pháp yêu cầu bạn xóa nội dung từ Web site của bạn, hoặc xóa bất kỳ tệp tin nào đã được tải
  - ISP của bạn có thể ngắt tất cả các dịch vụ liên quan đến tài khoản của bạn
  - có thể bị kiện vì bất kỳ tổn thất nào và phải thanh toán tiền bồi thường thiệt hại cho chủ sở hữu bản quyền.

Xác định các vấn đề về đạo đức

- **Cấp phép**
  - *Giấy phép đơn -Single seat:* Khi bạn mua một chương trình phần mềm, nghĩa là bạn đang mua giấy phép cài đặt và sử dụng chương trình chỉ trên một máy tính
    - Nếu phần mềm được mua trực tuyến, bạn thường thanh toán bằng thẻ tín dụng, và sau đó bạn nhận được các bức thư điện tử từ nhà phân phối xác nhận bạn đã mua và cung cấp mã cấp phép, hay thường gọi là mã *sản phẩm* hoặc *mã khóa*.
  - *Network* or *volume license:* dành cho các tổ chức hoặc một công ty lớn với số lượng lớn nhân viên sử dụng một chương trình phần mềm nào đó
    - Bộ phận quản trị mạng sẽ nhận được một tập hợp các phương tiện sau đó lưu vào một thư mục trên máy chủ
      - Chương trình sau khi cài đặt vào các máy sẽ cần mã khóa
    - Tùy chọn này tiết kiệm về mặt chi phí vì giảm được thời gian cần thiết để cài đặt một chương trình trên nhiều máy tính

Xác định các vấn đề về đạo đức

- *Site* license: Giấy phép cho một địa điểm gán quyền hạn cho người mua phần mềm trên mạng tại một địa điểm với số lượng không giới hạn người sử dụng.
  - đắt hơn nhiều so với giấy phép của một sản phẩm nhưng lại rẻ hơn nhiều nếu bạn mua giấy phép cho từng máy tính tại địa điểm đó
- *Phần mềm dịch vụ (SaaS)* hay *giấy phép nhà cung ứng dịch vụ (ASP)*: cho phép bạn truy cập và sử dụng chương trình phần mềm từ hệ thống thông qua mạng của tổ chức hoặc thông qua Internet.
  - được yêu cầu đăng nhập trước khi truy cập vào phần mềm
  - Khi hợp đồng SaaS đã hết hạn, bạn không thể truy cập tiếp vào phần mềm cho đến khi bạn gia hạn giấy phép

Xác định các vấn đề về đạo đức

- Một số hình thức phân phối và sử dụng phần mềm khác:
  - Shareware: sẻ là các phiên bản thử nghiệm của phần mềm mà bạn có thể tải miễn phí, nhưng thường các chức năng của phần mềm bị giới hạn hoặc hạn chế thời gian truy cập vào chương trình
    - Nếu bạn thích sử dụng chương trình này, bạn trả một khoản phí danh nghĩa để loại bỏ những hạn chế này
  - Freeware: những phần mềm không tính phí và có thể chia sẻ với người dùng khác
  - Software bundles: , khi bạn mua một PC mới bao gồm cả giấy phép sử dụng hệ điều hành, và có thể bao gồm phiên bản dùng thử của một số phần mềm khác.
    - Một vài chương trình có thể yêu cầu bạn mua phiên bản chương trình đầy đủ hoặc đăng ký trực tuyến trước khi bạn truy cập vào chương trình
  - Premium software: tải về phần mềm từ một trang web cụ thể để nhận được bản đầy đủ

Xác định các vấn đề về đạo đức

- Open Source: các đoạn mã chương trình được công khai cho bất kỳ ai muốn sử dụng
  - có thể chỉnh sửa chương trình cho phù hợp với nhu cầu của mình và có thể chia sẻ phiên bản đã chỉnh sửa cho người khác; tuy nhiên, bạn không được phép thu phí từ bất kỳ ai
- Cho dù bạn sử dụng phần mềm bằng cách nào đi nữa, trách nhiệm của bạn là quan sát cẩn thận các quy tắc về giấy phép sử dụng
  - Khi bạn mua một phần mềm có giấy phép, bạn sẽ được thông báo bởi nhà phân phối về bất kỳ cập nhật nào nếu có mà không mất thêm phí
  - Nếu bạn không có giấy phép sử dụng phần mềm hợp lệ, bạn sẽ vi phạm bản quyền của nhà cung cấp và có thể liên quan trách nhiệm pháp lý
  - Luôn đọc giấy phép sử dụng của người dùng cuối (EULA) tại thời điểm cài đặt, tuân thủ các quy tắc sử dụng phần mềm trên máy tính

Xác định các vấn đề về đạo đức

- **Tổ chức Creative Commons**
  - tổ chức phi lợi nhuận cung cấp sáu loại giấy phép cho những ai muốn chia sẻ sản phẩm làm việc sáng tạo hoặc tri thức của họ và giữ được bản quyền.
    - tổ chức phi lợi nhuận cung cấp sáu loại giấy phép cho những ai muốn chia sẻ sản phẩm làm việc sáng tạo hoặc tri thức của họ và giữ được bản quyền.
  - cung cấp một phương pháp chuẩn để cấp quyền trên sản phẩm làm việc sáng tạo của chủ sở hữu với các hạn chế về luật bản quyền và cũng đảm bảo chủ sở hữu bản quyền được thu phí cho sản phẩm đã tạo ra.
  - Chủ sở hữu bản quyền có thể quyết định giấy phép nào được sử dụng

Xác định các vấn đề về đạo đức

Attribution	Người khác có thể phân phối, thay đổi, tinh chỉnh và xây dựng dựa trên sản phẩm ban đầu của bạn, miễn là bạn trả phí cho chủ sở hữu bản quyền
Attribution – NoDerivs	Người khác có thể phân phối với mục đích thương mại hoặc phi thương mại nhưng ở dạng nguyên gốc và trả phí cho bạn.
Attribution – Non-Commercial – ShareAlike	Người khác có thể thay đổi, tinh chỉnh hoặc xây dựng dựa trên sản phẩm ban đầu của bạn với mục đích phi thương mại; họ cũng cần trả phí cho bạn và giấy phép của kết quả mới được tạo ra cũng có các điều khoản giống với giấy phép của bạn.
Attribution – ShareAlike	Người khác có thể thay đổi, tinh chỉnh hoặc xây dựng thêm dựa trên sản phẩm ban đầu của bạn với mục đích thương mại; họ cần trả phí cho bạn và giấy phép của kết quả mới được tạo ra cũng có các điều khoản giống với giấy phép của bạn
Attribution – Non-Commercial	Người khác có thể thay đổi, tinh chỉnh hoặc xây dựng thêm dựa trên sản phẩm ban đầu của bạn với mục đích phi thương mại. Bạn sẽ được trả phí cho bất kỳ công việc mới nào dựa trên sản phẩm ban đầu và phi thương mại, họ không cần giấy phép cho các sản phẩm mới sử dụng các điều khoản trong giấy phép gốc của bạn.
Attribution – Non-Commercial – NoDerivs	Người khác chỉ có thể tải sản phẩm ban đầu của bạn và chia sẻ với những người trả phí cho sản phẩm của bạn mà không được thay đổi hoặc sử dụng với mục đích thương mại.

Xác định các vấn đề về đạo đức

- Giấy phép cũng có thể chứa tất cả các quyền hạn được gán với mục đích để sản phẩm có thể được đặt ở những nơi công cộng
  - Chủ sở hữu từ bỏ tất cả quyền hạn với sản phẩm ban đầu
- Bằng cách sử dụng Creative Commons để quản lý cách thức các tài liệu có bản quyền có thể được chia sẻ hoặc sử dụng
  - Các tổ chức có thể đặt các thông tin của họ lên các địa điểm công cộng mà không cần lo về bất kỳ vi phạm luật bản quyền nào
  - Thông tin có thể được cập nhật và phân phối theo cách công bằng cho chủ sở hữu bản quyền, cũng như tổ chức sở hữu giấy phép

Xác định các vấn đề về đạo đức

- **Kiểm duyệt và lọc thông tin**
  - Không có một cơ quan nào giám sát các nội dung trực tuyến
    - có rất nhiều vùng xám chứa tài nguyên khó tách biệt được đó là xấu hay tốt, điều này dẫn đến những thông tin này cần được xem xét nên kiểm duyệt hay lọc thông tin với mục đích bảo vệ người dùng
  - **Bộ chặn và lọc dữ liệu**
    - cho phép bạn điều khiển loại thông tin hoặc lượng thông tin có thể được xem
    - Một vài trang Web mạng xã hội cũng thiết lập các bộ chặn bản tin hoặc bài đăng có thể chứa các thông tin có vấn đề hoặc gây sự khó chịu cho người dùng
      - Các bộ lọc này thường xuất phát từ ISP mỗi khi bạn truy cập vào trang mạng xã hội.
      - Các trang khác như các phòng nói chuyện có thể có người điều hành để theo dõi các thảo luận và cảnh báo khi anh/cô ta nhận thấy cuộc thảo luận không thích hợp

Xác định các vấn đề về đạo đức

- *Blacklisting:* khi bạn bị đánh dấu hoặc đặt trong danh sách những người dùng bị cấm truy cập vào một dịch vụ, đặc quyền hoặc công nhận/tín dụng cụ thể
  - Liên hệ với ISP nếu họ không thể được xóa khỏi một vài danh sách đen
  - Trong một vài trường hợp, họ cần phải gửi một bức thư chính thức để yêu cầu xóa tên họ ra khỏi danh sách đen
- Những công cụ này tương tự như kiểm duyệt thông tin ngoại trừ việc nó được thiết lập theo các hướng dẫn của những người quản trị tổ chức hay học viện đó
- Vẫn còn có những tranh luận về việc những gì được xem là thông tin tấn công, nguy hiểm, bóc lột?
- Một sự cố khác là khi có một ai đó có thể hack (đột nhập) vào phần mềm chặn hoặc lọc thông tin và thay đổi thông tin cấu hình của tổ chức.
- Một cơ quan có quyền kiểm soát nội dung bị kiểm duyệt trên toàn bộ đất nước thường có quyền kiểm soát tất cả các máy tính có kết nối với Internet trong quốc gia đó

Xác định các vấn đề về đạo đức

- **Những điều nên tránh**
  - **Đạo văn**
    - khi bạn sử dụng thông tin được tạo ra bởi người khác và biểu diễn nó như là sở hữu của mình với những thay đổi rất nhỏ hoặc không có sự thay đổi nào.
    - Cho dù đó chỉ là một đoạn văn bản hoặc một hình ảnh đơn lẻ; nó đều được coi là hành vi trộm cắp sở hữu trí tuệ hoặc sản phẩm gốc của người khác
    - Khi sử dụng thông tin từ Internet, bạn luôn phải sử dụng thông tin đó ở dạng gốc và trích dẫn nguồn tham khảo để đảm bảo bạn đang tuân theo nguyên lý sử dụng hợp lý
    - Bằng cách xác nhận rằng bạn đang mượn nội dung và cung cấp thông tin để tìm nội dung đó, trong hầu hết trường hợp, bạn sẽ tránh được các cáo buộc đạo văn

Xác định các vấn đề về đạo đức

- **Phỉ báng hoặc Vu khống**
  - viết những điều không đúng sự thật làm "tổn hại danh dự" của cá nhân hoặc danh tiếng của tổ chức.
    - Nếu những nhận xét phỉ báng được nói ra thì được gọi là vu khống
  - Bài học tốt nhất nên làm cả trực tuyến và trong đời sống, đó là đối xử với những vu khống đó như là các tin đồn:
    - không bắt đầu, không nghe và không phản ứng

Xác định các vấn đề về đạo đức

- **Vi phạm bản quyền**
  - Thường liên quan đến việc vi phạm quyền tác giả hoặc đạo văn khi sao chép lại sản phẩm gốc hoặc chỉnh sửa lại để phù hợp với mục đích nào đó mà không có quyền hạn từ chủ sở hữu
  - Cũng xảy ra khi một mục nào đó bị chia sẻ mà không trả bất kỳ phí nào cho chủ sở hữu, gây ra những thiệt hại cho chủ sở hữu bản quyền
  - Nếu bạn tải về các tài liệu đã mua bản quyền, có thể sử dụng
  - Vi phạm bản quyền được coi là tội phạm liên bang nếu tòa án xác định bạn cố tính vi phạm bản quyền với mục đích lợi nhuận
    - Hình phạt cho án hình sự có thể bị phạt tù lên đến 10 năm tùy thuộc vào mức độ vi phạm
  - Để bảo vệ bạn trước những khả năng phạm luật về vi phạm bản quyền không có chủ đích, bạn nên luôn mua phần mềm từ các đại lý bán lẻ có uy tín

Xác định các vấn đề về đạo đức

- **Hành vi không phù hợp**
  - Các trò đùa cợt có thể gây ra những sự tổn thương và nên tránh
  - Bắt nạt trực tuyến xảy ra khi làm cho một hoặc nhiều người bị tổn thương qua những bài viết truyền tải thông điệp thù địch, có hại một cách liên tục và cố ý
  - Tránh "gây sự" người khác
    - Có thể bằng một bản tin thư điện tử hoặc nói chuyện trong phòng tán gẫu với mục đích tấn công người nhận
    - Nếu bạn bị gây sự, cách tốt nhất là nên bỏ qua nó

Xác định các vấn đề về đạo đức

- Không gửi thư rác cho người khác
- Không chia sẻ thông tin cá nhân về người khác, thậm chí khi những người đó là người thân quen với bạn
  - Nếu một ai đó cho bạn biết thông tin bí mật hoặc nhạy cảm, bạn cần tôn trọng sự riêng tư và giữ điều đó cho riêng bạn
  - cần thận trọng nếu có kế hoạch đăng bất kỳ thứ gì lên trang mạng xã hội
- Đừng chế giễu hoặc bỏ qua các quan điểm của người khác
- Nếu bạn đang tạo ra thông tin được sử dụng trực tuyến, bạn cung cấp thêm thông tin và nguồn hỗ trợ thông tin đó
  - Hãy thực hiện điều đó một cách tôn trọng và chính xác với ngữ điệu và thông điệp của bạn một cách thích hợp cho người nghe
- Hãy luôn nhớ trong đầu quy luật vàng: hãy thực hiện những điều mà bạn muốn người khác thực hiện cho mình – cả trực tuyến và trong cuộc sống

Những thực hành tốt cho Công dân trực tuyến

- Những hướng dẫn để giúp bạn trở thành một công dân tốt trong xã hội thực tế giờ đây cũng cần được mở rộng để áp dụng khi bạn trực tuyến
- Không chỉ sử dụng duy nhất công cụ kiểm tra lỗi khi hiệu đính tài liệu
- Bạn cần rất thận trọng khi sử dụng từ hoặc chữ viết tắt
- Bạn luôn cần lưu ý ai là người nhận hoặc người nghe thông tin
- Bạn cần xem xét hình thức truyền thông nào là tốt nhất để đặt ra câu hỏi
- Bạn cần nhớ loại bỏ cảm xúc cá nhân ra khỏi những phiên truyền thông của mình, đặc biệt nếu bạn là người suy nghĩ tiêu cực
- Khi bạn đăng bài trực tuyến, bạn có thể đăng cả văn bản cùng với những hình ảnh và các liên kết đến các Web site khác với thái độ tốt

Bảo vệ dữ liệu hoặc máy tính của bạn

- **Ăn cắp**
  - Có thể mua các hệ thống để khóa máy tính trong các tủ đặc biệt hoặc sử dụng cáp bền để gắn máy tính với bàn làm việc
  - Camera quan sát rất hữu dụng với những khu vực làm việc có nhiều máy tính như văn phòng trung tâm và các phòng mạng
  - Đừng để các thiết bị di động mà không chú ý đến nó khi bạn ở các địa điểm công cộng.

Bảo vệ dữ liệu hoặc máy tính của bạn

- **Mất dữ liệu**
  - Bạn có thể bị mất mát dữ liệu với nhiều nguyên nhân như hacker, lỗi phần cứng, chập điện, vô tình xóa dữ liệu, bị mất thiết bị, hỏng thiết bị, hoặc do các nhân viên bất mãn
  - Nếu bạn cung cấp một dịch vụ rất quan trọng, bạn cần lên một kế hoạch khẩn cấp để đối phó với sự cố xảy ra do mất mát hệ thống của bạn
  - Với các thiết bị di động, bạn cần giữ các thiết bị bên cạnh mình khi ở những nơi công cộng
    - sử dụng một chương trình đồng bộ dữ liệu để sao dữ liệu từ các thiết bị di động sang các máy tính chuyên để sao lưu dữ liệu
  - Để giảm khả năng bị người khác thay đổi các tệp tin dữ liệu, xem xét thêm mật khẩu vào các tệp tin cụ thể hoặc xóa bất kỳ quyền hạn chia sẻ nào trên các tệp tin hoặc thư mục đó

Bảo vệ dữ liệu hoặc máy tính của bạn

- **Bảo mật dữ liệu**
  - Hacker là một ai đó có thể truy cập vào máy tính, thường là với mục đích
    - đánh cắp thông tin với mục đích bán chúng, hoặc
    - hủy dữ liệu trong công ty của bạn để không có khả năng cung cấp sản phẩm, dịch vụ, hoặc dự án đúng thời hạn,
    - thay đổi thông tin, gây ra sự lúng túng và phá hoại uy tín của công ty
  - Một cách hiệu quả để bảo vệ dữ liệu là thông qua việc sử dụng mật khẩu hợp lý
    - Sử dụng một công thức với lập luận đủ để cho bạn nhớ nhưng không dễ cho người khác đoán
    - Tránh sử dụng biệt hiệu hoặc tên của vợ/chồng, trẻ em, hoặc thú cưng
    - Thử kết hợp các ký tự và số, điều này làm cho mật khẩu khó đoán hơn

Bảo vệ dữ liệu hoặc máy tính của bạn

- Thay đổi mật khẩu của bạn thường xuyên
- Nếu bạn lo lắng về việc phải nhớ quá nhiều mật khẩu, bạn có thể chuyển đổi sử dụng từ ba đến năm mật khẩu qua lại.
- Sử dụng các mật khẩu khác nhau cho những tệp tin bí mật và để đăng nhập vào mạng hoặc Internet
- Hãy cận thận khi bạn lưu lại mật khẩu trên trình duyệt Web đối với từng Web site cụ thể
- cần cài đặt và duy trì các thiết bị tường lửa, cổng vào ra mạng và các phần mềm chuyên dụng để đảm bảo tính toàn vẹn của máy chủ
- thuê một đơn vị tư vấn bảo mật để thực hiện đánh giá rủi ro và đề xuất một kế hoạch bảo mật cho công ty

Bảo vệ dữ liệu hoặc máy tính của bạn

- **Sao lưu**
  - Dữ liệu nên được sao lưu trên các phương tiện có thể di chuyển được
  - Dữ liệu càng quan trọng, bạn cần càng thường xuyên sao lưu
  - Nếu người dùng lưu trữ các tệp tin dữ liệu trên ổ đĩa cục bộ, khuyến nghị họ tạo bản sao trên máy chủ để sao lưu hàng ngày hoặc tạo các bản sao lưu cho riêng họ
  - khuyến nghị người dùng lưu thường xuyên để đảm bảo không mất dữ liệu
  - lớn xây dựng các bản sao lưu như một phần trong kế khoạch đối phó với thiên tai và kế hoạch phục hồi
  - nhiều công ty sử dụng lưu trữ các bản sao lưu trên đám mây
    - bảo vệ dữ liệu ở một địa điểm mà còn cung cấp khả năng phục hồi dữ liệu từ bất kỳ địa điểm nào có kết nối với Internet.

Bảo vệ dữ liệu hoặc máy tính của bạn

- **Xác định các mối đe dọa từ phần mềm**
  - **Phần mềm gián điệp/Phần mềm quảng cáo/Cookie**
    - *Spyware:* là một phần mềm ứng dụng được đặt bí mật trong hệ thống của người dùng và thu thập các thông tin cá nhân hoặc riêng tư mà không có sự đồng ý hoặc cho phép của người dùng
      - có thể được đặt trên hệ thống của người dùng thông qua vi rút hoặc một chương trình được tải về từ Internet.
      - theo dõi hành động của người dùng trên Internet và gửi thông tin về người dùng cho chủ sở hữu phần mềm gián điệp. Người này có thể thu thập thói quen sử dụng Web site, thư điện tử và thậm chí là thông tin mật khẩu của người dùng, và sau đó sử dụng với mục đích gây hại hoặc quảng cáo
    - Cookies: các tệp tin nhỏ đặt trên máy tính của bạn bởi máy chủ chứa trang Web mà bạn tải về.
      - bản thân cookie không nguy hiểm, nhưng chúng có thể lưu trữ tên người dùng và mật khẩu
      - lưu vết hoạt động của trình duyệt.

Bảo vệ dữ liệu hoặc máy tính của bạn

- **Phần mềm độc hại**
  - là những chương trình hoặc tệp tin có mục đích gây hại cho các hệ thống máy tính
  - là một dạng phá hoại có phạm vi ảnh hưởng trên toàn cầu
  - bao gồm vi rút máy tính, sâu và Trojan
    - *Worms* Sâu là vi rút tự nhân bản để lây nhiễm vào các tài nguyên hệ thống và mạng, và có thể tự động lây nhiễm tới tất cả các máy tính được kết nối với mạng
    - *Trojan horse* là một chương trình được thiết kế để cho phép hacker truy cập từ xa tới hệ thống máy tính đích

Bảo vệ dữ liệu hoặc máy tính của bạn

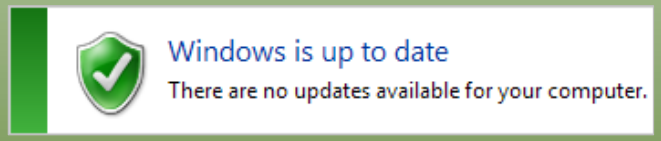
- **Tải về**
  - Đề cập đến các chương trình hoặc các tệp tin lớn có thể được thực thi hoặc chạy trên máy tính sau khi bạn sao chép chúng từ máy chủ Web
  - Có thể tải các tệp tin lên ổ đĩa cứng hoặc cài đặt phần mềm trực tiếp từ Internet
    - Các tệp tin thực thi được coi là những nguy hiểm tiềm tàng bởi vì nó thường được sử dụng để phát tán các phần mềm độc hại và gián điệp
    - Khuyến cáo một cách mạnh mẽ rằng bạn cần lựa chọn khi tải một tệp tin, bạn lưu tệp tin đó vào một thư mục được thiết kế riêng trên máy tính và sau đó quét các tệp tin đã tải để kiểm tra các mối đe dọa tiềm tàng trước khi chạy ứng dụng
  - Bạn cần đọc một cách cẩn thận trước khi tự động nhấp chuột vào bất kỳ nút nào, đặc biệt là nút Accept hoặc OK
    - cần đọc End User License Agreement để quan sát cách thức sử dụng thông tin

Bảo vệ dữ liệu hoặc máy tính của bạn

- **Các thiết lập tường lửa cá nhân**
  - bảo vệ máy tính khỏi những nguy hiểm tiềm tàng được truyền đến từ các mối đe dọa từ bên ngoài
  - được coi la các phần mềm ứng dụng
    - Windows cũng tích hợp sẵn một tường lửa, nhưng bạn có thể mua tường lửa của hãng thứ ba để tận dụng các ưu điểm của những tính năng mà hãng đó cung cấp
  - Thường được sử dụng với mục đích theo dõi các yêu cầu truyền thông đi tới hệ thống của mạng từ Internet, và các yêu cầu đi ra khỏi hệ thống.
  - có thể chặn các dòng truyền thông nếu nó không ghi nhận đó là một chương trình được phép gửi và nhận các yêu cầu truyền thông mà không có sự đồng ý của người sử dụng
  - Bạn có thể kiểm tra và điều chỉnh các thiết lập tường lửa cá nhân bằng cách chọn Windows Firewall từ Control Panel

Bảo vệ dữ liệu hoặc máy tính của bạn

- **Các bản cập nhật**
  - Cập nhật hệ điều hành là một điều cực kỳ quan trọng để giảm thiểu các sự cố bảo mật
  - Các vi rút mới được tạo ra thường xuyên và một trong những số đó được thiết kế để khai thác lỗ hổng bảo mật tiềm năng trong phần mềm Windows
  - Microsoft cũng đưa ra các bản cập nhật hệ điều hành một cách thường xuyên để bảo vệ hệ thống khỏi các hiểm họa đến từ phần mềm
    - Khi bạn nhận được thông báo về những bản cập nhật mới của Windows, bạn có thể kiểm ta những gì có trong các bản cập nhật đó và cài đặt bản cập nhật để giải quyết các sự cố bảo mật



Bảo vệ dữ liệu hoặc máy tính của bạn

- **Các tệp tin dư thừa**
  - Có thể tồn tại sau khi bạn gỡ bỏ một chương trình ứng dụng
  - hầu hết các tệp tin dư thừa là không gây hại, nó vẫn có thể chứa thông tin cá nhân có thể bị khai thác nếu hệ thống của bạn bị xâm nhập.
  - Sau khi bạn gỡ chương trình, kiểm tra ổ đĩa để quan sát nếu còn dư bất kỳ thư mục nào của chương trình
    - Nếu bạn tìm thấy bất kỳ tệp tin hoặc thư mục nào, bạn có thể xóa chúng một cách thủ công
  - Một vài chương trình không được gỡ một cách hoàn toàn và có thể để lại những mục dữ liệu lỗi trong Windows Registry
    - Windows Registry là một cơ sở dữ liệu trong Windows lưu trữ các thông tin cấu hình và các phần mềm đã được cài đặt
    - Các mục dữ liệu dư thừa hoặc bị lỗi trong Registry có thể là nguyên nhân dẫn đến các sự cố ảnh hưởng đến độ thực thi trong một vài trường hợp

Bảo vệ dữ liệu hoặc máy tính của bạn

- Các tệp tin dư thừa có thể vẫn còn sau khi bạn xóa các tệp tin dữ liệu
  - các tệp tin bị xóa khỏi ổ cứng có thể được lưu trữ trong Recyle Bin. Nếu bạn xóa các tệp tin nhạy cảm, cần đảm bảo bạn làm rỗng Recyle bin để các tệp tin không phục hồi đượ
- Nếu bạn dự định tặng một hệ thống máy tính cũ có lưu trữ thông tin cá nhân, bạn nên sử dụng một chương trình tiện ích chuyên dụng được gọi là “shredder” để phá hủy tất cả dữ liệu trên ổ cứng
  - Chỉ định dạng ổ đĩa cứng thôi là không đủ và nó không phá hủy toàn bộ dữ liệu trên ổ cứng
- Nếu bạn sử dụng các thiết bị lưu trữ di động, cần cảnh giác nếu các thiết bị này chứa các thông tin nhạy cảm
  - Đừng đặt các thiết bị đó ở những nơi mà người không có quyền hạn có thể truy cập vào chúng

Bảo vệ dữ liệu hoặc máy tính của bạn

- **Cookie**
  - Cookie là một mẩu văn bản được lưu trữ trong ổ đĩa cứng cho một Web site cụ thể để chia sẻ thông tin giữa máy tính của bạn và nhà phân phối Web site
  - Cơ bản thì Cookie ko có hại, nhưng có thể nguy hiểm hoặc chứa các thông tin cá nhân
  - Cookie có thể được xóa bằng cách làm sạch chúng từ trình duyệt Web bằng cách sử dụng lệnh Tools

Bảo vệ dữ liệu hoặc máy tính của bạn

- **Tìm hiểu về vi rút**
  - vi rút là một chương trình thực hiện điều khiển các thao tác của hệ thống và phá hủy hoặc làm hỏng dữ liệu
    - Tất cả các vi rút máy tính là do con người làm ra và thường được thiết kế để lây nhiễm cho những người sử dụng máy tính khác
    - Có thể lây lan thông qua mạng hoặc danh sách địa chỉ thư điện tử.
  - Vi rút có thể:
    - Hiển thị các bản tin vô hại trên màn hình.
    - Sử dụng bộ nhớ trống trên máy tính, vì thế làm cho máy tính chậm lại hoặc ngăn chặn các tiến trình khác hoạt động.
    - Làm hỏng hoặc phá hủy các tệp tin dữ liệu.
    - Xóa nội dung của cả ổ đĩa cứng

Bảo vệ dữ liệu hoặc máy tính của bạn

- Vi rút có thể lây nhiễm vào cả máy tính PC và Mac
  - Các loại vi rút thông thường lây nhiễm qua các mạng doanh nghiệp qua hình thức đính kèm vào thư điện tử. Sau đó nó sẽ gửi các bản sao của chính nó qua thư điện tử đến mọi người trong danh sách liên lạc của bạn
    - Loại vi rút thư điện tử này không phá hủy dữ liệu nhưng lại làm tiêu thụ tài nguyên mạng vì các tin nhắn đó được tạo ra và được gửi tự động từ các hệ thống trong doanh nghiệp đã nhận và mở các tệp tin đính kèm có chứa vi rút
  - Một vài vi rút có tính năng phá hoại rất lớn
    - Có thể xóa các tệp tin dữ liệu, làm tê liệt các chương trình và ghi lại các mục trong Registry

Bảo vệ dữ liệu hoặc máy tính của bạn

- **Sử dụng các chương trình chống vi rút**
  - Quét tất cả các tệp tin đính kèm cùng thư điện tử và các tệp tin có chứa những vi rút mà phần mềm có thể nhận ra để xóa các vi rút mà nó tìm được
  - Tất cả các chương trình chống vi rút đều có tính năng cập nhật các tệp tin định nghĩa vi rút một cách thường xuyên
  - Nếu máy tính của bạn bị nhiễm vi rút, thậm chí cho dù chương trình diệt vi rút của bạn nhận ra nó thì bạn cũng không thể được giải phóng khỏi tình trạng nhiễm vi rút một cách hoàn toàn cho đến khi bạn quét vi rút trên toàn bộ hệ thống
    - chương trình chống vi rút có thể không xóa được vi rút khỏi máy tính nhưng có thể cách ly vi rút khỏi máy tính
    - Điều đó giải thích tại sao vô cùng cần thiết để cài đặt một chương trình chống vi rút trên máy tính và thiết lập chương trình được chạy khi máy tính khởi động để bảo vệ máy tính

Bảo vệ dữ liệu hoặc máy tính của bạn

- Bạn nhận thấy máy tính của mình dường như chạy chậm hơn hoặc bạn đột nhiên thấy có các sự cố xảy ra với các chương trình.
- Các ứng dụng phần mềm không còn hoạt động được, hoặc các chương trình tự động được khởi động.
- Bạn nghe thấy các âm thanh hoặc bản nhạc ngẫu nhiên mà bạn chưa từng nghe trước đó.
- Tên ổ đĩa hoặc tên của các tệp tin dường như đã bị thay đổi, và bạn không phải là người thực hiện điều đó.
- Máy tính của bạn dường như có nhiều tệp tin hoặc ít tệp tin hơn trước đây.
- Bạn nhìn thấy các bản tin lỗi về thiếu tệp tin, thường là các tệp tin chương trình.
- Bạn nhận các bản tin có đính kèm tệp tin từ những người bạn không biết.
- Bạn bắt đầu nhận được nhiều bạn tin có đính kèm tệp tin từ những người bạn biết nhưng trong dòng tiêu đề có chứa tiền tố “RE:” hoặc “FW”, thậm chí bạn chưa từng gửi cho họ bất cứ điều gì

Bảo vệ dữ liệu hoặc máy tính của bạn

- Nếu bạn băn khoăn về chương trình chống vi rút của bạn có thể không bắt được mọi thứ trong máy tính:
  - Quét nội dung của tất cả các đĩa CD, đĩa flash trước khi mở
  - đừng bao giờ mở tệp tin mà không quét nó
  - thử truy cập vào trang Web của chương trình diệt vi rút và quét máy tính trực tuyến.
    - Chương trình quét vi rút trên Web site chứa tất cả những danh sách định nghĩa vi rút mới nhất, vì vậy nó có thể bắt mọi thứ trên hệ thống mà có thể bị bỏ qua bởi chương trình chống vi rút trên máy của bạn
    - Thiết lập tự động cập nhật cho các chương trình diệt vi rút hoặc cập nhật thường xuyên
  - Mang máy tính của mình đến để nhờ chuyên gia kỹ thuật giúp bạn quét các ổ đĩa trong hệ thống để phát hiện các vi rút tiềm năng, và sau đó tìm kiếm giải pháp để xóa hoặc cách ly vi rút.

Bảo vệ dữ liệu hoặc máy tính của bạn

- **Xóa vi rút khỏi máy tính**
  - khi phần mềm diệt vi rút tìm thấy vi rút hoặc các mối đe dọa với máy tính, nó sẽ thông báo cho bạn và cho bạn các tùy chọn để cách ly hoặc xóa mối đe dọa đó
    - Nếu bạn chọn cách ly vi rút, chương trình chống vi rút sẽ đặt tệp tin chứa vi rút vào một khu vực được cách ly để nó không lây nhiễm sang các tệp tin khác
    - Nếu bạn chọn cách xóa tệp tin, chương trình chống vi rút sẽ xóa vĩnh viễn tệp tin đó khỏi hệ thống của bạn
    - Nếu chương trình chống vi rút nhận thấy vi rút đó không thể xóa được, nó vẫn cách ly tệp tin
      - Bạn cần ghi lại các thông tin về tên vi rút khi quá trình quét vi rút hoàn thành và truy cập vào Web site của chương trình chống vi rút để tìm công cụ xóa vi rút này
  - Đôi khi bạn nên xem lịch sử về vi rút trên máy tính của bạn để kiểm tra các tệp tin trong khu vực bị cách ly
    - Xóa bất kỳ tệp tin nào chứa vi rút có thể tồn tại trong máy tính của bạn.

Ngăn ngừa chấn thương cá nhân

- **Làm việc một cách an toàn và thoải mái**
  - Điều kiện để xảy ra RSI là nó xảy ra một cách từ từ theo thời gian
    - xảy ra một cách từ từ theo thời gian và do người sử dụng máy tính thực hiện quá nhiều các hoạt động hoặc những chuyển động lặp lại không ngừng
    - tính thường ảnh hưởng đến tay, cổ tay, cánh tay, nhưng cũng có thể ảnh hưởng đến các khớp khác như khuỷu tay hoặc cổ.
  - Có thể sử dụng các đồ nội thất được thiết kế theo phương pháp công thái học và những kỹ thuật hợp lý để sử dụng máy tính một cách an toàn
    - Công thái học là khoa học thiết kế các trang thiết bị để tạo độ an toàn và thoải mái tối đa cho người sử dụng và hạn chế sự khó chịu khi sử dụng

Ngăn ngừa chấn thương cá nhân

- Để tránh RSI khi làm việc với máy tính gồm có:
  - Ngồi trên ghế hỗ trợ phía sau thấp hơn, có phần tỳ tay và có thể điều chỉnh độ cao.
  - Sử dụng một bàn phím hỗ trợ công thái học.
  - Nghiêng màn hình lên khoảng 10 độ để tránh mỏi cổ.
  - Sử dụng miếng đệm cổ tay để hỗ trợ cổ tay
  - Đặt màn hình cách mặt bạn khoảng 24 đến 30 inch.
  - Điều chỉnh độ phân giải màn hình để văn bản và biểu tượng hiển thị đủ lớn để quan sát một cách rõ ràng.
  - Đảm bảo màn hình không bị nhấp nháy. Tần số màn hình nên để ít nhất là 72 Hz.
  - Tránh nhìn màn hình hiển thị trong một khoảng thời gian dài.

Ngăn ngừa chấn thương cá nhân

- Nếu bạn làm việc với máy tính trong một khoảng thời gian vài giờ trong ngày:
  - Không bao giờ được làm việc hàng giờ bên máy tính mà không dành thời gian để nghỉ ngơi
  - Bề mặt làm việc cần vững chãi; mọi thứ trên bề mặt làm việc cần đặt trên nền phẳng.
  - Màn hình và bàn phím cần đặt trực tiếp trước mặt bạn, không phải đặt ở góc.
  - Cạnh trên của màn hình cần đặt cao hơn mắt khoảng 2 đến 3 inch.
  - Không nên để màn hình bị lóa hoặc phản xạ.
  - Đảm bảo ánh sáng thích hợp để đọc màn hình một cách rõ ràng tại bất kỳ thời điểm nào trong ngày
  - Đặt bất kỳ tài liệu nào mà bạn muốn quan sát khi nhập dữ liệu trong một hộp đựng tài liệu thẳng hàng với màn hình.
  - Khi đã ngồi thật thoải mái, đặt vị trí cánh tay của bạn sao cho cổ tay thẳng và đặt trên mặt phẳng, cánh tay để gần thân người của bạn.
  - Giữ cho đôi chân của bạn đặt trên sàn nhà và đùi cùng cánh tay đặt song song với sàn nhà

Ngăn ngừa chấn thương cá nhân

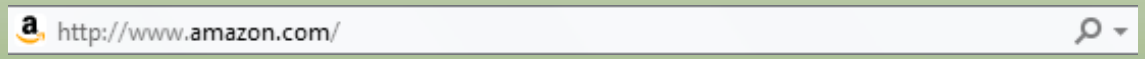
- Bàn phím cần đặt ở một vị trí thoải mái để cánh tay bạn không phải di chuyển lên hay xuống khó khăn trên bàn phím
- Điều này cũng đúng đối với chuột
- Khi bạn nhập dữ liệu, cố gắng không uốn cong cổ tay
- Nếu bạn cảm thấy căng thẳng trên cổ tay, cánh tay hoặc ngón tay khi sử dụng chuột truyền thống, bạn thử chuyển sang dùng chuột bi, chuột lớn hơn, hoặc xem xét sử dụng một thiết bị sử dụng công nghệ cảm ứng
- Những hướng dẫn trên cũng có thể áp dụng cho người sử dụng máy tính xách tay
  - Nếu bạn muốn đặt máy tính xách tay trên đùi của bạn, bạn cần ngồi ở vị trí thích hợp tuân theo những hướng dẫn trên, và nếu có thể bạn nên đặt máy tính xách tay trên một khay hoặc một thứ gì đó vững chãi để làm việc

Bảo vệ bản thân khi trực tuyến

- Need to be careful while online and protect personal information
- One guideline is ensure passwords are as secure as possible
  - Periodically change to ensure further protection
- For sites where you want to register for further information, use alternate email address
  - Helps reduce number of potential junk messages received in main email account
  - Use main email address only for sites where you purchase items and as general Inbox

Bảo vệ bản thân khi trực tuyến

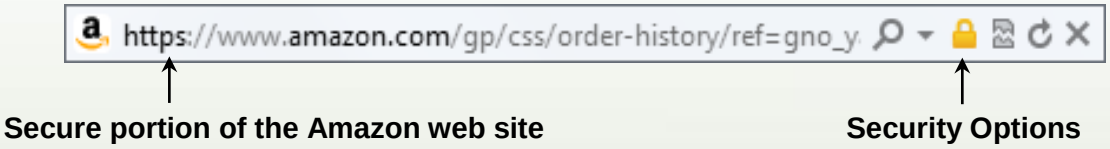
- **Mua hàng trực tuyến**
  - Bạn càng cảm thấy an toàn khi thực hiện các giao dịch trực tuyến như các hoạt động liên quan đến ngân hàng hoặc mua hàng trực tuyến thì sẽ quyết định đến sự tin tưởng của bạn khi thực hiện các hoạt động đó càng nhiều
  - Nếu một công ty cung cấp đơn hàng quá hấp dẫn để có thể là sự thật, bạn hãy nghiên cứu kỹ lời mời đó
    - Bạn cũng cần lưu ý tương tự như khi có ai đó mời bạn một món hàng ngoài đời thực
  - Kiểm tra địa chỉ Web để xem các tùy chọn bảo mật đi kèm với Web site



    - Khi bạn quyết định thiết lập một tài khoản với nhà phân phối đó, địa chỉ Web thay đổi thành:

    - Mỗi khi bạn nhìn thấy https, nghĩa là bạn đang nằm trong Web site bảo mật của nhà phân phối để có thể thực hiển một giao dịch tài chính

Bảo vệ bản thân khi trực tuyến



- Khi bạn gửi thông tin cá nhân tới một trang thương mại điện tử, bạn kết nối với trang qua một kết nối bảo mật, như được chỉ rõ trên URL (https) cũng như
  - Điều này chỉ ra bạn có một kết nối *Secure Socket Layer (SSL)* và thông tin được truyền tải ở dạng mã hóa
  - Khi thông tin điện tử được mã hóa, một khóa được áp dụng cho văn bản để chuyển nó thành một tài liệu dạng không đọc được. Nó được gọi là khóa công khai.
  - Khi một đối tác khác nhận được tài liệu đã được mã hóa, họ áp dụng một khóa vào tài liệu để "giải mã" và chuyển văn bản về dạng gốc
  - Khóa đó được gọi là khóa bí mật và không bao giờ được truyền tải qua Internet

Bảo vệ bản thân khi trực tuyến

- Đừng đưa thông tin thẻ tín dụng của bạn một cách bừa bãi.
  - Có nhiều tùy chọn khác để thực hiện thanh toán trực tuyến khi mua hàng mà không cần thẻ tín dụng
  - Cũng chú ý rằng khi bạn mua hàng trực tuyến, một khi bạn nhấp chuột vào nút thích hợp để mua hàng thực sự với thẻ tín dụng, nhà phân phối sau đó sẽ thực hiện giao dịch ở phía họ
- Một công ty đã đăng ký tên miền và cung cấp dịch vụ thương mại điện tử sẽ có www ở trước tên miền, cũng như biểu tượng khóa chưa được kích hoạt cho đến khi bạn đăng nhập tài khoản vào Web site đó
  - Một trang thương mại điện tử cũng sẽ có một chính sách hoặc điều lệ riêng ở trên trang Web của họ. Bạn cần đọc những điều khoản này để xem các điều kiện hoặc yêu cầu mà bạn phải tuân theo khi thực hiện giao dịch với nhà phân phối này
- Khi bạn truy cập vào trang nào đó để mua sản phẩm hoặc dịch vụ, bạn cần kiểm tra địa chỉ của Web site có được viết một cách chính xác, và trang đó được thiết lập theo đúng thứ bạn mong muốn từ công ty
  - giúp bạn xác định được đúng Web site của nhà phân phối mà bạn muốn giao dịch

Bảo vệ bản thân khi trực tuyến

- **Lừa đảo thông tin trực tuyến**
  - Phishing: tiến trình thu thập thông tin cá nhân từ ai đó với mục đích thực hiện một cuộc tấn công phạm tội
  - *Spoofing*: là khi một người hoặc Web ste xuất hiện như một tổ chức hợp pháp có giao diện mô phỏng y hệt công ty hợp pháp và sẽ thu thập thông tin cá nhân của bạn với mục đích bất hợp pháp
  - Identity theft: thông tin cá nhân bị đánh cắp mà không có sự cho phép từ chủ sở hữu với mục đích gian lận hoặc phạm tội như lấy thông tin thẻ tín dụng, các giao dịch tài chính hoặc mạo danh ai đó

Bảo vệ bản thân khi trực tuyến

- **Những thông tin nào tôi nên chia sẻ?**
  - Lượng thông tin và loại thông tin bạn muốn chia sẻ sẽ tùy thuộc vào cách riêng của bạn.
  - Hạn chế trong việc chia sẻ hoặc kinh doanh thông tin cá nhân với bất kỳ ai mà bạn trò chuyện trực tuyến
  - Hãy cẩn thận khi bạn tin tưởng một ai đó trong thế giới ảo
  - Tránh gửi các thông tin cá nhân như tuổi, giới tính, số điện thoại,… trực tuyến và không bao giờ đi gặp gỡ một mình với ai đó mà bạn quen trên mạng.
  - đừng chia sẻ thông tin cá nhân của bạn khi sử dụng bất kỳ chương trình mạng xã hội hoặc trò chuyện trực tuyến.
  - Bạn cần rất thận trọng khi đăng bài viết và hình ảnh của mình lên các trang mạng xã hội

Bảo vệ bản thân khi trực tuyến

- **Bảo vệ sự riêng tư của bạn**
  - Vi phạm quyền riêng tư của bạn xảy ra khi thông tin cá nhân của bạn bị chia sẻ hoặc bị bán cho người khác và không có sự đồng ý của bạn
  - Bất kỳ khi nào bạn ghé thăm một trang web, một vài thông tin về bạn đã bị mất
    - Không có gì đảm bảo riêng tư tuyệt đối khi bạn tham gia internet
  - Người khác có thể lưu vết thông tin bạn đã từng ghé thăm các trang Web nào trên Internet
    - Một vài trang Web lưu vết các hoạt động của bạn khi bạn ghé thăm
  - đọc kỹ các điều khoản riêng tư trên Web site
    - chỉ ra rõ ràng những thông tin nào họ tìm kiếm và kế hoạch sử dụng thông tin của họ

Bảo vệ bản thân khi trực tuyến

- Đừng điền vào bất kỳ biểu mẫu trực tuyến trừ khi bạn muốn thứ gì đó từ Web site
- Nếu bạn muốn đăng ký một Web site, cần chắc chắn không lừa chọn các tùy chọn xác định bạn muốn nhận thư điện tử từ các công ty thứ ba về các sản phẩm hoặc dịch vụ liên quan
- Xóa lịch sử các trang Web mà bạn đã ghé thăm
- *Nhìn trộm (Shoulder surfing)* là cách lấy thông tin nhạy cảm bằng cách nhìn trộm thông tin sau lưng một ai đó
- Việc mua phần mềm của hãng thứ ba cũng có thể giải quyết những sự cố về tính riêng tư
- Bạn cần tránh sử dụng các chương trình add-in hoặc các thanh công cụ được cài đặt cùng với chương trình mà bạn tải về với mục đích thử nghiệm hoặc giải trí

Bảo vệ bản thân khi trực tuyến

- Quy luật dễ nhất là theo cảm nhận cơ bản của bạn
- Có rất nhiều nguồn tham khảo trên Internet thảo luận và giải thích các sự cố về tính riêng tư một cách kỹ lưỡng hơn và cung cấp các đề xuất về cách thức bạn có thể bảo vệ bản thân và gia đình khi bạn trực tuyến
- Có rất nhiều cách đơn giản để ngăn chặn người khác lấy được thông tin hoặc liên lạc với bạn
  - sử dụng công cụ Opt-out Tool được phát triển bởi Network Advertising Initiative để quét máy tính của bạn và chỉ ra bất kỳ công ty nào đặt các tệp tin cookie quảng cáo trên máy tính của bạn

Tổng kết bài học

- các tiêu chuẩn truyền thông chuyên nghiệp
- cách thức để tránh các hành vi không phù hợp khi trực tuyến
- sở hữu trí tuệ, bản quyền và các quy định cấp phép
- công thái học và cách thiết lập máy tính của bạn
- bảo vệ máy tính khỏi các mối đe dọa phần mềm
- vi rút là gì và cách ngăn ngừa chúng gây tổn hại máy tính của bạn
- cách thức tự bảo vệ khi giao dịch thương mại điện tử hoặc mua hàng

Câu hỏi ôn tập

- 1.Khi bạn gửi thư điện tử đến một nhà tuyển dụng tiềm năng, phong cách viết nào bạn nên sử dụng cho tiêu đề thư và sơ yếu lý lịch?

  a.Kinh doanh và chuyên nghiệp

  b.Casual Bình thường

  c.Kết hợp với một vài yếu tố hài hước trong kinh doanh

  d.Kết hợp a và b

2.Ví dụ này là gì? Bạn đã viết một bài nghiên cứu xuất sắc về các điều kiện kinh tế trong năm 2010. Giáo viên của bạn đọc được một báo cáo khác có những phần giống hệt với bài nghiên cứu của bạn.

a.Vi phạm bản quyền

c.Đạo văn

b.Sử dụng hợp lý

d.Creative commons

Câu hỏi ôn tập

3.Phỉ báng khác với vu khống như thế nào?

a.Phỉ báng chỉ áp dụng khi nói về những người nổi tiếng.

b.Vu khống chỉ xảy ra khi có những điều nói sai bằng lời nói trong khi đó phỉ báng là bằng văn bản.

c.Kết quả của việc vu khống bị phạt tiền nhiều hơn.

d.Không có sự khác biệt.

e.a hoặc c

4.Để chọn một mật khẩu bảo mật, những hướng dẫn nào bạn nên xem xét?

a.Tối đa 8 ký tự.

b.Kết hợp các ký tự in hoa và in thường.

c.Sử dụng tất cả ký tự số.

d.Sử dụng ít nhất một ký hiệu.

e.Tối thiểu 8 ký tự.

f.Tất cả những điều trên.

g.b, d & e.

Câu hỏi ôn tập

5.Các tệp tin dư thừa là gì?

a.Các tệp tin nằm trên máy tính tại mọi thời điểm.

b.Các tệp tin của hệ điều hành giúp bạn cài đặt máy in (hoặc các thiết bị khác).

c.Các tệp tin xác định và kiểm tra định danh cùng mật khẩu mạng của bạn.

d.Các tệp tin còn lại trên thiết bị lưu trữ sau khi một chương trình ứng dụng bị gỡ bỏ.

6.Trước khi thêm bất kỳ đặc tính bổ sung nào vào chương trình chống vi rút mới được cài đặt, bạn nên làm gì?

a.Nhờ sự trợ giúp của nhà quản trị mạng.

b.Cài đặt các tệp tin đã tải có chứa bất kỳ vi rút, phần mềm gián điệp hoặc phần mềm quảng cáo nào.

c.Quét vi rút, phần mềm gián điệp hoặc phần mềm quảng cáo.

d.Khởi động lại nếu cần.

Câu hỏi ôn tập

7.Bên cạnh việc kiểm tra với người quản trị của nhà trường để hướng dẫn sử dụng máy tính tại trường học, bạn còn có thể kiểm tra ở đâu nữa?

a.Thư viện hoặc thủ thư của trường học.

b.Các bài viết trong tạp chí hướng dẫn cách sử dụng máy tính.

c.Bố mẹ của bạn.

d.Luật sư của bạn.

e.Bất kỳ đáp án nào ở trên.

f.a hoặc b

8.Một vài cách thức nào bạn có thể bảo vệ sự riêng tư của mình khi trực tuyến?

a.Không điền vào bất kỳ biểu mẫu trực tuyến nào khi bạn không hứng thú với việc thu thập thông tin từ công ty đó.

b.Sử dụng một bí danh trên các diễn đàn hoặc nhật ký cá nhân công khai.

c.Không kiểm tra tùy chọn nhận thông tin từ các đối tác bán lẻ của công ty.

d.Bất kỳ đáp án nào ở trên.

e.a hoặc b