IC3 GS6 – LEVEL 1

Bài 7

AN TOÀN VÀ BẢO MẬT

Lecturer: Nguyễn Phát Tài

Master of Science (Asian Institute of Technology - AIT)
Master of Microsoft Office Specialist 2010, 2013, 2016, 2019/365
Microsoft Master Trainer
IC3 Authorized Educator (IC3 GS3, GS4, GS5, GS6)

Mục tiêu bài học

- Mô tả các mối đe dọa bảo mật kỹ thuật số
- Bảo vệ thiết bị và nội dung kỹ thuật số
- Nhận thức về công nghệ thu thập dữ liệu
- Xác định các rủi ro sức khỏe liên quan đến việc sử dụng công nghệ kỹ thuật số

Sự cần thiết của bảo mật (Security)

- Ngay khi kết nối máy tính với mạng, người dùng đã phơi bày hệ thống và thông tin của mình đã lưu trữ trên mạng trước các rủi ro tiềm ẩn liên quan đến mạng.
- Thông tin được lưu trữ trên một máy tính có thể được truy cập bởi bất kỳ máy tính nào được kết nối với mạng. Nếu mạng truy cập Internet thì rủi ro càng tăng lên.
- Tin tặc sử dụng nhiều phương pháp khác nhau để có được những gì họ muốn.

Sự cần thiết của bảo mật (Security)

- Virus (Viruses)
  - Là một chương trình độc hại được con người thiết kế để kiểm soát các hoạt động của hệ thống, làm hỏng/phá hủy dữ liệu:
    - Hiển thị tin nhắn vô hại trên màn hình;
    - Chiếm dụng tất cả bộ nhớ khả dụng, làm chậm hoặc tạm dừng tất cả các quy trình khác;
    - Làm hỏng hoặc phá hủy các tập tin dữ liệu;
    - Xóa nội dung của toàn bộ đĩa cứng.

Sự cần thiết của bảo mật (Security)

- Virus được tải vào và hoạt động trong máy tính mà người dùng không hay biết.
- Tất cả các virus máy tính đều lây lan sang máy tính khác thông qua:
  - Mạng;
  - Tập tin đính kèm email;
  - Các chương trình/tập tin tải xuống từ Internet;
  - Đĩa, đĩa CD hoặc ổ đĩa flash bị nhiễm.

Sự cần thiết của bảo mật (Security)

- Sâu máy tính (Worm)
  - Là loại chương trình tự sao chép, làm tiêu tốn nhiều tài nguyên hệ thống và mạng.
  - Sâu máy tính tự động lây lan từ máy tính này sang máy tính khác
  - Sâu máy tính có thể cư trú trong bộ nhớ hoạt động và tự sao chép trên mạng và thường lây lan qua Internet thông qua các tập tin đính kèm email.

Sự cần thiết của bảo mật (Security)

- Trojans
  - Là loại chương trình được thiết kế để tin tặc truy cập từ xa vào hệ thống máy tính mục tiêu.
  - Trojan ẩn bên trong các ứng dụng (các trò chơi, các ứng dụng tiện ích,…). Trojans không tự sao chép.
  - Trojan cho phép tin tặc kiểm soát hệ thống đích, đánh cắp thông tin, cài đặt phần mềm khác (bao gồm cả virus), tải xuống hoặc tải lên tập tin hoặc làm sập hệ thống.
  - Trojan bị nhiễm qua việc tải xuống phần mềm, qua các trang web có chứa các điều khiển ActiveX, qua tập tin đính kèm email.

Sự cần thiết của bảo mật (Security)

- Malware: Phần mềm gián điệp (Spyware), phần mềm quảng cáo (Adware)
  - Phần mềm gián điệp được bí mật cài đặt trên hệ thống và thu thập thông tin cá nhân/riêng tư mà không có sự đồng ý hoặc hiểu biết của người dùng.
  - Phần mềm quảng cáo là loại phần mềm tự động hiển thị/tải xuống quảng cáo.
  - Các công ty có cả danh tiếng tốt và xấu đã bao gồm mã phần mềm gián điệp trong phần mềm của họ.

Sự cần thiết của bảo mật (Security)

- Ngoài việc giám sát hoạt động người dùng trên Internet và chuyển thông tin đến người khởi tạo phần mềm gián điệp, phần mềm gián điệp còn thực hiện các chức năng:
  - Quét tập tin trên ổ cứng;
  - Đọc cookie;
  - Giám sát tổ hợp phím;
  - Cài đặt các phần mềm gián điệp khác;
  - Thay đổi trang chủ mặc định trong trình duyệt Web;
  - Tự động gửi thông tin cho nhà phát triển phần mềm gián điệp.

Sự cần thiết của bảo mật (Security)

- Kết nối mạng
  - Là người dùng đã kết nối toàn bộ hệ thống của mình với các hệ thống khác trên cùng một mạng.
  - Luôn luôn có rủi ro tiềm ẩn, nhất là khi kết nối với các hệ thống bị nhiễm.
  - Kết nối có dây (Wired Connections)
    - Kết nối khá an toàn;
    - Sự bảo đảm này sẽ không được áp dụng khi kết nối vào mạng có dây công cộng;
    - Không có gì đảm bảo rằng tất cả mọi người kết nối với mạng đều sử dụng phần mềm chống virus đã được cập nhật

Sự cần thiết của bảo mật (Security)

- Kết nối không dây (Wireless Connections)
  - Những rủi ro tương tự có thể có từ kết nối có dây đều áp dụng cho các kết nối Wi-Fi;
  - Không ai có thể đảm bảo rằng tất cả các hệ thống được kết nối đều không có virus/tin tặc.
  - Mạng ad-hoc rất nguy hiểm do không có điểm truy cập trung tâm cũng như không có yêu cầu xác thực.
- Giảm thiểu rủi ro
  - Hãy luôn xác định với HĐH là mạng Công cộng (Public);
  - Tránh tham gia vào các mạng ad-hoc.

Sự cần thiết của bảo mật (Security)

- Sử dụng máy tính công cộng
  - Bất kỳ ai có quyền truy cập vật lý vào máy tính công cộng đều có thể truy cập bất kỳ thông tin nào được lưu trữ trên đó.
  - Cookie và bất kỳ thông tin nào khác được lưu trữ trên máy tính đều có thể truy cập được.
  - Để đảm bảo an toàn:
    - Đăng xuất khỏi tài khoản trực tuyến
    - Xóa bộ nhớ cache và cookie
    - Đăng xuất (Log out) khỏi Hệ điều hành

Sự cần thiết của bảo mật (Security)

- Kỹ thuật tấn công Social Engineering
  - Là các mánh khóe, kỹ thuật tấn công nhắm vào bản tính xã hội của con người, thứ mà không hề tồn tại trong máy móc (tấn công phi kỹ thuật).
  - Là quá trình đánh lừa người dùng hệ thống, nhằm phá vỡ hệ thống an ninh, lấy cắp dữ liệu hoặc tống tiền.
  - Các mục tiêu tiêu biểu bao gồm bất kỳ ai có quyền truy cập thông tin vào các hệ thống: thư ký, người gác cổng, quản trị viên, nhân viên an ninh,…

Sự cần thiết của bảo mật (Security)

- Giảm thiểu rủi ro của Kỹ thuật tấn công Social Engineering
  - Nhận ra các chiến lược kỹ thuật xã hội phổ biến:
    - Đóng vai trò là một kỹ thuật viên và sử dụng thẩm quyền đó để khiến nhân viên tiết lộ thông tin, thay đổi cấu hình máy chủ,…
    - Giả danh/nhân danh người có thẩm quyền để dọa nhân viên/người bảo vệ để được phép truy cập vật lý vào tòa nhà.
    - Gửi tin email trông có vẻ chính thức/trang trọng cho tất cả nhân viên với các hướng dẫn khiến họ tiết lộ thông tin nhạy cảm.

Sự cần thiết của bảo mật (Security)

- Lừa đảo (Phishing)
  - Là quá trình cố gắng thu thập thông tin nhạy cảm (mật khẩu, chi tiết thẻ tín dụng) bằng cách giả vờ là một thực thể đáng tin cậy.
  - Thông thường, kẻ lừa đảo gửi một email hợp pháp có vẻ như đến từ một nguồn hợp pháp như ngân hàng/công ty thẻ tín dụng.
  - Thông báo email thường bao gồm một cảnh báo sai và hướng dẫn nạn nhân thực hiện một hành động cụ thể.

Sự cần thiết của bảo mật (Security)

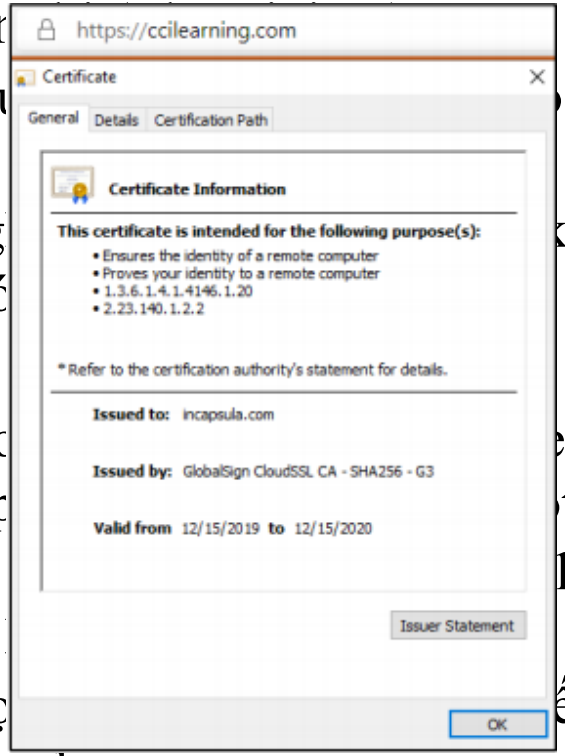
- Để bảo vệ bản thân khỏi lừa đảo:
  - Kích hoạt các tính năng chống lừa đảo trong trình duyệt;
  - Kiểm tra một trang web không xác định (trong Internet Explorer, chọn Tools → Safety → nhấp chọn Check This Website);
  - Tránh nhấp vào liên kết trong email nếu email dường như đến từ ngân hàng, công ty thẻ tín dụng hoặc cơ quan chính phủ;
  - Trước khi đăng nhập vào một trang web, hãy kiểm tra thanh Địa chỉ để chắc chắn rằng địa chỉ bắt đầu bằng tên trang web hợp pháp.

Sự cần thiết của bảo mật (Security)

- Thực hiện các giao dịch thương mại điện tử an toàn
  - Chọn lọc
    - Hãy mua sắm trực tuyến từ các công ty có uy tín và nổi tiếng về việc cung cấp:
      - Dịch vụ khách hàng tốt;
      - Giao hàng đáng tin cậy;
      - Chính sách hoàn trả công bằng và dễ dàng.

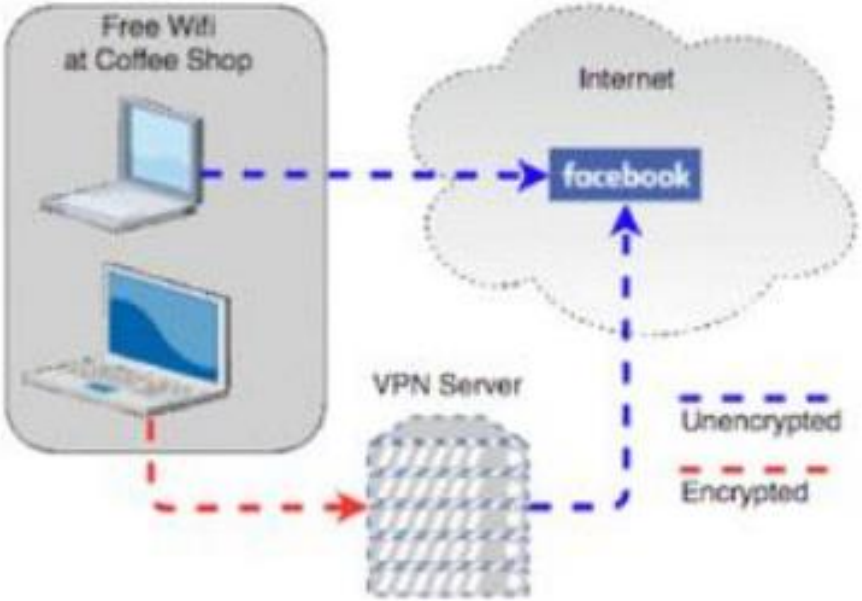
Sự cần thiết của bảo mật (Security)

- Thực thi tính hoài r
  - Nếu một công ty cu vẻ quá tốt, hãy nghiên cứu thỏa thuận đó.
  - Hãy chắc chắn ng khi mua bất cứ thứ gì trực tuyến từ công ty đó
- Luôn sử dụng giao
  - Thực hiện các giao t, với các máy chủ web sử dụng giao thức http tocol Secure).
  - Giao thức https và hanh địa chỉ cho biết người dùng đang ở trong web của nhà cung cấp.
  - Nhấp vào biểu tượ ết liên quan đến chứng chỉ bảo mật của trang web



Sự cần thiết của bảo mật (Security)

- Mạng riêng ảo VPNs (Virtual Private Networks)
  - Trước đây, t ng qua các máy chủ truy cập ại chuyên dụng.
  - Trong hầu h ừ xa được thực hiện bằng kế
  - VPN là kết n, cho phép liên lạc riêng tư, ài bằng cách sử dụng Interne ng



Xác định rủi ro

- Sử dụng VPN
  - Người dùng phải cài đặt và khởi chạy phần mềm máy khách VPN để mở kết nối với máy chủ VPN.
  - Các phần mềm VPN phổ biến: Teamviewer, Ultraviewer.
  - Người dùng phải đăng nhập bằng tên người dùng và mật khẩu hợp lệ.

Tên người dùng và mật khẩu

- Tên người dùng và mật khẩu có tác dụng bảo vệ tài khoản của người dùng khỏi sự truy cập trái phép.
- Tài khoản người dùng được liên kết với các quyền và sự ủy quyền cụ thể cả trên hệ thống cục bộ và trên hệ thống mạng.
- Để bảo vệ tài khoản, người dùng cần có một mật khẩu "mạnh":
  - Sử dụng tối thiểu tám ký tự, với 15 ký tự được coi là an toàn nhất;
  - Bao gồm hỗn hợp các số, chữ cái, ký hiệu và chữ in hoa;
  - Chọn mật khẩu dễ nhớ đối với mình, nhưng khó đoán đối với người khác;

Tên người dùng và mật khẩu

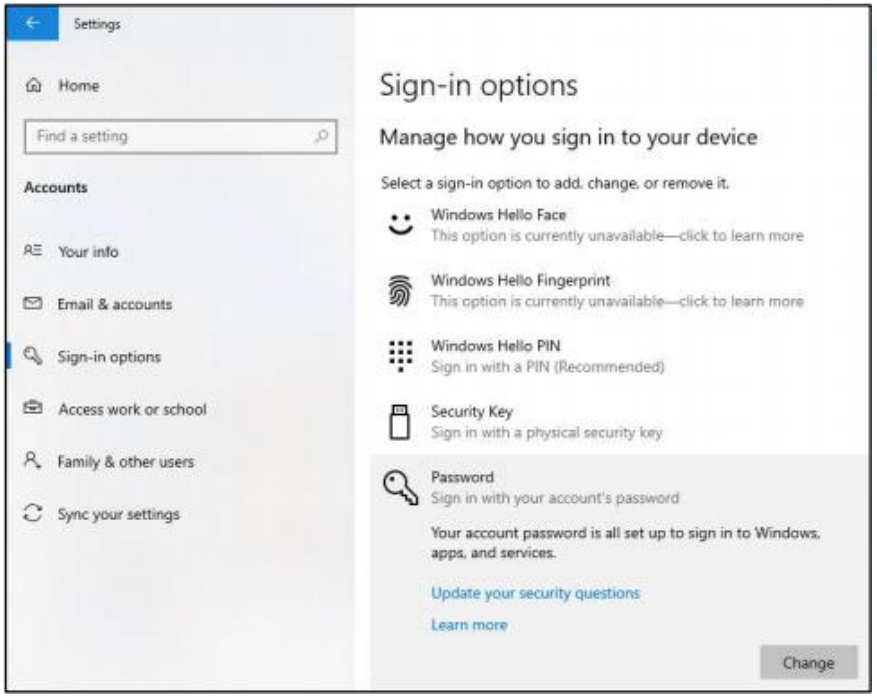
- Tránh sử dụng tên của những người gần gũi (thành viên trong gia đình, tên thú cưng);
- Tránh sử dụng các biến thể của tên hoặc bao gồm tên, địa chỉ hoặc ngày sinh trong mật khẩu;
- Tránh sử dụng một biến thể của mật khẩu có thể dễ đoán, chẳng hạn như PasswordJan, Password-Feb, password001, password_003, DrewJ12, DrewF12, pa$$w0rd,…

Tên người dùng và mật khẩu

- Giữ tài khoản an toàn
  - Không bao giờ chia sẻ thông tin tài khoản cho người khác;
  - Nếu vô tình chia sẻ thông tin đăng nhập, hãy thay đổi ngay lập tức;
  - Đừng ẩn giấu mật khẩu gần máy tính (một tờ giấy dính dưới bàn phím, trong ngăn bàn,…);
  - Không sử dụng cùng một mật khẩu cho tất cả các tài khoản.

Tên người dùng và mật khẩu

- Thay đổi mật khẩu
  - Các thao tác thay đổi mật khẩu trong Windows 10: Chọn Start → Settings → Accounts → Sign-in options → Chọn Password → Chọn Change → Nhập Password cũ → Nhập Password mới → Nhập xác nhận Password và gợi ý Password (Hint) → Next → Finish.



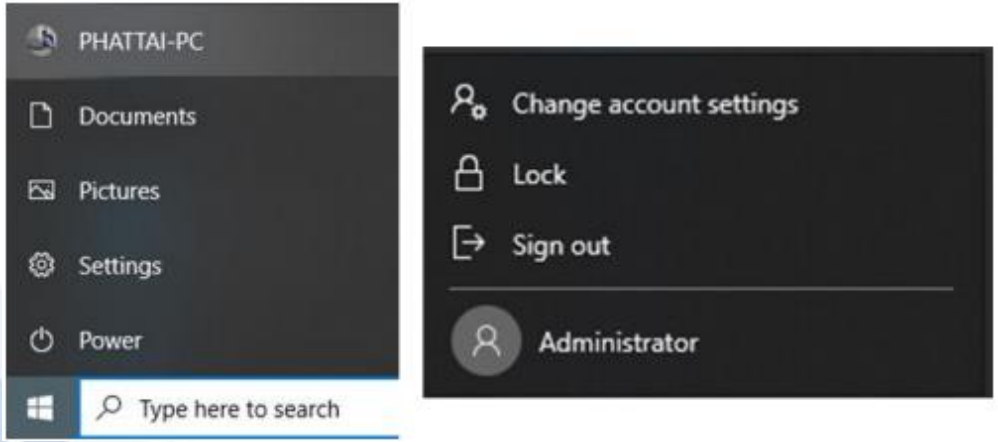
Tên người dùng và mật khẩu

- Nếu người dùng là thành viên của một miền trên mạng (Domain network), người dùng sẽ được yêu cầu thay đổi mật khẩu thường xuyên hơn:

  Nhấn Ctrl+Alt+Delete → Chọn Change a password → Nhập Password cũ → Nhập Password mới → Nhập Password xác nhận → Nhấn Enter.

Tên người dùng và mật khẩu

- Khóa hệ thống (Locking the System)
  Chọn Start → Chọn biểu tượng tài khoản người dùng ở góc trên bên phải của Start menu → Chọn Lock.



Tên người dùng và mật khẩu

- Xóa bộ nhớ Cache của trình duyệt
  - Là một thư mục trên ổ cứng lưu trữ các tập tin đã tải xuống từ các trang web, hình ảnh hoặc font chữ.
  - Bộ nhớ cache nhằm cải thiện hiệu suất của trình duyệt.
  - Để cập nhật nội dung, bấm F5 để yêu cầu trình duyệt cập nhật trang mới từ máy chủ.

Công nghệ thu thập dữ liệu

- Cookie
  - Là các tập tin văn bản nhỏ được đặt trên máy tính người dùng mỗi khi truy cập một trang web.
  - Cookie lưu trữ thông tin về sở thích, thoái quen duyệt web của người dùng.
  - Bản thân cookie không nguy hiểm, nhưng chúng có thể được sử dụng để lưu trữ tên người dùng và mật khẩu nếu nhấp vào "Yes" khi trình duyệt của bạn hỏi có muốn lưu trữ thông tin hay không?

Công nghệ thu thập dữ liệu

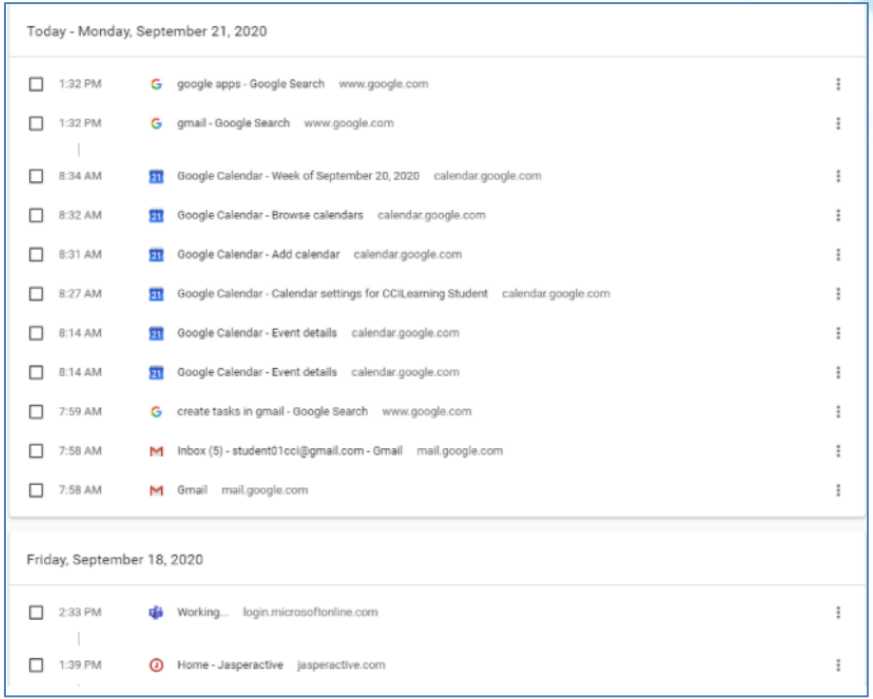
- Có nhiều loại cookie khác nhau:
  - First-party cookies: Đến từ trang web đang xem.
  - Third-party cookies: Đến từ một trang web khác với trang web đang xem (trang web cung cấp nội dung quảng cáo trên trang web đang xem).
  - Session cookies: Chỉ được lưu trữ trong bộ nhớ tạm thời và bị xóa khi đóng trình duyệt web.
  - Theo mặc định, trình duyệt cho phép cookie hoạt động.
  - Người dùng có thể kiểm soát cách xử lý cookie trong mỗi trình duyệt.

Công nghệ thu thập dữ liệu

- Lịch sử duyệt web (Browsing History)
  - Mỗi trình duyệt bao gồm một chức năng History lưu trữ các URL đã truy cập vào trong thư mục History của trình duyệt.
  - Cung cấp cách thuận tiện để truy cập lại các trang web.

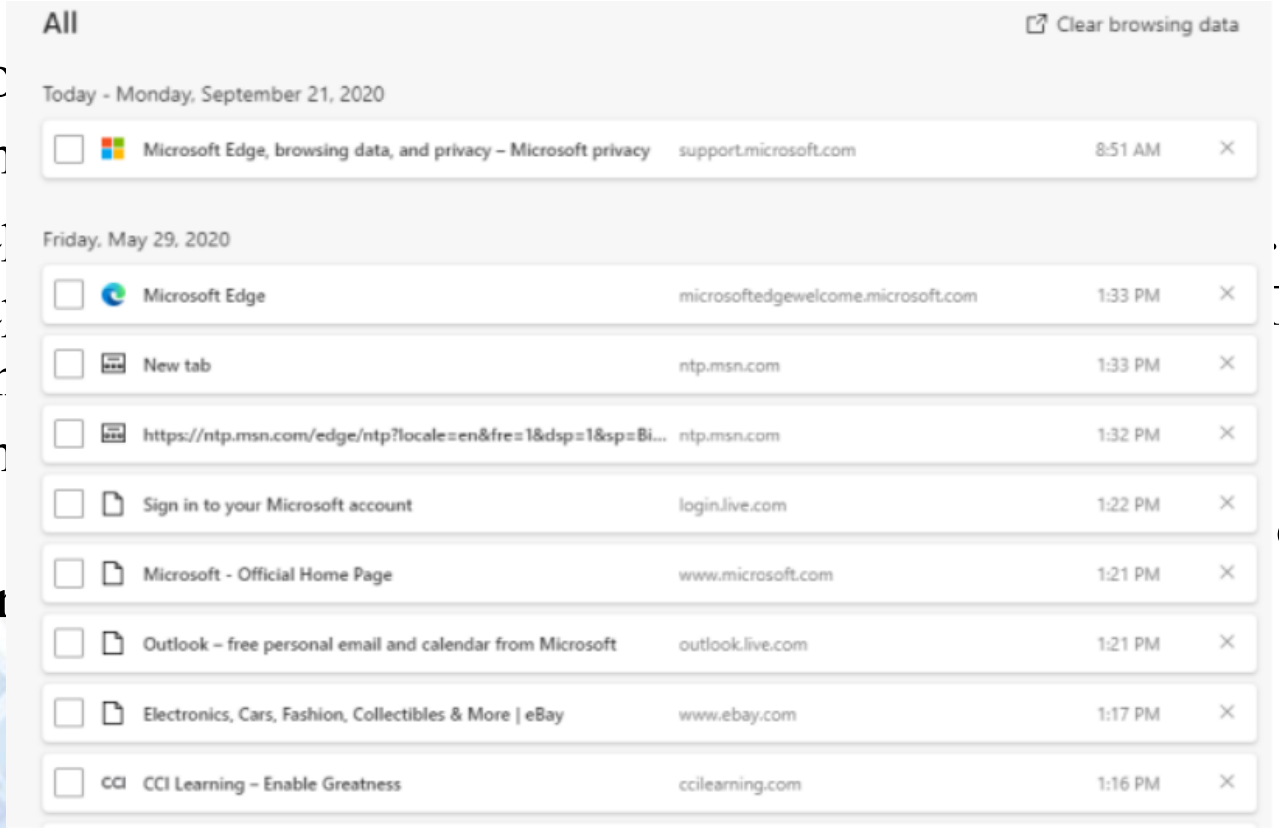
Công nghệ thu thập dữ liệu

- Google Chrome:
  - Nhấp vào Customize and control Google Chrome, trỏ tới History → nhấp vào History.
    - Để truy cập vào một trang web, nhấp vào liên kết trong danh sách.
    - Để xóa một hay nhiều URL, chọn hộp kiểm cho trang web → nhấp vào Remove selected items.



Công nghệ thu thập dữ liệu

- Micro
  - Bấm
  - Nhấ
  - Nhấ
    danh
  - Bấm
  - Trỏ
    mở



Trong một

danh sách

Công nghệ thu thập dữ liệu

- Xóa lịch sử duyệt web
  - Nếu sử dụng web cho nhiều tác vụ, thư mục History có thể trở nên lớn không thể quản lý được.
  - Xóa lịch sử duyệt web giúp bảo vệ quyền riêng tư, đặc biệt nếu đang sử dụng PC được chia sẻ hoặc công khai.
  - Khi xóa lịch sử duyệt web, người dùng cũng có thể xóa các tập tin Internet tạm thời, cookie, dữ liệu trang web, dữ liệu biểu mẫu và mật khẩu được lưu trữ.

Công nghệ thu thập dữ liệu

- Duyệt web riêng tư (Private Browsing)
  - Duyệt web riêng tư trong Google Chrome sẽ diễn ra trên tab "ẩn danh" (“incognito”).
    - Bấm Setting, sau đó nhấp vào New incognito window.
    - Trên thiết bị di động chạy trình duyệt Chrome, nhấp vào nút Menu, nhấp vào New incognito tab.
  - Duyệt web riêng tư trong Internet Explorer, Microsoft Edge diễn ra trong tab "InPrivate".
    - Trong Microsoft Edge, nhấp vào nút Settings and More, nhấp vào New InPrivate window.
  - Để dừng duyệt web riêng tư, hãy đóng mọi tab duyệt web riêng tư đang mở

Máy tính và sức khỏe

- Bắt nạt trên mạng (Cyber Bullying)
  - Tạo ra các mối đe dọa trực tuyến.
  - Sử dụng ngôn từ kích động thù địch trong phương tiện truyền thông xã hội hoặc tin nhắn điện thoại di động.
  - Tin đồn lan truyền.
  - Đưa ra ý kiến bình luận gây tổn thương.
  - Chụp những bức ảnh đáng xấu hổ mà không có ý kiến hoặc sự đồng ý của nạn nhân, sau đó đăng chúng lên.

Máy tính và sức khỏe

- Bạn nên làm những gì?
  - Hãy nhớ rằng nó không phải là lỗi của bạn.
  - Bạn nên bỏ qua nó nếu có thể.
  - Kết thúc tất cả các thông tin liên lạc với một kẻ bắt nạt.
  - Giữ một bản ghi cứng các tin nhắn bắt nạt bạn nhận được.
  - Nếu bạn là trẻ vị thành niên, hãy tâm sự với một người lớn đáng tin cậy, người cố vấn hoặc người giám sát.
  - Bạn có thể báo cáo sự cố cho các thầy cô tại trường học hoặc cảnh sát.

Máy tính và sức khỏe

- Những gì không nên làm
  - Không trả lời tin nhắn có ý đe dọa trở lại kẻ tấn công.
  - Không chuyển tiếp nội dung hoặc tin nhắn bắt nạt do có thể vô tình khuyến khích người khác chuyển sang bạo lực thay cho bạn.
  - Đừng bao giờ tin kẻ bắt nạt;
  - Không cho phép bất cứ ai phá hủy lòng tự trọng của bạn

Máy tính và sức khỏe

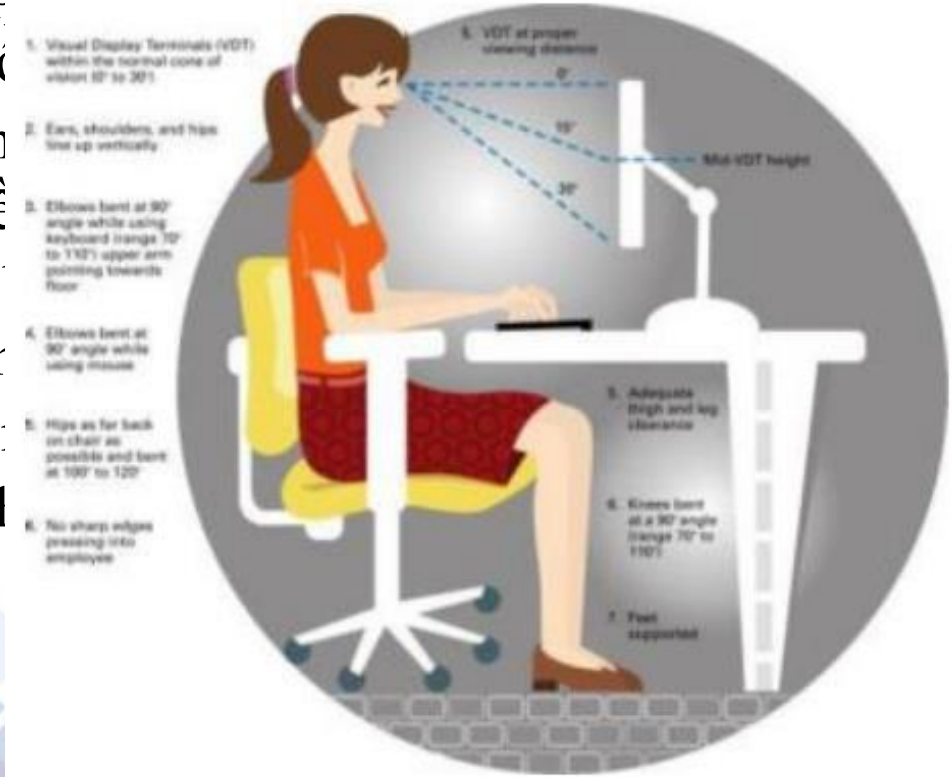
- Quấy rối
  - Khi ai đó gửi cho bạn một bình luận hay một bài đăng đe dọa hoặc một cái gì đáng ngờ. Nếu điều này tiếp tục từ cùng một người thì có thể dẫn đến tình huống quấy rối như rình rập hoặc tống tiền.
    - Rình rập xảy ra khi ai đó liên tục giao tiếp với bạn, thậm chí theo dõi mọi hoạt động bạn.
    - Tống tiền có thể xảy ra khi ai đó tuyên bố có thông tin và cố gắng thuyết phục bạn đưa ra một số tiền bồi thường để giữ cho thông tin đó không được công khai.

Máy tính và sức khỏe

- Những thực hành công thái học tốt (Ergonomics)
  - Hội chứng RSI (Repetitive Strain Injury) trở nên phổ biến khi làm việc trên máy tính trong thời gian dài.
  - Hội chứng RSI xảy ra dần dần theo thời gian, do sự lặp lại liên tục nhiều lần của một hoạt động/chuyển động, đặc biệt nếu hoạt động hoặc chuyển động không tự nhiên.
  - Để chống lại RSI, người dùng có thể sử dụng đồ nội thất được thiết kế công thái học và các kỹ thuật phù hợp.

Máy tính và sức khỏe

- Các biện p… thực hiện để ngăn chặn RSI khi sử dụng máy tính bao gồ…
  - Ngồi trên… và điều chỉnh được chiề…
  - Sử dụng … ngơi ở vị trí tự nhiên hơn…
  - Nghiêng … cổ.
  - Sử dụng l… ông gõ.



Máy tính và sức khỏe

- Để ngăn ngừa mỏi mắt hoặc đau đầu:
  - Đặt màn hình cách mắt từ 24 đến 30 inch.
  - Điều chỉnh độ phân giải màn hình để văn bản và biểu tượng đủ lớn giúp nhìn rõ hơn.
  - Đảm bảo rằng màn hình không nhấp nháy, tốc độ làm mới tối thiểu là 72 Hz.
  - Tránh nhìn chằm chằm vào màn hình trong thời gian dài.

Máy tính và sức khỏe

- Nếu làm việc với máy tính vài giờ mỗi ngày, hãy ghi nhớ công thái học:
  - Bề mặt làm việc phải ổn định; tất cả mọi thứ bố trí làm việc trên một mặt phẳng.
  - Màn hình và bàn phím phải ở ngay trước mặt, không phải ở một góc.
  - Phần trên cùng của màn hình nên cao hơn mắt khoảng 2 đến 3 inch.
  - Không được có ánh sáng chói hoặc phản chiếu trên màn hình.
  - Đảm bảo có ánh sáng thích hợp để đọc màn hình rõ ràng bất cứ lúc nào trong ngày.
  - Cần có một nguồn sáng trực tiếp phía trên màn hình, cho dù đó là đèn huỳnh quang hay đèn bàn.

Máy tính và sức khỏe

- Đặt tài liệu sẽ xem khi nhập văn bản vào ngăn kẹp tài liệu phù hợp với màn hình.
- Khi ngồi thoải mái, đặt hai cánh tay sao cho cổ tay thẳng và phẳng và cánh tay sát với cơ thể.
- Giữ bàn chân bằng phẳng trên sàn, đùi và cẳng tay song song với sàn. Nếu bàn chân không chạm sàn, hãy sử dụng kê vật chân.
- Bàn phím phải ở vị trí thoải mái để cánh tay không bị quá căng khi vươn lên hoặc vươn xuống để nhấn các phím.
- Khi gõ, cố gắng không uốn cong cổ tay.

Máy tính và sức khỏe

- Nếu cảm thấy căng ở cổ tay, cánh tay, ngón tay khi sử dụng chuột truyền thống, hãy chuyển sang trackball, chuột lớn hơn hoặc xem xét sử dụng thiết bị sử dụng công nghệ cảm ứng.
- Nếu đặt máy tính xách tay lên đùi, hãy đảm bảo ngồi một cách thích hợp như được mô tả trong hướng dẫn.
- Nếu có thể, hãy sử dụng khay/vật chắc chắn để đặt máy tính xách tay lên khi làm việc nhằm:
  - Đảm bảo một bề mặt phẳng cho máy tính xách tay
  - Giảm lượng nhiệt được tạo ra bởi máy tính xách tay trên đùi.