2.1.1 Sổ tay Học viên Tổng quan về Internet & An toàn trên Internet

Tổng quan về Internet & An toàn trên Internet - là một khóa học hai giờ được thiết kế để giúp các học viên làm quen với các vấn đề cơ bản của trình duyệt web, công cụ tìm kiếm và các chiến lược tìm kiếm. Các quan ngại về mặt đạo đức và an toàn cũng sẽ được xem xét.

Mục tiêu Học tập:

- Miêu tả sự khác nhau giữa Internet and World Wide Web (Mạng lưới Thông tin Toàn cầu)
- Miêu tả các trình duyệt web và cách sử dụng của chúng
- Xác định các cấu phần màn hình của Internet Explorer
- Xác định các cấu phần cơ bản của World Wide Web
- Xác định các cấu phần của URL
- Tiến hành tìm kiếm Internet hiệu quả
- Hiểu các kết quả tìm kiếm
- Đánh giá các trang web
- Thảo luận An toàn trên Internet (an toàn trong Internet)

Các Định nghĩa

Mạng -……

……

Internet.....

.....

World Wide Web

.....

Trình duyệt Web.....

.....

Xem xét các thành phần màn hình của Internet Explore từ trên xuống dưới

Title Bar (Thanh Tiêu đề):.....

.....

Minimize (Thu nhỏ):.....

.....

Restore (Khôi phục):.....

.....

Close (Đóng):.....

.....

Address Bar (Thanh Địa chỉ):.....

.....

Các Nút Back (Quay lại) & Forward (Chuyển tiếp):.....

.....

Tabs (Thẻ):

.....

Status Bar (Thanh Trạng thái):.....

.....

Thêm Các Định nghĩa

Siêu liên kết.....

.....

URL

.....

Công cụ Tìm kiếm.....

.....

Gợi ý Tìm kiếm Internet

- **Mỗi từ đều có ý nghĩa**. Thông thường, tất cả các từ chúng ta đưa vào tìm kiếm sẽ đều được sử dụng.
- **Tìm kiếm không quan tâm đến những chữ cái viết hoa hay dấu câu**. Một tìm kiếm đối với [new york times] tương tự như tìm kiếm [New York Times].
- **Lưu ý rằng một** công cụ tìm kiếm không phải là con người. Thay vì nhập vào [Tôi có bị sốt không?], hãy nhập vào [các triệu chứng của sốt].
- **Chọn các từ miêu tả.** Từ tìm kiếm càng độc đáo, khả năng cho bạn các kết quả càng có liên quan hơn. Các từ không mang tính miêu tả, như

'tài liệu,' 'trang web,' 'công ty,' hay 'thông tin,' thường không cần đến.

***2.0.2 Trò chơi Truy tìm Kho báu trên Internet** được hoàn thành sử dụng các câu hỏi dưới đây và máy tính của bạn.*

1. William Barret Travis đã viết lá thư nổi tiếng của mình từ Alamo khi nào?

2. Những lời hứa của sự trung thành với lá cờ của tiểu bang Texas là gì?

3. Ai là “Bandit Queen of Dallas” (Nữ tướng cướp của Dallas)?

4. Ai tuyên bố “móc sừng” là biểu tượng tay chính thức của UT vào năm 1955?

5. Lyle Lovett sinh ra ở đâu:

6. Tên của trường học ở Rusk Country nơi một vụ rò rỉ khí đốt tự nhiên dẫn tới vụ nổ, làm chết 319 học sinh và giáo viên?

7. Số bài hát ước tính có từ Texas hoặc các nơi ở Texas trong tên bài hát?

8. Texas State Shell (Ốc xoắn của tiểu bang Texas) là gì?

9. King Ranch lớn hơn tiểu bang nào?

10. Cuốn sách nào dành cho trẻ em được đặt ở Camp Green Lake Texas?

Làm thế nào để Đánh giá một Trang Web

1. **Mục đích: Tại sao** trang web được tạo ra? Để:
    - Thông tin
    - Giải trí
    - Quảng cáo hoặc Bán một sản phẩm hay dịch vụ
    - Tác động đến lượt xem, niềm tin, bầu cử
    - Cung cấp tin tức cập nhật
    - Giải trí cá nhân

2. **Nhà Tài trợ/Chủ Sở hữu:** Trang web đó thuộc về dạng nhà cung cấp dịch vụ Internet hay tổ chức nào?
    - Cơ quan nhà nước
    - Giáo dục
    - Doanh nghiệp/Công ty
    - Hiệp hội: Nghề nghiệp, Thương mại, Giải trí
    - Cơ quan báo chí: truyền hình, báo, truyền thanh
    - Tư nhân (cá nhân)

3. **Tổ chức và Nội dung:** Trang web có được tổ chức tốt và tập trung không? Nó được thiết kế tốt không? Đoạn văn bản được viết hay không? Các liên kết có liên quan và phù hợp? Các liên kết đã được đánh giá?

4. **Thiên vị--lập trường chính trị hoặc vấn đề** (của tác giả hoặc nhà tài trợ): Hầu hết các trang web có sự thiên vị vốn có ảnh hưởng đến cách thông tin được chuyển tải trong chúng. Tác giả hay nhà tài trợ là người:
    - thuộc cánh trái/tự do?
    - thuộc cánh phải/bảo thủ?
    - trung lập?
    - một nhóm hay hiệp hội hành động chính trị?
    - một doanh nghiệp?

5. **Ngày** Tạo ra**/Chỉnh sửa:** Trang web đó đã được tạo ra khi nào? Nó được chỉnh sửa gần đây nhất khi nào? Các liên kết có mức độ cập nhật như thế nào? Các liên kết vẫn có tác dụng?

6. **Sự hữu ích**: Trang web có liên quan với việc tìm kiếm của bạn không?

7. **Quyền tác giả/Tác giả** Ai chịu trách nhiệm đối với trang web? Tác giả có phải là một chuyên gia trong lĩnh vực này không? Ông/bà ấy còn viết hay tạo ra cái gì nữa? Tác giả có cung cấp địa chỉ email không? Thông tin được cung cấp có mức độ chính xác như thế nào? Trang web có thể hiện sự thiên vị rõ ràng không?

8. **Độc giả:** Trang web được hướng đến các loại đối tượng độc giả nào? Mức độ có phù hợp đối với các nhu cầu của bạn không? Trang web dành cho:

    - các đối tượng độc giả nói chung?
    - học sinh (tiểu học, trung học, cao đẳng, tốt nghiệp đại học)?
    - chuyên gia hay chuyên viên?
    - các nhà nghiên cứu hay học giả?

9. **Độ bao phủ:** Trang web có bao hàm chủ đề một cách toàn diện, một phần hay nó là một cái nhìn toàn cảnh?

10. **Các minh họa:** Các hình ảnh đồ họa có thể hiện rõ ràng mục đích, sự liên quan và chuyên nghiệp? Các hình ảnh đồ họa có bổ sung hay cải thiện nội dung không?

11. **Bảo mật:** Các hệ thống bảo mật và/hoặc mã hóa có được sử dụng khi cần không?

***2.0.3 Các Chuyên mục Đánh giá Trang Web** được hoàn thành sử dụng các câu hỏi dưới đây và máy tính của bạn.*

HTTP://WWW.LOC.GOV/EXHIBITS/LEWISANDCLARK/LEWISANDCLARK.HTML

TRANG WEB # 1	1	2	3	4	5
Mục đích					
Nhà Tài trợ/ Chủ Sở hữu					
Tổ chức và Nội dung					
Thiên vị--lập trường chính trị hoặc vấn đề					
Ngày Tạo ra/ Chỉnh sửa					
Sự hữu ích					
Thẩm quyền/ Tác giả					
Độc giả					
Độ bao phủ					
Các minh họa					
Bảo mật					

LƯU Ý: .....

.....

2.0.3 Các Chuyên mục Đánh giá Trang Web (Tiếp theo)

HTTP://WWW.UNMUSEUM.ORG/UNMAIN.HTM

TRANG WEB # 2	1	2	3	4	5
Mục đích					
Nhà Tài trợ/ Chủ Sở hữu					
Tổ chức và Nội dung					
Thiên vị--lập trường chính trị hoặc vấn đề					
Ngày Tạo ra/ Chỉnh sửa					
Sự hữu ích					
Thẩm quyền/ Tác giả					
Độc giả					
Độ bao phủ					
Các minh họa					
Bảo mật					

LƯU Ý: .....

.....

Phần mềm quảng cáo như vi rút: Mã độc hại hiển thị quảng cáo không mong muốn trên máy tính của bạn.

Bài viết Blog: Một tạp chí cá nhân hoặc chuyên nghiệp được giữ trên một trang web được cập nhật thường xuyên. Các blog thường có chủ đề và có thể mang tính riêng tư hoặc công khai.

Phòng Chat: Trang web trực tuyến được sử dụng cho tương tác xã hội, thường dựa trên một chủ đề hoặc đề tài, nơi những người có cùng sở thích có thể "trò chuyện" với người khác.

Lọc Nội dung: Cho phép bạn chặn truy cập internet vào một số loại nội dung nhất định.

Cookie *(cookie theo dõi, cookie trình duyệt, cookie HTTP)***:** Cookie là những đoạn văn bản nhỏ được lưu trữ mà một trình duyệt web đặt vào trong máy tính người dùng.

Đe dọa trực tuyến, đe dọa trên internet, kẻ đe dọa trực tuyến: Đe đọa diễn ra trực tuyến.

Tội phạm trên internet: Hoạt động phạm tội nhằm vào máy tính hoặc việc sử dụng thông tin trực tuyến để nhằm vào các nạn nhân trong thế giới thực.

Tải xuống: Chuyển tài liệu từ máy chủ hoặc máy tính từ xa sang máy tính của bạn.

Chữ ký Email: Đây là một phần văn bản được thêm vào cuối email. Nó thường bao gồm tên đầy đủ của bạn, có thể có miêu tả công việc, địa điểm, điện thoại của bạn, một suy nghĩ gây cảm hứng, v.v...

Chia sẻ tập tin: Đề cập đến khả năng lưu trữ các tập tin hoặc ở một nơi trung tâm có thể được chia sẻ với ít nhất là một người khác hoặc công khai.

Phần mềm miễn phí: Đây là phần mềm sở hữu hay có bản quyền, nhưng chủ sở hữu phần mềm cho đi miễn phí.

Hành vi trộm cắp danh tính: Trộm cắp danh tính của một ai đó nhằm mạo danh họ.

Malware (Phần mềm độc hại): viết tắt của từ **Mal**icious (Độc hại) soft**Ware** (Phần mềm) và là thuật ngữ chung bao gồm bất kỳ loại mã độc hại nào – "trojans", "worms", "spyware", "adware", v.v... xâm nhập máy tính mà không có sự đồng ý của người dùng máy tính và được thiết kế để làm hỏng máy tính, thu thập thông tin, hoặc làm cho máy tính của bạn bị phá vỡ và sử dụng từ xa để gửi thư rác v.v...

Phishing (Xây dựng hệ thống lừa đảo nhằm đánh cắp thông tin nhạy cảm)**:** sự mưu hại của những kẻ mạo danh một doanh nghiệp nhằm lừa bạn đưa ra thông tin cá nhân của mình.

Đăng tải: Có nghĩa tải thông tin lên trang web

Scam (mưu đồ bất lương): để điều khiển, lừa đảo, bịp bợm, gian lận, những trò lừa bịp khác**.**

Phần mềm chia sẻ: Phầm mềm chia sẻ là phương pháp quảng cáo sản phẩm bằng cách để bạn 'thử trước khi mua'. Loại phần mềm này có thể tải xuống từ Internet hoặc có thể được phân phối bằng đĩa CD và có thể được sử dụng miễn phí.

Mạng xã hội: Đề cập đến một danh mục các ứng dụng Internet giúp kết nối bạn bè, đối tác kinh doanh hoặc các cá nhân khác lại với nhau bằng cách sử dụng nhiều công cụ

Spam (Thư rác): Email không mong muốn để cố bán cho bạn cái gì đó. Cũng được biết đến là junk mail.

Spyware (Phần mềm cài đặt lén lút vào máy tính): Là phần mềm lén lút tận dụng kết nối Internet của bạn để thu thập thông tin về bạn mà bạn không hề biết hay đồng ý và gửi thông tin cho bất kỳ ai đã viết chương trình phần mềm spyware đó. Như phần mềm quảng cáo, nó thường được cài đặt khi bạn tải về các chương trình 'phần mềm miễn phí' hoặc 'phần mềm chia sẻ'. Spyware có thể tìm kiếm thông tin ngân hàng, thông tin cá nhân, v.v... của bạn. Nó là bất hợp pháp và xâm phạm.

URL: (Định vị Tài nguyên Thống nhất) đề cập đến một địa chỉ internet duy nhất của một tập tin hay đích đến. Để tìm một trang web hay tài liệu cụ thể, bạn đánh máy URL vào trong cửa sổ trình duyệt và trình duyệt sẽ hiện ra địa chỉ cụ thể.

Vi rút: một chương trình máy tính có thể tự nhân đôi và lan truyền từ máy tính này sang máy tính khác.

Trang Web: một tài liệu trên mạng. Mỗi trang web có một URL duy nhất.

Tập hợp các trang web: một nhóm các trang web có liên quan.

Máy chủ Web: các máy tính được kết nối với Internet lưu trữ các trang web.

11 Gợi ý để Mua hàng Trực tuyến An toàn

Do thiếu khoảng trống, các gợi ý này được viết tắt. Đọc toàn bộ các gợi ý tại http://www.pcmag.com/article2/0,2817,2373131,00.asp

1. **Sử dụng Các Trang Web Quen thuộc:** Bắt đầu với một trang web tin cậy hơn là mua hàng với một công cụ tìm kiếm.
2. **Tìm kiếm biểu tượng Ổ Khóa:** Ít nhất— không bao giờ mua bất kỳ thứ gì trực tuyến sử dụng thẻ tín dụng của bạn từ một trang web không có cài đặt mã hóa SSL (bảo mật tầng truyền tải). Bạn sẽ biết liệu trang web có SSL không bởi URL cho trang web sẽ bắt đầu với HTTPS:// (thay vì chỉ HTTP://). Biểu tượng khóa móc bị khóa sẽ xuất hiện, thông thường trên thanh trạng thái ở cuối trình duyệt web của bạn hoặc ngay bên cạnh URL trên thanh địa chỉ.
3. **Đừng Nói Tất cả:** Không cửa hàng mua sắm trực tuyến nào cần số an sinh xã hội của bạn hay ngày sinh của bạn để hoạt động kinh doanh. Khi có thể, đưa ra càng ít thông tin càng tốt.
4. **Kiểm tra Các Bảng Sao kê:** Truy cập mạng thường xuyên và kiểm tra bảng sao kê điện tử của thẻ tín dụng, thẻ ghi nợ, và các tài khoản ngân hàng của bạn. Nếu bạn thấy có gì sai, nhanh chóng gọi điện thoại để đề cập vấn đề.
5. **Phòng ngừa cho Máy tính của Bạn:** Bạn cần bảo vệ chống lại malware với việc luôn cập nhật phần mềm chống vi rút của bạn.
6. **Sử dụng Mật khẩu Mạnh:** Chúng tôi cực kỳ muốn nhấn mạnh việc đảm bảo việc sử dụng mật khẩu mạnh, nhưng nó quan trọng hơn cả khi thực hiện giao dịch ngân hàng và mua sắm trực tuyến.
7. **Suy Nghĩ mang tính Di động:** Không cần phải lo lắng nhiều về việc mua sắm trên thiết bị di động hơn là trực tuyến. Mẹo là sử dụng các ứng dụng được trực tiếp cung cấp bởi các nhà bán lẻ, như Amazon, Target, v.v...
8. **Tránh Các Thiết bị Công cộng:** Hy vọng chúng tôi không phải nói với bạn rằng việc sử dụng máy tính công cộng để mua sắm là một ý tưởng cực tồi tệ, *nhưng chúng tôi vẫn sẽ phải nói. Nếu bạn làm vậy, chỉ cần nhớ đăng xuất mỗi lần bạn sử dụng thiết bị công cộng, th*ậm chí nếu bạn chỉ kiểm tra email.

9. **Cá nhân hóa Wi-Fi của bạn:** Nếu bạn quyết định đi ra ngoài với máy tính xách tay để mua sắm, bạn sẽ cần kết nối Wi-Fi. Chỉ dùng mạng không dây nếu bạn truy cập Web qua kết nối mạng riêng ảo (VPN).
10. **Đếm các Thiệp:** Các thiệp quà tặng là những quà tặng kỳ nghỉ có nhu cầu lớn nhất, và năm nay cũng phải là ngoại lệ. Nếu bạn phải mua thiệp quà tặng, hãy chọn nơi quen biết; những kẻ lừa đảo thích bán đấu giá thẻ quà tặng trên các trang web như eBay và thẻ thường có ít hoặc không có tiền trong thẻ.
11. **Biết Cái gì là Quá Tốt để Có thể thành Sự thật:** Thái độ hoài nghi, trong hầu hết các trường hợp, có thể giúp bạn thoát khỏi việc bị đánh cắp thẻ.

An toàn Mạng Xã hội (từ AARP)

Các trang web mạng xã hội như MySpace, Facebook, Twitter và Windows Live Spaces là những dịch vụ mọi người có thể sử dụng để kết nối với những người khác và chia sẻ thông tin như ảnh, video, và tin nhắn cá nhân. Khi sự phổ biến của các trang xã hội này tăng lên, dẫn đến các rủi ro từ việc sử dụng chúng cũng tăng lên.

1. **Hãy cận trọng khi bạn nhấp vào liên kết** mà bạn nhận được trong tin nhắn từ bạn bè trên trang web xã hội của bạn. Xử lý các liên kết trong tin nhắn trên các trang web này như bạn sẽ làm đối với liên kết trong các email.
2. **Biết những gì bạn đăng tải về bản thân mình.** Cách phổ biến mà những kẻ lập trình máy tính đột nhập vào tài khoản tài chính hoặc các tài khoản khác là nhấp vào liên kết “Quên mật khẩu?” trên trang đăng nhập tài khoản. Để đột nhập vào tài khoản của bạn, họ tìm kiếm câu trả lời cho các câu hỏi bảo mật của bạn, như ngày sinh, quê quán, lớp thời trung học hoặc tên đệm của mẹ bạn.
3. **Đừng tin tưởng một tin nhắn thực sự là từ người mà tin nhắn nói người đó gửi.** Những kẻ lập trình trái phép có thể đột nhập vào các tài khoản và gửi tin nhắn như là chúng từ bạn bè bạn, nhưng thực ra không phải. Nếu bạn nghi ngờ rằng một tin nhắn là giả mạo, hãy sử dụng phương pháp khác để liên lạc với bạn mình để tìm ra sự thật.

4. **Để tránh đưa ra địa chỉ email của bạn bè mình, không cho phép dịch vụ mạng xã hội quét danh sách địa chỉ email của bạn.** Khi bạn tham gia một mạng xã hội mới, bạn có thể nhận được một đề nghị xâm nhập địa chỉ email và mật khẩu của bạn để tìm hiểu xem bạn bè của bạn có trên mạng hay không. Trang web có thể sử dụng thông tin này để gửi email cho tất cả mọi người trong danh sách liên hệ của bạn hoặc ngay cả những người mà bạn chỉ từng gửi một email tới địa chỉ email đó. Các trang mạng xã hội cần giải thích họ sẽ làm điều này, nhưng một số trang không làm vậy.
5. **Nhập địa chỉ trang web mạng xã hội trực tiếp vào trình duyệt của bạn hoặc sử dụng đánh dấu trang cá nhân của bạn.** Nếu bạn nhấp vào liên kết tới trang web của bạn qua email hoặc trang web khác, bạn có thể nhập tên tài khoản và mật khẩu của mình vào một trang web giả mạo nơi mà thông tin cá nhân của bạn có thể bị đánh cắp.
6. **Hãy chọn lựa người bạn chấp nhận làm bạn bè trên mạng xã hội.** Những tên trộm danh tính có thể tạo các hồ sơ cá nhân giả nhằm lấy thông tin từ bạn.
7. **Chọn mạng xã hội của bạn cẩn thận.** Đánh giá trang web mà bạn định sử dụng và đảm bảo bạn hiểu chính sách về quyền riêng tư. Tìm hiểu liệu trang web có giám sát nội dung mọi người đăng tải. Bạn sẽ cung cấp thông tin cá nhân cho trang web này, vì vậy hãy sử dụng các tiêu chí giống như khi bạn chọn một trang web nơi bạn nhập vào thẻ tín dụng của mình.
8. **Hãy giả định rằng tất cả những gì bạn nhập vào trang mạng xã hội là vĩnh viễn.** Ngay cả khi bạn có thể xóa tài khoản của mình, bất kỳ ai trên Internet cũng có thể dễ dàng in ảnh hoặc đoạn văn bản hoặc lưu hình ảnh và video vào máy tính.
9. **Hãy cẩn thận trong việc cài đặt thêm những phần bổ sung trên trang web của bạn.** Nhiều trang mạng xã hội cho phép bạn tải các ứng dụng của bên thứ ba mà các ứng dụng này cho phép bạn làm nhiều thứ hơn với trang cá nhân của mình. Để tải xuống và sử dụng các ứng dụng của bên thứ ba một cách an toàn, hãy thực hiện các biện pháp đề phòng an toàn như bạn thực hiện với bất kỳ chương trình hoặc tập tin nào khác mà bạn tải xuống từ trang web.

10. **Suy nghĩ kỹ trước khi bạn sử dụng các trang mạng xã hội ở nơi làm việc.**
11. **Nói chuyện với con cái bạn về mạng xã hội.**