1. Lời nói đầu

Ngày nay, Internet đã trở thành một công cụ phổ biến. Đối tượng sử dụng Internet ngày càng đa dạng và tăng không ngừng về số lượng. Theo thống kê, gần như tất cả người dùng Internet tại Việt Nam đều ít nhiều có nhu cầu truy cập các trang web, thuật ngữ gọi là "lướt web", để thực hiện công việc, giải trí, đọc tin tức, tìm kiếm thông tin, chơi game…

Trong thực tế, khi lướt web, người dùng có thể gặp những vấn đề đơn giản như nhiễm virus, hoặc phức tạp như lộ thông tin bảo mật cá nhân dẫn đến hệ quả nghiêm trọng như bị lợi dụng thông tin để lừa đảo, chiếm đoạt tài sản, thông tin... từ quá trình lướt web, tham gia mạng xã hội…

Vì vậy, bài viết này xin được đề cập tới vấn đề an toàn khi lướt web, hy vọng sẽ giúp được đa số người dùng Internet tránh được những nguy cơ tiềm ẩn đằng sau những cú click chuột vào trình duyệt web.

2. Các khái niệm, định nghĩa

- **Lướt web**: là một thuật ngữ chỉ hành động sử dụng trình duyệt web để truy cập vào các website nhằm mục đích tra cứu thông tin, đọc báo, làm việc, giải trí…
- **Trình duyệt web**: là một phần mềm ứng dụng cho phép người dùng xem và tương tác với các văn bản, hình ảnh, đoạn phim, nhạc, trò chơi và các thông tin khác ở trên một trang web của một địa chỉ web trên mạng toàn cầu hoặc mạng nội bộ (Theo wiki). Một số trình duyệt web thông dụng được sử dụng rộng rãi là Internet Explorer (Microsoft), Firefox (Mozilla), Chrome (Google), Opera, Safari…

3. Những hình thức lừa đảo trực tuyến mà người dùng cần biết

- **Hình thức tiếp cận phổ biến:** Giả danh cơ quan công quyền (công an, viện kiểm sát), ngân hàng, tổ chức tài chính, hoặc người thân để tạo sự tin tưởng.
- **Kênh tiếp cận chính:** Sử dụng cuộc gọi, tin nhắn SMS, email, mạng xã hội, và các ứng dụng nhắn tin như Zalo, WhatsApp để dễ dàng thao túng nạn nhân.
- **Phương thức lừa đảo:** Đánh cắp thông tin cá nhân qua đường dẫn giả, yêu cầu quét mã QR, hoặc gửi mã độc qua email/tệp đính kèm.
- **Thao túng tâm lý:** Đánh vào lòng tham, nỗi sợ hãi, sự tò mò hoặc tình thương, thường tạo cảm giác khẩn cấp để nạn nhân hành động ngay.
- **Cài cắm mã độc:** Thông qua ứng dụng giả mạo hoặc các tệp tin độc hại như .pdf, .exe để chiếm quyền truy cập thiết bị.
- **Tạo dựng lòng tin:** Giả danh các tổ chức uy tín, gửi email hoặc tin nhắn trông chuyên nghiệp, yêu cầu thông tin nhạy cảm.
- **Kịch bản lừa đảo tinh vi:** Lên kế hoạch chi tiết, sử dụng vai diễn giả để thao túng tâm lý và điều hướng hành vi của nạn nhân.

4. Những mối nguy hiểm khi lướt web

Các mã độc hại, virus, trojan…

Máy tính bị nhiễm virus có nguy cơ bị đánh cắp tài khoản, mật khẩu, thông tin cá nhân. Điển hình trong thời gian qua là hiện tượng bị mất mật khẩu Yahoo! Messenger, sau đó hacker sử dụng tài khoản này để lừa tiền của người thân, bạn bè nạn nhân. Nguyên nhân là do người dùng đã bị nhiễm virus, keylogger ghi lại thao tác bàn phím khi gõ mật khẩu.

Ngoài ra, khi bị nhiễm virus, máy tính có thể trở thành những máy tính ma trong mạng botnet của hacker, từ đó phát tán virus sang các máy khác (qua mạng, qua USB) và tấn công từ chối dịch vụ các hệ thống mạng…

Lừa đảo trực tuyến

Hiện tượng lừa đảo trực tuyến ngày càng trở nên phổ biến. Chỉ cần một chút sơ suất, người dùng hoàn toàn có thể trở thành nạn nhân.

Chúng ta có thể gặp những trường hợp lừa đảo theo cách truyền thống nhưng sử dụng công cụ là mạng Internet, chẳng hạn những email lừa tiền từ nước ngoài, với một kịch bản cuốn hút những người thiếu tỉnh táo, hoặc những hình ảnh bắt mắt, những chương trình hấp dẫn để móc túi những người nhẹ dạ.

Hiện tượng lừa đảo rất đa dạng về phương thức và mục đích. Hacker sẽ sử dụng những phương pháp đánh lừa để thực hiện được các hành vi bất chính của mình.

Để thực hiện những mục đích đó, hacker thường sử dụng những biện pháp lừa đảo như sau:

- Các đường link độc hại: người dùng khi click vào các đường link này có thể bị nhiễm virus. Các đường link này có thể được gửi qua chat, hay ẩn giấu dưới các hình ảnh hấp dẫn…
- Các trang web giả mạo (fake login): hacker tạo một trang web giả mạo với giao diện giống hệt với các website nổi tiếng, nhưng khi người dùng gõ mật khẩu đăng nhập, nó sẽ được gửi tới hacker thay vì trang web thật.
- Các email độc hại: Các email có chứa đường link, file đính kèm độc hại, nội dung lừa đảo.
- Phần mềm giả mạo: một phần mềm có giao diện giống như một phần mềm có ích, nhưng thực tế lại độc hại và kéo virus vào máy, hoặc lừa tiền người dùng mua chúng.

Đánh cắp thông tin cá nhân, spam mail, tin nhắn…

Hiện tượng đánh cắp tài khoản ngân hàng tại những nước phát triển sử dụng thanh toán qua thẻ rất phổ biến. Ở Việt Nam, hiện tượng này ít hơn do chưa sử dụng rộng rãi các phương thức thanh toán trực tuyến.

Khi email bị lộ, bạn có thể nhận được hàng trăm những thư rác, spam qua email mỗi ngày, gây khó chịu. Đó là do có những mạng gửi thư rác bằng cách thu thập những địa chỉ email trên Internet, tương tự với số điện thoại.

Bị làm phiền khi lướt web, popup, banner quảng cáo

Vấn đề này tuy không trực tiếp gây hại cho máy tính người dùng, nhưng thường gây khó chịu. Có trang web mỗi khi thao tác, lại bật ra từ vài đến hàng chục popup quảng cáo khiến người dùng phải tắt bỏ mất thời gian, ảnh hưởng tới công việc khác, đôi khi làm treo máy, hay những banner quảng cáo nhấp nháy liên tục, không nằm trong mối quan tâm của người dùng.

Những popup, banner này cũng có thể ẩn chứa những nguy hiểm, bởi nội dung của chúng thường từ các trang nước ngoài, không đáng tin cậy, có thể tiềm tàng những link nguy hiểm, lừa đảo.

Nguy cơ khi lướt web trên di động

Khi điện thoại thông minh ngày càng trở nên phổ biến, việc lướt web trên di động cũng chiếm một thị phần không nhỏ. Bởi vậy, nảy sinh ra các nguy cơ bảo mật trên di động khi người dùng lướt web trên di động.

Người dùng di động cũng có thể bị nhiễm virus. Đặc điểm của những virus, mã độc trên di động là chủ yếu đánh cắp thông tin, đánh cắp tài khoản, truy cập vào các dịch vụ trả phí một cách âm thầm...

Các nguy cơ xã hội

Một dạng nguy cơ ít được để ý tới nhưng lại rất nguy hiểm đối với người dùng, và đã thể hiện sự có mặt trong xã hội. Đó là các nguy cơ như tiêm nhiễm văn hóa ngoại lai, đồi trụy, phản động, trái pháp luật, lối sống lệch lạc, sa đà vào thế giới ảo mà quên đi cuộc sống thực…

Những thông tin trên mạng khi lướt web của bạn cũng có thể trở thành nguy cơ ngoài đời thực. Sự thật là đã có những vụ án xảy ra do những thông tin trên mạng xã hội như cướp của, giết người hay xích mích trên thế giới ảo...

5. Kỹ năng nắm bắt, phát hiện các phương thức lừa đảo

- **Cuộc gọi lừa đảo:** Tạo cảm giác khẩn cấp, yêu cầu thông tin hoặc chuyển tiền ngay lập tức. Dấu hiệu: thông tin không rõ ràng, danh tính không xác thực.
- **Tin nhắn/email:** Chứa lỗi chính tả, liên kết dẫn đến trang web giả mạo, hoặc yêu cầu hành động khẩn cấp (xác nhận tài khoản, nhận thưởng).
- **Trang web giả mạo:** Thiết kế kém chất lượng, tên miền lạ, không có chứng chỉ bảo mật SSL. Thường yêu cầu nhập thông tin cá nhân hoặc tài khoản ngân hàng.
- **Ứng dụng giả mạo:** Tải từ nguồn không chính thức, giao diện không chuyên nghiệp, yêu cầu quyền truy cập bất thường (danh bạ, vị trí, tài khoản).
- **Mạng xã hội:** Kết bạn từ người lạ, quảng cáo đầu tư lợi nhuận cao, hoặc yêu cầu chuyển tiền cọc trước. Công nghệ Deepfake cũng được sử dụng để giả mạo người thân.
- **Kiểm tra thông tin:** Đối chiếu nguồn gốc email, kiểm tra URL trước khi nhấp vào liên kết, không mở tệp đính kèm không rõ ràng.

6. Thủ thuật, kinh nghiệm lướt web an toàn

Áp dụng Quý tắc “6 KHÔNG”

KHÔNG cung cấp thông tin cá nhân, địa chỉ, số điện thoại, số tài khoản ngân hàng của mình cho đối tượng không quen biết; thận trọng rà soát và kiểm tra kỹ thông tin trước khi thực hiện các giao dịch chuyển tiền.

KHÔNG kết bạn và nói chuyện với người lạ, đặc biệt là những tài khoản có hình ảnh ngoại hình đẹp và bắt mắt. Tuyệt đối không nhận lời mời tham gia các hội nhóm mà không rõ mục đích đối tượng

KHÔNG truy cập, đăng nhập vào các đường dẫn, liên kết, website, ứng dụng hoặc mở tệp đính kèm đến từ người gửi không xác định, không rõ nguồn gốc.

KHÔNG cán bộ cơ quan nhà nước, bộ công an, viện kiểm sát, tòa án hay đơn vị tài chính… nào gọi điện để điều tra qua điện thoại, yêu cầu phải cung cấp thông tin cá nhân hay đóng tiền.

KHÔNG thực hiện chuyển khoản trước, tuyệt đối không đặt cọc, chuyển khoản tiền cho các đối tượng lạ trong bất cứ trường hợp nào.

KHÔNG tham lam những tài sản, món quà không rõ nguồn gốc có thể nhận được một cách dễ dàng, những lợi nhuận "phi thực tế" mà không tốn sức lao động, những lời mời chào, dụ dỗ "việc nhẹ lương cao"...

Cài đặt phần mềm diệt virus hiệu quả

Một phần mềm diệt virus hiệu quả sẽ giúp bạn tránh được phần lớn các nguy cơ khi lướt web. Bạn nên sử dụng một phần mềm có tính năng tổng hợp hoặc Internet Security (thường chỉ xuất hiện ở các phiên bản có trả phí) bởi vì các phần mềm này thường có đầy đủ tính năng để bảo vệ bạn khỏi các nguy cơ từ xa hơn so với các bản miễn phí, chỉ có tính năng Antivirus.

Một máy tính nối mạng Internet bắt buộc phải có một phần mềm diệt virus chạy thường trực.

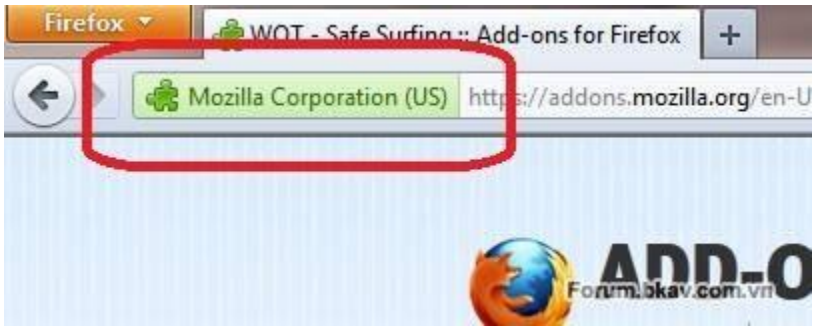
Ngoài ra, để phòng chống virus một cách tốt nhất, bạn nên sử dụng phần mềm có bản quyền và cập nhật hệ điều hành đầy đủ. Các trình duyệt web cũng cần được cập nhật phiên bản mới nhất để tránh những lỗ hổng mà virus có thể khai thác khi lướt web.

Nguyên tắc để nhận biết website, link an toàn

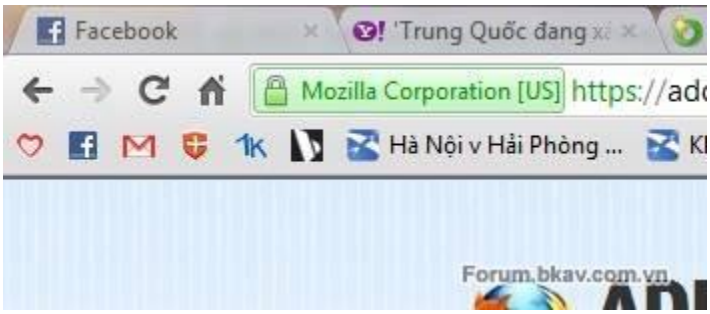
- Luôn chú ý đến thanh địa chỉ (Address Bar) của trình duyệt.
- Không click vào những đường link, banner lạ mà bạn không biết hoặc nghi ngờ không an toàn, những mẩu quảng cáo bạn không quan tâm (nhất là những đường link, banner toàn tiếng nước ngoài hoặc gợi tới một chương trình trúng thưởng đáng ngờ nào đó). Kể cả những đường link đó do một người quen gửi cho bạn qua mail, qua chat…

  Nếu bạn vô tình click vào chúng và cảm thấy nghi ngờ, hãy tắt ngay cửa sổ trình duyệt.

- Rê chuột vào đường link nhưng không bấm để xem trước đường link. Đường link xem trước của cả 3 trình duyệt phổ biến là IE, Chrome và Firefox đều nằm ở phía dưới bên trái của cửa sổ trình duyệt. Nếu đường link này lạ lẫm, bạn không nên click vào.
- Có những website gần như tuyệt đối an toàn, đó là các website có chứng thực số. Đặc điểm nhận diện của chứng thực số nằm ở góc bên trái của thanh địa chỉ. Tuy nhiên, KHÔNG PHẢI những trang không có điều này nghĩa là không an toàn.



Hình 1:Chứng thực số ở Firefox.



Hình 2: Chứng thực số Google Chrome.

- Chỉ sử dụng những trình duyệt thông dụng, an toàn. Khuyến cáo nên sử dụng Chrome hoặc Firefox vì 2 trình duyệt này bảo mật và có nhiều add-ons, extensions hỗ trợ bảo vệ khi lướt web.

Nhận biết các website lừa đảo, các dạng lừa đảo phổ biến khi lướt web

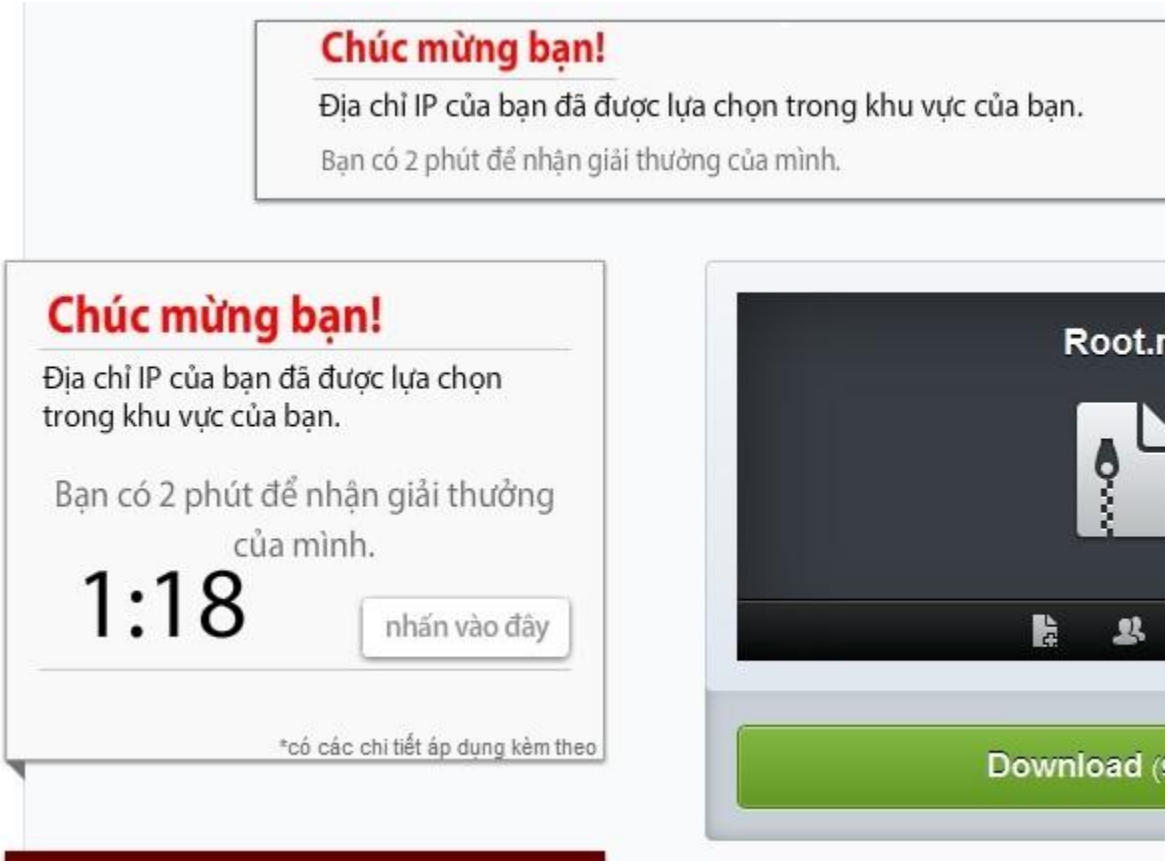
- Hãy luôn là người tỉnh táo, cân nhắc sự việc với tiêu chí: Không có món lợi từ trên trời rơi xuống. Vì vậy, những thông tin cho thấy quá dễ dàng để nhận được phần thưởng luôn đáng nghi ngờ đầu tiên.

- Những đường link, website yêu cầu bạn nhắn tin để nhận phần thưởng phần lớn là lừa đảo.
- Vừa chú ý giao diện trang web, vừa chú ý địa chỉ trang web ở trên trình duyệt. Ví dụ bạn đang thấy giao diện trang đăng nhập Yahoo! mail nhưng trên thanh địa chỉ lại không phải là yahoo.com hoặc yahoo.com.vn mà lại là một địa chỉ lạ lẫm thì chắc chắn đó là trang lừa đảo ăn cắp mật khẩu yahoo của bạn.

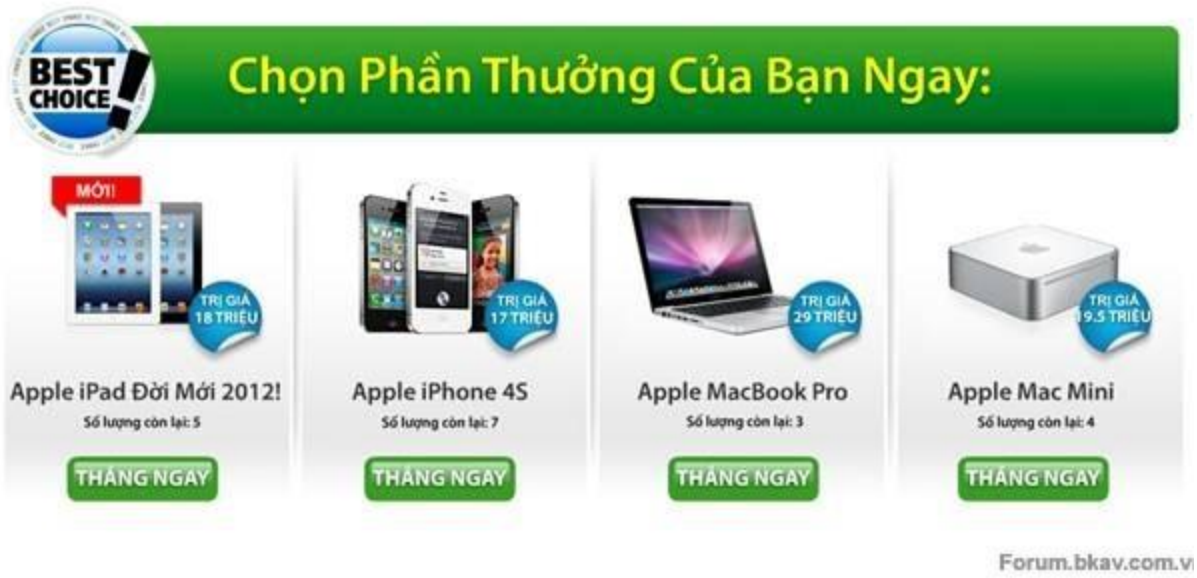
  Đôi khi hacker đánh lừa người dùng bằng những đường link gần giống, vì vậy cần chú ý xem xét cẩn thận.

- Cảnh giác với cả những đường link bạn bè, người thân gửi cho bạn. Có thể họ đã bị hacker lợi dụng, chiếm đoạt tài khoản.
- Một số banner quảng cáo lừa đảo thường hay xuất hiện ở những trang web tải file của nước ngoài như mediafire.com, hotfile.com. Khi tải file ở đây, nếu nội dung bản tải xuống không đúng như file đang cần tải, lập tức dừng tải và tắt cửa sổ trình duyệt.

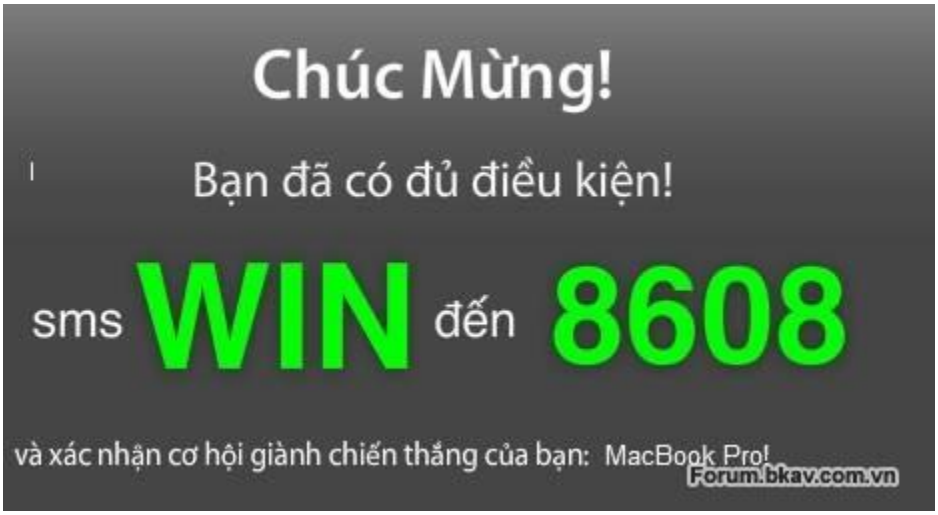
  Một kịch bản lừa đảo tiền điện thoại thường thấy là một vài banner, đường link mời tham gia chương trình trúng thưởng. Giải thưởng thường rất lớn, có giá trị nhưng bạn gần như không phải làm gì, hoặc chỉ chơi một vài trò chơi, làm vài câu hỏi rất đơn giản. Sau đó, trang web yêu cầu bạn nhập số điện thoại của mình rồi yêu cầu soạn tin gửi tới một đầu số nào đó. Mỗi tin nhắn gửi đi, bạn sẽ mất tiền mà không được gì.



Hình 3: Các thông báo “CHÚC MỪNG BẠN” trong hình đều là lừa đảo.



Hình 4: Không có cái gì dễ dàng như thế này, bởi vì chúng đang lừa đảo tiền điện thoại của bạn.



Hình 5: Thông báo lừa bạn nạp tiền

Bảo vệ thông tin cá nhân khi lướt web

Như đã nói ở phần đầu, thông tin cá nhân là tài nguyên bạn cần phải bảo vệ khi lướt web. Thực tế, khi sử dụng Internet, rất nhiều trang web yêu cầu bạn cung cấp thông tin cá nhân khi đăng ký.

Duyệt web riêng tư

Khi sử dụng Internet ở máy tính công cộng, hoặc máy của người khác, bạn không muốn những thông tin mình đã truy cập, mật khẩu… được lưu lại. Rất đơn giản là sử dụng chế độ riêng tư, ẩn danh của trình duyệt.

- Với Google Chrome: Dùng tổ hợp phím Shift + Ctrl + N.
- Với Firefox: Dùng tổ hợp phím Shift + Ctrl + P

- Với Internet Explorer: Dùng tổ hợp phím Shift + Ctrl + P

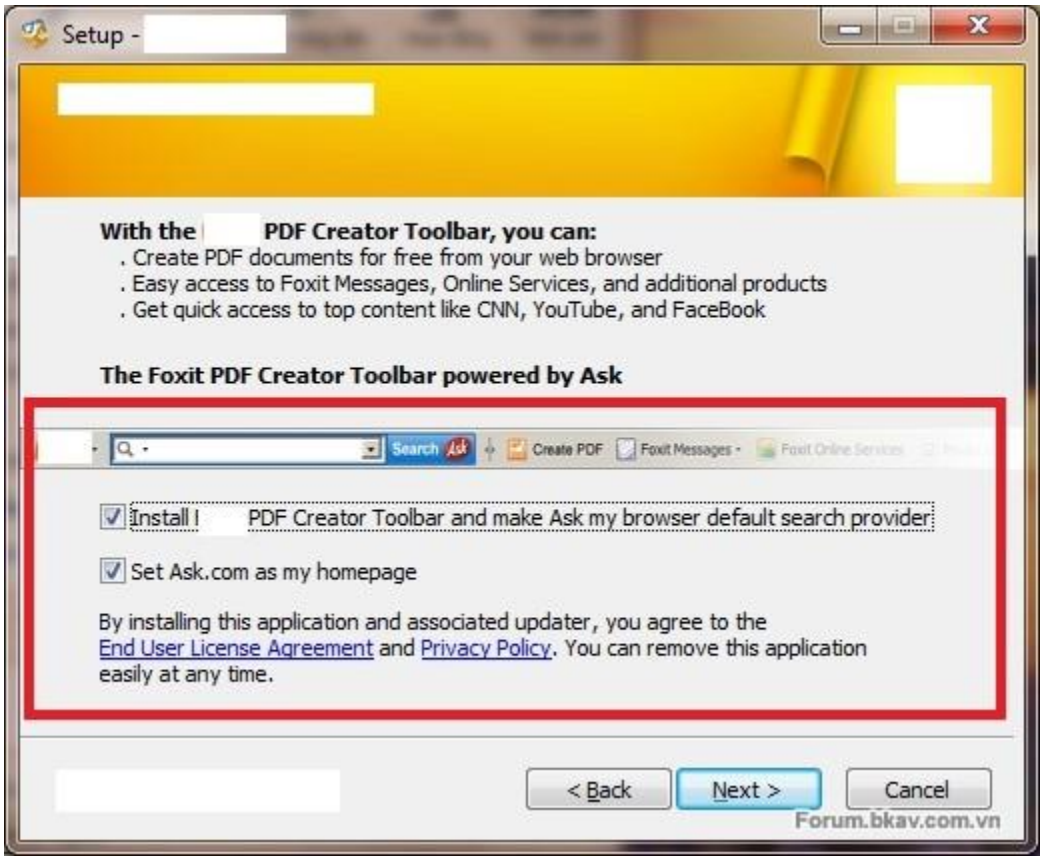
  Khi đó, một cửa sổ trình duyệt hiện ra cho biết bạn đang ở chế độ Private. Mọi thứ bạn truy cập sẽ không bị lưu lại sau khi bạn thoát ra.

Những thủ thuật khác bảo vệ thông tin cá nhân

Ngoài những phương thức đã nêu trên, bạn cũng cần áp dụng những biện pháp sau để đảm bảo thông tin cá nhân, tài khoản của mình được bảo vệ:

- **Đặt mật khẩu đủ mạnh. Mật khẩu mạnh nên là:**
  - Có từ 8 ký tự trở lên.
  - Có cả chữ và số, tốt hơn nữa là nên có các ký tự đặc biệt như @ # $ %.
  - Không đặt mật khẩu dễ đoán, dễ dò như ngày sinh, số điện thoại, biển số xe… của mình hoặc người thân.
  - Không đặt chung mật khẩu cho tất cả các tài khoản, dịch vụ (Tài khoản ngân hàng, Windows, Yahoo!, Gmail, tài khoản Game…)
  - Thay đổi mật khẩu định kỳ nếu có thể.
  - Không chia sẻ mật khẩu với người khác hoặc ghi ra giấy, lưu trong điện thoại…
  - Xem thêm quy định mật khẩu - VAB
- **Không cài các phần mềm lạ, Toolbar quảng cáo.**

  Một số phần mềm có kèm thêm việc cài đặt các Toolbar quảng cáo, gây khó chịu trong khi lướt web, thay đổi trang chủ, máy tìm kiếm…người dùng rất hay không để ý mà không hề biết Toolbar được cài vào khi nào. Vì vậy, khi cài đặt các phần mềm, bạn nên chú ý đọc các điều khoản, nếu thấy yêu cầu cài một Toolbar nào đó thì bấm bỏ không cài.



Hình 6: Một phần mềm yêu cầu cài Toolbar trong khi cài đặt phần mềm.

Một số phần mềm lạ hiện nay xuất hiện và có nhiều hành vi đáng ngờ, các phần mềm không danh tiếng. Trước khi cài, bạn có thể tìm kiếm tên phần mềm trên trang Google.com.vn để xem các bài viết về phần mềm đó, qua đó đánh giá độ tin cậy. Các phần mềm nên chú ý là các phần mềm tối ưu hệ thống, diệt virus, tìm kiếm driver, game…vì tiềm ẩn nguy cơ là phần mềm giả mạo và gây nguy hiểm.

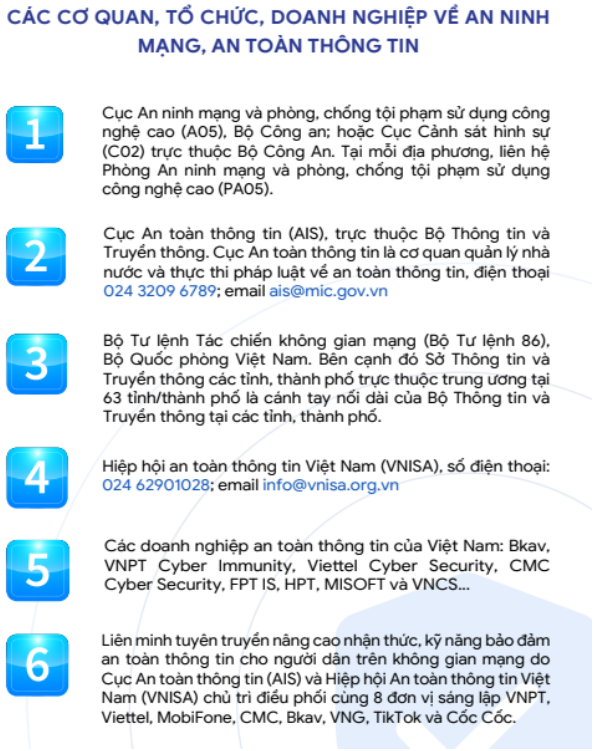
Lướt web an toàn ở các điểm truy cập Internet công cộng

Khi truy cập Internet ở các điểm truy cập Internet công cộng bạn gặp rất nhiều nguy cơ do có nhiều người dùng chung máy tính và mạng. Mặt khác, các biện pháp bảo vệ sẽ bị hạn chế do không phải máy tính cá nhân. Vì vậy, bạn cần áp dụng các biện pháp sau với trường hợp đặc thù này:

- Sử dụng bàn phím ảo khi gõ mật khẩu. Để mở bàn phím ảo có sẵn của Windows, bạn mở hộp thoại **Run** (hoặc bấm phím Windows + R), gõ **OSK** và Enter để mở bàn phím ảo.
- Cẩn thận với những đường link, những trang web giả mạo để ăn cắp mật khẩu bằng cách xem kỹ những đường link trên thanh địa chỉ có đúng là của trang web bạn đang truy cập hay không.
- Không truy cập các trang web lạ, các banner, popup lạ.
- Chú ý xung quanh khi gõ mật khẩu, tránh bị người khác, camera nhìn trộm, quay trộm...

Cập nhật kiến thức

Theo dõi và cập nhật các thông tin, tình huống, dấu hiệu về lừa đảo trực tuyến tại kênh thông tin Cổng không gian mạng quốc gia trên các nền tảng mạng xã hội như Facebook, Tiktok, … hoặc website Khonggianmang.vn



7. Kỹ năng xử lý khi đối mặt với lừa đảo

- **Khi phát hiện dấu hiệu lừa đảo:** Ngắt liên lạc, chặn số điện thoại, báo cáo tin nhắn hoặc cuộc gọi với cơ quan chức năng.
- **Hành động ngay sau khi bị lừa đảo:** Dừng chuyển tiền, liên hệ ngân hàng để khoá tài khoản và sao lưu bằng chứng.
- **Trình báo vụ việc:** Báo cáo sự cố với các cơ quan chức năng như công an, Cục An toàn thông tin.
- **Cập nhật bảo mật:** Thay đổi mật khẩu phức tạp, kích hoạt xác thực hai lớp, và quét hệ thống bằng phần mềm diệt virus.
- **Kiểm tra thiết bị:** Gỡ bỏ phần mềm độc hại, cài đặt lại hệ thống nếu cần thiết để đảm bảo không còn lỗ hổng.
- **Theo dõi tài khoản:** Giám sát giao dịch tài chính và tín dụng, phát hiện sớm các hoạt động bất thường.

8. Tổng kết

Lướt web an toàn là một vấn đề cần được chú ý để tránh các nguy cơ về bảo mật, an ninh thông tin. Trong mọi trường hợp, người dùng đều có nguy cơ gặp nguy hiểm khi lướt web. Tuy nhiên, chỉ cần chú ý và áp dụng các biện pháp kỹ thuật cơ bản, người dùng hoàntoàn có thể phòng tránh được các nguy cơ trên.

Việc sử dụng trình duyệt phù hợp cũng đóng một vai trò quan trọng. Chrome hoặc Firefox là những trình duyệt ngoài khả năng duyệt web nhanh còn có nhiều tiện ích mở rộng, Add-ons đi kèm (như đã nêu ở các phần trên) rất đa dạng và giúp ích cho việc bảo mật của người dùng.

Một hình mẫu của việc lướt web an toàn một cách cơ bản mà bạn có thể tham khảo bao gồm:

- **Sử dụng Chrome hoặc Firefox có cài các tiện ích bảo mật** (có nêu một vài ví dụ ở trên).
- **Cẩn thận và ứng đối thông minh trước các đường link, file lạ gửi đến.**
- **Áp dụng thêm các biện pháp bảo mật đã nêu trong bài trong trường hợp cần thiết.**