Hướng dẫn bảo vệ bản thân và gia đình trên môi trường mạng

***1. Dấu hiệu nhận biết Websites không an toàn***

Mặc dù có nhiều cách khác nhau để biết một trang web có an toàn hay không, nhưng có một phương pháp thường hữu ích nhất đó là **Quan sát** bởi vì một trang web lừa đảo sẽ không được đầu tư bài bản và chỉnh chu như một website chính thống. Vì vậy, bạn có thể nhận diện qua các dấu hiệu sau:

*a) Dấu hiệu 1: Đường dân URL*

Hãy cùng thực hiện một thử thách nhỏ, đó là phân biệt các URL sau đây, xem đâu là thật, đâu là giả mạo.

1. posmart.vn

2. s-facebook.com; coccoc-ooo.com;

3. coccoc.com

Kết quả, đường dẫn số 1 và 3 là an toàn. Đường dẫn số 2 là giả mạo do “s” và “facebook.com” được ngăn cách bởi dấu “-”, tạo nên một tên miền hoàn toàn khác.

Trên đây chỉ là một ví dụ đơn giản về sự dễ nhầm lẫn giữa các đường link thật - giả. Hãy luôn cảnh giác nếu đường dẫn có các dấu hiệu sau đây:

* Tên miền có lỗi chính tả: Sai khác, thiếu hoặc thừa một ký tự, hoặc thay thế một ký tự với ký tự khác gần giống.

Ví dụ: vietnamairslines.com

* Tên miền có tiền tố hoặc hậu tố sử dụng ký tự lạ.

Ví dụ: s-facebook.com; coccoc-ooo.com

* Tên miền phụ cố bắt chước tên miền của một trang hợp pháp.

Ví dụ: coccoc.xyz.com, trong đó coccoc là tên miền phụ, tên miền thực tế là xyz.

* Tên miền có top-level domain có độ tin cậy thấp.

Ví dụ: Trong đường dẫn coccoc.tech, top-level domain là .tech.

Các đuôi trang .org, .gov (chính phủ), .edu (giáo dục đào tạo). thường là những top - level domain đáng tin cậy. Trong khi đó, các đuôi trang ít phổ biến như .info, .asia, .vip. thường có độ tin cậy thấp hơn.

* Tên miền quốc tế (IDN) chứa ký tự đặc biệt.

Ví dụ: facebook.com, chữ “ã” là một ký tự đặc biệt, domain thật là xn--febook- bua499c.com

* Tên miền dài bất thường nhằm đánh lừa người dùng nhầm lẫn.

Ví dụ: facebook.com-account.application-settingsindexphp.xyz

* Tên miền phụ đã bị chiếm đoạt.

Ví dụ: Kẻ tấn công thiết lập một trang giả mạo (phishing) trên tên miền phụ của một tên miền hợp pháp (chẳng hạn, subdomain.microsoft.com) nhờ lợi dụng lỗ hổng Sub­domain Takeover (tiếp quản tên miền phụ). Điều này xảy ra khi tên miền phụ trỏ đến một dịch vụ đã bị gỡ bỏ hoặc xóa trên GitHub, Heroku hay Azure, cho phép kẻ tấn công phân phối nội dung giả mạo hoặc điều hướng nạn nhân đến trang do chúng quản lý.

Hơn nữa, các tên miền mới được đăng ký cũng có thể xếp vào diện khả nghi. Để đảm bảo an toàn, bạn hãy kiểm tra thông tin tên miền tại who.is.

Ngoài ra, nếu biểu tượng bảo mật trên thanh địa chỉ không phải là hình ổ khóa, điều đó có nghĩa là thông tin bạn gửi hoặc nhận thông qua trang web không được đảm bảo an toàn, riêng tư.

*b) Dấu hiệu 2: Giao diện web*

Hãy để ý các yếu tố như logo, hình nền và chắc chắn rằng chúng không phải là phiên bản ‘nhái’ (sai khác về chi tiết, màu sắc) hay phiên bản lỗi thời (sử dụng hình ảnh cũ). Một trang web sử dụng hình ảnh không đúng quy chuẩn thương hiệu chắc chắn là trang web không an toàn.

*Ảnh: Trang web giả mạo thường sử dụng giao diện lỗi thời và cung cấp thông tin đơn vị chủ quản không chính xác. Ví dụ, số tống đài dịch vụ khách hàng.*

*c) Dấu hiệu 3: Nội dung web*

Ở mức độ nâng cao hơn, bạn hãy đọc kỹ nội dung web. Các trang web không an toàn sẽ để lộ những điểm yếu sau:

* Thông tin đơn vị chủ quản website không chính xác. Ví dụ, website giả mạo có thể sử dụng đúng tên doanh nghiệp nhưng cung cấp số tổng đài hoặc địa chỉ không có thực.
* Nội dung chứa lỗi chính tả. Nguyên nhân là do các trang web giả mạo thường không kiểm duyệt kỹ nội dung. Hoặc, các trang này được tạo bởi hacker nước ngoài, không thành thạo ngôn ngữ đang được sử dụng để lừa đảo.

*d) Dấu hiệu 4: Thông báo trên web*

Trong suốt quá trình ở trên trang web, bạn hãy luôn cảnh giác với các thông báo có nội dung ‘giật gân’. Trang web giả mạo thường sẽ ‘nhử’ bạn bằng cách đưa ra những thông báo khiến bạn quá hoảng sợ, hoặc quá vui mừng. Ví dụ như thông báo về sự cố giao dịch hoặc thông báo trúng thưởng, kèm theo đó là yêu cầu bạn nhập thông tin tài khoản, mật khẩu, số thẻ tín dụng để xác minh. Hãy nhớ rằng, một trang web thật sự sẽ không bao giờ làm bạn hoang mang.

Ngoài ra, bạn cũng nên cẩn thận trước các lời mời tải phần mềm hoặc clickbait (mồi nhấn chuột) trên các trang web lạ, đặc biệt là những trường hợp sau:

+ Lời mời tải xuống phần mềm kèm theo thông báo thiết bị đã bị nhiễm virus.

+ Lời mời tải miễn phí nội dung có bản quyền đắt tiền.

+ Lời mời nhận giải thưởng hấp dẫn.

+ Lời mời tải xuống ‘siêu phần mềm’ (như tăng tốc độ máy tính, bẻ khóa WiFi, v.v.). + Lời mời xem những nội dung nhạy cảm, hay tin tức đánh vào lòng tốt, tin tức gây shock.

+ Lời mời tham gia kiếm tiền nhanh, giới thiệu bạn bè để nhận hoa hồng cao.

*e) Dấu hiệu 5: Trình duyệt bật cảnh báo*

Khi bạn sử dụng trình duyệt Cốc Cốc trên máy tính, hoặc cài đặt tiện ích Chống Lừa Đảo, trình duyệt sẽ bật hộp thoại cảnh báo ngay khi bạn truy cập vào một trang web lừa đảo, giả mạo.

1. ***Cảnh giác khi sử dụng điện thoại thông minh***

Trong cuộc sống hiện đại ngày nay, điện thoại thông minh đã trở thành một vật bất ly thân đối với mỗi người bởi vì nó chứa rất nhiều thông tin quan trọng như tài khoản ngân hàng, hình ảnh cá nhân, tin nhắn riêng tư, mật khẩu, lịch sử duyệt web,.. .Điện thoại thông minh với nhiều tiện ích như camera, microphone, xác định vị trí, kết nối mạng không dây và nhiều chức năng khác có thể trở thành “gián điệp” gây mất an toàn bảo mật thông tin cho người dùng. Theo đó, chiếc điện thoại thông tin mà bạn thường lưu trữ những thông tin quan trọng chính là thiết bị lý tưởng để theo dõi, nghe lén, lấy vị trí, dữ liệu riêng tư thậm chí mạo danh để lừa đảo, chiếm đoạt tài sản.

Hãy giữ an toàn cho điện thoại thông minh của mình bằng một số cách thức sau:

*a. Lựa chọn cài đặt các ứng dụng uy tín*

Cài đặt các ứng dụng được đánh giá tốt trên các kho ứng dụng uy tín như CH Play (với hệ điều hành Android) hay App Store (với hệ điều hành iOS). Hạn chế cài đặt các ứng dụng trôi nổi không rõ nguồn gốc.

*b. Hiểu rõ các ứng dụng mà mình đã cài trên điện thoại/ thiết bị thông minh*

Các thiết bị đó cho phép người dùng kiểm soát, cấp quyền phù hợp cho từng ứng dụng theo nhu cầu chức năng sử dụng. Bạn hãy xóa các ứng dụng mình không dùng, tự mình phân quyền cho các ứng dụng một cách hợp lý.

*c. Thiết lập mật khẩu mạnh khi sử dụng điện thoại và các ứng dụng*

Một trong những điều quan trọng người dùng có thể làm để giúp bảo vệ điện thoại của mình là bảo mật điện thoại bằng mật khẩu, mã PIN hoặc xác minh sinh trắc học, tất cả những điều này có thể giúp ngăn chặn những kẻ xâm nhập vào dữ liệu cá nhân nếu điện thoại chẳng may bị đánh cắp.

*d. Cập nhật các bản vá mới nhất của hệ điều hành và ứng dụng*

Các bản cập nhật phần mềm mới nhất này sẽ khắc phục các lỗ hổng bảo mật trong hệ điều hành. Vì vậy, cập nhật các bản phần mềm mới nhất là cách tốt nhất để ngăn chặn bọn tội phạm mạng khai thác các lỗ hổng bảo mật. Thông thường, việc cập nhật phần mềm mới rất dễ dàng vì điện thoại thông minh sẽ gửi thông báo rằng bản cập nhật đã sẵn sàng để người dùng tải xuống và cài đặt. Người dùng cũng nên cập nhật các ứng dụng trên điện thoại thông minh của mình với các bản cập nhật bảo mật mới nhất vì cũng như với chính điện thoại, việc sử dụng phiên bản mới nhất của ứng dụng sẽ giúp cho thiết bị của người dùng được an toàn hơn.

1. ***Sử dụng trình duyệt an toàn để bảo vệ bản thân và gia đình trên không gian mạng***
2. *Chặn quảng cáo và trình theo dõi*

Tính năng Chặn quảng cáo và chương trình theo dõi được tích hợp trên trình duyệt phiên bản máy tính và điện thoại giúp người dùng chặn các quảng cáo gây phiền nhiễu như hộp thoại tự động bật tiếng, che khuất phần lớn màn hình và có hiệu ứng nhấp nháy. Từ đó, người dùng hạn chế được trường hợp click truy cập vào các quảng cáo độc hại chứa dấu hiệu lừa đảo, phát tán virus. Đồng thời, tính năng cũng chặn các chương trình theo dõi hành vi nhằm tăng cường độ bảo mật cho dữ liệu của người dùng.

1. *Duyệt web an toàn*

Khi bạn truy cập một trang web, Cốc Cốc sẽ hiển thị hộp thoại cảnh báo Trang web chứa nội dung không an toàn nếu trang web đó nằm trong danh sách đen của Cốc Cốc, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), và tiện ích ChongLuaDao. Lý do là các trang này có thể chứa phần mềm độc hại, thông tin lừa đảo, tin tức giả mạo, nội dung phản cảm, hoặc tiện ích mở rộng tiềm ẩn rủi ro.

Khi bạn cố gắng điều hướng tới đường dẫn URL không an toàn, Cốc Cốc sẽ đưa ra cảnh báo cho bạn bằng 02 cách:

* Chế độ mặc định: Hiển thị trang cảnh báo giải thích rằng nội dung mà bạn đang cố truy cập có thể độc hại (kế thừa dịch vụ Duyệt web an toàn của Google).
* Chế độ nâng cấp của Cốc Cốc: Hiển thị hộp thoại cảnh báo (pop-up) “Trang web chứa nội dung không an toàn” (dựa vào danh sách đen của Cốc Cốc, dự án Chống Lừa Đảo và của Trung tâm Giám sát an toàn không gian mạng quốc gia cùng chia sẻ cho ngành công nghiệp web).

Từ tháng 01/2021, người dùng Cốc Cốc có thể chủ động báo cáo nội dung không an toàn cho đội ngũ phát triển Cốc Cốc, sau đó Cốc Cốc sẽ trực tiếp kiểm tra và hiển thị cảnh báo rộng rãi tới toàn thể người dùng. Nỗ lực này của Cốc Cốc nhằm hướng tới đẩy lùi vấn nạn lừa đảo qua mạng cùng các nguy cơ không lường trước và đem tới trải nghiệm duyệt web an toàn cho tất cả mọi người.

1. *Xác thực trang web:* Giúp bạn nhận biết trang web chính chủ thông qua biểu tượng Khóa xanh trên thanh địa chỉ của trình duyệt. Các trang web được gắn Khóa xanh trên Trình duyệt Cốc Cốc là các trang web đã được xác thực bởi Cốc Cốc, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) và tiện ích ChongLuaDao.

Các trang được ưu tiên gắn Khóa xanh là: *Trang web của tổ chức, cơ quan nhà nước; Trang web của tổ chức ngân hàng - tài chính; Trang web của các đơn vị tin tức, báo chí; Trang web của các công ty, thương hiệu hoặc dịch vụ trực tuyến.*

Danh sách các trang web được xác thực sẽ được Cốc Cốc liên tục mở rộng, cập nhật và chia sẻ với Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) và tổ chức Chống Lừa Đảo để chung tay giúp người dùng Internet Việt Nam lên mạng an toàn hơn.

1. *Chế độ ẩn danh*

Khi bạn duyệt web ở Chế độ ẩn danh, Cốc Cốc sẽ không lưu lịch sử duyệt web, cookie, dữ liệu trang web, hoặc thông tin đã nhập trong biểu mẫu. Khi bạn đóng tất cả cửa sổ ẩn danh, tất cả phiên đăng nhập của bạn ở Chế độ ẩn danh sẽ kết thúc. Do đó, người khác sử dụng thiết bị này sẽ không thấy hoạt động của bạn.

Tính năng này giúp bạn: Không hiển thị trong lịch sử trình duyệt; Khi đóng tất cả thẻ ẩn danh, Cốc Cốc sẽ xóa mọi dữ liệu trang web và cookie liên kết với phiên duyệt web đó.

Kích hoạt nhanh Chế độ ẩn danh: Trên máy tính: Sử dụng phím tắt Ctrl + Shift + N Trên điện thoại: Nhấn và giữ nút Nhóm tab (biểu tượng là số lượng tab đang mở) trong 2s, sau đó chọn Tab ẩn danh mới.

1. *Khóa trình duyệt*

Tính năng Khóa trình duyệt cho phép bạn thiết lập mã PIN, mật khẩu vân tay (Touch ID) dành cho thiết bị sử dụng hệ điều hành Android hoặc nhận diện khuôn mặt (Face ID) dành cho thiết bị iOS để mở ứng dụng. Nhờ đó, bạn có thể ngăn truy cập trái phép vào ứng dụng và chủ động bảo vệ quyền riêng tư.

Để sử dụng tính năng này: Vào Cài đặt. Chọn Khóa trình duyệt; Thiết lập bảo mật bằng mã pin, vân tay hoặc/và nhận diện khuôn mặt; Mở khóa mỗi lần sử dụng ứng dụng.

**Lưu ý:** Để kích hoạt hiệu lực của tính năng Khóa trình duyệt, người dùng cần lưu ý kiểm tra cài đặt về Touch ID (Android) hoặc Face ID (iOS) trên thiết bị của mình.

***4. Các cách sử dụng điện thoại thông minh hiệu quả, hợp lý nhất***

**1. Sắp xếp các ứng dụng của bạn**

Những ứng dụng bạn tải về và để chúng rải rác khắp màn hình điện thoại có thể gây bối rối khi bạn muốn tìm và sử dụng chúng. Dù là dữ liệu ảo hay giấy tờ ngoài đời thực thì việc bạn rất nên làm chính là sắp xếp chúng một cách ngăn nắp.

Ví dụ các app về mạng xã hội như [Facebook](https://www.thegioididong.com/game-app/facebook-mang-xa-hoi-pho-bien-nhat-219963), [Instagram](https://www.thegioididong.com/game-app/instagram-mang-xa-hoi-anh-pho-bien-nhat-the-gioi-219969) hay [Zalo](https://www.thegioididong.com/game-app/zalo-ung-dung-mang-xa-hoi-pho-bien-viet-nam-219921) thì bạn nên để chúng trong cùng một chủ đề và đặt tên cho chúng. Việc này sẽ tiết kiệm không gian màn hình của bạn, cùng với đó bạn sẽ thấy thoải mái hơn khi dùng điện thoại của mình đấy!



*Sắp xếp các ứng dụng của bạn (ảnh minh họa)*

**2. Sử dụng lệnh đọc thoại và tính năng sửa lỗi chính tả**

Bạn đang sử dụng cách nào để ghi lại những thông tin quan trọng trên điện thoại của mình? Nếu câu trả lời chỉ là soạn văn bản thuần túy thì hãy cân nhắc việc sử dụng các lệnh đọc thoại xem sao.

Bạn có thể chỉ cần nói vào điện thoại và để "dế yêu" của bạn chuyển tải nó thành văn bản, thậm chí là tự sửa lỗi chính tả cho các văn bản đó mà không cần đến sự can thiệp thủ công của bạn, như vậy sẽ nhanh chóng và tiện lợi hơn rất nhiều đấy!



*Sử dụng lệnh đọc thoại và tính năng sửa lỗi chính tả (ảnh minh họa)*

**3. Xóa những ứng dụng không dùng đến**

Nếu bạn là người có thói quen thích trải nghiệm những ứng dụng mới thì ngay bây giờ hãy cầm điện thoại lên và xem có ứng dụng nào bị bạn bỏ quên trong một khoảng thời gian dài không nhé.

Thông thường thì bạn nên dọn dẹp các app mà mình không sử dụng trong khoảng 30 ngày, vì có thể chúng không thực sự cần thiết với bạn. Việc để quá nhiều ứng dụng có thể làm đầy bộ nhớ điện thoại của bạn, thậm chí dung lượng pin cũng nhanh tiêu hao vì một số ứng dụng chạy ngầm ngay cả khi bạn không sử dụng chúng đấy.



*Xóa những ứng dụng không dùng đến (ảnh minh họa)*

**4. Sử dụng tai nghe**

Nghe thì có vẻ đơn giản nhưng việc sử dụng [tai nghe](https://www.thegioididong.com/tai-nghe) sẽ làm cho trải nghiệm sử dụng điện thoại của bạn trở nên tối ưu hơn rất nhiều.

Loa ngoài làm cho âm thanh bị nhiễu động rất nhiều trước khi đến tai bạn. Hãy tưởng tượng bạn đang xem một phim yêu thích, đến một câu thoại quan trọng thì tạp âm bên ngoài làm bạn chẳng nghe thấy gì. Vậy nên hãy đeo tai nghe khi sử dụng điện thoại để không bỏ lỡ những âm thanh tuyệt vời nhé.



*Sử dụng tai nghe (ảnh minh họa)*

**5. Tắt các thông báo cập nhật trạng thái**

Thông báo cập nhật của các ứng dụng sẽ giúp bạn nắm bắt những thông tin quan trọng thường xuyên, tuy nhiên nếu chúng cứ nhảy liên tục thì công việc bạn đang làm có thể sẽ bị gián đoạn vì mất tập trung.

Vậy nên để tăng hiệu quả khi làm việc trên điện thoại, bạn nên tắt thông báo cập nhật. Nhưng cũng đừng lo bỏ lỡ những thông báo quan trọng, vì sau đó bạn có thể vào app để kiểm tra lại.



*Tắt các thông báo cập nhật trạng thái (ảnh minh họa)*

**6. Đặt hẹn giờ**

Tính năng hẹn giờ trên điện thoại và một số ứng dụng vô cùng hữu ích với tính chất công việc bận rộn của bạn. Bạn chỉ cần soạn sẵn một thư trong Gmail hoặc bài đăng Facebook và hẹn giờ cho chúng để chúng tự động được thực hiện sau đó.

Ngoài ra bộ đếm thời gian có sẵn trên điện thoại cũng giúp ích cho công việc của bạn rất nhiều. Hãy thiết lập hẹn giờ rồi làm việc và bạn sẽ nhận được thông báo khi hết thời gian.



*Đặt hẹn giờ (ảnh minh họa)*

**7. Tạm thời tắt kết nối internet**

Nếu vừa có một ngày làm việc mệt mỏi, hãy thử tắt kết nối mạng và làm gì đó thư giãn xem sao. Đọc sách điện tử, nghe nhạc offline, hoặc đơn giản chỉ là kiểm tra lại lịch làm việc của bạn vào ngày mai.

Có một số thao tác trên điện thoại vốn dĩ không cần đến internet, vậy nên đôi lúc hãy tắt tạm thời kết nối mạng để tránh bị phân tâm nhé.



*Tạm thời tắt kết nối internet (ảnh minh họa)*

**8. Cập nhật hệ thống thường xuyên**

Nếu điện thoại của bạn hay gặp lỗi hoặc bị chậm trong quá trình sử dụng thì rất có thể phần mềm điện thoại của bạn là phiên bản cũ. Hãy thường xuyên cập nhật để tận hưởng những tính năng mới và tối ưu.

Bạn có thể cập nhật thủ công hoặc cài đặt tự động cập nhật để hệ thống tự động nâng cấp mỗi khi có phiên bản mới.



*Cập nhật hệ thống thường xuyên (ảnh minh họa)*

**9. Sử dụng những ứng dụng chăm sóc sức khỏe**

Những ứng dụng dùng để theo dõi tình trạng sức khỏe của người dùng smartphone ngày càng phổ biến. Chúng có thể hỗ trợ bạn chăm sóc sức khỏe cá nhân, thư giản, xả stress,... vô cùng hữu ích.



*Sử dụng những ứng dụng chăm sóc sức khỏe (ảnh minh họa)*

Võ Trọng Phú