



SỬ DỤNG MẠNG XÃ HỘI AN TOÀN TRÊN KHÔNG GIAN MẠNG

Trung tâm CNTT và Truyền thông Hải Phòng

SỬ DỤNG MẠNG XÃ HỘI AN TOÀN TRÊN KHÔNG GIAN MẠNG



Sự thay đổi công nghệ trong công tác truyền thông



Thực trạng sử dụng mạng xã hội tại Việt Nam



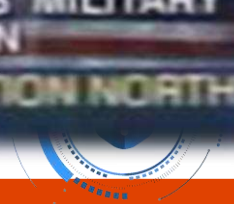
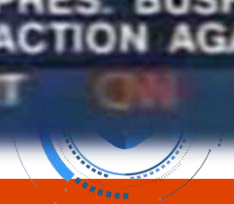
Cảnh giác các thủ đoạn tin giả mạo, chiếm đoạt tài sản



Kỹ năng cơ bản bảo đảm an toàn trên không gian mạng

SỬ DỤNG MẠNG XÃ HỘI AN TOÀN TRÊN KHÔNG GIAN MẠNG

Năm 2001, cả thế giới xem Mỹ tấn công Afghanistan qua CNN (cỡ 4:3)



SỬ DỤNG MẠNG XÃ HỘI AN TOÀN TRÊN KHÔNG GIAN MẠNG



Following

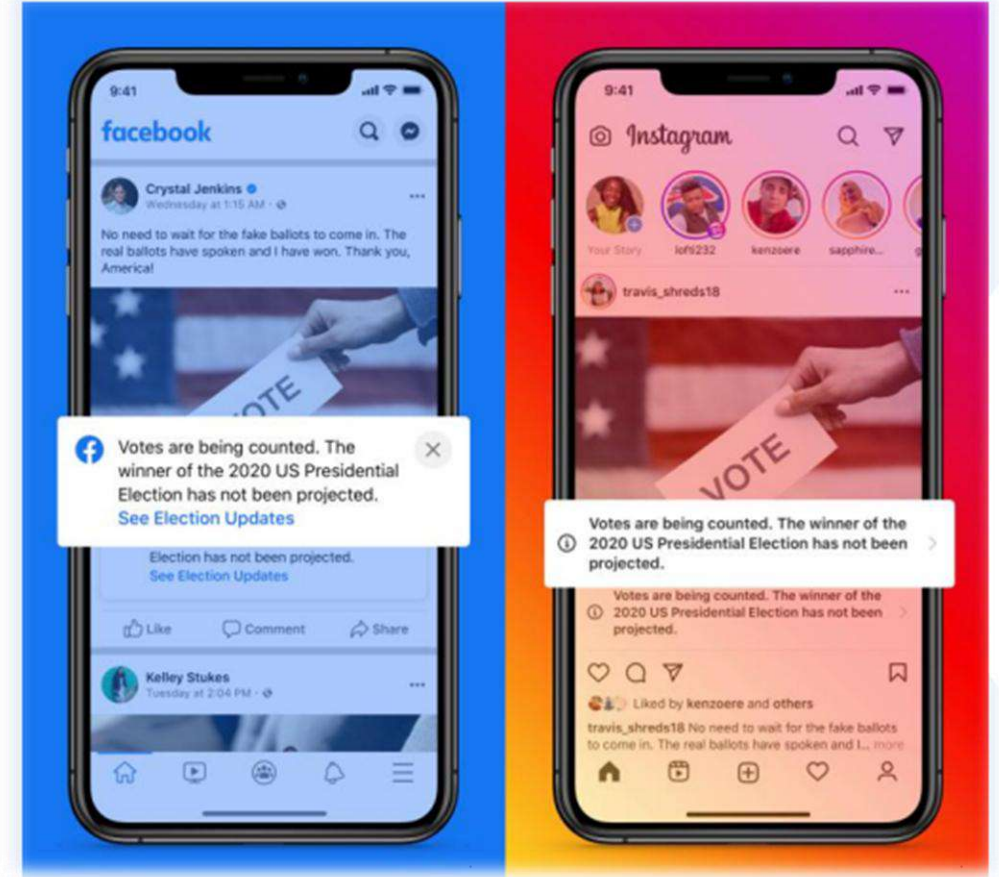
Đến năm 2022, mạng xã hội mới là kênh truyền thông chủ đạo



SỬ DỤNG MẠNG XÃ HỘI AN TOÀN TRÊN KHÔNG GIAN MẠNG



Mỗi khi có sự kiện lớn thì Facebook, Twitter, tiktok,... đều thu hút người dùng bởi tính năng tương tác (like, comment, share)





SỬ DỤNG MẠNG XÃ HỘI AN TOÀN TRÊN KHÔNG GIAN MẠNG

Thống kê sử dụng mạng xã hội năm 2026

- Gần **73,8%** dân số thế giới sử dụng mạng xã hội hiện nay (6,12 tỷ người)
- **5,79** tỷ tài khoản người dùng mạng xã hội hoạt động trên toàn cầu, tương đương 69,9% dân số.
- **56,3%** người dùng Internet từ 16 tuổi trở lên cho biết đã sử dụng Facebook trong tháng gần nhất.
- Người dùng Internet trên toàn cầu hiện dành trung bình hơn 2 giờ 30 phút mỗi ngày cho các nền tảng mạng xã hội và video xã hội (Facebook, Instagram, TikTok, YouTube, X...), tương đương khoảng 18 giờ 36 phút mỗi tuần.
- Hơn 80% người dùng TikTok cho biết họ truy cập nền tảng này chủ yếu để xem nội dung giải trí;

THỰC TRẠNG SỬ DỤNG MẠNG XÃ HỘI TẠI VIỆT NAM

Người dùng mạng xã hội tại Việt Nam



85,6 triệu người sử dụng Internet.

84,2% dân số Việt Nam đang sử dụng Internet.

Số người dùng Internet tăng 508.000 người so với năm trước.

Cứ 10 người Việt Nam thì có hơn 8 người sử dụng Internet.

Gần 8/10 người dân có tài khoản mạng xã hội hoạt động.



Việt Nam là nước có số lượng người sử dụng dịch vụ mạng xã hội Facebook, Tiktok **tăng nhanh nhất** trên thế giới.



THỰC TRẠNG SỬ DỤNG MẠNG XÃ HỘI TẠI VIỆT NAM

Người dùng mạng xã hội tại Việt Nam



Trong đó 85% người có dùng mạng xã hội truy cập vào những trang này ít nhất một lần mỗi ngày và 70% người thừa nhận rằng họ phải truy cập vào mạng xã hội đầu tiên ngay khi vừa mở điện thoại hoặc thiết máy tính.



Thời gian trung bình một người dùng ở Việt Nam sử dụng mạng xã hội là 2 giờ 22 phút. 89% người sử dụng internet có tham gia hoặc đóng góp vào mạng xã hội trong thời gian một tháng gần nhất.



THỰC TRẠNG SỬ DỤNG MẠNG XÃ HỘI TẠI VIỆT NAM

Lợi ích của mạng xã hội, những lợi ích mạng xã hội mang lại là vô cùng lớn và cần thiết cho cuộc sống hiện nay:



Cập nhật tin tức đời sống xã hội



Kết nối các mối quan hệ



Nâng cao kỹ năng sống và sự hiểu biết



Tránh được nhiều hiểm họa trong cuộc sống



Kinh doanh và quảng cáo thương hiệu miễn phí



"MOBILE FIRST" -> "MOBILE ONLY"



THỰC TRẠNG SỬ DỤNG MẠNG XÃ HỘI TẠI VIỆT NAM

Tác hại của sử dụng mạng xã hội, mạng xã hội tiềm ẩn không ít những hiểm họa, khiến cho con người gặp phải nhiều vấn đề vô cùng phức tạp, khó lường trước được:



Làm trì trệ các hoạt động sống của con người



Mạng xã hội tốn quá nhiều thời gian



Nguy cơ tiếp xúc với các nguồn tin lá cải không chính xác



Nguy cơ bị lừa đảo



Ảnh hưởng tới sức khỏe



THỰC TRẠNG SỬ DỤNG MẠNG XÃ HỘI TẠI VIỆT NAM



Thiếu kỹ năng mềm

Ngoại ngữ, CNTT, kỹ năng làm việc nhóm, giao tiếp, tác phong công nghiệp



Fear Of Missing Out

HỘI CHỨNG FOMO



Quy định pháp luật



Khoản 1 Điều 21 Hiến pháp năm 2013: “Mọi người có quyền bất khả xâm phạm về đời sống riêng tư, bí mật cá nhân và bí mật gia đình; có quyền bảo vệ danh dự, uy tín của mình. Thông tin về đời sống riêng tư, bí mật cá nhân, bí mật gia đình được pháp luật bảo đảm an toàn.”



Khoản 5 Điều 9 của Luật Báo chí 2016 quy định cấm “Tiết lộ thông tin thuộc danh Mục bí mật nhà nước, bí mật đời tư của cá nhân và bí mật khác theo quy định của pháp luật.”



THỰC TRẠNG SỬ DỤNG MẠNG XÃ HỘI TẠI VIỆT NAM



Điều 288 BLHS 2015. Tội đưa hoặc sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông

- a) Đưa lên mạng máy tính, mạng viễn thông những thông tin trái với quy định của pháp luật,
- b) Mua bán, trao đổi, tặng cho, sửa chữa, thay đổi hoặc công khai hóa thông tin riêng hợp pháp của cơ quan, tổ chức, cá nhân trên mạng máy tính, mạng viễn thông mà không được phép của chủ sở hữu thông tin đó;
- c) Hành vi khác sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông.



Hành vi bị cấm trong luật an ninh mạng



A) Chiếm đoạt, mua bán, thu giữ, cố ý làm lộ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân;



B) Cố ý xóa, làm hư hỏng, thất lạc, thay đổi thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư được truyền đưa, lưu trữ trên không gian mạng;



THỰC TRẠNG SỬ DỤNG MẠNG XÃ HỘI TẠI VIỆT NAM



C) Cố ý thay đổi, hủy bỏ hoặc làm vô hiệu hóa biện pháp kỹ thuật được xây dựng, áp dụng để bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư.



D) Đưa lên không gian mạng những thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trái quy định của pháp luật;



E) Cố ý nghe, ghi âm, ghi hình trái phép các cuộc đàm thoại;



F) Hành vi khác cố ý xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư.



Quyền của trẻ em



Điều 16 Công ước quốc tế về quyền trẻ em: Không trẻ em nào phải chịu sự can thiệp tùy tiện hay bất hợp pháp vào việc riêng tư, gia đình, nhà cửa hoặc thư tín cũng như những sự công kích bất hợp pháp vào danh dự và thanh danh của các em; trẻ em có quyền được pháp luật bảo vệ chống lại sự can thiệp hay công kích như vậy.



khoản 11 Điều 6 Luật Trẻ em năm 2016 cấm: Công bố, Tiết lộ thông tin về đời sống riêng tư, bí mật cá nhân của trẻ em mà không được sự đồng ý của trẻ em từ đủ 07 tuổi trở lên và của cha, mẹ, người giám hộ của trẻ em.



THỰC TRẠNG SỬ DỤNG MẠNG XÃ HỘI TẠI VIỆT NAM



Điều 33 của Nghị định 56/2017/NĐ-CP quy định chi tiết một số điều của Luật Trẻ em giải thích rõ:

Thông tin **bí mật đời sống riêng tư, bí mật cá nhân** của trẻ em là các thông tin về:

- tên, tuổi;
- đặc điểm nhận dạng cá nhân;
- thông tin về tình trạng sức khỏe và đời tư được ghi trong bệnh án;
- hình ảnh cá nhân;
- thông tin về các thành viên trong gia đình, người chăm sóc trẻ em;
- tài sản cá nhân;
- số điện thoại;
- địa chỉ thư tín cá nhân;
- địa chỉ, thông tin về nơi ở, quê quán;
- địa chỉ, thông tin về trường, lớp, kết quả học tập và các mối quan hệ bạn bè của trẻ em;
- thông tin về dịch vụ cung cấp cho cá nhân trẻ em



Quyền của cá nhân đối với hình ảnh theo quy định của BLDS 2015

Cá nhân có quyền đối với hình ảnh của mình.

Việc sử dụng hình ảnh của cá nhân phải được người đó đồng ý.

Việc sử dụng hình ảnh của người khác vì mục đích thương mại thì phải trả thù lao cho người có hình ảnh, trừ trường hợp các bên có thỏa thuận khác

Việc sử dụng hình ảnh trong trường hợp sau đây không cần có sự đồng ý của người có hình ảnh hoặc người đại diện theo pháp luật của họ:

- a) Hình ảnh được sử dụng vì lợi ích quốc gia, dân tộc, lợi ích công cộng;
- b) Hình ảnh được sử dụng từ các hoạt động công cộng, bao gồm hội nghị, hội thảo, hoạt động thi đấu thể thao, biểu diễn nghệ thuật và hoạt động công cộng khác mà không làm tổn hại đến danh dự, nhân phẩm, uy tín của người có hình ảnh.



THỰC TRẠNG SỬ DỤNG MẠNG XÃ HỘI TẠI VIỆT NAM



Nghị định số 174/2026/NĐ-CP quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử.



CẢNH GIÁC CÁC THỦ ĐOẠN TIN GIẢ MẠO, CHIẾM ĐOẠT TÀI SẢN

Mạo danh các nhà mạng, cơ quan nhà nước

Các đối tượng lừa đảo thông qua những thông tin của nạn nhân chia sẻ trên mạng xã hội đã giả mạo thành nhân viên các nhà mạng VNPT, FPT,... hoặc giả mạo cán bộ Công an, Viện kiểm sát để gọi điện thoại lừa nạn nhân chuyển cho chúng một số tiền nhất định.



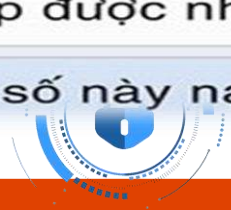
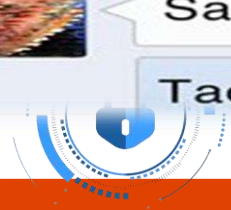
CẢNH GIÁC CÁC THỦ ĐOẠN TIN GIẢ MẠO, CHIẾM ĐOẠT TÀI SẢN

Hack tài khoản mạng xã hội để lừa đảo

Các đối tượng lừa đảo sau khi chiếm được tài khoản mạng xã hội của một người nào đó, sẽ dùng tài khoản đó để nhắn tin đến bạn bè, người thân của người đó để mượn tiền. Nhiều người vì tin đó là bạn bè, người thân mình thật nên đã chuyển tiền cho các tài khoản này và đã bị mất rất nhiều tiền.



The screenshot shows a chat interface with a scammer's profile picture (a blurry, pixelated face). The scammer sends a message: "Mua hộ cái thẻ cào 100k vina nhé!". A friend replies: "Đây, tự cào đi!". The scammer then sends a screenshot of a "HƯỚNG DẪN SỬ DỤNG" (Usage Instructions) for a 100k Vina card. The instructions are: "1. Cào nhẹ lớp phủ dưới đây để biết 13 chữ số mã thẻ" (Gently scratch the layer below to know the 13-digit card number) and "2. Từ bàn phím máy điện thoại di động bấm" (From the mobile phone keyboard, press). The friend replies: "Cào hộ cái". The scammer sends another screenshot of the same instructions, but this time the card number "4680 98700 5189" is visible. The friend replies: "Này thì cào...". The scammer asks: "Sao không nạp được nhỉ?". The friend replies: "Tao vừa dùng số này nạp ngon mà".



CẢNH GIÁC CÁC THỦ ĐOẠN TIN GIẢ MẠO, CHIẾM ĐOẠT TÀI SẢN

Link clip, hình ảnh nóng

Dạng lừa đảo này thường xuất hiện dưới dạng comment kèm theo link dưới các bài viết trong các group. Nạn nhân vì tò mò mà bấm vào, dẫn đến bị chiếm đoạt tài khoản mạng xã hội và thông tin cá nhân. Chưa kể đường link đó còn kèm theo yêu cầu cài đặt phần mềm như Flash Player mà nếu nạn nhân cài vào máy thì sẽ bị kiểm soát cả máy tính, mất các thông tin, tài liệu quan trọng lưu trữ trong máy tính.



CẢNH GIÁC CÁC THỦ ĐOẠN TIN GIẢ MẠO, CHIẾM ĐOẠT TÀI SẢN

Tặng quà từ nước ngoài

Đánh vào tâm lý sính ngoại của nạn nhân, đối tượng lừa đảo sẽ giả mạo người nước ngoài, sau khi nói chuyện một thời gian sẽ đề nghị được tặng nạn nhân một món quà, nhưng để nhận được món quà đó thì nạn nhân phải chi một khoản tiền để thanh toán phí hải quan và phí vận chuyển. Món quà thường được nói là có giá trị lớn để mức phí hải quan cao, khiến nạn nhân không nghi ngờ mà chuyển một số tiền lớn cho đối tượng lừa đảo. Sau khi được chuyển tiền thì các đối tượng sẽ chặn tài khoản nạn nhân và tiếp tục lừa đảo đối tượng khác.



CẢNH GIÁC CÁC THỦ ĐOẠN TIN GIẢ MẠO, CHIẾM ĐOẠT TÀI SẢN

Giả mạo bán hàng

Đối tượng lừa đảo mở ra các page bán hàng online trên mạng xã hội, yêu cầu khách mua hàng ứng trước một khoản tiền trước khi giao hàng. Những khách hàng nhẹ dạ, cả tin sau khi ứng tiền cho các đối tượng lừa đảo thì sẽ bị chặn tài khoản và không thể nào lấy lại tiền.





KỸ NĂNG CƠ BẢN BẢO ĐẢM AN TOÀN TRÊN
KHÔNG GIAN MẠNG

KỸ NĂNG

NHẬN BIẾT, PHÁT HIỆN TIN GIẢ
PHÁT HIỆN QUAN ĐIỂM CÁ NHÂN



KỸ NĂNG CƠ BẢN BẢO ĐẢM AN TOÀN TRÊN KHÔNG GIAN MẠNG

Tin giả là gì?



Tin giả là những thông tin giả mạo, sai sự thật hay hoàn toàn hư cấu, câu chuyện không đúng sự thật.



Từ điển Collins: tin tức giả là “những thông tin sai, thường là giật gân, được phát tán dưới vỏ bọc tin tức”.



KỸ NĂNG CƠ BẢN BẢO ĐẢM AN TOÀN TRÊN KHÔNG GIAN MẠNG

Phân loại tin tức giả



Loại thứ nhất là những thông tin hoàn toàn không chính xác (bao gồm cả những thông tin thông thường và những thông tin được trình bày giống như một tin báo chí) được cố tình đăng tải, lan truyền vì một mục đích nào đó.



Loại thứ hai là những thông tin có thể có một phần sự thật nhưng không hoàn toàn chính xác do người viết chúng không kiểm chứng toàn bộ sự thật trước khi đăng tải chia sẻ hoặc có thể họ phóng đại một phần của câu chuyện đó.



KỸ NĂNG CƠ BẢN BẢO ĐẢM AN TOÀN TRÊN KHÔNG GIAN MẠNG



TIN VU KHỔNG

Cắt ghép, ngụy tạo hình ảnh, clip, tạo ra 1 câu chuyện không đúng... để bôi nhọ



TIN LỪA ĐẢO

Chỉ chứa 1 phần thông tin sự thật (1 thông tin, 1 câu trích lấy ra từ 1 bối cảnh)... để trục lợi



TIN CÂU "VIEW"

Tựa bài gây sốc nhưng khác nội dung, kích thích người đọc bấm vào để tăng view



TIN THIÊN VỊ

Sự kiện thực tế bị người viết thao túng theo hướng có lợi cho 1 mục đích

KỸ NĂNG CƠ BẢN BẢO ĐẢM AN TOÀN TRÊN KHÔNG GIAN MẠNG



Đặc trưng chung nhất của những tin tức giả kiểu này là chúng thường xuất phát từ **những sự kiện, hiện tượng nóng**, gây tranh cãi trong đời sống thực. Những sự kiện nào càng nóng, càng gây tranh cãi thì càng là đề tài béo bở cho tin tức giả phát tác từ đó. Chẳng hạn như những tin tức về **các sự kiện chính trị quan trọng** như bầu cử, họp Quốc hội, về thiên tai nghiêm trọng, khủng bố,...



Động cơ của các đối tượng sản xuất loại tin tức giả này có thể vì mục đích tài chính, chính trị hay hạ uy tín của cá nhân, tổ chức một cách có chủ đích. Tuy nhiên, có những trường hợp, các đối tượng tạo ra tin tức giả chỉ đơn giản để được nổi bật, thu hút sự chú ý.



KỸ NĂNG CƠ BẢN BẢO ĐẢM AN TOÀN TRÊN KHÔNG GIAN MẠNG

Các quan điểm sai trái mà các thế lực thù địch tuyên truyền trên mạng xã hội

-  Thứ nhất, xuyên tạc nền tảng tư tưởng chính trị và thủ tiêu ý thức hệ (các bài viết, video phủ định, phản bác Chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh, phủ nhận vai trò lãnh đạo của Đảng và con đường đi lên CNXH của nước ta)
-  Thứ hai, bôi nhọ, xuyên tạc đường lối và thể chế chính trị xã hội chủ nghĩa, ca ngợi chủ nghĩa tư bản với những giá trị khác nhau.
-  Thứ ba, vu khống Đảng Cộng sản Việt Nam cầm quyền, áp bức người dân, chia rẽ phá hoại mối quan hệ mật thiết giữa Nhân dân với Đảng và Nhà nước.





KỸ NĂNG CƠ BẢN BẢO ĐẢM AN TOÀN TRÊN KHÔNG GIAN MẠNG

Các quan điểm sai trái mà các thế lực thù địch tuyên truyền trên mạng xã hội



Thứ tư, khoét sâu vấn đề tôn giáo, dân tộc, nhân quyền với thể chế xã hội chủ nghĩa nhằm phá vỡ khối đại đoàn kết toàn dân tộc



Thứ năm, lợi dụng các vấn đề nhạy cảm trong đời sống chính trị xã hội của nước nhà, vụ việc phức tạp thu hút sự quan tâm của quần chúng làm hạ uy tín, bôi nhọ cá nhân các lãnh tụ, lãnh đạo của Đảng như tham nhũng, khiếu kiện, tội phạm, tệ nạn xã hội, tình hình dịch bệnh Covid-19, việc bắt, xử lý các đối tượng chống phá Nhà nước Việt Nam



Thứ sáu, xuyên tạc lịch sử dân tộc, lịch sử Đảng, lịch sử đấu tranh giải phóng dân tộc và xây dựng đất nước làm cho một bộ phận quần chúng thiếu hiểu biết về lịch sử dân tộc nhất là giới trẻ hoài nghi, phai nhạt niềm tin đối với Đảng, chia rẽ Đảng với Nhân dân.

KỸ NĂNG CƠ BẢN BẢO ĐẢM AN TOÀN TRÊN KHÔNG GIAN MẠNG

Hậu quả của tin giả, tin sai sự thật



Làm ảnh hưởng xấu đến uy tín, danh dự của cá nhân, tổ chức, thậm chí nguy hiểm tính mạng



Gây bất bình trong dư luận, tạo dư luận xấu, gây hoang mang trong xã hội, giảm sút lòng tin với Đảng,



Ảnh hưởng kinh tế (lừa đảo....)



Làm suy giảm niềm tin của công chúng vào truyền thông nói chung và của báo chí chủ lưu nói riêng. Chúng khiến cho công chúng không xác định được đâu là những nguồn tin đáng tin cậy để tiếp nhận,...



KỸ NĂNG CƠ BẢN BẢO ĐẢM AN TOÀN TRÊN KHÔNG GIAN MẠNG



KIỂM TRA XUẤT XỨ THÔNG TIN

Tin từ các trang có "đuôi" tên miền lạ lẫm như ".co" hay ".su"..., hãy cảnh giác!!!



XEM XÉT NGUỒN TIN TRONG BÀI

Tin giả không nêu được thông báo hay tuyên bố gì của những đơn vị liên quan tới thông tin phát tán



KIỂM TRA TỰA BÀI CÓ KHỚP VỚI NỘI DUNG

Đừng nên chỉ đọc tựa mà thậm chí không nhấp vào để xem thực chất nội dung



KIỂM TRA THỜI GIAN THÔNG TIN

Nhiều thông tin bị "khai quật" chỉnh sửa thời gian ngụy tạo như sự kiện vừa xảy ra



XEM XÉT ĐỘ PHỦ SÓNG

Tìm kiếm thêm các nguồn tin chính thống khác xem có nói gì về sự việc đó không



TRUY LẠI NHỮNG CÂU TRÍCH DẪN

Tìm kiếm, kiểm tra phát ngôn của những người nổi tiếng vừa được đề cập trong bài báo



XEM LẠI CHỦ QUAN BẢN THÂN

Nếu đọc được một thông tin và nhận thấy có vẻ như "hay tới mức khó tin" và "đúng như mình nghĩ" thì hãy cẩn trọng!!



KIỂM TRA CHÉO

Thông qua các trang web kiểm tra sự thật (Snopes, Politifact)

KỸ NĂNG CƠ BẢN BẢO ĐẢM AN TOÀN TRÊN KHÔNG GIAN MẠNG

Học cách phát hiện ra các quan điểm cá nhân



“Sự kiện” là khách quan, còn “quan điểm” là chủ quan



Cái thực sự cần, đó là “sự thật khách quan”! Bởi vì “quan điểm” thường tìm cách lôi kéo người đọc nghĩ theo cách mà họ muốn, còn “sự kiện” cho phép người đọc tự đánh giá và rút ra kết luận.



“Quan điểm” thường mang tính kích động, “sự kiện” thường mang tính tường thuật/miêu tả, và tin giả thường nhắm vào cái đầu tiên.



KỸ NĂNG CƠ BẢN BẢO ĐẢM AN TOÀN TRÊN KHÔNG GIAN MẠNG

Cẩm nang “Phòng chống tin giả, tin sai sự thật trên không gian mạng”

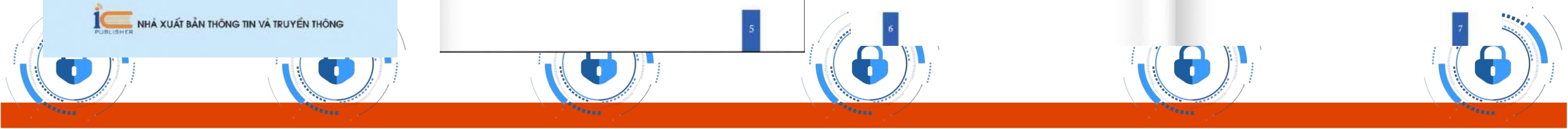
http://vnbook.com.vn/books/camnagphongchongtingia_output/web/index.html



MỤC LỤC	
<i>Giới thiệu cẩm nang</i>	9
08 Điều cần nhớ	11
1. Dấu hiệu nhận biết một tin giả	12
2. Cách xác định tin giả	13
3. Làm thế nào để tránh “bẫy tin giả”?	14
4. Phải làm gì nếu lỡ đăng tải, chia sẻ tin giả, tin sai sự thật?	15
5. Cách xử lý khi thấy tin giả	16
6. Hành động có trách nhiệm trên không gian mạng	18
7. Hậu quả của việc cung cấp, chia sẻ tin giả, tin sai sự thật	21
8. Các mức phạt hành chính/xử lý hình sự	22
Khái niệm tin giả trên không gian mạng	25
1. Thế nào là tin giả	26
2. Tin giả được tạo ra như thế nào?	27
3. Tin giả tác động đến công chúng bằng cách nào?	28
4. Phân loại tin giả	30
Tác động của tin giả, tin sai sự thật trên không gian mạng	34
1. Tác động đến an ninh - kinh tế	35
2. Tác động đến an ninh quốc gia	36

3. Tác động đến niềm tin của người dân với các thông tin trên báo chí chính thống	37
4. Tác động đến sức khỏe cộng đồng	38
Hướng dẫn nhận biết tin giả, tin sai sự thật trên không gian mạng	42
1. Xem xét nguồn tin, kiểm tra tác giả	43
2. Kiểm tra thông tin, hình ảnh minh họa và đường dẫn liên kết	47
3. Kiểm tra thời gian	48
4. Đọc toàn bộ nội dung, tìm những điểm nghi ngờ, mâu thuẫn	48
5. Đối chiếu với thông tin trên báo chí chính thống hoặc tham khảo ý kiến chuyên gia hoặc các cơ quan chức năng	50
Trách nhiệm của các tổ chức, cá nhân trên không gian mạng	53
1. Trách nhiệm của người sử dụng Internet, mạng xã hội	54
2. Trách nhiệm của nhà cung cấp dịch vụ	57
3. Trách nhiệm của người kinh doanh dịch vụ quảng cáo, người phát hành quảng cáo, người quảng cáo	58
Các quy định của pháp luật liên quan đến hành vi đăng tải, lan truyền tin giả, tin sai sự thật trên không gian mạng	62
Quy trình tiếp nhận và xử lý tin giả trên không gian mạng	71
Những câu hỏi thường gặp	75
Phụ lục 1: Các bộ quy tắc ứng xử trên mạng xã hội	84
I. Bộ quy tắc ứng xử trên mạng xã hội do Bộ Thông tin và Truyền thông ban hành	84

II. Quy tắc sử dụng mạng xã hội của người làm báo Việt Nam do Hội Nhà báo Việt Nam ban hành	87
III. Quy tắc ứng xử của người hoạt động trong lĩnh vực nghệ thuật do Bộ Văn hóa, Thể thao và Du lịch ban hành	88
Phụ lục 2: Quy định về tin giả trong tiêu chuẩn cộng đồng trên một số mạng xã hội xuyên biên giới	90
I. Facebook	90
II. YouTube	92
III. TikTok	93
Tài liệu tham khảo	96



1. Dấu hiệu nhận biết một tin giả



Khi đọc thông tin trên mạng, nếu thấy có những dấu hiệu sau thì rất có thể bạn đang đọc một tin giả:

- ➡ Tiêu đề giật gân, thu hút, nội dung thông tin mới lạ, thường đề cập đến một vấn đề nóng đang được nhiều người quan tâm.
- ➡ Thông tin không ghi nguồn hoặc nguồn không rõ ràng.
- ➡ Thông tin xuất phát từ những trang web, tài khoản, kênh nội dung trên mạng xã hội thường xuyên tung tin giả, hoặc từ những trang, tài khoản, kênh không thuộc cơ quan báo chí chính thống hoặc cơ quan nhà nước.

2. Cách xác định tin giả

Khi nghi ngờ một tin giả, bạn cần thực hiện những bước sau để kiểm tra, xác minh:

- ➡ Xem xét nguồn tin, kiểm tra tác giả.
- ➡ Kiểm tra thông tin, hình ảnh minh họa và đường dẫn liên kết.
- ➡ Kiểm tra thời gian.
- ➡ Đọc toàn bộ nội dung, tìm những điểm nghi ngờ, mâu thuẫn.
- ➡ Đối chiếu với thông tin trên báo chí chính thống hoặc tham khảo ý kiến chuyên gia hoặc các cơ quan chức năng.



3. Làm thế nào để tránh bẫy “tin giả”?



Ngày nay, tin giả có thể được tạo ra bằng nhiều phương thức tinh vi khiến cho ngay cả khi bạn là một công dân có trách nhiệm thì vẫn có thể vô tình sập “bẫy tin giả”. Vì vậy, bạn cần tự trang bị một số kiến thức cần thiết để bảo vệ chính mình khỏi những nguy cơ từ trên mạng.

- ✎ Không tin ngay vào tất cả mọi thứ bạn thấy trên mạng.
- ✎ Suy nghĩ hai lần trước khi chia sẻ, đăng tải hoặc bình luận video, hình ảnh, tin tức trên mạng.
- ✎ Hỏi thăm, tham khảo ý kiến của bạn bè, người thân khi bạn cảm thấy chưa chắc chắn hoặc chờ sự xác nhận thông tin từ cơ quan báo chí chính thống hoặc cơ quan có thẩm quyền.

4. Phải làm gì nếu lỡ đăng tải, chia sẻ tin giả, tin sai sự thật?

- ✎ Gỡ bỏ thông tin sai sự thật.
- ✎ Đưa ra lời đính chính, xin lỗi.
- ✎ Hợp tác với cơ quan chức năng nếu có yêu cầu.





QUY TẮC ỨNG XỬ CHUNG

- ▶ Tôn trọng, tuân thủ pháp luật
- ▶ Lành mạnh
- ▶ An toàn, bảo mật thông tin
- ▶ Trách nhiệm



01 QUY TẮC ỨNG XỬ CHO TỔ CHỨC, CÁ NHÂN

- ▶ Tìm hiểu và tuân thủ các điều khoản hướng dẫn sử dụng của nhà cung cấp mạng xã hội
- ▶ Sử dụng họ, tên thật cá nhân, tên hiệu thật của tổ chức, cơ quan
- ▶ Tự quản lý, bảo mật tài khoản
- ▶ Thông báo tới cơ quan chức năng khi bị mất tài khoản, giả mạo
- ▶ Chia sẻ thông tin có nguồn chính thống, đáng tin cậy
- ▶ Có hành vi, ứng xử phù hợp với đạo đức, văn hóa, truyền thống của dân tộc
- ▶ Không sử dụng từ ngữ gây thù hận, kích động bạo lực
- ▶ Không đăng tải nội dung vi phạm pháp luật
- ▶ Không tung tin giả, tin sai sự thật
- ▶ Sử dụng mạng xã hội để quảng bá đất nước, con người Việt Nam
- ▶ Cùng tham gia bảo vệ, hướng dẫn trẻ em sử dụng mạng xã hội an toàn



02 QUY TẮC ỨNG XỬ CHO CÁN BỘ, CÔNG CHỨC, VIÊN CHỨC VÀ NGƯỜI LAO ĐỘNG TRONG CƠ QUAN NHÀ NƯỚC



- ▶ Thực hiện những quy tắc dành cho cá nhân, tổ chức như trên
- ▶ Thực hiện nội quy của cơ quan, tổ chức về cung cấp thông tin lên mạng xã hội
- ▶ Thông báo tới cơ quan chủ quản khi có ý kiến, thông tin trái chiều, vi phạm pháp luật

03 QUY TẮC ỨNG XỬ CHO CÁC CƠ QUAN NHÀ NƯỚC

- ▶ Quản lý, bảo mật tài khoản mạng xã hội
- ▶ Thông báo khi tài khoản của cơ quan, tổ chức bị mất hoặc giả mạo
- ▶ Cung cấp thông tin trên mạng xã hội thống nhất với thông tin trên truyền thông
- ▶ Phản hồi ý kiến trên mạng xã hội liên quan đến cơ quan, tổ chức



04 QUY TẮC ỨNG XỬ CHO CÁC NHÀ CUNG CẤP DỊCH VỤ MẠNG XÃ HỘI



- ▶ Công bố rõ ràng các điều khoản sử dụng dịch vụ
- ▶ Công khai biện pháp xử lý, ngăn chặn nội dung thông tin vi phạm
- ▶ Phối hợp với tổ chức, cá nhân sử dụng mạng xã hội để xử lý theo pháp luật
- ▶ Hướng dẫn người sử dụng mạng xã hội, hỗ trợ và bảo vệ quyền, lợi ích hợp pháp của "người yếu thế"
- ▶ Không thu thập thông tin cá nhân và cung cấp thông tin cho bên thứ ba



KỸ NĂNG CƠ BẢN BẢO ĐẢM AN TOÀN TRÊN
KHÔNG GIAN MẠNG

KỸ NĂNG

PHÒNG TRÁNH HACK TÀI KHOẢN FACEBOOK



KỸ NĂNG CƠ BẢN BẢO ĐẢM AN TOÀN TRÊN KHÔNG GIAN MẠNG

Cách phòng tránh



Không đăng nhập vào Facebook trên các thiết bị lạ
Đề phòng các email yêu cầu đăng nhập tài khoản facebook

Kiểm tra địa chỉ trang đăng nhập có đúng là facebook.com hay không.

Sử dụng trình duyệt Chrome khi đăng nhập. Do Chrome tích hợp tiện ích xác định trang phishing.

Bật tính năng xác thực 2 bước, nhận mã xác nhận qua điện thoại khi đăng nhập Facebook trên máy tính lạ.

Không truy cập các liên kết lạ được gửi bởi bạn bè thông qua Messenger.

Cài đặt và thường xuyên cập nhật phần mềm diệt virus



KỸ NĂNG CƠ BẢN BẢO ĐẢM AN TOÀN TRÊN KHÔNG GIAN MẠNG

Mật khẩu được lưu trên trình duyệt

Hầu hết các trình duyệt web đều hỗ trợ tính năng mặc định về lựa chọn lưu “tên người dùng” và “mật khẩu” sau khi đăng nhập Facebook thành công. Nhằm bỏ qua bước nhập lại mật khẩu khi đăng nhập trong các lần truy cập tiếp theo sau đó.

Các mật khẩu đó đều được lưu trữ tại máy tính và có thể được xem lại dễ dàng. Chính vì vậy mà bất kỳ ai cũng có thể hack tài khoản facebook từ trang quản lý mật khẩu của trình duyệt.

Mật khẩu

Mật khẩu đã lưu

Tìm kiếm mật khẩu

m	community.mytheshop.com/for...		X
G	datingguru101.com/wp-login.php		
	www.bidvertiser.com/bdv/BidVertis...		
	www.bidvertiser.com/bdv/BidVertis...		
	www4.cbox.ws/box/		
	https://jetpack.wordpress.com/jetp...		
	https://public-api.wordpress.com/...		
	https://www.fttech.vn		

Cách phòng tránh

Không lưu mật khẩu trên trình duyệt.

Luôn sử dụng mật khẩu mạnh cho máy tính





KỸ NĂNG CƠ BẢN BẢO ĐẢM AN TOÀN TRÊN KHÔNG GIAN MẠNG

Hack từ điện thoại

Hiện nay, đa số người dùng đều truy cập Facebook bằng smartphone. Việc chiếm quyền truy cập vào smartphone của nạn nhân cũng dẫn đến việc truy cập được vào tài khoản Facebook. Hoặc tin tặc có thể bí mật cài phần mềm độc hại để theo dõi và lấy cắp thông tin - trong đó có mật khẩu Facebook một cách dễ dàng. Hai trong số các phần mềm gián điệp dùng để theo dõi smartphone phổ biến nhất là Spy Phone Gold và Mobile Spy.

Cách phòng tránh

- Cài đặt phần mềm diệt virus uy tín.
- Không cài các ứng dụng không rõ nguồn gốc.
- Gỡ bỏ các ứng dụng đáng nghi ngờ.



KỸ NĂNG CƠ BẢN BẢO ĐẢM AN TOÀN TRÊN KHÔNG GIAN MẠNG

USB Hacking

Tin tặc có thể sử dụng USB độc hại để truy cập vào được máy tính của nạn nhân, nhằm quét và trích xuất mật khẩu lưu trong trình duyệt Internet.

Cách phòng tránh

- Sử dụng các USB đã được kiểm tra và xác định an toàn.
- Quét mã độc USB ngay khi được kết nối vào thiết bị.
- Cập nhật phần mềm diệt virus thường xuyên.
- Thay đổi mật khẩu định kỳ cho tài khoản facebook





KỸ NĂNG CƠ BẢN BẢO ĐẢM AN TOÀN TRÊN KHÔNG GIAN MẠNG

Sử dụng kỹ nghệ xã hội (Social Engineering)

Tấn công Social Engineering là hình thức phổ biến và dễ thực hiện nhất. Với các mật khẩu Facebook có thể dễ dàng được đoán ra như ngày sinh, số điện thoại, tên công ty hay thậm chí là tên bạn gái, tin tặc có thể dễ dàng sử dụng kỹ thuật này để đoán và chiếm đoạt tài khoản Facebook người dùng.

Cách phòng tránh

- Không chia sẻ thông tin cá nhân thông qua email, điện thoại, chat Messenger.
- Không sử dụng mật khẩu dễ đoán.
- Không sử dụng một mật khẩu cho nhiều tài khoản ở các trang web khác nhau.





KỸ NĂNG CƠ BẢN BẢO ĐẢM AN TOÀN TRÊN KHÔNG GIAN MẠNG

Hack từ mạng Wifi

Tin tặc có thể hack router WiFi nếu mật khẩu để thiết lập bảo mật cho router yếu. Từ đó, chiếm quyền điều khiển lưu lượng Internet, lấy cắp tài khoản Facebook của nạn nhân.

Cách phòng tránh

- Hạn chế sử dụng các điểm truy cập Wifi công cộng.
- Thay đổi mật khẩu Wifi thường xuyên.



KỸ NĂNG CƠ BẢN BẢO ĐẢM AN TOÀN TRÊN KHÔNG GIAN MẠNG

Log out



Nhiều người dùng thường xuyên quên (thậm chí không bao giờ) thoát tài khoản Facebook sau khi sử dụng.



Do đó, bất kỳ ai cũng có thể truy cập vào tài khoản Facebook mà chẳng cần đến các kỹ thuật phức tạp để có được mật khẩu, đặc biệt nếu quên thoát khỏi tài khoản tại tiệm net hay những chiếc máy tính công cộng.



Vì vậy, hãy chắc chắn đăng xuất khỏi tài khoản Facebook sau mỗi lần đăng nhập



KỸ NĂNG CƠ BẢN BẢO ĐẢM AN TOÀN TRÊN KHÔNG GIAN MẠNG

Chúng ta hoàn toàn có thể hướng dẫn sử dụng mạng xã hội an toàn, hiệu quả, có văn hóa.

-  Bảo mật thông tin cá nhân. ...
-  Suy nghĩ kỹ trước khi chia sẻ bất cứ điều gì ...
-  Ứng xử văn minh trên mạng. ...
-  Nhận biết các dạng lừa đảo qua mạng. ...
-  Giới hạn thời gian sử dụng mạng xã hội.





HƯỚNG DẪN KỸ NĂNG SỬ DỤNG INTERNET AN TOÀN VÀ PHÒNG TRÁNH LỪA ĐẢO TRỰC TUYẾN CHO HỌC SINH

PHẦN 1: NHẬN DIỆN CÁC HÌNH THỨC LỪA ĐẢO TRỰC TUYẾN

Các đối tượng xấu thường lợi dụng sự cả tin, tâm lý ham rẻ hoặc thiếu kinh nghiệm của học sinh, sinh viên để thực hiện hành vi lừa đảo. Hãy cảnh giác và bảo vệ bản thân trên không gian mạng!



1 GIẢ MẠO NGƯỜI QUEN (THẤY CÔ, BẠN BÈ, NGƯỜI THÂN)



Tội phạm mạng thường chiếm đoạt tài khoản Facebook, Zalo của người quen để nhắn tin vay tiền, xin mã OTP hoặc gửi đường link giả mạo.

2 “TRÚNG THƯỞNG - HỌC BỔNG - NHẬN QUÀ”



HSSV được gửi tin nhắn thông báo trúng thưởng, nhận học bổng, nhận quà... yêu cầu truy cập trang web lạ hoặc cung cấp thông tin cá nhân.

3 QUÉT MÃ QR - ĐƯỜNG LINK ĐỘC HẠI



Nhiều trang web giả mạo yêu cầu nhập số căn cước công dân, mật khẩu, mã OTP hoặc tải ứng dụng không rõ nguồn gốc.

4 LỪA ĐẢO MUA BÁN ONLINE



Lợi dụng nhu cầu mua sắm giá rẻ của HSSV để rao bán hàng kém chất lượng, yêu cầu chuyển khoản trước nhưng không giao hàng.

5 GIẢ MẠO TUYỂN DỤNG, LÀM THÊM



VIỆC NHẹ LƯƠNG CAO

- ✓ Không cần kinh nghiệm
- ✓ Thu nhập 10-50 triệu/tháng
- ✓ Làm online tại nhà

ĐĂNG KÝ NGAY

Đăng tin việc nhẹ - lương cao, yêu cầu “đặt cọc”, “mua mã nhiệm vụ”, “ứng phí” trước.



6 LỪA ĐẢO TRÊN FACEBOOK, ZALO



Giả mạo fanpage thương hiệu lớn, lập nhóm đầu tư ảo, dụ dỗ tham gia khóa học làm giàu nhanh, kêu gọi chuyển tiền đầu tư.

Nhóm đầu tư ảo

LỢI NHUẬN KHỦNG



7 ỨNG DỤNG GIẢ MẠO, PHẦN MỀM ĐỘC HẠI



Ứng dụng giả dạng ngân hàng, game, tiện ích học tập, ứng dụng công gây đánh cắp dữ liệu, theo dõi thiết bị, chiếm quyền điều khiển tài khoản.



GHI NHỚ QUAN TRỌNG

Cảnh giác - Kiểm tra kỹ - Không vội tin - Không vội chuyển tiền
Bảo vệ thông tin cá nhân chính là bảo vệ an toàn cho chính bạn!



AN TOÀN TRÊN MẠNG
HỌC TẬP HIỆU QUẢ - TƯƠNG LAI VỮNG CHẮC



HÃY CẢNH GIÁC ĐỂ KHÔNG TRỞ THÀNH NẠN NHÂN CỦA LỪA ĐẢO TRỰC TUYẾN!



HƯỚNG DẪN KỸ NĂNG SỬ DỤNG INTERNET AN TOÀN VÀ PHÒNG TRÁNH LỪA ĐẢO TRỰC TUYẾN CHO HỌC SINH

PHẦN 2: CÁC KỸ NĂNG AN TOÀN THÔNG TIN

Thực hiện đúng các nguyên tắc an toàn thông tin giúp bạn bảo vệ bản thân, bảo vệ tài khoản và dữ liệu cá nhân trên môi trường số.



CẨN TRỌNG TRÊN MẠNG AN TOÀN CHO CHÍNH BẠN!

1 KHÔNG NHẤP VÀO LIÊN KẾT LẠ, CHỈ TRUY CẬP CÁC TRANG WEB UY TÍN

Ưu tiên các tên miền .gov.vn, .edu.vn khi liên quan đến dịch vụ công hoặc giáo dục.



2 TUYỆT ĐỐI KHÔNG CHIA SẺ MÃ OTP, MẬT KHẨU, SỐ CĂN CƯỚC CÔNG DÂN

Không cung cấp thông tin cá nhân cho bất kỳ ai, kể cả người tự xưng là giáo viên, cán bộ, ngân hàng.



3 BẬT XÁC THỰC HAI BƯỚC (2FA)

Áp dụng cho các tài khoản quan trọng như Facebook, Google, Zalo, tài khoản học tập.



4 TẠO MẬT KHẨU MẠNH VÀ THAY ĐỔI ĐỊNH KỲ

Mật khẩu kết hợp chữ hoa - chữ thường - số - ký tự đặc biệt; không dùng chung một mật khẩu.



5 CHỈ TẢI ỨNG DỤNG TỪ CỬA HÀNG CHÍNH THỨC

Google Play, App Store; kiểm tra kỹ nhà phát triển và các quyền truy cập của ứng dụng.



CẨN TRỌNG VỚI ỨNG DỤNG

- Không rõ nguồn gốc
- Yêu cầu quyền truy cập không hợp lý
- Đánh cắp dữ liệu cá nhân

6 NÂNG CAO TƯ DUY PHẢN BIỆN

Không tin vào các lời hứa hẹn lợi nhuận cao, trúng thưởng không rõ ràng hoặc yêu cầu chuyển tiền nhanh.



7 THƯỜNG XUYỀN CẬP NHẬT THIẾT BỊ

Cập nhật hệ điều hành, trình duyệt, ứng dụng để vá lỗ hổng bảo mật.



AN TOÀN THÔNG TIN – TRÁCH NHIỆM CỦA MỖI HỌC SINH

BẢO VỆ BẢN THÂN – BẢO VỆ GIA ĐÌNH – GÓP PHẦN XÂY DỰNG MÔI TRƯỜNG SỐ AN TOÀN, LÀNH MẠNH



GHI NHỚ QUAN TRỌNG

An toàn trên Internet bắt đầu từ những thói quen nhỏ nhất của bạn mỗi ngày! Hãy luôn cảnh giác và chủ động bảo vệ thông tin cá nhân.





MỘT SỐ LƯU Ý KHI SỬ DỤNG WIFI CÔNG CỘNG



Hiện nay, các cửa hàng cà phê, khách sạn, trung tâm mua sắm, sân bay và nhiều địa điểm khác thường cung cấp cho khách hàng quyền truy cập Wifi công cộng miễn phí.

Từ đó, khi sử dụng các dịch vụ tại những nơi này, người dùng vẫn có thể kiểm tra email, truy cập mạng xã hội hoặc lướt web một cách thuận tiện.



Tuy nhiên, tin tặc sẽ thường theo dõi các mạng Wifi công cộng và chặn bắt dữ liệu được truyền qua mạng. Bằng cách này, **tin tặc có thể truy cập thông tin tài khoản ngân hàng, mật khẩu và các thông tin có giá trị khác của người dùng.**



Để đảm bảo an toàn khi sử dụng Wifi công cộng đội ngũ chuyên gia bảo mật Internet của **Kaspersky Lab** đưa ra lời khuyên:



Sử dụng Wifi công cộng đúng cách sẽ giúp giảm thiểu nguy cơ mất an toàn thông tin, bảo vệ tài khoản, dữ liệu cá nhân và các giao dịch trực tuyến của mỗi người dùng.

1



Nhận thức được sự nguy hiểm:

Wifi công cộng vốn không được an toàn, do đó hãy thận trọng khi sử dụng.

2



Bất kỳ thiết bị nào cũng có thể bị tấn công:

Tất cả các thiết bị như máy tính xách tay, điện thoại thông minh và máy tính bảng đều có thể gặp rủi ro khi sử dụng Wifi công cộng.

3



Thận trọng với tất cả các kết nối Wifi:

Không nên tin tưởng các kết nối Wifi là hợp pháp. Nó có thể là một kết nối giả mạo đã được thiết lập bởi tin tặc nhằm thu thập thông tin cá nhân có giá trị từ những người dùng thiếu thận trọng. Hãy nghi ngờ và thận trọng với mọi kết nối Wifi và không kết nối với những Wifi chưa được xác định, nhận diện. Không dùng wifi công cộng để chuyển tiền online và các công việc cần sự bảo mật cao.

4



Tìm hiểu và xác thực kết nối Wifi đó là hợp pháp:

Một số kết nối giả mạo đã được thiết lập bởi tin tặc sẽ có tên tương tự như quán cà phê, khách sạn hoặc địa điểm cung cấp Wifi miễn phí. Nếu có thể nói chuyện với nhân viên của địa điểm cung cấp kết nối Wifi công cộng đó, thì người dùng cần hỏi thông tin về điểm truy cập Wifi hợp pháp như tên kết nối và địa chỉ IP.

5



Sử dụng mạng riêng ảo (VPN):

Bằng cách sử dụng VPN khi kết nối với mạng Wifi công cộng, người dùng sẽ sử dụng một luồng mạng (tunnel) riêng tư, mã hóa tất cả dữ liệu đi qua mạng. Điều này có thể giúp ngăn chặn việc chặn bắt và thu thập dữ liệu của người dùng.

6



Tránh sử dụng một số trang web cụ thể:

Người dùng nên tránh đăng nhập vào các trang web mà tin tặc sẽ có khả năng thu thập danh tính, mật khẩu hoặc thông tin cá nhân như các trang mạng xã hội, dịch vụ ngân hàng trực tuyến hoặc các trang web lưu trữ thông tin thẻ tín dụng.

7



Cân nhắc sử dụng dữ liệu di động:

Trong trường hợp bắt buộc cần truy cập vào các trang web có lưu trữ hoặc yêu cầu nhập thông tin nhạy cảm, người dùng nên sử dụng dữ liệu di động thay vì kết nối Wifi công cộng.

8



Bảo vệ thiết bị khỏi các cuộc tấn công mạng:

Đảm bảo tất cả các thiết bị được bảo vệ bởi các giải pháp đảm bảo an toàn và chống phần mềm độc hại có hiệu quả, cũng như cần cập nhật chúng thường xuyên nhất có thể./.



CÁCH XỬ LÝ KHI VÔ TÌNH NHẬP VÀO **MỘT LIÊN KẾT ĐỘC HẠI** hoặc **NGHI NGỜ ĐỘC HẠI** TRÊN KHÔNG GIAN MẠNG



KHI VÔ TÌNH NHẬP VÀO MỘT LIÊN KẾT ĐỘC HẠI
HOẶC NGHI NGỜ ĐỘC HẠI, HÃY NHANH CHÓNG THỰC HIỆN:

1



Ngay lập tức **ngắt kết nối** máy tính hoặc thiết bị
khỏi mạng internet để ngăn chặn sự lây lan của mã độc.

2



Tiến hành **thay đổi mật khẩu** của tài khoản bị ảnh hưởng
ngay lập tức. Nếu sử dụng mật khẩu đó cho các tài khoản
khác, hãy lập tức thay đổi tất cả.

3



Nhanh chóng chạy một chương trình **quét chống virus**
đáng tin cậy trên thiết bị đang dùng.

4



Báo cáo sự cố cho bộ phận phụ trách hoặc nhà cung cấp
dịch vụ liên quan.



CHỦ ĐỘNG PHÒNG NGỪA – AN TOÀN TRÊN KHÔNG GIAN MẠNG

Là bảo vệ chính bạn và cộng đồng!

HỌC SINH - SINH VIÊN

CẦN LÀM GÌ ĐỂ QUẢN LÝ THÔNG TIN VÀ BẢO MẬT KHI SỬ DỤNG CÁC NỀN TẢNG AI?



Khi sử dụng các công cụ AI, Học sinh - Sinh viên cần đặc biệt chú ý đến an toàn thông tin để tránh rủi ro rò rỉ dữ liệu hoặc bị khai thác thông tin cá nhân.



1



KHÔNG CHIA SẺ DỮ LIỆU CÁ NHÂN NHẠY CẢM

Tuyệt đối không nhập số Chứng minh thư nhân dân/Căn cước công dân, tài khoản ngân hàng, mật khẩu hay thông tin gia đình vào các công cụ AI công cộng.

2



SỬ DỤNG TÀI KHOẢN HỌC TẬP THAY VÌ TÀI KHOẢN CÁ NHÂN

Khi đăng ký các nền tảng AI miễn phí hoặc công cộng. Điều này giúp hạn chế rò rỉ dữ liệu quan trọng.

3



SAO LƯU DỮ LIỆU QUAN TRỌNG

Như bài làm, tài liệu học tập hoặc dự án vào Google Drive, OneDrive hoặc thiết bị lưu trữ cá nhân để tránh mất mát khi hệ thống gặp sự cố.

4



KÍCH HOẠT XÁC THỰC HAI LỚP (2FA)

Nếu nền tảng hỗ trợ, giúp tài khoản được bảo vệ tốt hơn trước nguy cơ bị truy cập trái phép.

5



THỰC HIỆN CÁC BIỆN PHÁP NÀY

Sẽ giúp Học sinh - Sinh viên an toàn hơn khi khai thác các công cụ AI phục vụ học tập và nghiên cứu.



AN TOÀN THÔNG TIN – BẢO VỆ BẢN THÂN – SỬ DỤNG AI THÔNG MINH, HIỆU QUẢ!

