BẢN TIN
AN TOÀN THÔNG TIN
TRUNG TÂM CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG THANH HÓA

Số 08
tháng 5/2018

CHỊU TRÁCH NHIỆM XUẤT BẢN
ThS. Lê Xuân Lâm
Giám đốc Trung tâm CNTT&TT Thanh Hóa

BIÊN SOẠN
Cao Việt Cường; Trần Ngọc Hưng; Trịnh Ngọc Quỳnh; Trần Lê Phúc

THIẾT KẾ
Chung Nguyễn

TRUNG TÂM CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG THANH HÓA
Địa chỉ: 73 Hàng Than, TP Thanh Hóa
Điện thoại: 02373.718.298
Fax: 02373.718.299
Website: ict.thanhhoa.gov.vn
Giấy phép xuất bản số: 10/GP-XBBT
Sở TTTT Thanh Hóa cấp ngày 12/02/2018

In 500 cuốn, khổ 19x27cm
Tại Công ty TNHH In & TBGD Thanh Huệ
In xong và nộp lưu chiểu tháng 5/2018

Tăng cường quản lý đối với hoạt động trang thông tin điện tử và mạng xã hội trong giai đoạn hiện nay

ThS. ĐỖ HỮU QUYẾT
Phó Giám đốc Sở Thông tin và Truyền thông

Tăng cường công tác quản lý đối với hoạt động trang thông tin thông tin điện tử và mạng xã hội trong giai đoạn hiện nay là một vấn đề đặt ra không chỉ với cơ quan quản lý nhà nước mà cần có sự phối hợp và vào cuộc đồng bộ của các cấp ủy Đảng, chính quyền và các cơ quan chức năng.

Hoạt động truyền thông xã hội hiện nay đã và đang phát triển nhanh chóng, hiệu quả, vượt ra ngoài giới hạn về không gian và thời gian, có vai trò ngày càng quan trọng trong đời sống xã hội hiện đại; thông qua môi trường mạng giúp cho các tổ chức, cá nhân giao tiếp với các cơ quan nhà nước một cách minh bạch và thuận tiện. Sự phát triển của truyền thông xã hội, với ưu thế thông tin được cập nhật thường xuyên, nội dung thông tin phong phú, đa dạng từ nhiều nguồn, nhiều lĩnh vực đời sống xã hội, không biên giới, có khả năng giao lưu, chia sẻ, kết nối cộng đồng rất nhanh và thuận lợi đã tạo ra hiệu ứng rất lớn, ngày càng thu hút đông đảo người dùng internet, nhất là trong giới trẻ, và đang có sự dịch chuyển thói quen tìm kiếm thông tin từ các website thông tin chính thống sang các website truyền thông xã hội, nhất là các trang thông tin điện tử tổng hợp.

Việc quản lý các trang thông tin điện tử và mạng xã hội đã được Chính phủ, Bộ Thông tin và Truyền thông quan tâm chỉ đạo, ban hành nhiều văn bản hướng dẫn triển khai, quản lý cũng như những quy định bắt buộc trong việc cung cấp thông tin, đăng tải, trích dẫn nội dung thông tin và trách nhiệm của các tổ chức, cá nhân trong việc thiết lập, quản trị thông tin như: Chỉ thị số 30-CT/TW ngày 25/12/2013 của Bộ Chính trị về phát triển và tăng cường quản lý báo chí điện tử, mạng xã hội và các loại hình truyền thông khác trên Internet; Nghị định 72/2013/NĐ-CP của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng; Thông tư số 09/2014/TT-BTTTT của Bộ Thông tin và Truyền thông quy định chi tiết về hoạt động, quản lý, cung cấp, sử dụng thông tin trên trang thông tin điện tử và mạng xã hội và gần đây nhất là Thông tư số 38/2016/TT-BTTTT ngày 26-12-2016 của Bộ Thông tin và Truyền thông quy định chi tiết về việc cung cấp thông tin công cộng qua biên giới...

Trong thời gian qua, nhiều cơ quan, tổ chức, doanh nghiệp, địa phương trên địa bàn tỉnh đã thiết lập và tổ chức hoạt động trang thông tin điện tử nhằm phục vụ công tác chỉ đạo, điều hành; thông tin, tuyên truyền và thực hiện các nhiệm vụ chính trị của đơn vị, địa phương. Tuy nhiên, thực trạng hoạt động của các trang thông tin điện tử trên địa bàn tỉnh và việc tham gia mạng xã hội của giới trẻ hiện nay cho thấy vẫn còn nhiều các tổ chức, cá nhân chưa cập nhật và nắm bắt đầy đủ các quy định của pháp luật trong tổ chức hoạt động trang thông tin điện tử và tham gia mạng xã hội, dẫn đến tình trạng một số cơ quan, đơn vị, doanh nghiệp tổ chức hoạt động trang thông tin điện tử chưa đúng với quy định; một số trang thông tin điện tử hoạt động dưới dạng tổng hợp nhưng không xin cấp phép; có trang hoạt động chưa đúng quy định tại giấy phép đã cấp, chưa cập nhật thường xuyên và đầy đủ các thông tin liên quan

đến công tác chỉ đạo điều hành, các chương trình quy hoạch, kế hoạch, thủ tục hành chính của đơn vị; vi phạm các quy định về việc tự ý trích dẫn lại các thông tin từ các cơ quan báo chí nhưng không tuân thủ các quy định về bản quyền...; Một số trang thông tin điện tử tổng hợp cung cấp thông tin lên trang tin vượt quá chức năng, nhiệm vụ của cơ quan được cấp phép; có trang thông tin điện tử tổng hợp không phải là trang thông tin điện tử tổng hợp của các cơ quan báo chí nhưng vẫn cho phép người sử dụng bình luận sau mỗi bài viết. Hiện tượng những thông tin bịa đặt, sai trái, xấu độc được tung lên mạng xã hội với dụng ý xấu có ngày càng nhiều và được nhiều người dùng tham gia bình luận, chia sẻ những thông tin đó, đã gây nên những tác hại không nhỏ trong đời sống xã hội. Để chấn chỉnh tình trạng này, ngày 08/11/2017, Bộ Thông tin và Truyền thông đã ban hành Công văn số 4064/BTTTT-PTTH&TTĐT về việc tăng cường công tác quản lý hoạt động trang thông tin điện tử tổng hợp, trong đó nghiêm cấm việc tổng hợp, trích dẫn lại thông tin từ các cơ quan báo chí nhưng không tuân thủ các quy định về bản quyền, tự ý trích dẫn các tin, bài không xin phép; thay đổi tiêu đề bài viết, cắt xén, thêm bớt nội dung, hình ảnh bài viết, yêu cầu các đơn vị, doanh nghiệp thận trọng khi trích dẫn lại các nguồn tin từ các báo, tạp chí điện tử không thực hiện đúng tôn chỉ, mục đích, thường xuyên bị cơ quan quản lý nhà nước nhắc nhở, xử lý; Ban Thường vụ Tỉnh ủy Thanh Hóa ban hành Chỉ thị số 13 –CT/TU, ngày 29/11/2017 về " Tăng cường sự lãnh đạo của Đảng đối với công tác phòng ngừa đấu tranh chống âm mưu "diễn biến hòa bình" trên lĩnh vực tư tưởng văn hóa trong tình hình mới".

Nhằm tăng cường công tác quản lý hoạt động thông tin điện tử và mạng xã hội, trong

thời gian qua, Sở Thông tin và Truyền thông đã ban hành nhiều văn bản chỉ đạo, hướng dẫn đối với các tổ chức, cá nhân, trong đó, tập trung yêu cầu các tổ chức, doanh nghiệp thiết lập trang thông tin điện tử chủ động rà soát toàn bộ hoạt động, nâng cao trách nhiệm trong quản lý tổ chức hoạt động thông tin trên môi trường mạng do đơn vị thực hiện, cung cấp thông tin, cũng như nâng cao nhận thức đối với người tham gia sử dụng mạng xã hội. Đồng thời Sở Thông tin và Truyền thông thường xuyên chủ trì tổ chức các cuộc thanh tra, kiểm tra, xử lý nghiêm những tổ chức, cá nhân vi phạm các quy định trong tổ chức hoạt động thông tin trên môi trường mạng và tham gia mạng xã hội. Tuy nhiên qua thực tế công tác kiểm tra cũng cho thấy, nguồn phát tán thông tin sai phạm chủ yếu là từ các máy chủ đặt ở nước ngoài, nên việc xử lý, ngăn chặn thông tin sai phạm còn nhiều bất cập và khó khăn; lực lượng và phương tiện kỹ thuật phục vụ cho công tác thanh tra, kiểm tra còn thiếu không đáp ứng yêu cầu đặt ra, mức xử lý vi phạm đối với một số hành vi vi phạm chưa đủ sức răn đe đối tượng...

Theo xu thế phát triển của Internet, thì sự bùng nổ của truyền thông tin trên môi trường mạng trong thời gian tới càng mạnh mẽ hơn. Do đó, công tác quản lý của nhà nước đối với lĩnh vực này trong thời gian tới càng khó khăn, phức tạp hơn. Để thực hiện tốt nhiệm vụ này cần phải có sự tham gia, vào cuộc của các ngành, các cấp, các tổ chức xã hội và trước mắt các cơ quan, đơn vị, doanh nghiệp cần phối hợp thực hiện những nội dung sau:

1. Các cơ quan, đơn vị, địa phương, doanh nghiệp hoạt động trang TTĐT, trang TTĐT tổng hợp và mạng xã hội chủ động rà soát toàn bộ hoạt động cung cấp dịch vụ; triển khai đầy đủ các điều kiện, thủ tục xin cấp phép hoạt động, bảo đảm hoạt động cung cấp dịch vụ của đơn vị mình được thực hiện theo đúng quy định của pháp luật.

Thực hiện nghiêm việc cung cấp thông tin trên trang chủ của trang thông tin điện tử tổng hợp theo đúng quy định tại Khoản 3 Điều 2 Thông tư số 09/2014/TT-BTTTT ngày 9 tháng 8 năm 2014 của Bộ Thông tin và Truyền thông quy định chi tiết về hoạt động quản lý, cung cấp, sử dụng thông tin trên trang thông tin điện tử và mạng xã hội. Không tự ý tổng hợp, trích dẫn lại các thông tin từ các cơ quan báo chí khi chưa thực hiện các quy định về bản

quyền; không tự ý thay đổi tiêu đề bài viết, cắt xén hoặc thêm bớt các nội dung, hình ảnh trong bài viết đăng tải lại từ các báo. Đặc biệt cần thận trọng khi dẫn lại nguồn tin từ các báo, tạp chí điện tử không thực hiện đúng tôn chỉ, mục đích và thường xuyên bị cơ quan quản lý nhà nước nhắc nhở, xử phạt.

2. Các cơ quan báo chí trên địa bàn tỉnh, cơ quan đại diện, phóng viên thường trú tăng cường công tác thông tin, tuyên truyền các quy định của pháp luật trong việc quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng xã hội; tuyên truyền nâng cao ý thức, trách nhiệm đối với người tham gia mạng xã hội; tích cực đấu tranh phản bác các thông tin xấu độc, xuyên tạc, vu khống ảnh hưởng đến tình hình chính trị và trật tự an toàn xã hội.

3. Các sở, ban, ngành cấp tỉnh, UBND các huyện, thị xã, thành phố, các Tổ chức chính trị - Xã hội, Tổ chức chính trị - Xã hội nghề nghiệp và Doanh nghiệp trên địa bàn tỉnh:

- Tăng cường công tác tuyên truyền, giáo dục cho cán bộ, công chức, viên chức và người lao động nâng cao ý thức, trách nhiệm khi tham gia mạng xã hội; nghiên cứu thiết lập trang thông tin điện tử theo hình thức phù hợp để phục vụ nhiệm vụ của cơ quan, đơn vị, qua đó để tăng cường giao tiếp với các tầng lớp nhân dân trong quá trình thực hiện nhiệm vụ lãnh đạo, điều hành, tuyên truyền đường lối, chủ trương của Đảng, chính sách pháp luật của Nhà nước, thực hiện an sinh xã hội;

- Hướng dẫn cán bộ, công chức, người lao động không tham gia đăng tải, chia sẻ cũng như nâng cao ý thức trách nhiệm trong việc đấu tranh, phản bác đối với những thông tin xuyên tạc, xấu, độc, lợi dụng diễn đàn để tuyên truyền, kích động bạo lực, ảnh hưởng đến tình hình an ninh chính trị, gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội; thông tin vu khống, xúc phạm uy tín danh dự của tổ chức, cá nhân gây chia rẽ mất đoàn kết nội bộ, đoàn kết dân tộc.

- Tăng cường theo dõi, kiểm tra, phát hiện kịp thời các sai phạm để có giải pháp ngăn chặn xử lý hoặc phối hợp với Sở Thông tin và Truyền thông xử lý vi phạm theo quy định của pháp luật; phối hợp với Sở Thông tin và Truyền thông tổ chức tập huấn về cách khai thác, sử dụng mạng xã hội qua đó phát huy tính tích cực của mạng xã hội trong thực thi công vụ.

4. Các cơ quan nhà nước thường xuyên đăng tải kịp thời, chính xác các thông tin chính thống trên trang thông tin điện tử của cơ quan đơn vị theo quy định tại Nghị định số 43/2011/NĐ-CP ngày 13/6/2011 của Chính phủ quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử nhà nước để mọi người dân có thể tiếp cận thông tin. Bên cạnh website của mình cần mở thêm một kênh thông tin giới thiệu về chuyên ngành và lĩnh vực mình quản lý qua đó tiếp cận và đưa thông tin dễ dàng đến người dân.

Khi phát hiện thông tin bịa đặt, vu khống, sai sự thật, xúc phạm danh dự của tổ chức và cá nhân của cơ quan, đơn vị, địa phương, gây hoang mang và bất bình trong dư luận xã hội đăng tải trên mạng xã hội, cần chủ động phản bác thông tin, đồng thời phối hợp với các cơ quan chức năng để kịp thời có biện pháp xử lý, ngăn chặn.

5. Sở thông tin và Truyền thông sẽ tiếp tục phối hợp với các cơ quan chức năng của tỉnh tăng cường công tác thanh tra, kiểm tra, xử lý nghiêm các hành vi, sai phạm theo quy định của pháp luật.

Hoạt động trang thông tin điện tử và mạng xã hội trong tình hình hiện nay ngày càng phát triển là một xu hướng tất yếu, có vai trò ngày càng quan trọng trong đời sống xã hội hiện đại, để quản lý tốt hoạt động này cần có sự phối hợp chặt chẽ và vào cuộc đồng bộ của các cấp ủy Đảng, chính quyền và các cơ quan, tổ chức, cũng như mỗi cán bộ, đảng viên và người dân phải nâng cao nhận thức và trách nhiệm khi tham gia sử dụng thông tin trên mạng internet, qua đó phục vụ tốt công tác học tập, nghiên cứu, bảo vệ quan điểm, chủ trương của Đảng, chính sách pháp luật nhà nước, thực hiện thắng lợi mục tiêu phát triển kinh tế - xã hội, quốc phòng, an ninh của đất nước./.

Chủ động tích cực đấu tranh phản bác thông tin xấu, độc trên internet và các trang mạng xã hội

PHẠM VĂN TUẤN
Trưởng Phòng Tuyên truyền, Ban Tuyên giáo Tỉnh ủy

Ngày nay, cùng với sự phát triển của internet, mạng xã hội là "mảnh đất màu mỡ" cho việc phát tán thông tin xấu, độc.

Những thông tin bịa đặt, sai sự thật, bóp méo, xuyên tạc vấn đề, "đổi trắng, thay đen", thật giả, đúng sai lẫn lộn; hoặc có một phần sự thật nhưng được đưa tin với dụng ý xấu, phân tích và định hướng dư luận bằng các quan điểm và luận điệu sai trái, thù địch. Là các dạng thông tin có nội dung không phù hợp về chuẩn mực đạo đức, văn hóa, thuần phong mỹ tục, như: Bôi nhọ đời tư, vu khống cá nhân...; thông tin có tính chất tội phạm tin học, như: Lừa đảo trên mạng, đánh cắp thông tin, mật khẩu, tán phát vi rút...; thông tin sai trái có tính chất chính trị, như: Xuyên tạc sự thật lịch sử, phủ nhận Chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh, chống phá đường lối, chủ trương, chính sách của Đảng, Nhà nước và địa phương, bịa đặt, vu cáo, nói xấu các đồng chí lãnh đạo cấp cao của Đảng, Nhà nước và địa phương, điển hình như, cuối năm 2016, Bộ Công an phối hợp với Công an tỉnh Thanh Hóa bắt đối tượng Nguyễn Danh Dũng, thường trú tại phường Tào Xuyên (TP Thanh Hóa), là chủ tài khoản và quản trị, điều hành kênh Youtube "ThienAn TV" đăng tải hàng trăm video có nội dung xuyên tạc, bôi nhọ, hạ uy tín các đồng chí lãnh đạo Đảng, Nhà nước và phát tán trên mạng internet, mạng xã hội.

Tác hại của những thông tin xấu, độc trên internet và mạng xã hội do các thế lực "mạng đen" tung ra có tác động tiêu cực đến tình hình tư tưởng, dư luận xã hội, gây nghi ngờ, gieo rắc sự hoang mang, dao động, làm giảm sút lòng tin của một bộ phận cán bộ, đảng viên và nhân dân đối với Đảng, Nhà nước và cấp ủy, chính quyền các cấp. Hệ lụy của thông tin xấu, độc ảnh hưởng rất lớn đến đạo đức, lối sống, nhân cách của cá nhân và cộng đồng xã hội.

Điều đáng băn khoăn hiện nay là có không ít cán bộ, đảng viên và nhân dân do nhìn nhận các vấn đề chưa toàn diện, nên đã đưa ra những quan điểm bất mãn đối với Đảng, với chế độ; chia sẻ, bình luận những thông tin thiếu chính xác, tạo dư luận trái chiều, gây ảnh hưởng tiêu cực đến sự ổn định, phát triển chung của tỉnh và đất nước. Không ít cán bộ, đảng viên núp dưới danh nghĩa trí thức, văn nghệ sĩ, nhà từ thiện... thông qua facebook, zalo đưa nhiều thông tin quy chụp, phiến diện, ảnh hưởng đến việc thực hiện các nhiệm vụ chính trị của các địa phương, đơn vị, là cơ sở để

các thế lực thù địch thổi phồng, xuyên tạc sự thật. Khi có người nào đó lên án thủ đoạn, mưu mô của các đối tượng này thì chúng dùng lực lượng "đánh hội đồng", lăng mạ, chửi bới, đe dọa, triệt tiêu người tốt, người thể hiện chính kiến. Nhiều người do chủ quan, mất cảnh giác nên dễ bị rơi vào "bẫy" của những kẻ cơ hội, phản động.

Các thông tin xấu, độc đã được lan truyền nhanh chóng sau khi chủ nhân của chúng đăng tải trên trang thông tin cá nhân. Hàng nghìn lượt người, trong đó có cán bộ, đảng viên đã thể hiện quan điểm cá nhân trên facebook như "Like" (thích), nhiều người trong số đó còn nhiệt tình "Share" (chia sẻ) tạo dư luận xôn xao, bất an.

Chỉ thị số 13-CT/TU, ngày 29-11-2017 của Ban Thường vụ Tỉnh ủy Thanh Hóa nêu: "Hiện nay một số cấp ủy đảng, chính quyền, MTTQ, các đoàn thể và một bộ phận cán bộ, đảng viên và nhân dân chưa nhận thức đầy đủ tính chất nguy hiểm về âm mưu, hoạt động "diễn biến hòa bình" của các thế lực thù địch; chưa nhận thức rõ tác hại của "tự diễn biến", "tự chuyển hóa" trong nội bộ, tiềm ẩn nguy cơ có thể gây mất ổn định chính trị - xã hội trên địa bàn, nên trong công tác lãnh đạo, chỉ đạo chưa quan tâm đúng mức tổ chức thực hiện các biện pháp đấu tranh, ngăn chặn; nhất là công tác đấu tranh phản bác thông tin sai trái, xuyên tạc và các hoạt động chống phá của các thế lực thù địch còn lúng túng, bị động, thiếu sắc bén, hiệu quả chưa cao".

Để tạo sự thống nhất và chủ động tích cực đấu tranh phản bác thông tin xấu, độc trên internet và các trang mạng xã hội, thiết nghĩ các cấp ủy đảng, chính quyền, đoàn thể, cơ quan, đơn vị cần thực hiện tốt các giải pháp sau:

Một là, làm tốt công tác tuyên truyền nâng cao nhận thức của các cấp ủy, chính quyền, đoàn thể, cơ quan, đơn vị, cán bộ, đảng viên và các tầng lớp nhân dân thấy rõ tính hai mặt của internet và mạng xã hội; nhận diện các thủ đoạn, nội dung chưa được kiểm chứng, những thông tin xấu độc, tính chất nguy hại của nó đối với cá nhân và xã hội. Qua đó trang bị kiến thức cần thiết để mỗi người có thể tự sàng lọc, tiếp nhận thông tin hữu ích, chính thống, đồng thời "miễn dịch" với những thông tin xấu, độc làm nhiễu loạn môi trường xã hội.

Hai là, định hướng kịp thời việc sử dụng mạng xã hội trong cán bộ, đảng viên, công chức, viên chức, học sinh, sinh viên; ngăn chặn, chấn chỉnh việc sử dụng các mạng xã hội để đăng tải, chia sẻ, bình luận những thông tin có nội dung xấu, độc, xuyên tạc chủ trương của Đảng, chính sách, pháp luật của Nhà nước, những hình ảnh trái với thuần phong, mỹ tục và chuẩn mực đạo đức xã hội, xâm phạm đời tư, danh dự, nhân phẩm người khác.

Ba là, chủ động nắm bắt tình hình tư tưởng và dư luận xã hội; sớm phát hiện và xử lý kịp thời những biểu hiện phức tạp, nổi cộm phát sinh, những vấn đề bất cập bức xúc trong xã hội, không để các thế lực thù địch lợi dụng kích động, khiếu kiện, biểu tình gây mất ổn định chính trị. Cần tổ chức tập huấn, bồi dưỡng nghiệp vụ trang bị kiến thức, kỹ năng cho lực lượng nòng cốt,

thường trực đấu tranh, phản bác các thông tin xấu, độc trên các trang mạng xã hội.

Bốn là, phát huy vai trò của các tổ chức quần chúng, các tổ chức chính trị - xã hội, huy động lực lượng quần chúng sẵn sàng tổ chức đấu tranh trực diện với những thông tin xấu, độc trên internet và mạng xã hội; sẵn sàng tham gia chia sẻ, bình luận, nhân rộng các bài viết về gương người tốt, việc tốt, điển hình tiên tiến, mô hình mới, cách làm hay nhằm cổ vũ, động viên đông đảo mọi người tham gia, tạo hiệu ứng tốt trong xã hội. Khi tiếp cận với các bài viết, các thông tin thiếu chuẩn xác với mục đích phá hoại sự ổn định, kích động, xuyên tạc đường lối, chủ trương của Đảng, chính sách, pháp luật của Nhà nước và địa phương phải thể hiện rõ chính kiến bảo vệ chính nghĩa, lẽ phải, tránh tình trạng a dua. Không tham gia chia sẻ, bình luận những thông tin không chính thống có nội dung gây phương hại đến uy tín của tổ chức, danh dự, nhân phẩm của cá nhân.

Năm là, tăng cường các biện pháp kỹ thuật ngăn chặn thông tin xấu, độc; phát hiện yếu tố mất an toàn, an ninh thông tin, các vụ lộ, lọt tài liệu bí mật Nhà nước trên internet; thực hiện tốt công tác quản lý báo chí điện tử, mạng xã hội và các loại hình truyền thông khác trên internet và mạng xã hội; kịp thời phát hiện, xử lý nghiêm những trường hợp vi phạm theo quy định của Đảng, Nhà nước, góp phần bảo vệ an toàn, an ninh thông tin, bí mật Nhà nước./.

Kỹ năng phân biệt TIN TỨC GIẢ TRÊN MẠNG

NGUYỄN THỊ THU HÀ
Phòng quản lý CNTT, Sở Thông tin và Truyền thông

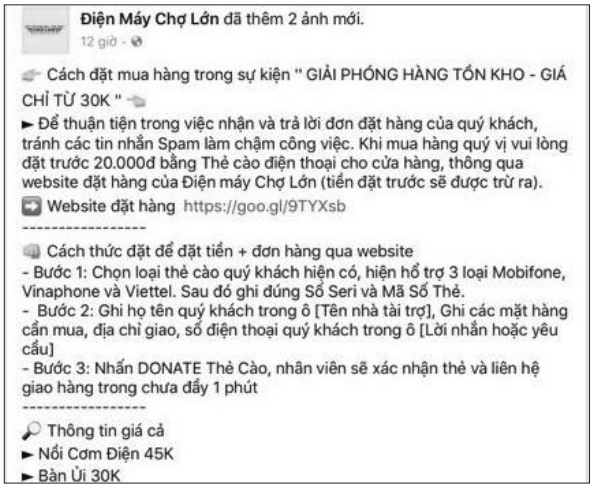
Mạng Internet cho chúng ta cơ hội tiếp xúc với tin tức một cách nhanh chóng, đôi khi sự việc chưa kịp lên báo chí chính thống thì chúng ta đã kịp biết thông qua internet. Tuy nhiên, việc mọi người đều có thể làm nhà báo cũng mang đến một phiền phức hết sức lớn, đó là vấn nạn tin tức giả mạo, hay còn gọi là fake news. Trên thế giới, tin giả tràn lan, và Việt Nam cũng không nằm ngoài xu thế này. Chúng ta đã chứng kiến có rất nhiều nội dung vô thưởng vô phạt, thậm chí sai lệch, đã được người dùng mạng xã hội góp phần phát tán rộng rãi. Trong số những người chia sẻ các thông tin thất thiệt như vậy trên mạng xã hội có cả những nhân vật có uy tín, có ảnh hưởng, thậm chí được cho là "thạo tin" hơn nhiều người dùng khác.

Sự bùng nổ của tin tức giả mạo (tin bịa đặt, không đúng sự thật) đã lan tràn trên mạng xã hội trong năm vừa qua. Tại Mỹ, tin tức giả mạo (fake news) cũng tràn ngập trên Facebook, Google, Twitter... Tại Việt Nam, theo số liệu thống kê từ chương trình đánh giá an ninh mạng của Bkav cho thấy, 63% người dùng thường xuyên đọc được tin tức giả mạo trên Facebook, trong đó 40% là nạn nhân hằng ngày.

Việc đọc thông tin giả mạo không chỉ khiến người đọc

hoang mang mà còn tiềm ẩn nguy cơ gây bất ổn xã hội khi kẻ xấu cố tình đưa tin sai sự thật liên quan đến tình hình kinh tế, chính trị của đất nước.

Thậm chí, nhiều người còn mất tiền oan bởi những thông tin giả mạo trên mạng xã hội. Trong đó, trang tin của các nhãn hàng lớn tại Việt Nam bị giả mạo nhiều nhất. Vì quá tin vào những thương hiệu này với những lời mời chào hấp dẫn như share trang và để lại thông tin được tặng quà, mua hàng giảm giá khủng còn vài chục ngàn đồng, khuyến mãi đến hơn 70% giá trị hàng hóa... đã khiến nhiều người bị lừa. Hình thức lừa phần lớn là khi để lại số điện thoại, thông tin cá nhân trên trang thông tin lừa đảo, những người này sẽ nhận được tin nhắn chuyển khoản để "đặt cọc" món quà, món hàng siêu rẻ...



Một Fanpape giả mạo trên Facebook khiến nhiều người bị lừa mất tiền.

Ngoài ra, nhiều người khi thấy trang tin có tiêu đề hay, hấp dẫn đã vào xem, nhưng sau đó đã bị lừa vào trang khác bắt đăng nhập thông tin tài khoản Facebook; hay khi mua hàng trúng trang web lừa đảo đã "vô tình" tiết lộ thông tin tài khoản ngân hàng... cũng khiến nhiều người bị mất tiền oan.

Như mới đây nhất, ngày 19/12/2017, nhiều người dùng tại Việt Nam đã lây nhiễm mã độc đào tiền ảo trên Facebook với tốc độ lây lan chóng mặt, cứ 3 phút lại có một người bị lây nhiễm mã độc này. Sau khi lây nhiễm, mã độc sẽ âm thầm sử dụng tài nguyên của máy nạn nhân để chạy các chương trình đào tiền. Thống kê từ hệ thống giám sát virus của Bkav, tính đến nay đã có hơn 23.000 máy tính tại Việt Nam nhiễm loại mã độc đào tiền ảo này.

Một hình thức phổ biến trong việc giả danh những trang báo chính thống, những kênh tin tức nổi tiếng nhằm làm tăng mức tin tưởng của người dùng facebook vào những tin tức đó. Điển hình như khi chúng ta đọc tin tức trên facebook và thấy thông tin chia sẻ như sau:

Thoạt nhìn thì đây cũng là một tin tức bình thường, nói lên cái vấn đề mà mọi người đều quan tâm nhất là các bậc phụ huynh. Nhìn tin này, chắc chắn không ít người sẽ chẳng suy nghĩ và nhấn vào để đọc tin. Để ý thấy góc bên trái có chữ "Tuổi trẻ Việt Nam", trong đầu ai cũng nghĩ chắc là tên trang web chứa tin đó, nghe nó cũng giống tên một trang chính thống đấy chứ, như tuoitrevietnam.vn chẳng hạn, một trang về đoàn.

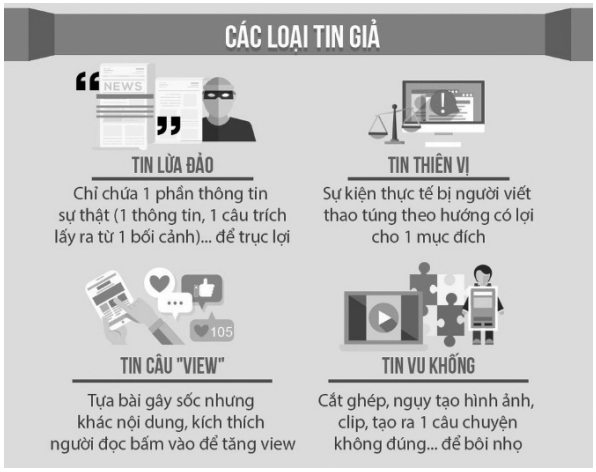
Khi nhấp vào tin đó, nó sẽ đưa ta đến một trang web như sau:

Vấn đề chính ở đây là những kẻ xấu lợi dụng điều này để thực hiện đưa những tin tức giả, giật gân nhằm gây hoang mang cho người đọc cũng như thu được lợi nhuận từ quảng cáo khi có người đọc tin tức và click vào quảng cáo trong bài viết.

Chúng ta có thể dễ dàng thay đổi banner của trang web thành bất kì trang web nào mình muốn, nhằm dễ dàng đánh lừa người đọc tin tưởng vào tin tức hơn khí đó là những trang web tin tức chính thống. Tuy nhiên, nếu chúng ta kiểm tra kỹ địa chỉ của trang web đưa tin trên bằng cách bấm chuột vào "Sao chép liên kết" để copy địa chỉ ra một chỗ khác hoặc "Mở bằng trình duyệt" để biết được link trang web gốc.

Chúng ta có thể thấy, trang web gốc là *quochoi.org* thay vì địa chỉ hiện thị như ban đầu.

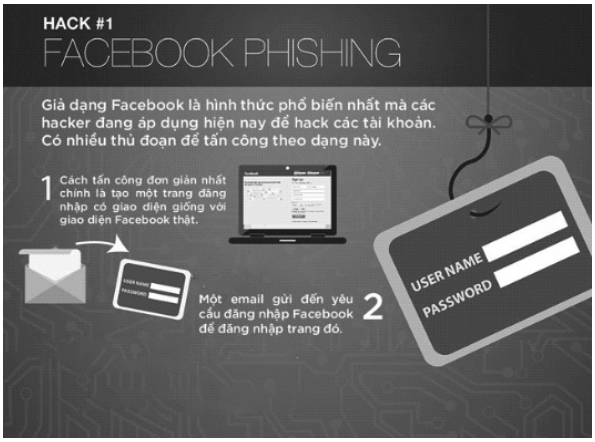
Như vậy, tin tức giả mạo mang lại nhiều hệ quả cho người dùng trên môi trường mạng. Sau đây là những kỹ năng cơ bản giúp cho người dùng dễ dàng phân biệt tin tức giả mạo trên môi trường mạng.

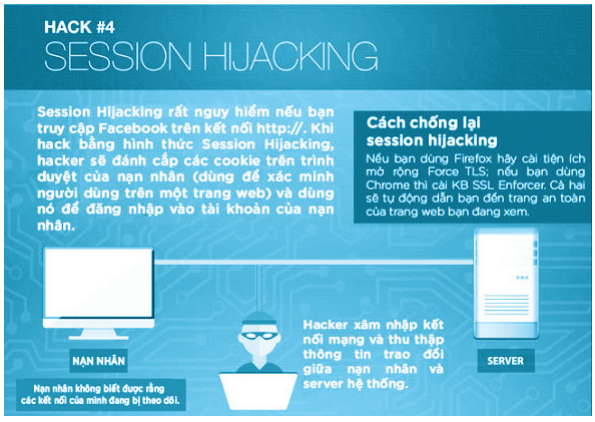


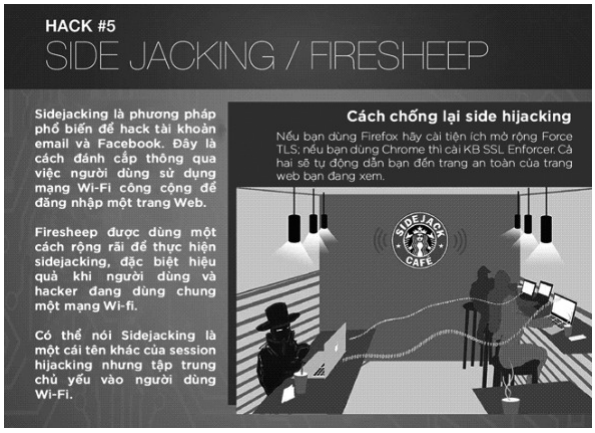
Tổng hợp các biện pháp bảo vệ tài khoản mạng xã hội an toàn

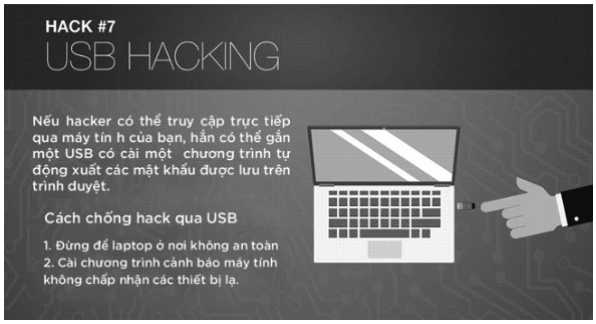
NGÔ THỊ PHƯƠNG
Trung tâm CNTT&TT Thanh Hóa

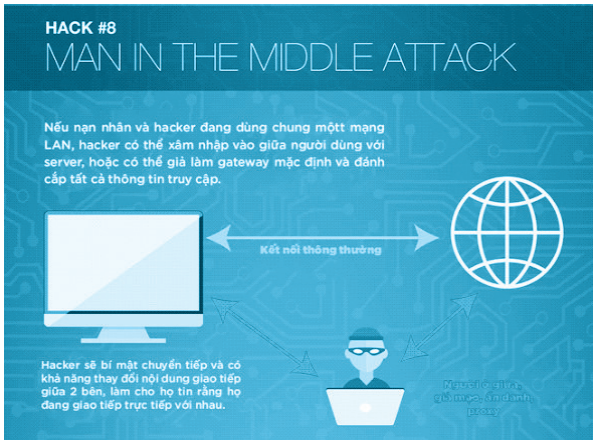
Facebook là mạng xã hội khổng lồ với gần 2 tỷ người dùng. Chính điều này đã biến Facebook trở thành mục tiêu tấn công với các tội phạm mạng. Sau đây là tổng hợp 10 cách mà các hacker dùng để tấn công và chiếm đoạt tài khoản Facebook của người dùng. Cũng như các biện pháp bảo vệ tài khoản mạng xã hội an toàn.

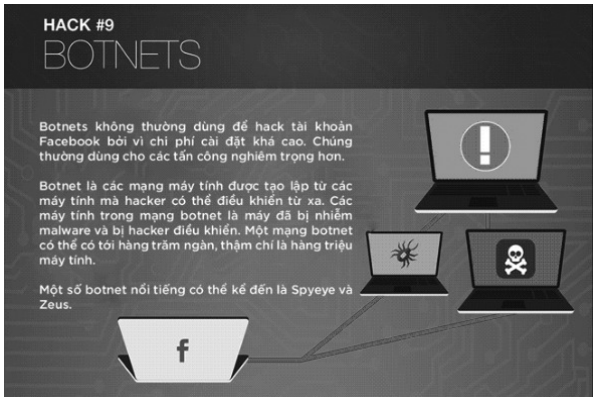






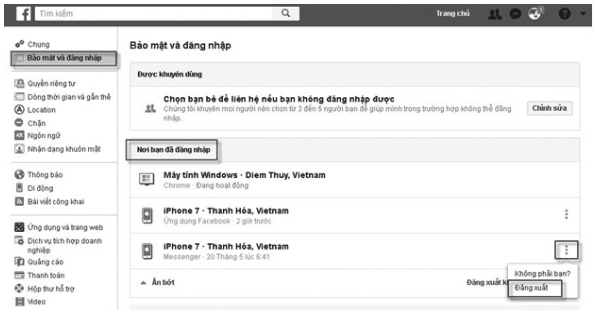






Làm sao để biết tài khoảnFacebookcó bị hack hay không?

Có một cách đơn giản để kiểm tra. Trên giao diện của Facebook sau khi đã đăng nhập vào, vào biểu tượng có hình dạng 3 gạch ngang ở góc phải (trên thiết bị di động) hoặc dấu tam giác ngược (trên PC). Đến phần **Cài đặt** > **Cài đặt tài khoản** > **Bảo mật** > **Nơi bạn đã đăng nhập**.



Danh sách tất cả các thiết bị mà bạn đã đăng nhập và vị trí của chúng sẽ được nêu ra ở đây. Nếu có một địa chỉ đăng nhập bất thường thì rất có thể bạn đã bị tấn công. Nếu bạn thấy bất cứ thứ gì không phải là bạn, hãy click vào biểu tượng ⋮ Đăng xuất tài khoản đó ngay hoặc click vào Đăng xuất khỏi tất cả các phiên

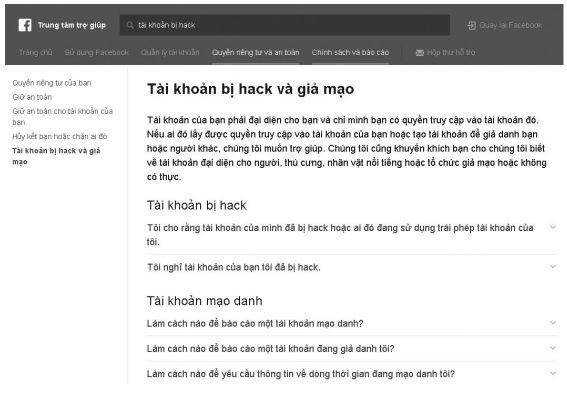
1.1. Một vài dấu hiệu cho thấy tài khoản facebook đã bị tấn công

Một số biểu hiện cho thấy tài khoản facebook đã bị tấn công là:

- Tên, ngày sinh, email hoặc mật khẩu của người dùng đã bị thay đổi.
- Một người nào đó đã gửi yêu cầu kết bạn tới những người mà chúng ta không biết.
- Tin nhắn messenger đã được gửi từ tài khoản của chúng ta, nhưng chúng ta không soạn tin nhắn đó.
- Bài đăng xuất hiện trên dòng thời gian mà chúng ta không đăng.

1.2. Làm gì khi tài khoản bị tấn công?

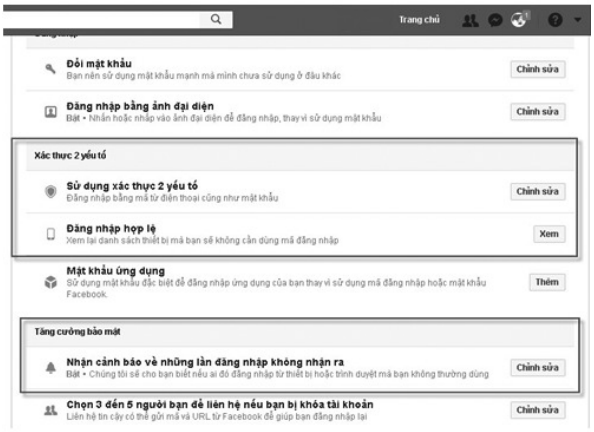
Sau khi đã kết thúc những đăng nhập không rõ nguồn gốc ở bước trên, hãy thay đổi ngay mật khẩu của tài khoản facebook. Tiếp theo, nhờ đến sự giúp đỡ của Facebook. Facebook có một hệ thống giúp bạn nếu chúng ta bị tấn công.



Truy cập trangTrợ giúpcủa Facebook, click chuột vào *Tôi nghĩ rằng tài khoản của tôi đã bị hack* sau đó click vào *Các công cụ và mẹo sau*. Facebook sẽ đưa chúng ta đến một trang mới, hướng dẫn các bước để bảo vệ tài khoản của người dùng.

1.3 Làm sao để tự bảo vệ tài khoản?

Facebook có rất nhiều tính năng bảo mật, chỉ cần kích hoạt chúng. Bằng cách vào biểu tượng có hình dạng 3 gạch ngang ở góc phải (trên thiết bị di động) hoặc dấu tam giác ngược (trên PC). Đến phần **Cài đặt** > **Bảo mật**. Bật **Cảnh báo đăng nhập** để nhận được thông báo khi tài khoản đăng nhập. Điều này giúp phát hiện sớm những đăng nhập trái phép, ngăn chặn sớm nhất các thiệt hại gặp phải.



Tiếp theo kích hoạt **Xác thực 2 yếu tố** để tăng cường khả năng bảo mật.

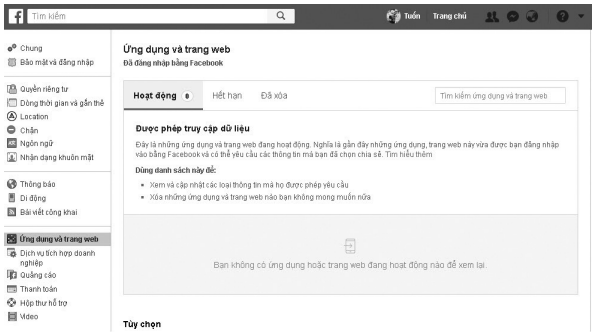
Các thiết lập cơ bản để bạn bảo vệ cho tài khoản Facebook của cá nhân

2.1 Đăng ký số điện thoại với Facebook

Điều đầu tiên cần làm là thiết lập số điện thoại của mình gắn với tài khoản Facebook, bằng cách truy cập vào **Cài đặt** > **Di động**. Sau đó nhấn tiến hành nhập số điện thoại của mình vào ô trống theo yêu cầu để nhận mã xác nhận.

Sau khi đã nhập mã xác nhận xong, sẽ có thể kích hoạt tính năng nhận tin nhắn SMS từ Facebook. Với tính năng này, khi có tin nhắn mới hoặc bài viết mới được đăng trên trang cá nhân của mình, chúng ta sẽ nhận được tin nhắn gửi đến điện thoại.

2.2 Thường xuyên "sàng lọc" lại những ứng dụng đã liên kết với tài khoản Facebook của mình



Hầu hết các ứng dụng và website hiện nay đều bổ sung thêm tính năng liên kết với tài khoản Facebook nhằm đơn giản hóa việc đăng nhập và sử dụng dịch vụ của họ. Tuy nhiên, đôi khi chúng ta cũng nên rà soát lại danh sách các ứng dụng và website mà mình đã liên kết với tài khoản Facebook để tránh bị rò rỉ những thông tin cá nhân khi không còn sử dụng cách dịch vụ của họ nữa bằng cách truy cập vào **Cài đặt** > **Ứng dụng**.

2.3. Sao lưu dữ liệu trên Facebook

Để tránh các trường hợp xấu nhất cho tài khoản của mình, chúng ta nên sao lưu tất cả nội dung như những bức ảnh, video, các bài viết, các tin nhắn,... của mình về máy tính bằng cách sử dụng tùy chọn "**Tải xuống bản sao dữ liệu Facebook**" trong mục "**Cài đặt tài khoản chung**".

2.4. Thiết lập một mật khẩu mạnh cho tài khoản Facebook

Một sự thật là có khá nhiều người dùng sử dụng ngày sinh, họ tên, số điện thoại của mình ra để làm mật khẩu, hoặc sử dụng những mật

khẩu đơn giản để đăng nhập. Khi hacker muốn tấn công nick facebook thì đầu tiên họ sẽ nhắm vào những thông tin đó để dò tìm mật khẩu. Riêng email đăng ký tài khoản facebook thì cũng nên đặt mật khẩu thật an toàn, vì nếu tấn công không được ở facebook thì hacker sẽ chuyển sang tấn công email.

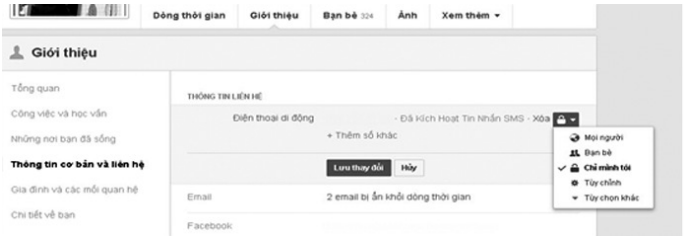
2.5. Không công khai thông tin cá nhân trên Facebook

Để tấn công được một tài khoản facebook theo kiểu dò tìm mật khẩu thì kẻ tấn công dựa vào thông tin của người dùng. Vì thế chẳng có lí do gì public (công khai) thông tin cá nhân để mọi người đều có thể xem cả. Thông tin cá nhân khi bạn đăng ký facebook bao gồm ngày sinh, số điện thoại, email. Và về sau facebook bắt bạn phải cập nhật những thông tin như: quê quán, trường học, công việc...

Để ẩn được thông tin cá nhân thì có thể vào đây để thiết lập:

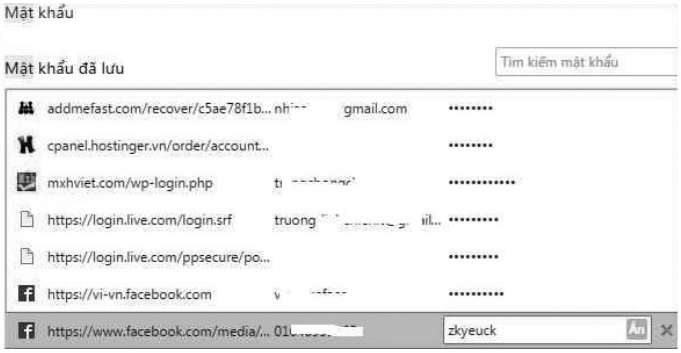
Vào *trang facebook cá nhân > Giới thiệu:*

Vào các mục tương ứng: Tổng quan, Thông tin cơ bản và liên hệ... ở đây cần ẩn hết những thông tin không cần thiết bằng cách bấm vào **chỉnh sửa** > **chỉ mình tôi (biểu tượng cái khóa)**. Hãy ẩn những thông tin sau: số điện thoại, email, ngày tháng năm sinh... Nếu chúng ta đã cảm thấy chưa an toàn thì cho ẩn hết tất cả.



2.6. Không lưu lại mật khẩu trên trình duyệt

Hiện nay các trình duyệt đều hỗ trợ lưu lại mật khẩu khi người dùng đăng nhập một website nào đó, cũng như tính năng **duy trì đăng nhập** của facebook. Chúng ta không nên chọn tính năng này bởi tác dụng của nó là lưu lại mật khẩu tài khoản facebook cho lần đăng nhập tiếp theo. Tuy nhiên, điều này cũng tiềm ẩn các rủi ro trong việc lộ/lọt mật khẩu. Kẻ tấn công chỉ làm vài thao tác là lấy được mật khẩu lưu trên trình duyệt.



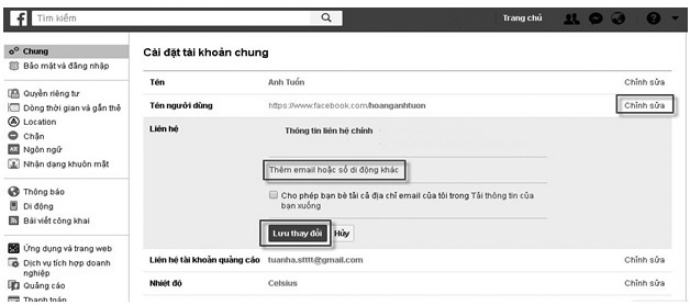
Vì thế hãy bỏ dấu check ở ô duy trì đăng nhập của facebook và vào **chrome://settings/** (google chrome) kéo xuống phần **Mật khẩu và biểu mẫu** và bỏ dấu check để trình duyệt không lưu lại mật khẩu khi đăng nhập nữa.

2.7. Thiết lập email cho tài khoản facebook

Khi đăng ký tài khoản facebook thì dùng số điện thoại đăng ký và không thêm email vào. Hoặc có người lại đăng ký bằng email và không thêm số điện thoại vào. Bình thường không có vấn đề gì thì không sao, nhưng nếu tài khoản facebook bị hack hay bị block tài khoản thì mọi liên lạc hỗ trợ với Facebook đều thông qua email. Sau đây là hướng dẫn đăng ký thêm email và số điện thoại cho Facebook.

Nhấp vào dấu tam giác ngược (trên PC) ở góc trên cùng bên phải của Facebook và chọn Cài đặt

1. Bấm chuột vào ***Chung***
2. Bấm chuột vào ***Liên hệ*** để thêm một email mới vào tài khoản hoặc nhấp vào ***Xóa*** để xóa email khỏi tài khoản của bạn
3. Nhấp vào ***Lưu thay đổi***



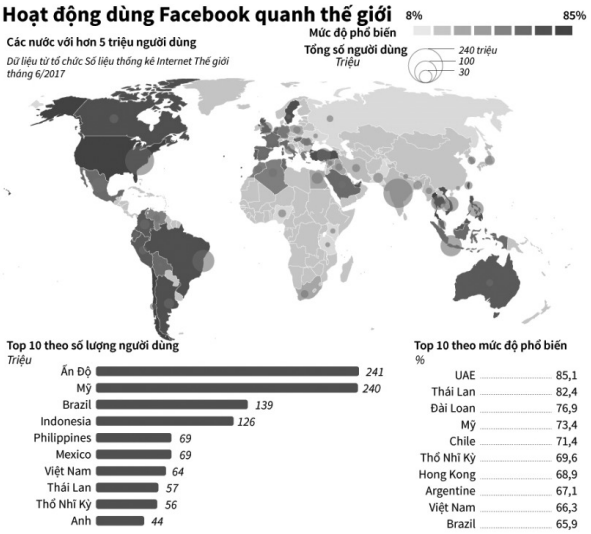
Cũng tại bước này, bạn cũng có thể thêm cả số điện thoại vào tài khoản Facebook.

Facebook thu thập thông tin người dùng như thế nào?

TRỊNH VĂN KIỆM
Trung tâm CNTT&TT Thanh Hóa

Facebook, mạng xã hội lớn nhất thế giới tại thời điểm hiện tại đã chính thức thông báo vào ngày 4/4, thông tin cá nhân của 87 triệu người dùng có thể đã được chia sẻ với công ty tư vấn chính trị Cambridge Analytica của Anh. Con số tài khoản bị thu thập thông tin do công ty này trước đó là 50 triệu.

Theo đó có 86.273.879 tài khoản Facebook bị lộ lọt thông tin cá nhân, Việt Nam đứng thứ 9 trong danh sách các quốc gia có số người dùng bị lộ thông tin với 427.446 tài khoản (chiếm 0,5%), đứng đầu danh sách là Mỹ với 70.632.350 tài khoản (chiếm 81,6%), thứ 2 là Philipines với 1.175.870 tài khoản (chiếm 1,4%). Công ty Cambridge Analytica bị cáo buộc đã sử dụng toàn bộ những thông tin đó vào chiến dịch tranh cử của Tổng thống Mỹ Donald Trump năm 2016 và cuộc trưng cầu dân ý Brexit về việc Anh rời khỏi Liên minh châu Âu trên các trang mạng xã hội. Theo đó, một số chuyên gia nhận định từ dữ liệu thu thập được, công ty Cambridge Analytica tiến hành phân tích hành vi, thói quen, sở thích, tính cách của người dùng để đưa ra những quảng cáo trên Facebook tương ứng để tác động người dùng hành động, quyết định theo hướng mà nhà quảng cáo muốn.



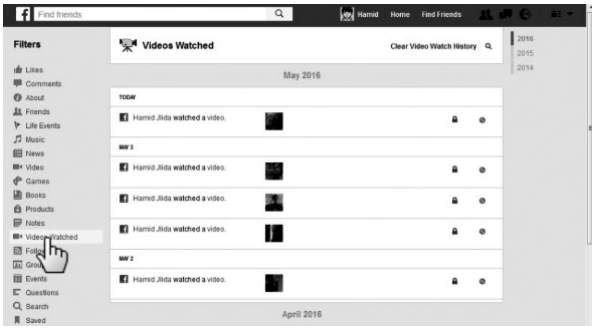
Bằng cách nào mà Facebook có thể thu thập được thông tin của người sử dụng? Dưới đây là các cách Facebook có được thông tin người dùng.

1. Khai báo khi đăng ký tài khoản Facebook

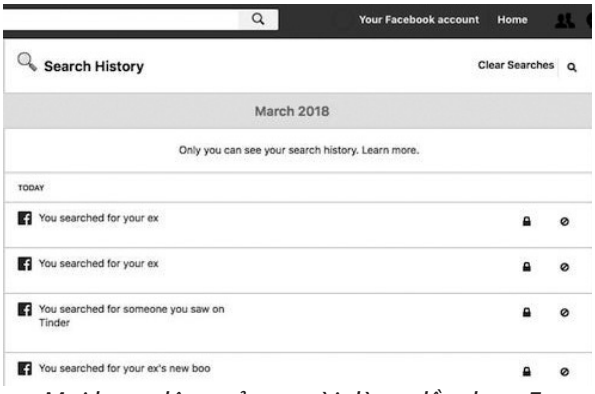
Để sử dụng Facebook, người dùng phải khai báo họ tên, ngày tháng năm sinh, giới tính, số điện thoại/ địa chỉ email của mình. Đây cũng là cách thức đơn giản nhất để Facebook thu thập những thông tin đầu tiên về người dùng.

2. Thu thập thông qua hành vi người dùng

Facebook cũng lưu trữ danh sách các địa chỉ mạng (IP) mà người dùng đã sử dụng để đăng nhập tài khoản, các quảng cáo mà người dùng đã truy cập vào... Mạng xã hội này cũng theo dõi các dữ liệu mà người dùng khai báo như tên thời trẻ, thông tin thẻ tín dụng, quê quán, địa chỉ, trường học hay quan điểm chính trị...



Facebook lưu trữ dữ liệu chi tiết về tất cả sở thích của người dùng và mọi thứ chúng ta "like". Mạng xã hội cũng sử dụng chính những thông tin này nhằm tiếp cận quảng cáo một cách "siêu chính xác". Phản ứng của chúng ta với các bài đăng trên Facebook là cách người dùng vô tình tham gia vào cuộc khảo sát về mức độ tiếp cận chính xác của các quảng cáo.



Mọi hoạt động của người dùng đều được Facebook ghi lại.

Nhật ký hoạt động (Activity log) lưu lại tất cả các hành động của người dùng trên Facebook, từ việc chúng ta tìm kiếm điều gì, "like" bài viết nào hay bình luận ra sao. Những gì xuất hiện trên Tường (Timeline) thì chỉ có bạn bè của chúng ta mới thấy nhưng Facebook thì biết tất cả mọi hành động, thông tin của họ.

3. Qua các ứng dụng bên thứ ba của Facebook

Nhiều ứng dụng và website cho đăng nhập bằng tài khoản Facebook.

Không chỉ nắm giữ thông tin của người dùng cho riêng mình, Facebook còn chia sẻ nó với bên thứ ba khi người dùng đồng ý. Rất nhiều ứng dụng và website hiện nay có tuỳ chọn đăng nhập nhanh bằng Facebook và một khi chúng ta bấm "tiếp tục" thì đồng nghĩa với việc người dùng chấp nhận chia sẻ dữ liệu cá nhân cho bên đó.

Chẳng hạn, ứng dụng hẹn hò Tinder yêu cầu truy cập vào danh sách bạn bè, giới tính mà bạn quan tâm, ngày sinh nhật, công việc, ảnh, các nội dung mà bạn "like" hay địa chỉ email. Điều đáng quan tâm là chúng ta thường "nhắm mắt" bấm "tiếp tục" mà không để ý kỹ các dữ liệu bên thứ ba thu thập là gì.

4. Quyền truy cập trên thiết bị di động

Thiết bị di động cá nhân được cài đặt ứng dụng Facebook sẽ yêu cầu nhiều quyền truy cập khác nhau để hoạt động. Việc này cho phép mạng xã hội thu thập được rất nhiều thông tin quan trọng.

Các bước hạn chế mạng xã hội thu thập thông tin cá nhân

1. Tắt chức năng xác định địa điểm của người dùng

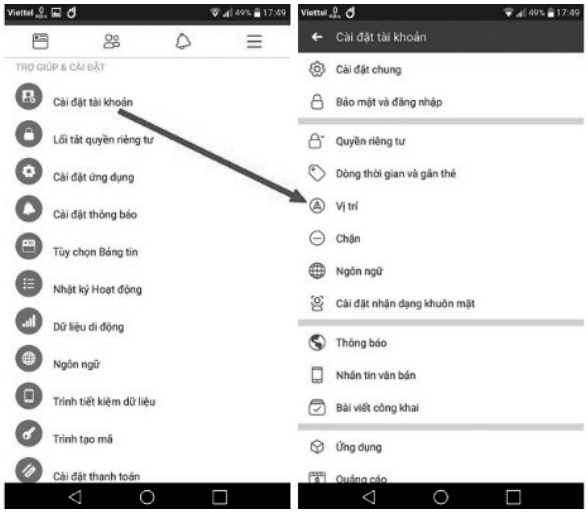
Thông tin về địa điểm hiện tại của người dùng là một dữ liệu nhạy cảm mà các ứng dụng hay dịch vụ luôn mong muốn được biết đến. Với thông tin này, các công ty sẽ biết được người dùng đến từ đâu, đang đi đâu, yêu thích những địa điểm nào... Với Facebook, dữ liệu này thực sự quan trọng, có thể giúp mạng xã hội này đưa ra những nội dung quảng cáo phù hợp với những địa điểm mà người dùng hay lui tới.

Nếu không muốn Facebook quản lý nơi mình ở hay những nơi mình đi tới thì nên tắt đi chức năng định vị trên ứng dụng Facebook.

Để thực hiện điều này, đối với người dùng iOS, truy cập vào chức năng cài đặt ứng dụng trên

smartphone, tìm đến mục "Privacy" bên dưới tab General, sau đó chọn mục "Location Services". Tại đây kéo xuống dưới để tìm Facebook chuyển sang chế độ "While Using the App" hoặc "Never".

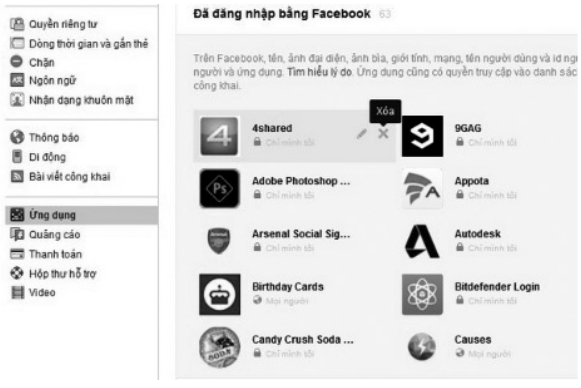
Còn đối với người dùng Android, truy cập vào ứng dụng Facebook trên smartphone, nhấn vào biểu tượng cài đặt ở góc trên bên phải, kéo xuống tìm "Cài đặt tài khoản" và chọn "Vị trí" từ menu hiện ra.



2. Kiểm tra các ứng dụng liên kết với tài khoản Facebook

Nếu chúng ta đang dùng Facebook để đăng nhập vào các trang web, trò chơi hoặc ứng dụng với bên thứ ba thì rất có thể các dịch vụ này vẫn đang khai thác thông tin của người dùng hàng ngày.

Tới phần **Cài đặt** > **Ứng dụng** để kiểm tra các quyền cấp ứng dụng. Nếu thấy có bất kỳ ứng dụng nào đáng ngờ, hãy xóa ngay lập tức.



3. Kiểm tra Cài đặt bảo mật Facebook

Giảm thiểu chia sẻ các thông tin cá nhân, hình ảnh và bài viết dưới chế độ công khai. Cách tốt nhất là cài đặt tất cả ở chế độ bạn bè và tùy chỉnh danh sách bạn bè về chế độ xem riêng tư.

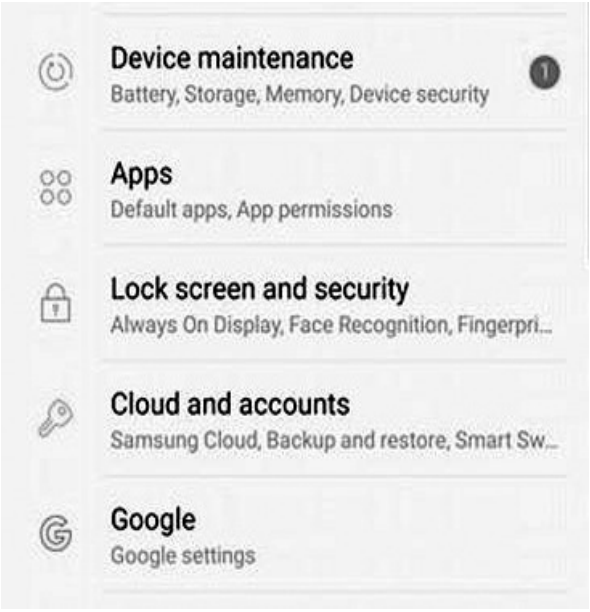
4. Đọc chính sách bảo mật

Khi đăng ký tài khoản trên Facebook, chúng ta nên đọc kỹ các điều khoản, đặc biệt là các điều khoản liên quan đến quyền và việc cấp quyền chia sẻ.

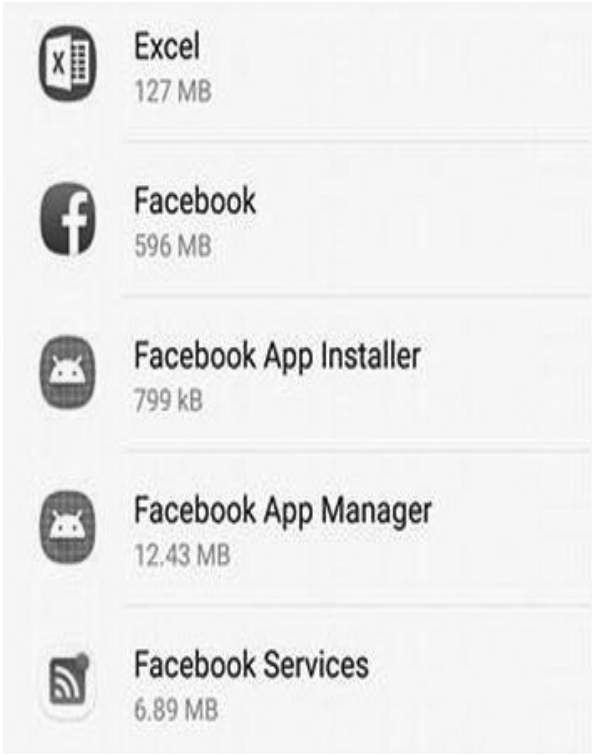
5. Thiết lập quyền truy cập facebook trên điện thoại

Thiết lập hạn chế quyền thu thập các dữ liệu cuộc gọi cũng như tin nhắn SMS trên điện thoại di động của chúng ta nữa.

Đầu tiên, truy cập mục *Cài đặt (Settings)* trên điện thoại Android. Chọn mục *Ứng dụng (Apps)* để tiến hành thao tác.

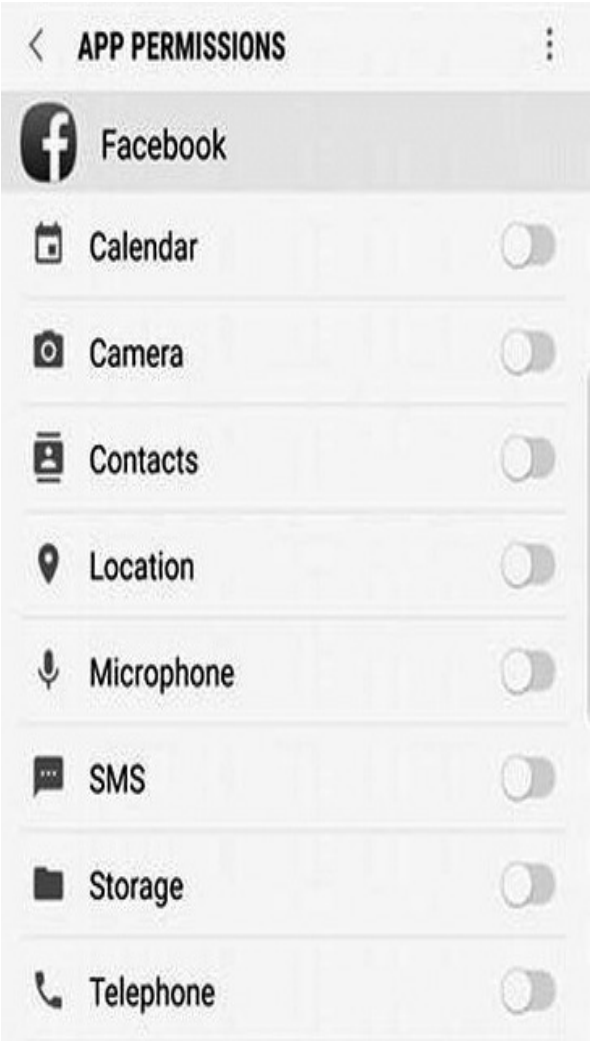


Tìm và nhấp vào ứng dụng Facebook.



Cuộn xuống mục *Quyền (Permissions)*.

Đảm bảo rằng cả hai quyền Telephone và SMS đều được tắt.



4. Cài đặt trình chặn theo dõi

Vớimột số ứng dụng người dùng có thể cài đặt trên trình duyệt của mình để chặn theo dõi chúng trên các trang web. Tuy nhiên đôi khi các ứng dụng này có thể gây ảnh hưởng đến quá trình hoạt động truy cập vào một số trang web.

Chúng ta có thể tham khảo cài đặt Disconnect và Privacy Badger, đây là hai công cụ được đánh giá cao trong việc chặn theo dõi trên trình duyệt Chrome.

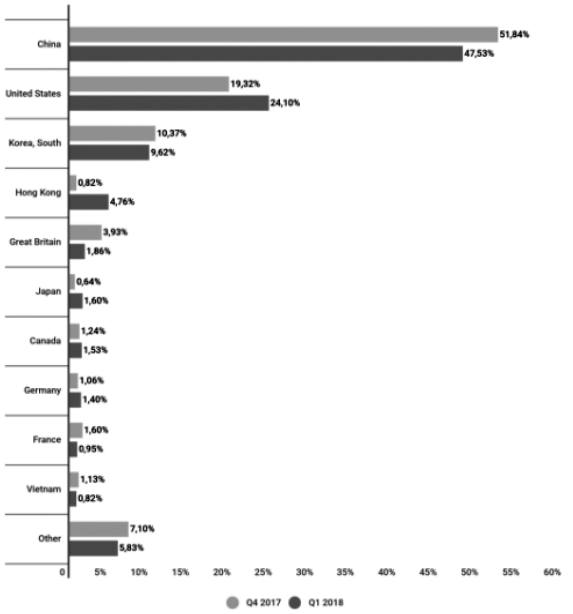
Hơn nữa, việc kiểm tra và hạn chế quyền chia sẻ thông tin trên Facebook nói riêng và các mạng xã hội nói chung còn bảo vệ người dùng khỏi các mối nguy hiểm khác như bị đánh cắp tài khoản, mật khẩu tín dụng, quấy rối, lừa đảo hay thậm chí là tống tiền.

THỐNG KÊ TÌNH HÌNH AN TOÀN THÔNG TIN
TỔ ỨNG CỨU SỰ CỐ

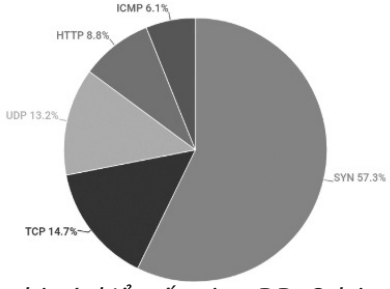
I. Tình hình An toàn thông tin Quý I năm 2018 trong nước và quốc tế

1. Tình hình tấn công DDoS

Theo báo cáo của An ninh mạng trong Quý 1 của Kaspersky các cuộc tấn công DDoS tiếp tục diễn biến phức tạp. Với mục tiêu tấn công ở 79 quốc gia (giảm so với 84 quốc gia trong quý trước). Cuộc tấn công dài nhất lên đến 297 giờ (12 ngày). Trong số 10 quốc gia bị tấn công nhiều nhất, Việt Nam đứng thứ 10.



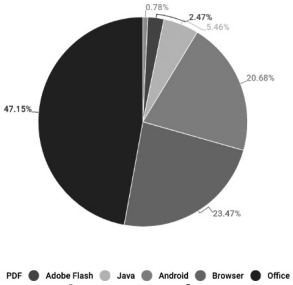
Danh sách 10 quốc gia bị tấn công DDoS trong quý I/2018 (nguồn securelist.com)



Thống kê các kiểu tấn công DDoS thông qua các giao thức trong quý III.

2. Thống kê danh sách các ứng dụng bị khai thác điểm yếu để tấn công

Theo tổng hợp của Kaspersky trong quý I/2018 danh sách các ứng dụng bị tội phạm mạng khai thác các điểm yếu/lỗ hổng để tấn công. Tỷ lệ khai thác của Microsoft Office (47,15%) tăng hơn gấp đôi so với mức trung bình của năm 2017. Thứ 2 là khai thác thông qua trình duyệt (23,47%).



Nguồn: Kaspersky

3. Tình hình tấn công bằng mã độc mã hóa dữ liệu

Báo cáo tổng kết của Kaspersky Lab về tình hình mã độc hại trong quý I/2018 cho biết, Việt Nam đứng ở vị trí thứ 3 trong 10 nước bị tấn công bằng loại hình mã độc đòi tiền chuộc /mã hóa dữ liệu.

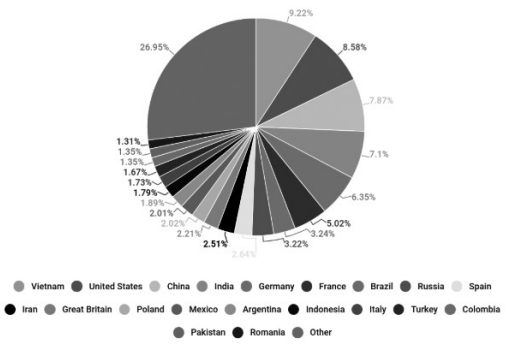
	Country*	% of users attacked by cryptors**
1	Uzbekistan	1.12
2	Angola	1.11
3	Vietnam	1.04
4	Venezuela	0.95
5	Indonesia	0.95
6	Pakistan	0.93
7	China	0.87
8	Azerbaijan	0.75
9	Bangladesh	0.70
10	Mongolia	0.64

Danh sách 10 dòng mã độc mã hóa lây nhiễm nhiều nhất

	Name	Verdicts*	% of attacked users**
1	WannaCry	Trojan-Ransom.Win32.Wanna	38.33
2	PolyRansom/VirLock	Virus.Win32.PolyRansom	4.07
3	Cerber	Trojan-Ransom.Win32.Zerber	4.06
4	Cryakl	Trojan-Ransom.Win32.Cryakl	2.99
5	(generic verdict)	Trojan-Ransom.Win32.Crypren	2.77
6	Shade	Trojan-Ransom.Win32.Shade	2.61
7	Purgen/GlobeImposter	Trojan-Ransom.Win32.Purgen	1.64
8	Crysis	Trojan-Ransom.Win32.Crusis	1.62
9	Locky	Trojan-Ransom.Win32.Locky	1.23
10	(generic verdict)	Trojan-Ransom.Win32.Gen	1.15

4. Tình hình Spam và tấn công Phishing

Báo cáo tổng kết của Kaspersky Lab về tình hình thư rác và lừa đảo trực tuyến trong quý I/2018 cho biết, Việt Nam tiếp tục nằm trong nhóm các quốc gia có nguồn phát tán thư rác đứng đầu với vị trí thứ 1 (9,22%), đứng thứ 2 là Mỹ (8,58%) và thứ 3 là Trung Quốc (7,87%).



Báo cáo của Kaspersky Lab về tình hình tấn công Phishing trên phạm vi toàn cầu trong quý I/2018. Dẫn đầu là Brazil với 19.07%, thứ 2 là Argentina với 13.301%...

Country	%
Brazil	19.07
Argentina	13.30
Venezuela	12.90
Albania	12.56
Bolivia	12.32
Réunion	11.88
Belarus	11.62
Georgia	11.56
France	11.40
Portugal	11.26

Top 10 countries by percentage of users attacked by phishers

Thống kê tình hình tấn công Phishing trên phạm vi toàn cầu *(Nguồn: Kaspersky)*

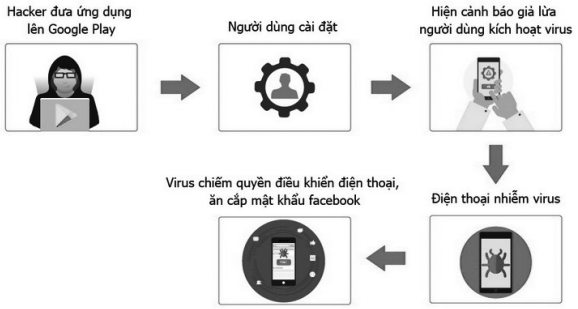
5. Lỗ hổng Spectre và Meltdown ảnh hưởng đến hàng tỉ thiết bị

Đầu tháng 1/2018, giới công nghệ toàn thế giới chấn động khi thông tin về các lỗ hổng Spectre và Meltdown trong bộ vi xử lý của Intel, AMD, ARM và Apple được công bố. Các lỗ hổng cho phép kẻ tấn công đọc được thông tin nhạy cảm trên máy người dùng, ảnh hưởng đến gần như mọi hệ điều hành: iOS, MacOS, tvOS, Microsoft Windows (Windows 7 đến Windows 10, Windows Server), Windows Phone, Linux (Ubuntu, Cent OS, FreeBSD...), Android và Chrome OS...

Meltdown (CVE-2017-5754) và Spectre (CVE-2017-5753 và CVE-2017-5715) là các lỗ hổng trên CPU, cho phép người dùng quyền thấp (không có quyền quản trị/root, chỉ cần chạy được file thực thi trên hệ thống), đọc được các thông tin nhạy cảm trong bộ nhớ, bao gồm hệ điều hành và các chương trình khác. Nghiêm trọng hơn, các lỗ hổng này có thể bị khai thác bằng mã javascript thông qua trình duyệt khi truy cập web.

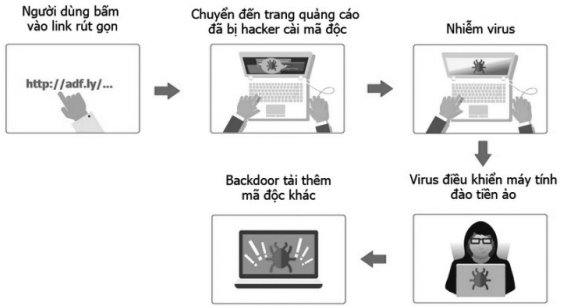
6. Hơn 35.000 smartphone tại Việt Nam nhiễm virus GhostTeam đánh cắp mật khẩu Facebook

Theo thống kê từ hệ thống giám sát virus của Bkav, đến ngày 25/01, đã có hơn 35.000 thiết bị smartphone tại Việt Nam nhiễm virus GhostTeam đánh cắp mật khẩu Facebook. Mã độc này lợi dụng hàng loạt ứng dụng Việt phổ biến như lịch vạn niên, đèn pin, la bàn... trên Google Play để phát tán. Chuyên gia Bkav khuyến cáo người dùng cần tiến hành quét virus và đổi ngay mật khẩu tài khoản Facebook nếu phát hiện điện thoại của mình nhiễm.



7. Hàng trăm nghìn máy tính tại Việt Nam bị chiếm quyền điều khiển do nhiễm virus đào tiền ảo

Theo hệ thống giám sát của Bkav, hơn 139.000 máy tính tại Việt Nam bị nhiễm virus đào tiền ảo mới W32.AdCoinMiner, phát tán qua dịch vụ quảng cáo trực tuyến Adf.ly và lỗ hổng phần mềm. Nguy hiểm hơn, sau khi chiếm được quyền điều khiển máy tính, virus có thể tải thêm mã độc khác từ server điều khiển của hacker phục vụ mục đích gián điệp, ăn cắp thông tin cá nhân, thậm chí là xóa dữ liệu.



Chuyên gia khuyến cáo người dùng cần cập nhật ngay bản vá mới nhất cho hệ điều hành và cài thường trực phần mềm diệt virus có tích hợp tường lửa cá nhân trên máy tính để được bảo vệ tự động.

8. Dữ liệu gần 87 triệu tài khoản Facebook bị sử dụng trái phép

Facebook cho biết 87 triệu người dùng bị chia sẻ thông tin cho Cambridge Analytica, trong khi người sáng lập mạng xã hội này, Mark Zuckerberg, sẽ sớm điều trần trước quốc hội Mỹ. Trước đó, Facebook bị tố đã làm lộ dữ liệu của 50 triệu người dùng Facebook cho Cambridge Analytica khai thác trái phép trong suốt cuộc bầu cử tổng thống Mỹ năm 2016.

Trong số hơn 87 triệu người dùng Facebook bị Cambridge Analytica, công ty có trụ sở tại Anh, khai thác và sử dụng thông tin trái phép, có đến hơn 420 ngàn người dùng tại Việt Nam. Việt Nam xếp thứ 9 trong tổng số 10 quốc gia có số người dùng Facebook bị Cambridge Analytica khai thác thông tin nhiều nhất.

9. Lỗ hổng trong giao thức Remote Desktop ảnh hưởng tất cả phiên bản Windows

Một lỗ hổng nghiêm trọng đã được phát hiện trong giao thức Credential Security Support Provider (CredSSP). Lỗ hổng CredSSP này gây ảnh hưởng trực tiếp đến tất cả các phiên bản hệ điều hành Windows và cho phép attacker khai thác RDP và WinRM từ xa để ăn cắp dữ liệu và chạy mã độc hại.

Giao thức CredSSP được thiết kế để sử dụng bởi RDP (Remote Desktop Protocol) và Windows Remote Management (WinRM) nhằm đảm bảo việc chuyển tiếp các thông tin được mã hoá từ khách hàng của Windows sang các máy chủ với mục đích xác thực từ xa.

CVE-2018-0886 được phát hiện bởi các nhà nghiên cứu tại công ty Cybersecurity Preempt Security là một lỗ hổng mật mã trong CredSSP. Nó có thể được khai thác bởi attacker sử dụng phương thức tấn công man-in-the-middle, thông qua Wi-Fi hoặc truy cập vật lý vào mạng để lấy cắp dữ liệu xác thực người dùng hoặc thực hiện một cuộc tấn công Remote Procedure Call (tạm dịch là tấn công cuộc gọi thủ tục từ xa).

Để bảo vệ bản thân và tổ chức của bạn khỏi

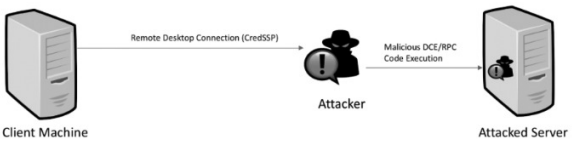


Figure 1 - An illustration of CVE-2018-0886 exploit scenario

sự khai thác của attacker thông qua lỗ hổng CredSSP, người dùng được khuyến khích vá các máy trạm và máy chủ của họ bằng các bản cập nhật có sẵn từ Microsoft. Đồng thời cần thiết lập bổ sung một số các chính sách bảo mật trong hệ thống thông tin của đơn vị.

10. Lỗ hổng an toàn thông tin trên hệ quản trị nội dung Drupal

Trong năm 2017 và các tháng đầu năm nay, Drupal đã công bố 7 lỗ hổng bảo mật. Tuy nhiên, chỉ riêng từ cuối tháng 3/2018 đến nay Drupal đã bộc lộ 2 lỗ hổng bảo mật có mức độ nguy hiểm cao ở mức nghiêm trọng cần được theo dõi, xử lý khẩn cấp: một là, lỗ hổng Drupal cho phép thực thi các lệnh điều khiển từ xa trái phép (Remote Code Execution, mã lỗi quốc tế CVE-2018-7600 hoặc SA-CORE-2018-002), được công bố ngày 28/3/2018.

Lỗ hổng nguy hiểm thứ hai là lỗ hổng tấn công kịch bản liên trang (Cross Site Scriptting, mã lỗi quốc tế là SA-CORE-2018-003), được công bố ngày 18/4/2018. Lỗi Cross Site Scriptting được đánh giá có mức độ nghiêm trọng ở mức cao.

Ngày 25/4/2018, Drupal tiếp tục công bố lỗ hổng an toàn thông tin nghiêm trọng có mã SA-CORE-004 (mã quốc tế theo CVF có tên CVE-2018-7602), lỗ hổng thứ ba này đặc biệt nguy hiểm có thể cho phép kẻ tấn công chiếm quyền điều khiển hoàn toàn các trang web có lỗi.

Theo thống kê trong tổng số khoảng 1.000 website Drupal tại Việt Nam được quét, có đến hơn 500 website vẫn đang sử dụng phiên bản Drupal có lỗ hổng và có khả năng bị hacker khai

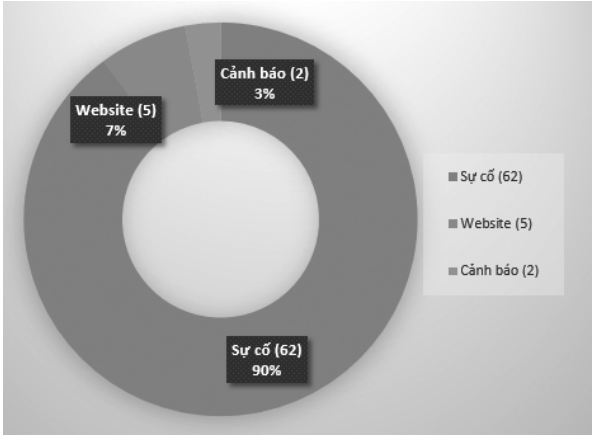
thác, trong đó có nhiều website quan trọng của các ngân hàng, tập đoàn công nghệ, các trường đại học, và cả các website cơ quan nhà nước...

II. Tình hình An toàn thông tin trên địa bàn tỉnh trong quý I/2018

1. Thống kê các website trên địa bàn tỉnh bị tấn công

Ngày	Domain
19/01/2018	http://daxaydungthanhhoa.com/pcs.php
27/3/2018	http://dulich.samson.com.vn/by.htm
27/3/2018	http://noihoithanhhoa.com/by.htm
27/3/2018	http://lohoithanhhoa.com/by.htm
27/3/2018	http://daoplatthanhhoa.com.vn/by.htm

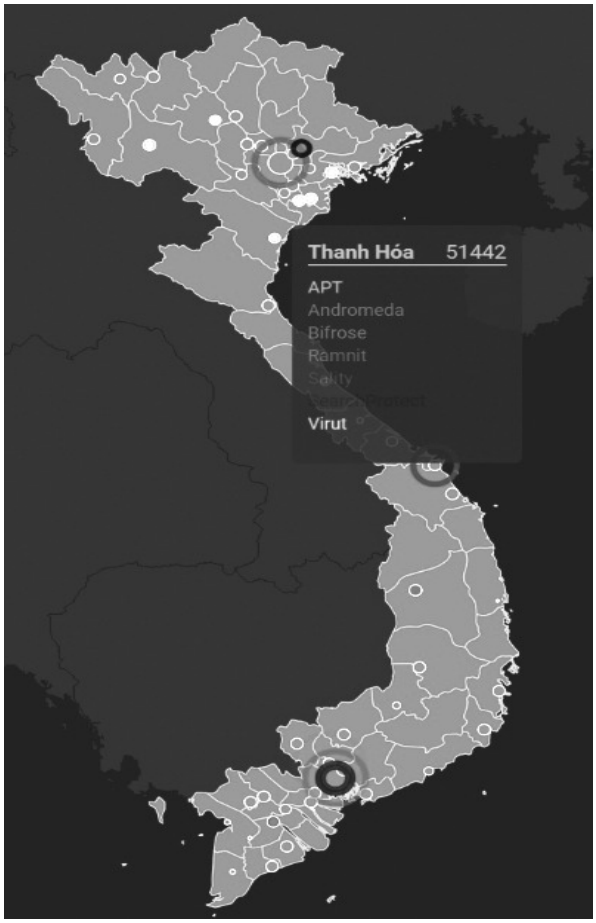
2. Tổng hợp tình hình ứng cứu sự cố trên địa bàn tỉnh



Trong quý I, Tổ Ứng cứu sự cố của Trung tâm hỗ trợ ứng cứu sự cố cho các cơ quan nhà nước trên địa bàn tỉnh với 62 lượt hỗ trợ, ban hành 07 công văn cảnh báo liên quan đến mã độc, Website và an toàn thông tin.

Theo số liệu giám sát an toàn thông tin của nhà mạng Viettel, trên địa bàn tỉnh ghi nhận hơn 51.000 các lượt tấn công bao gồm các tấn công có chủ đích APT, các mã độc kết nối và tham gia vào mạng máy tính ma Botnet như Andromeda, APT, Kazy, Ramnit, Sality...

Theo ghi nhận của Trung tâm An ninh mạng và An toàn dữ liệu, trong thời gian từ 01/01-30/3 ghi nhận có 544 cuộc tấn công khai thác chiếm quyền quản trị; 286 cuộc tấn công bằng mã độc; 155 cuộc tấn công vào ứng dụng Website; 04 cuộc tấn công từ chối dịch vụ vào các dịch vụ



đang hoạt động tại Trung tâm.

3. Công văn an toàn thông tin

- Ngày 25/01/2018 Sở Thông tin và Truyền thông ban hành công văn số 86/STTTT-CNTT về việc cảnh báo các sản phẩm máy tính xách tay của hãng HP bị cài cắm mã độc.
- Ngày 08/02/2018 Sở Thông tin và Truyền thông ban hành công văn số 134/STTTT-CNTT về việc rà soát, kiểm tra, phòng chống mã độc trên hệ thống máy tính.
- Ngày 20/4/2018 Sở Thông tin và Truyền thông ban hành công văn số 416/STTTT-CNTT về hướng dẫn, kiểm tra, rà soát, vá lỗ hổng bảo mật trên các thiết bị modem, router.
- Ngày 19/01/2018 Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa ban hành kế hoạch số 27/KH-TTCNTT&TT về việc phối hợp kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin cho các hệ thống thông tin và hỗ trợ ứng cứu sự cố an toàn thông tin mạng của các cơ quan quản lý nhà nước trên địa bàn tỉnh Thanh

Hóa năm 2018.

- Ngày 24/4/2018 Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa ban hành công văn số 75/TTCNTT&TT-QTHT về cảnh báo lỗ hổng an toàn thông tin hệ quản trị nội dung Drupal.

- Ngày 03/5/2018 Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa ban hành công văn số 77/TTCNTT&TT-QTHT về việc cảnh báo lỗ hổng an toàn thông tin SA-CORE-2018-004 của hệ quản trị nội dung Drupal.

TIN HOẠT ĐỘNG

Hội nghị trực tuyến triển khai một số nhiệm vụ ứng dụng công nghệ thông tin của tỉnh năm 2018

Ngày 05/3/2018, UBND tỉnh tổ chức Hội nghị triển khai một số nhiệm vụ ứng dụng công nghệ thông tin (CNTT) của tỉnh năm 2018, gồm: Kiến trúc Chính quyền điện tử tỉnh Thanh Hóa, phiên bản 1.0; Quy chế quản lý, vận hành, khai thác sử dụng phần mềm quản lý văn bản, hồ sơ công việc; quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng CNTT của các cơ quan quản lý nhà nước tỉnh Thanh Hóa; kế hoạch ứng dụng CNTT trong các cơ quan nhà nước trên địa bàn tỉnh năm 2018. Hội nghị được tổ chức trực tuyến với 03 điểm cầu trung tâm đặt tại Văn phòng Tỉnh ủy, Văn phòng UBND tỉnh, Sở Thông tin và Truyền thông và 28 điểm cầu đầu cuối (27 huyện, thị xã, thành phố và Ban Quản lý Khu Kinh tế Nghi Sơn). Đây là hội nghị trực tuyến đầu tiên của tỉnh sau khi dự án xây dựng hệ thống phòng họp trực truyến cho các cơ quan nhà nước tỉnh Thanh Hóa hoàn thành việc đầu tư xây dựng và sẵn sàng đi vào hoạt động.

Phát biểu chỉ đạo hội nghị, đồng chí Nguyễn Văn Phát - Ủy viên Ban Thường vụ, Trưởng ban Tuyên giáo Tỉnh ủy ghi nhận và đánh giá cao sự cố gắng của Sở Thông tin và Truyền thông và các ngành, đơn vị liên quan trong việc xây dựng hệ thống phòng họp trực tuyến trên địa bàn tỉnh. Hệ thống phòng họp trực tuyến là phương tiện, công cụ hiện đại để phổ biến, quán triệt các chủ trương của Đảng, chính sách pháp luật của nhà nước; các ý kiến lãnh đạo, chỉ đạo của cấp ủy đảng và chính quyền các cấp đến cán bộ, công chức, viên chức, doanh nghiệp và người dân được nhanh nhất, kịp thời và hiệu quả. Thông qua việc quản lý, vận hành, khai thác hiệu quả hệ thống hội nghị trực tuyến sẽ góp phần quan trọng để nâng cao hiệu quả, hiệu lực lãnh đạo, chỉ đạo, điều hành của cấp ủy, chính quyền các cấp, từng bước đổi mới tác phong, lề lối làm việc trong các cơ quan nhà nước trên địa bàn tỉnh theo hướng hiện đại, chuyên nghiệp; đồng thời, góp phần giảm thiểu các chi phí hành chính, thúc đẩy cải cách hành chính của tỉnh. Đồng chí yêu cầu Sở Thông tin và Truyền thông chủ trì, phối hợp với các cơ quan đơn vị (Văn phòng Tỉnh ủy, Văn phòng UBND tỉnh và các điểm cầu đầu cuối tại các huyện, Ban Quản lý Khu Kinh tế Nghi Sơn) tăng cường tổ chức tập huấn, bồi dưỡng để nâng cao trình độ và kỹ năng sử dụng, vận hành hệ thống cho đội ngũ cán bộ trực tiếp quản lý, vận hành kỹ thuật để hệ thống hội nghị trực tuyến của tỉnh hoạt động ổn định, chất lượng và phát huy tốt hiệu quả đầu tư.

Thay mặt các đại biểu tham dự hội nghị tại các điểm cầu, đồng chí Trần Duy Bình - Giám đốc Sở TT&TT đã phát biểu cảm ơn các đồng chí lãnh đạo Tỉnh ủy, UBND tỉnh đã quan tâm lãnh đạo, chỉ đạo sát sao trong quá trình thực hiện nhiệm vụ xây dựng hệ thống Hội nghị trực tuyến của tỉnh. Sở Thông tin và Truyền thông khẩn trương phối hợp với các cơ quan, đơn vị liên quan tham mưu xây dựng phương án quản lý vận hành, khai thác hiệu quả hệ thống hội nghị trực tuyến của tỉnh; tổ chức tập huấn, bồi dưỡng nâng cao kỹ năng nghiệp vụ cho đội ngũ cán bộ trực tiếp quản lý, vận hành hệ thống tại các điểm cầu trung tâm và các điểm cầu đầu cuối để hệ thống hoạt động ổn định, chất lượng tốt để phục vụ có hiệu quả các hoạt động chung của tỉnh. Bắt đầu từ tháng 3/2018 Tỉnh ủy, HĐND tỉnh, UBND tỉnh; các Ban của tỉnh ủy; các đoàn thể chính trị cấp tỉnh; các sở, ban, ngành cấp tỉnh bắt đầu đăng ký và tổ chức các hội nghị giao ban trực tuyến giữa cấp tỉnh đến cấp huyện để tiết kiệm thời gian, chi phí và số lượng các cuộc họp tập trung, nâng cao

hiệu quả công việc trong công tác lãnh đạo,chỉ đạo, điều hành của lãnh đạo các cấp ủy đảng và chính quyền./.

Lê Văn Tuấn

Ra mắt giao diện mới của Báo Thanh Hóa điện tử

Sáng 29/3, đồng chí Trịnh Văn Chiến - Ủy viên Trung ương Đảng, Bí thư Tỉnh uỷ, Chủ tịch HĐND tới dự và phát biểu ý kiến tại buổi gặp mặt giữa các thế hệ người làm Báo Thanh Hoá nhân kỷ niệm 56 năm ngày Báo Thanh Hoá ra số đầu tiên (20/3/1962 - 20/3/2018). Cùng tham dự buổi toạ đàm có các đồng chí: Nguyễn Văn Phát - Ủy viên Ban Thường vụ, Trưởng ban Tuyên giáo Tỉnh ủy; Phạm Đăng Quyền, Phó Chủ tịch UBND tỉnh; đại diện lãnh đạo các sở, ngành có liên quan.

Đến thăm và gửi những lời chúc mừng tốt đẹp nhất đến các cán bộ, phóng viên, biên tập viên đang công tác tại các phòng chuyên môn của Báo Thanh Hoá, đồng chí Bí thư Tỉnh ủy động viên, khích lệ những người làm báo Thanh Hoá tiếp tục nỗ lực vươn lên, vượt qua mọi khó khăn, thách thức, bám sát cuộc sống, phản ánh chân thực khách quan tình hình thực tế, đưa ra nhiều ý kiến phản biện xác đáng thể hiện ở những tác phẩm báo chí xuất sắc, đóng góp tích cực vào phong trào cách mạng chung của tỉnh.

Tại Tòa soạn, đồng chí Bí thư Tỉnh ủy, Chủ tịch HĐND tỉnh đã thực hiện nghi thức ấn nút ra mắt giao diện mới của Báo Thanh Hóa điện tử.

Trước đó, Trung tâm CNTT&TT Thanh Hóa đã phối hợp với Báo Thanh Hóa trong việc xây dựng giao diện mới của Báo Thanh Hóa điện tử trên nền tảng công nghệ, kỹ thuật hiện đại, có tính bảo mật cao, bảo đảm các yêu cầu của báo chí đa đa phương tiện theo xu hướng truyền thông hiện đại, thân thiện, dễ dàng tương tác với bạn đọc trên máy tính và các thiết bị di động... Ngoài giao diện mới của Báo điện tử. Trung tâm cũng đã phối hợp trong việc triển khai phần mềm tòa soạn hội tụ, quản lý văn bản và nhuận bút cho Báo Thanh Hóa.

Cao Việt Cường

Trung tâm CNTT&TT Thanh Hóa xây dựng trang thông tin điện tử của Đài Truyền thanh, truyền hình huyện Thạch Thành

Ngày 03/3/2018, được sự đồng ý của Huyện ủy, HĐND, UBND huyện và Sở Thông tin và Truyền thông tỉnh Thanh Hóa, Đài TTTH huyện Thạch Thành đã long trọng tổ chức lễ khai trương trang thông tin điện tử tại địa chỉ http://thachthanhtv.vn

Tham dự có đ/c Lê Quang Tuấn, Phó Giám đốc cùng các đ/c trong đoàn công tác của Sở Thông tin và truyền thông tỉnh Thanh Hóa. Về phía huyện Thạch Thành, tới dự có các đ/c: Bùi Thị Mười, Tỉnh ủy viên, Bí thư Huyện ủy, Chủ tịch HĐND huyện; Lê Văn Trinh, Phó Bí thư, Chủ tịch UBND huyện cùng các đ/c trong BTV Huyện ủy, Thường trực HĐND, UBND, UBMTTQ; các đ/c lãnh đạo các phòng, ban, ngành, đoàn thể; cơ quan, đơn vị đóng trên địa bàn huyện. Các đ/c lãnh đạo đại diện các Đài TTTH huyện bạn cùng tập thể đội ngũ cán bộ, viên chức, người lao động của Đài TTTH Thạch Thành.

Trang thông tin điện tử của Đài ra đời nhằm phục vụ nhu cầu nắm bắt thông tin của các cơ quan, đơn vị, doanh nghiệp và toàn thể nhân dân các dân tộc huyện Thạch Thành, nhân dân trong và ngoài nước. Nội dung Website sẽ đăng tải toàn bộ các chương trình truyền hình, chương trình phát thanh, các phóng sự, bài viết đặc sắc phản ánh về tình hình kinh tế - chính trị, văn hóa - xã hội, an ninh - quốc phòng của huyện; đồng thời giới thiệu, quảng bá những hình ảnh về đất và người Thạch Thành nhằm giới thiệu, quảng bá với bạn bè cả nước cũng như quốc tế về thế mạnh, tiềm năng phát triển kinh tế, du lịch... của huyện.

Trên cơ sở hợp tác giữa Trung tâm CNTT&TT Thanh Hóa và Đài Truyền thanh, truyền hình huyện Thạch Thành. Trung tâm đã xây dựngtrang thông tin điện tử cho Đài TTTH huyện với thiết kế với giao diện hiện đại, bảo đảm an toàn thông tin. Thông qua trang thông tin điện tử trên môi trường mạng giúp người truy cập có thể theo dõi các chương trình phát thanh, truyền hình, các tin tức thời sự nổi bật và xem lại tất cả các chương trình của Đài ở bất kỳ đâu, trên nhiều loại thiết bị như máy tính bàn, laptop hay điện thoại thông minh thông qua mạng Internet.

Lê Duy