**SỔ TAY AN TOÀN SỐ**

**DÀNH CHO NHÀ BÁO**

**Hà Nội, tháng 5. 2018**

**MỤC LỤC**

LỜI NÓI ĐẦU

I. AN TOÀN SỐ TRONG TÁC NGHIỆP BÁO CHÍ Ở VIỆT NAM

1.1. Hiện trạng

1.2. Khung pháp lý bảo vệ nhà báo, phóng viên

II. NHỮNG NGUY CƠ, TỔN HẠI MẤT AN TOÀN SỐ TRONG TÁC NGHIỆP BÁO CHÍ Ở VIỆT NAM

III. NHỮNG KỸ NĂNG XỬ LÝ ĐỂ TĂNG CƯỜNG AN TOÀN SỐ TRONG TÁC NGHIỆP BÁO CHÍ Ở VIỆT NAM

3.1. Những kỹ năng cơ bản

3.2. Những lời khuyên bổ sung

3.3. Những địa chỉ hỗ trợ

IV. KẾT LUẬN

**CÁC TỪ VIẾT TẮT**

ATS - an toàn số

TNBC - tác nghiệp báo chí

ATTNBC - an toàn tác nghiệp báo chí

MXH - mạng xã hội

**LỜI NÓI ĐẦU**

“Sổ tay An toàn số” này là một trong những sản phẩm trong khuôn khổ dự án “Chất lượng xây dựng và thực thi chính sách kinh tế tại Việt Nam được cải thiện với sự tham gia hiệu quả của báo chí truyền thông và tổ chức xã hội” do Bộ Các vấn đề toàn cầu Canada (GAC) tài trợ cho Trung tâm nghiên cứu Truyền thông phát triển (RED). Mục tiêu của Sổ tay là:

a) Cung cấp cho nhà báo, phóng viên một cái nhìn tổng quan về hiện trạng AST trong tác nghiệp báo chí ở Việt Nam.

b) Cung cấp cho nhà báo, phóng viên các kỹ năng giúp tăng cường an toàn tác nghiệp báo chí trong thời đại số.

Ngoài tài trợ trực tiếp của GAC, Sổ tay này còn nhận được sự cố vấn quý báu về nội dung của ông Nguyễn Chí Dũng (Cố vấn chính sách của RED), ông Nguyễn Tất Vinh (chuyên gia công nghệ thông tin),

Chúng tôi hoan nghênh mọi góp ý xây dựng cho Sổ tay từ các nhà báo, phóng viên, chuyên gia báo chí, chuyên gia công nghệ thông tin nói riêng, cũng như từ mọi độc giả nói chung.

Mọi góp ý xây dựng xin gửi về:

**Trung tâm nghiên cứu Truyền thông phát triển**

**Địa chỉ:** Phòng 707, tòa nhà 142 Lê Duẩn, Đống Đa, Hà Nội  
**Tel/Fax:** 0243.856.6777  
**Email:** [center@red.org.vn](mailto:center@red.org.vn)  
**Website:** <http://red.org.vn>

**I. HIỆN TRẠNG AN TOÀN SỐ TRONG TÁC NGHIỆP BÁO CHÍ Ở VIỆT NAM**

**1.1. Tình hình**

Với tư cách là những người sử dụng thiết bị kỹ thuật số thì nhà báo, phóng viên cũng chịu chung những rủi ro, tổn hại mà những người sử dụng thiết bị kỹ thuật số khác gặp phải. Dưới đây là một số thông tin về bức tranh ATS ở Việt Nam:

* Theo Thống kê thường niên 2017 của Kaspersky Lab, Việt Nam đứng đầu trong danh sách có nguy cơ bị lây nhiễm mã độc cục bộ; đứng thứ ba trong danh sách các quốc gia bị tấn công vào lỗ hổng mật mã hóa; đứng thứ sáu trong danh sách các quốc gia có nguy cơ bị lây nhiễm mã độc trực tuyến.
* Năm 2016 đã có tổng cộng khoảng 145 000 cuộc tấn công mạng khác nhau nhằm vào hệ thống thông tin Việt Nam, với ba loại hình chính là: lừa đảo, mã độc và thay đổi giao diện, gây thiệt hại hơn 10 400 tỷ đồng;
* Hơn 10 000 trang/cổng thông tin điện tử có tên miền “.vn” bị tấn công, chiếm quyền điều khiển, thay đổi giao diện, cài mã độc và có hơn 70% số máy tính bị lây nhiễm.
* Theo ghi nhận của Trung tâm ứng cứu khẩn cấp máy tính (VNCERT) thì Quý I năm 2017 đã có gần 7 700 sự cố tấn công mạng vào các website tại Việt Nam.
* Tháng 7/2016 đã xảy ra vụ tấn công vào hệ thống mạng của Hàng không Việt Nam theo hình thức APT (tấn công có chủ đích) làm ảnh hưởng hơn 100 chuyến bay, đồng thời làm rò rỉ dữ liệu của hơn 400 000 tài khoản khách hàng thường xuyên của hãng.
* Tháng 3/2017, một số website của các cảng hàng không như Tân Sơn Nhất, Rạch Giá, Tuy Hòa đã bị tin tặc tấn công.
* Tình trạng vi phạm sở hữu trí tuệ, đánh cắp công nghệ, bản quyền trên Internet ngày càng tăng, nguy cơ gián điệp mạng, tội phạm mạng trở nên phức tạp, nguy hiểm.
* Môi trường Internet cũng bị lợi dụng để tán phát thông tin bịa đặt, không kiểm chứng, độc hại nhằm vu khống, bôi nhọ cá nhân, tổ chức, hoạt động khủng bố, phá hoại, hoạt động tội phạm mạng ngày càng tinh vi, phức tạp, nguy hiểm với mức độ thiệt hại ngày càng tăng.

…

Với sự gia tăng mạnh mẽ của những nhà báo tác nghiệp, trao đổi thông tin, xuất bản,… bằng các thiết bị kỹ thuật số, công cụ trực tuyến thì bên cạnh thế mạnh của mình họ cũng gặp rất nhiều thách thức, nguy cơ.

Chẳng hạn, nhà báo Lại Văn Sâm bị làm phiền bởi các tài khoản mạo danh mình trên MXH. Nhà báo Trương Châu Hữu Danh liên tục bị tạm ngừng sử dụng tài khoản Facebook. Báo điện tử Vietnamnet, Dân Trí, Tầm Nhìn,… không ít lần bị tin tặc (hacker) tấn công.

**1.2. Khung pháp lý để bảo đảm an toàn số trong tác nghiệp báo chí ở Việt Nam**

Cho đến nay, ở Việt Nam, khung pháp lý về ATTNBC chủ yếu tập trung vào lĩnh vực an toàn thân thể, an toàn về mặt vật lý trong TNBC. Bao gồm:

- Luật Báo chí 2016.

- Nghị định 159/2013/NĐ-CP.

Tuy nhiên, như đã nói ở trên, đòi hỏi tăng cường ATS trong TNBC ngày càng trở nên bức thiết. Ngoài việc nâng cao nhận thức và kỹ năng bảo đảm ATS của nhà báo, phóng viên, tòa soạn,… thì cần có hành lang pháp lý và cơ chế phối hợp cụ thể để bảo đảm ATS trong TNBC.

**II. NHỮNG NGUY CƠ, TỔN HẠI MẤT AN TOÀN SỐ TRONG TÁC NGHIỆP BÁO CHÍ Ở VIỆT NAM**

Khi bạn trở thành một “công dân số” thì bên cạnh lợi ích của nó còn có rất nhiều nguy cơ, tác hại đang chờ đợi bạn. Cụ thể, nếu bạn là nhà báo, phóng viên thì bạn có thể chịu những nguy cơ, tổn hại chính sau đây:

- Bị vô hiệu hóa/khóa tài khoản trên MXH.

- Bị chiếm tài khoản trên MXH.

- Bị giả mạo tài khoản trên MXH.

- Không truy cập được tài khoản trên MXH.

- Bị lộ, mất, sai lạc những thông tin chỉ mình biết trên tài khoản MXH.

- Không truy cập được thiết bị điện tử, kỹ thuật số.

- Bị mất, hỏng hóc, sai lạc dữ liệu trên thiết bị điện tử, kỹ thuật số.

- Bị chiếm tài khoản CMS.

- Không truy cập được tài khoản CMS.

- Bị giả mạo tài khoản CMS.

- Bị đe dọa, vu khống, bôi nhọ trên MXH.

- Bị lừa đảo bởi những tin tức, nguồn tin sai trên MXH.

- Bị báo cáo dẫn tới tạm ngừng tài khoản MXH.

- Bị lộ vị trí địa lý của mình.

- Bị tấn công từ chối dịch vụ (DoS, DDoS).

- Bị nhiễm các phần mềm độc hại. Bị hacker khai thác.

- Bị xâm phạm bản quyền sở hữu trí tuệ trên MXH.

…

Có hàng nghìn nguy cơ, tổn hại khác mà chúng tôi không thể liệt kê hết trong khuôn khổ Sổ tay nhỏ bé này.

Chúng tôi tập trung vào đối tượng cần hỗ trợ, bảo vệ là nhà báo, phóng viên đang TNBC ở Việt Nam và cho rằng những nguy cơ, tổn hại kể trên là phổ biến nhất trong TNBC.

Chúng tôi cho rằng trong thời đại báo chí đa phương tiện, đặc biệt là báo chí điện tử thì dữ liệu, thông tin số vừa là tư liệu, vừa là sản phẩm, tài sản chủ yếu của báo chí. Chúng tôi kêu gọi và hoan nghênh mọi nhà báo, phóng viên chia sẻ câu chuyện, kinh nghiệm của mình về ATS trong TNBC.

**III. NHỮNG KỸ NĂNG XỬ LÝ ĐỂ TĂNG CƯỜNG AN TOÀN SỐ TRONG TÁC NGHIỆP BÁO CHÍ Ở VIỆT NAM**

**3.1. Những kỹ năng cơ bản**

Dưới đây là những kỹ năng cơ bản để ứng phó với từng nguy cơ, tổn hại mất ATS trong TNBC ở Việt Nam.

**3.1.1. Khi bị vô hiệu hóa/khóa tài khoản trên MXH**

Đừng hoảng loạn. Hầu như mọi MXH đều có chính sách, hướng dẫn rõ ràng về quyền riêng tư, khiếu nại, đường dây nóng, hỗ trợ kỹ thuật,… Trước hết hãy rà soát, chắc chắn rằng bạn tuân thủ mọi quy định của ban quản lý MXH. Sau đó, hãy liên hệ với các bộ phận khác của ban quản lý MXH để đề nghị giải quyết. Tất nhiên, bạn hoàn toàn có thể nhờ sự trợ giúp của các chuyên gia, bạn hữu,…

**3.1.2. Khi bị chiếm tài khoản trên MXH**

Có thể bạn vô tình tiết lộ thông tin truy cập tài khoản; có thể bạn bị người khác dùng những công nghệ đánh cắp thông tin;… dẫn tới việc tài khoản của bạn bị kẻ xấu truy cập và chiếm đoạt.

Bạn cũng đừng hoảng loạn, và hãy làm theo các khuyến nghị của chúng tôi trong trường hợp 1.1.

Ngoài ra, để giảm thiểu tác hại bị kẻ xấu lợi dụng tài khoản của bạn để làm những điều giả mạo khác, bạn cần thông báo kịp thời thông tin về việc mất tài khoản của mình.

Sau đó, hãy dùng những phần mềm anti-virus có tiếng, nhờ chuyên gia hoặc dùng dịch vụ thuê ngoài để rà soát, khắc phục và giám sát những “lỗ hổng” của mình.

**3.1.3. Bị giả mạo tài khoản trên MXH**

Thay vì chiếm đoạt tài khoản của bạn và làm những điều bạn không muốn bằng tài khoản ấy, kẻ xấu có thể tự tạo một tài khoản của hắn nhưng sử dụng nhiều thông tin của bạn để đánh lừa những người khác rằng hắn chính là bạn, và ngược lại, bạn chính là hắn.

Bạn cũng hãy làm theo những khuyến nghị của chúng tôi trong trường hợp 1.2.



*Nhiều tài khoản gây lầm tưởng rằng*

*nó là của nhà báo Lại Văn Sâm*

**3.1.4. Không truy cập được tài khoản trên MXH**

Trường hợp này được xét tới với điều kiện bạn không bị nhà quản lý vô hiệu hóa/xóa tài khoản, cũng không bị chiếm đoạt tài khoản. Tuy nhiên, do bạn có quá nhiều thông tin tài khoản khác nhau, nơi lưu trữ và cách lưu trữ chúng khác nhau,… khiến cho bạn quên mất một trong số đó hoặc nhầm lẫn cái này với cái khác.

Cũng không nên quá lo lắng. Hãy tận dụng mọi sự hỗ trợ kỹ thuật của ban quản lý MXH. Thêm nữa, bạn nên dùng một phần mềm quản lý các password của những tài khoản khác nhau mà bạn sử dụng. Ví dụ: LastPass, KeyPassX, 1Password,…

**3.1.5. Bị lộ, mất, sai lạc những thông tin chỉ mình có quyền truy cập**

Có những thông tin chỉ bạn mới biết, bạn lưu trữ nó bằng dịch vụ lưu trữ trực tuyến, và bạn chưa bao giờ có ý định chia sẻ nó với người khác. Bỗng nhiên một ngày bạn thấy nó trôi nổi trên internet cũng như bị người khác biết.

Khả năng rất lớn là thông tin truy cập tài khoản của bạn đã bị kẻ xấu biết và dùng nó để truy cập vào tài khoản của bạn, lấy trộm thông tin của bạn.

Một số ứng dụng (ví dụ: facebook) có tính năng ghi lại phiên truy cập trên các thiết bị khác nhau, tại những địa điểm khác nhau và vào những thời điểm khác nhau. Nó sẽ giúp bạn phát hiện những điều bất thường.

Tuy nhiên, chúng tôi vẫn khuyến cáo bạn nên thường xuyên (tối thiểu 1 lần/1 tháng) thay đổi thông tin truy cập tài khoản của mình. Đồng thời tránh những sự quên lãng hoặc nhầm lẫn các thông tin truy cập tài khoản, bằng cách sử dụng một phần mềm quản lý password như chúng tôi đã lưu ý ở trường hợp 1.4.

**3.1.6. Không truy cập được thiết bị điện tử, kỹ thuật số**

Trong thời đại kỹ thuật số hiện nay, nhiều thiết bị điện tử đã được trang bị tính năng đăng nhập để sử dụng thiết bị. Chẳng hạn chiếc điện thoại thông minh của bạn.

Nếu bạn không đăng nhập được vào thiết bị của mình thì ngoài những nguyên nhân về mặt vật lý đến từ chính thiết bị đó (mà bạn cần sự hỗ trợ của chuyên gia kỹ thuật, của nhà sản xuất hoặc cung cấp thiết bị) thì cũng vẫn có thể có nguyên nhân chủ quan là bạn có quá nhiều thông tin đăng nhập khác nhau, nơi lưu trữ và cách lưu trữ chúng khác nhau,… khiến cho bạn quên mất một trong số đó hoặc nhầm lẫn cái này với cái khác.

Một lần nữa chúng tôi khuyến nghị bạn hãy lưu trữ cẩn thận, sắp xếp hợp lý để dễ dàng tìm lại đủ và đúng những thông tin đăng nhập tài khoản khi cần thiết.

**3.1.7. Bị chiếm đoạt, không truy cập được, hoặc bị giả mạo tài khoản CMS tại cơ quan báo chí**

Những lời khuyên của chúng tôi về cơ bản là giống với những lời khuyên ở trên dành cho các thông tin truy cập tài khoản khác.

Nhưng chúng tôi đề nghị nhà báo, phóng viên dành sự quan tâm, gìn giữ đặc biệt cho tài khoản CMS của mình, vì đó là một phần quan trọng trong công việc quan trọng của họ.

**3.1.8. Bị đe dọa, bôi nhọ, vu khống trên MXH**

Bị đe dọa, bôi nhọ, vu khống trên MXH là nguy cơ, tác hại chung đối với mọi người dùng MXH chứ không chỉ riêng với nhà báo, phóng viên. Ngoài những cách thức ứng xử theo thông lệ pháp lý của nhà nước, cơ quan chủ quản, tòa soạn, ngoài việc tố cáo và khiếu nại lên nhà quản lý MXH, thì các nhà báo, phóng viên nên - nếu không ngại - nên đưa câu chuyện của mình lên những diễn đàn, nhóm hoạt động để huy động thêm sự bảo vệ quyền và lợi ích hợp pháp của nhà báo, phóng viên.

Chúng tôi mạnh dạn kể ra một số địa chỉ như:

- Vietnamjournalism (facebook group)

- Diễn đàn Nhà báo trẻ (facebook group)

- Diễn đàn Nhà báo và Chính sách (facebook group)

- Diễn đàn Những người hành nghề Luật (facebook group)

**3.1.9. Bị lừa đảo bởi những tin tức, nguồn tin sai trên MXH**

Tại Hội thảo “An toàn số cho nhà báo” do Trung tâm nghiên cứu Truyền thông phát triển (RED Communication) tổ chức tại Hà Nội, vào ngày 19/04/2018, Tiến sĩ Terry F. Buss đã cảnh báo các nhà báo, phóng viên Việt Nam về nguy cơ thông tin, nguồn tin thật-giả lẫn lộn trên MXH. Theo Tiến sĩ Terry F. Buss, nếu các nhà báo, phóng viên vô tình đưa tin sai lệch trên MXH thì sẽ gây tổn hại rất lớn đến uy tín, chất lượng, giá trị, sự bền vững của tòa soạn, nền báo chí cũng như nền dân chủ nói chung.

Chúng tôi khuyến nghị các nhà báo, phóng viên những nguyên tắc sau đây đối với nguồn tin, thông tin trên MXH để giảm thiểu nguy cơ bị lừa đảo:

- Đối với những thông tin dẫn lại, nên truy cập vào nguồn ban đầu.

- Cảnh giác với thông tin trên các trang web không chính thống, không có địa chỉ và chủ quản,… Ví dụ: trang web trandaiquang.org không phải trang web của Chủ tịch nước Việt Nam Trần Đại Quang.



*Trang web trandaiquang.net*

Phần thông tin ở chân trang web là quan trọng giúp nhà báo, phóng viên dễ dàng xác minh độ tin cậy.



*Thông tin chân trang báo Vietnamnet*

- Không chia sẻ, truyền bá thông tin trên MXH khi bạn chưa xác minh được sự trung thực của thông tin.

- Khi thấy những tài khoản, số điện thoại thân thiết nhưng có biểu hiện lạ thì bạn hãy nhanh chóng xác minh lại. Rất có thể tài khoản, số điện thoại đó đã bị kẻ xấu chiếm đoạt và lợi dụng.

**3.1.10. Bị báo cáo dẫn tới tạm ngừng tài khoản MXH**

Chúng tôi đã nghe được nhiều lời than phiền của người dùng nói chung, nhà báo, phóng viên Việt Nam nói riêng về tình trạng bị số đông những người không quen biết báo cáo với ban quản lý MXH, dẫn tới tài khoản MXH bị tạm ngừng hoạt động, điển hình là tài khoản Facebook. Đây là mặt trái của cơ chế báo cáo của các MXH.

Đối với MXH nói chung, như chúng tôi đã nói, bạn buộc phải tôn trọng quy tắc hành xử, đăng phát nội dung và trình tự xử lý sự cố, khiếu nại mà ban quản lý MXH đã đặt ra.

Đối với Facebook nói riêng thì chúng tôi khuyên bạn sử dụng dịch vụ xác thực/verify (với chi phí khoảng 8 triệu VNĐ) của họ để tăng cường sự an toàn cho tài khoản của mình.

**3.1.11. Bị lộ vị trí địa lý của mình**

Đây có lẽ là điều không mong muốn của chung nhiều người, đặc biệt là các nhà báo, phóng viên điều tra.

Trong thời đại “điện thoại thông minh” hiện nay, có rất nhiều ứng dụng đòi hỏi, mời chào bạn bật tính năng định vị. Ví dụ: ứng dụng đặt xe. Hãy thận trọng, cân nhắc lợi-hại trước khi quyết định cho phép hay không cho phép tính năng này.

Khi bạn gọi điện, chat, trao đổi thư từ,… hãy cẩn thận với những thông tin (âm thanh, hình ảnh,… ) có thể làm lộ vị trí của bạn nếu bạn không muốn.

**3.1.12. Bị tấn công từ chối dịch vụ (DoS, DDoS)**

Điều này rất dễ xảy ra đối với các tòa soạn. Hậu quả là độc giả không thể truy cập được trang web của báo. Ngoài việc đầu tư nâng cấp trang thiết bị, các tòa soạn cần tổ chức các lớp tập huấn bắt buộc về an ninh mạng cho nhân viên của mình.

Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) là địa chỉ đáng tin cậy mà các tòa soạn cần liên hệ khi gặp sự cố máy tính, an ninh mạng mà mình không thể tự khắc phục.

Ngoài ra, bản thân từng nhà báo, phóng viên cần có ý thức bảo đảm ATS cho cá nhân mình, để không để mình trở thành công cụ (bot) cho những cuộc tấn công DDoS nhắm vào tòa soạn. Chúng tôi khuyến nghị các nhà báo, phóng viên tránh sử dụng những phần mềm lậu; hãy sử dụng những công cụ anti-virus của những doanh nghiệp có tiếng để góp phần giám sát sự ATS của bản thân. Ví dụ: BKAV, Kaspersky Lab, Norton,…

**3.1.13. Bị nhiễm các phần mềm độc hại. Bị hacker khai thác.**

Biểu hiện dễ nhận thấy nhất là thiết bị kỹ thuật số của bạn hoạt động bất thường; dữ liệu bị mất; đột nhiên xuất hiện ký tự lạ hoặc những chương trình quảng cáo;…

Ngoài các công cụ anti-virus như chúng tôi đã kể ra ở trên, còn một số lời khuyên của chuyên gia mà các nhà báo, phóng viên nên lưu ý:

- Sử dụng PGP/OpenPGP (Pretty Good Privacy) để trao đổi email, email của bạn sẽ được mã hóa, kẻ xấu khó đọc và lợi dụng được.

- Dùng các trình duyệt Safari, Opera, Chrome trên điện thoại thông minh.

- Không cài các Extensions vào trình duyệt.

- Không dùng chung một thiết bị kỹ thuật số chung cho mục đích giải trí và công việc.

- Dùng mạng riêng ảo (VPN) cho công việc.

- Không dùng Microsoft Office, hãy dùng Google Docs để xử lý, soạn thảo văn bản.

- Thiết lập các mức chia sẻ tài liệu (riêng tư, công khai).

- Mở các file ảnh bằng phần mềm Photoshop.

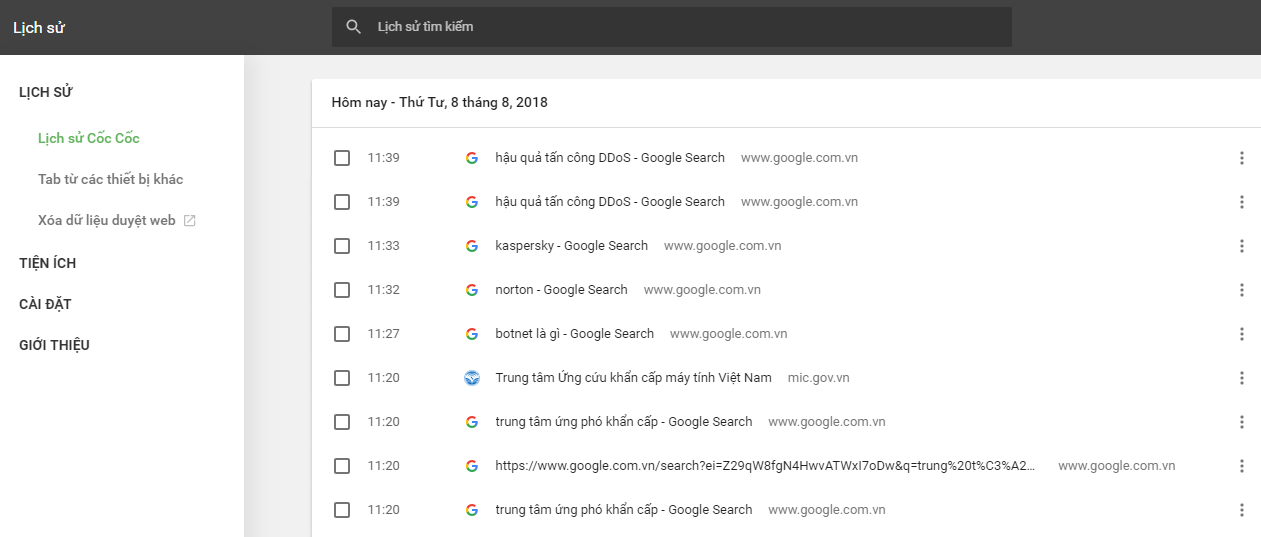
- Dùng Bitlocker, TrueCrypt, FileVault,… để mật mã hóa ổ cứng.

**3.2. Những lời khuyên bổ sung**

Ở phần 3.1, chúng tôi đã gửi tới các bạn một số khuyến nghị cho những trường hợp mất ATS cụ thể. Sau đây là những khuyến nghị bổ sung mà chúng tôi thấy có lợi ích cho nhà báo, phóng viên.

- Tránh ngồi quay lưng với cửa, cũng như chỗ ngồi khiến bạn dễ bị lộ thông tin trên màn hình.

- Nếu bạn sử dụng máy tính ở quán internet, máy tính dùng chung,… thì khi hết phiên làm việc hoặc có việc phải đi đâu đó, bạn hãy nhớ đăng xuất mọi tài khoản của mình, xóa mọi dữ liệu duyệt web của mình.



*Hãy xóa dữ liệu duyệt web*

- Tránh ẩm, hãy giữ khô ráo cho máy tính, điện thoại.

- Hãy thường xuyên xóa lịch sử cuộc gọi, tin nhắn nếu không dùng để tránh quá tải, nhầm lẫn hoặc bị lộ.

- Hãy tắt điện thoại, để điện thoại ngoài phòng, tháo pin điện thoại nếu có thể khi bạn dự một cuộc họp quan trọng, cần độ bảo mật cao.

- Dùng phần mềm mật mã hóa dữ liệu, thông tin,…

**3.3. Những địa chỉ hỗ trợ**

**3.3.1. Những chuyên gia công nghệ thông tin, chuyên gia báo chí**

**3.3.2. Những cơ quan, đơn vị**

- Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT)

**Địa chỉ liên hệ:**

***• Trụ sở chính:***  
- Địa chỉ: Tầng 5 - Tòa nhà Cục Tần số Vô tuyến điện - 115 Trần Duy Hưng - Phường Trung Hoà - Quận Cầu Giấy - TP. Hà Nội.  
- Email: vncert@mic.gov.vn / office@vncert.vn  
- Website: http://www.vncert.gov.vn  
- Điện thoại: 024.6404423

***• Chi nhánh tại Miền Trung:***  
- Địa chỉ: Tầng 3, số 42 đường Trần Quốc Toản, quận Hải Châu, thành phố Đà Nẵng  
- Điện thoại: 0236.3843228

***• Chi nhánh tại Miền Nam:***  
- Địa chỉ: 27 Nguyễn Bỉnh Khiêm, phường Đa Kao, Quận 1, TP Hồ Chí Minh.  
- Điện thoại: 028.39104925

- Trung tâm Tư vấn và Hỗ trợ nghiệp vụ an toàn thông tin, Cục An toàn thông tin, Bộ Thông tin và Truyền thông.

Điện thoại: +84 2432096789

Fax: +84 2439436684

Email: vanthucattt@mic.gov.vn

Máy lẻ: 819, 820, 821

- Hội Nhà báo Việt Nam

Địa chỉ: 59 Lý Thái Tổ - Hoàn kiếm - Hà Nội  
Tel: (84 - 4) 3825 3608 ; Fax: (84 - 4) 382 50797  
Website: [www.vja.org.vn](http://vja.org.vn/)  -  [www.hoinhabaovietnam.org.vn](http://www.hoinhabaovietnam.org.vn/)  
Email: [admin@vja.org.vn](mailto:admin@vja.org.vn)

**IV. KẾT LUẬN**

Công nghệ điện tử, công nghệ thông tin vừa là một cuộc cách mạng của nhân loại, vừa đặt ra nhiều thách thức về an toàn dữ liệu, an toàn thông tin đối với người sử dụng. Vấn đề ATTNBC trong môi trường số càng trở nên quan trọng đối với các nhà báo, phóng viên vì 2 lý do:   
a) Trong thời đại báo chí đa phương tiện, đặc biệt là báo chí điện tử thì dữ liệu, thông tin số vừa là tư liệu, vừa là sản phẩm, tài sản chủ yếu của báo chí;   
b) Ngành báo chí không thuộc lĩnh vực khoa học - công nghệ cho nên kiến thức, kỹ năng về an toàn số của nhà báo, phóng viên còn nhiều hạn chế.

Trong khi trên thế giới đã có rất nhiều tổ chức, trường đào tạo báo chí, các tổ chức xã hội về báo chí nghiên cứu sâu và có chương trình, hành động cụ thể để tăng cường an toàn tác nghiệp báo chí (UNESCO, SEAPA, Dart Center,…), thì ở Việt Nam câu chuyện an toàn tác nghiệp báo chí vẫn chưa được đặt ra một cách toàn diện.  
  
Là một tổ chức trực thuộc Liên hiệp các hội khoa học và kỹ thuật Việt Nam (VUSTA), chúng tôi đã có nhiều năm hoạt động trong lĩnh vực báo chí, truyền thông phát triển và đã xây dựng và điều phối mạng lưới Bảo vệ An toàn tác nghiệp cho nhà báo. Chúng tôi xây dựng Sổ tay này với hai mục tiêu chính:

1) Nâng cao nhận thức của nhà báo, phóng viên Việt Nam về tầm quan trọng của việc tăng cường an toàn tác nghiệp báo chí trong môi trường số;   
2) Trang bị những kiến thức, kỹ năng cơ bản góp phần tăng cường an toàn tác nghiệp báo chí trong môi trường số cho nhà báo, phóng viên Việt Nam;

Chúng tôi trân trọng cảm ơn các quý chuyên gia đã góp ý, các quý độc giả đã theo dõi Sổ tay này. Chúng tôi kêu gọi và hoan nghênh quý vị chung tay vì một nền báo chí Việt Nam an toàn.