VĂN PHÒNG UBND TỈNH
TRUNG TÂM PHỤC VỤ HÀNH CHÍNH CÔNG

SỔ TAY

HƯỚNG DẪN ĐẢM BẢO AN TOÀN THÔNG TIN TẠI VĂN PHÒNG ỦY BAN NHÂN DÂN TỈNH

(Tài liệu nội bộ)

Các văn bản quy phạm pháp luật chính quy định về bảo đảm an toàn thông tin theo cấp độ gồm:

a) ***Luật An toàn thông tin mạng*** số 86/2015/QH13 do Quốc hội Việt Nam

khóa 13 ban hành ngày 19/11/2015, có hiệu lực thi hành từ ngày 01/7/2016 (sau đây gọi tắt là Luật An toàn thông tin mạng):

Luật An toàn thông tin mạng quy định một số nội dung cơ bản về bảo đảm an toàn hệ thống thông tin theo cấp độ tại Mục 3. Bảo vệ hệ thống thông tin thuộc Chương II. Bảo đảm an toàn thông tin mạng, gồm 7 Điều, cụ thể: (1) Điều 21 quy định về việc phân loại cấp độ an toàn hệ thống thông tin; (2) Điều 22 quy định các nhiệm vụ bảo vệ hệ thống thông tin; (3) Điều 23 quy định về các biện pháp bảo vệ hệ thống thông tin; (4) Điều 24 quy định về giám sát an toàn hệ thống thông tin; (5) Điều 25 quy định trách nhiệm của chủ quản hệ thống thông tin; (6) Điều 26 quy định về hệ thống thông tin quan trọng quốc gia; (7) Điều 27 quy định về trách nhiệm bảo đảm an toàn thông tin mạng cho hệ thống thông tin quan trọng quốc gia.

b) ***Nghị định số 85/2016/NĐ-CP*** ngày 01/7/2016 của Chính phủ về bảo đảm an toàn thông tin theo cấp độ, có hiệu lực thi hành từ ngày 01/7/2016 (sau đây gọi tắt là Nghị định số 85/2016/NĐ-CP):

Nghị định này quy định chi tiết về tiêu chí, thẩm quyền, trình tự, thủ tục xác định cấp độ an toàn hệ thống thông tin và trách nhiệm bảo đảm an toàn hệ thống thông tin theo từng cấp độ. Căn cứ các quy định tại Nghị định, các cơ quan, tổ chức thuộc đối tượng áp dụng tại Điều 2 Nghị định phải thực hiện quy trình, thủ tục xác định cấp độ và phương án bảo đảm an toàn thông tin cho các hệ thống thông tin do mình quản lý. Trên cơ sở đó, căn cứ vào các quy định về quyền và trách nhiệm bảo đảm an toàn thông tin theo cấp độ tương ứng, chủ quản hệ thống thông tin và đơn vị vận hành hệ thống thông tin sẽ triển khai các biện pháp về quản lý và kỹ thuật phù hợp để thực thi công tác bảo đảm an toàn thông tin.

c) ***Thông tư số 12/2022/TT-BTTTT*** ngày 12/8/2022 quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ, có hiệu lực thi hành từ ngày 01/10/2022 (sau đây gọi tắt là Thông tư số 12/2022/TT-BTTTT).

d) ***Thông tư 31/2017/TT-BTTTT*** ngày 15/11/2017 quy định về hoạt động giám sát an toàn hệ thống thông tin.

e) ***Chỉ thị 14/CT-TTg*** ngày 25/5/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại.

f) ***Chỉ thị 14/CT-TTg*** ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam.

2.2. Tiêu chuẩn, quy chuẩn kỹ thuật

Hệ thống tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn hệ thống thông tin theo cấp độ hiện chỉ có duy nhất *Tiêu chuẩn quốc gia TCVN 11930:2017* về Công nghệ thông tin - Các kĩ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ (sau đây gọi tắt là Tiêu chuẩn quốc gia TCVN 11930:2017), trong đó:

- Tiêu chuẩn này quy định các yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ, bao gồm hai nhóm yêu cầu quản lý và yêu cầu kỹ thuật. Nhóm các yêu cầu quản lý là cơ sở để cơ quan, tổ chức xây dựng chính sách, quy trình quản lý an toàn thông tin cho hệ thống thông tin của mình trong quá trình thiết kế, xây dựng, vận hành, khai thác và sử dụng. Nhóm yêu cầu kỹ thuật là cơ sở để cơ quan, tổ chức thiết kế, thiết lập cấu hình hệ thống trong quá trình xây dựng hệ thống thông tin;

Phạm vi đối tượng áp dụng quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ

Căn cứ quy định tại Điều 2 Nghị định số 85/2016/NĐ-CP, việc triển khai các nhiệm vụ bảo đảm an toàn hệ thống thông tin theo cấp độ đối với các hệ thống thông tin là bắt buộc đối với:

(1) Các cơ quan, tổ chức nhà nước gồm các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương, các doanh nghiệp nhà nước theo quy định tại khoản 11 Điều 4 Luật Doanh nghiệp 2020 và các cơ quan, tổ chức nhà nước khác;

(2) Các cơ quan, doanh nghiệp, cán nhân, tổ chức khác (như ngân hàng, tổ chức tài chính, doanh nghiệp tư nhân…) có triển khai các ứng dụng công nghệ thông tin cung cấp dịch vụ trực tuyến phục vụ người dân và doanh nghiệp.

(3) *Đối với các hệ thống thông tin khác, không thuộc phạm vi nêu trên:* Khuyến khích các cơ quan, tổ chức triển khai áp dụng để bảo vệ các hệ thống thông tin do mình xây dựng, quản lý, vận hành.

Trách nhiệm quản lý nhà nước

Từ ngày 01/3/2025, Bộ Công an tiếp nhận chức năng, nhiệm vụ quản lý nhà nước về an toàn thông tin mạng từ Bộ Thông tin và Truyền thông. Căn cứ Nghị quyết số 190/2025/QH15 của Quốc hội, hiện nay, Bộ Công an là cơ quan chủ trì, phối hợp Bộ Quốc phòng thẩm định hồ sơ đề xuất cấp độ an toàn thông tin cấp độ 4, 5 (trừ các hệ thống do Bộ Quốc phòng quản lý).

Thực hiện chỉ đạo của Ban Chỉ đạo về tổng kết thực hiện Nghị quyết số 18NQ/TW của Chính phủ tại văn bản số 05/CV-BCDDTKNQ18 ngày 12/01/2025 về việc bổ sung, hoàn thiện phương án sắp xếp tổ chức các cơ quan chuyên môn thuộc Ủy ban nhân dân cấp tỉnh, cấp huyện, Công an các tỉnh, thành phố trực thuộc trung ương (sau đây gọi là Công an tỉnh) tiếp nhận nhiệm

vụ quản lý nhà nước về an toàn thông tin mạng từ Sở Thông tin và Truyền thông. Theo đó, Công an tỉnh sẽ là cơ quan chuyên trách về an toàn thông tin mạng của các tỉnh, thành phố trực thuộc trung ương, thực hiện thẩm định đối với hồ sơ đề xuất cấp độ 1, 2, 3.

Kinh phí bảo đảm an toàn hệ thống thông tin theo cấp độ

Theo quy định tại Điều 24 Nghị định số 85/2016/NĐ-CP, kinh phí thực hiện yêu cầu về an toàn thông tin theo cấp độ trong hoạt động của cơ quan, tổ chức nhà nước do Ngân sách nhà nước bảo đảm. Do đó, có thể xem xét sử dụng Ngân sách nhà nước để chi cho các hoạt động bảo đảm an toàn hệ thống thông tin theo cấp độ. Việc sử dụng kinh phí phải tuân thủ các quy định của pháp luật về ngân sách và các quy định có liên quan.

Cụ thể: Bộ Tài chính có trách nhiệm hướng dẫn Mục chi cho công tác bảo đảm an toàn thông tin trong dự toán ngân sách, hướng dẫn quản lý và sử dụng kinh phí sự nghiệp chi cho công tác bảo đảm an toàn thông tin trong hoạt động của các cơ quan, tổ chức nhà nước. Đối với nhiệm vụ này, Bộ Tài chính đã ban hành Thông tư số 121/2018/TT-BTC ngày 12/12/2018 quy định về lập dự toán, quản lý, sử dụng và quyết toán kinh phí để thực hiện công tác ứng cứu sự cố, bảo đảm an toàn thông tin mạng, trong đó các nội dung chi và mức chi được quy định cụ thể tại Điều 5 và Điều 6 của Thông tư;

(1) Kinh phí đầu tư cho an toàn thông tin sử dụng vốn đầu tư công thực hiện theo quy định của Luật Đầu tư công. Đối với dự án đầu tư công để xây dựng mới hoặc mở rộng, nâng cấp hệ thống thông tin, kinh phí đầu tư cho an toàn thông tin theo cấp độ được bố trí trong vốn đầu tư của dự án tương ứng;

(2) Kinh phí thực hiện giám sát, đánh giá, quản lý rủi ro an toàn thông tin; đào tạo ngắn hạn, tuyên truyền, phổ biến nâng cao nhận thức, diễn tập an toàn thông tin và ứng cứu sự cố của cơ quan, tổ chức nhà nước được cân đối bố trí trong dự toán ngân sách hàng năm của cơ quan, tổ chức nhà nước đó theo phân cấp của Luật Ngân sách nhà nước;

(3) Bộ Tài chính có trách nhiệm hướng dẫn Mục chi cho công tác bảo đảm an toàn thông tin trong dự toán ngân sách, hướng dẫn quản lý và sử dụng kinh phí sự nghiệp chi cho công tác bảo đảm an toàn thông tin trong hoạt động của các cơ quan, tổ chức nhà nước. Đối với nhiệm vụ này, Bộ Tài chính đã ban hành Thông tư số 121/2018/TT-BTC ngày 12/12/2018 quy định về lập dự toán, quản lý, sử dụng và quyết toán kinh phí để thực hiện công tác ứng cứu sự cố, bảo đảm an toàn thông tin mạng, trong đó các nội dung và mức chi được quy định cụ thể tại Điều 5 và Điều 6 của Thông tư;

(4) Căn cứ nhiệm vụ được giao, cơ quan, tổ chức nhà nước thực hiện lập dự toán, quản lý, sử dụng và quyết toán kinh phí thực hiện nhiệm vụ bảo đảm an toàn thông tin theo quy định của Luật Ngân sách nhà nước;

(5) Tỷ lệ kinh phí chi cho hoạt động bảo đảm an toàn thông tin:

- Tại Chỉ thị số 14/CT-TTg năm 2019, Thủ tướng Chính phủ chỉ đạo: *"e) Bảo đảm tỷ lệ kinh phí chi cho các sản phẩm, dịch vụ an toàn thông tin mạng đạt* ***tối thiểu 10% trong tổng kinh phí triển khai kế hoạch ứng dụng công nghệ thông tin hàng năm, giai đoạn 5 năm và các dự án công nghệ thông tin*** *(trong trường hợp chủ đầu tư chưa có hệ thống kỹ thuật hoặc thuê dịch vụ bảo đảm an toàn thông tin mạng chuyên biệt đáp ứng được các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ);"*;

- Tại Chiến lược an toàn, an ninh mạng quốc gia, Thủ tướng Chính phủ tiếp

tục chỉ đạo về đầu tư nguồn lực và bảo đảm kinh phí thực hiện: *"đ) Bố trí kinh phí chi cho an toàn, an ninh mạng đạt* ***tối thiểu 10% kinh phí chi cho khoa học công nghệ, chuyển đổi số, ứng dụng công nghệ thông tin.****"*.

1. Sử dụng tài khoản và mật khẩu

Tài khoản và mật khẩu là yêu cầu bắt buộc đối với bất kỳ người sử dụng nào khi truy cập và sử dụng tài nguyên trên mạng Internet để làm việc và trao đổi thông tin một cách định danh.

Nguy cơ – hiểm họa

- Nguy cơ bị mất tài khoản là rất lớn nếu bạn không biết cách quản trị. Người dùng quên mật khẩu khiến tài khoản bị khóa, không thể sử dụng trong công việc.

- Nguy cơ bị mất tài khoản thư điện tử, tài khoản trong công việc (hệ thống văn bản, chữ ký số, đăng nhập phần mềm,…) hoặc tài khoản mạng xã hội, tài khoản ngân hàng,…

Biện pháp đề phòng

- Không được lưu mật khẩu trên bất kỳ trình duyệt web nào

- Phải có phương thức quản lý tài khoản và mật khẩu của riêng mình (ghi chép ám hiệu, lưu trữ theo phương thức bảo mật,…) Đặt mật khẩu mạnh:

+ Ít nhất 08 ký tự

+ Bao gồm chữ hoa, chữ thường, số, ký tự đặc biệt (!@#$%^&*...)

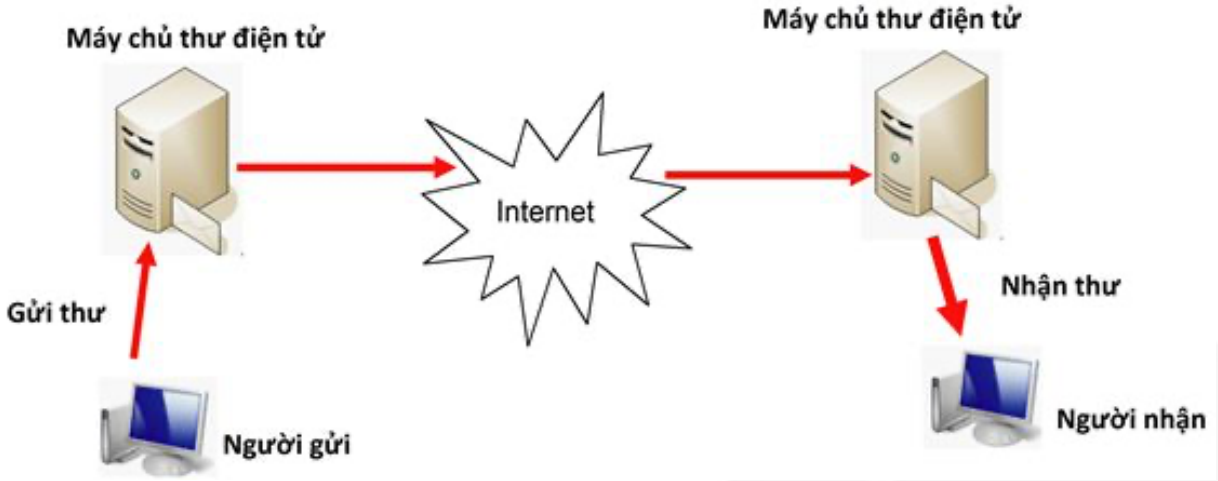
+ Đổi mật khẩu mỗi 06 tháng/ lần, mật khẩu mới không trùng mật khẩu cũ đã đặt trước đó

+ Mật khẩu không chứa thông tin cá nhân như tên, ngày tháng năm sinh, những ký tự đơn giản dễ đoán,…

+ Thường xuyên thay đổi mật khẩu theo cách riêng của từng người (theo quy luật riêng mà dễ gợi nhớ nhưng lại khó đoán)

2. Sử dụng Thư điện tử

Thư điện tử là một phương tiện gửi nhận văn bản thông dụng và tiện lợi. Không có giới hạn về địa lý, thư điện tử giúp con người nhận thông tin của nhau nhanh chóng, gần như là tức thì.



Nguy cơ – hiểm họa

- Nguy cơ bạn thường xuyên gặp phải là tình trạng thư rác. Thư rác làm ngắt quãng công việc, gây mất thời gian, tốn dung lượng lưu trưc của hệ thống email.

- Thư rác tiềm ẩn nguy cơ mất an toàn khi có những đường link không đáng tin cậy, những lời mời chào hay là quà tặng khi tham gia. Phía sau đó là những mã độc tấn công hệ thống mạng.

- Một số thư mang tính chất giả mạo dịch vụ, lừa đảo người sử dụng cung cấp thông tin bảo mật, kèm theo đó là các virus khi click vào các đường link hay tải văn bản về.

Biện pháp đề phòng

- Sử dụng hệ thống thư điện tử công vụ tỉnh Gia Lai trong trao đổi công việc yêu cầu đảm bảo an toàn bảo mật. Hệ thống thư điện tử công vụ hoàn toàn đảm bảo khả năng gửi nhận thông thường, đặc biệt đảm bảo tính an toàn bảo mật cho các thao tác gửi nhận và đính kèm file văn bản.

- Hạn chế sử dụng hệ thống thư điện tử miễn phí, lưu ý khi khai báo thông tin đăng ký sử dụng. Nếu phải sử dụng thư điện tử với tần suất cao hãy chọn những nhà cung cấp uy tín lâu năm (Gmail, Microsoft ,…).

- Xác định thư điện tử khi gửi nhận, định danh đúng người khi trao đổi công việc. Thường các đối tượng xấu lợi dụng việc hiển thị tên email dễ gần, quen thuộc để đánh lừa người dùng.

- Hãy đọc kỹ nội dung các email gửi đến, không click hay tải bất kỳ nội dung gì mà không biết hoặc nghi ngờ.

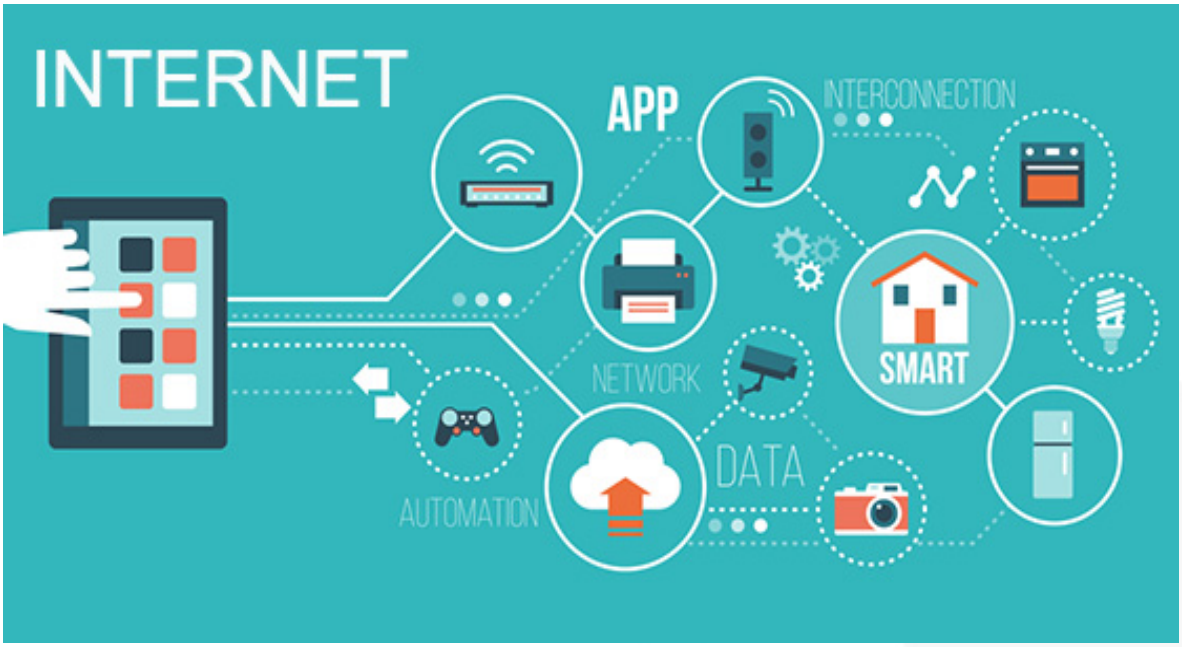
- Đặt mật khẩu mạnh và không lưu mật khẩu khi đăng nhập khi sử dụng trình duyệt web.

- Cài phần mềm diệt virus có bản quyền. Phần mềm diệt virus sẽ có tính năng quét các truy cập, các file được tải về và khi mở thư điện tử.

- Ngắt kết nối mạng và liên hệ bộ phận kỹ thuật để khắc phục nếu nghi ngờ bị tấn công qua kết nối thư điện tử.

3. Sử dụng mạng Internet

Truy cập mạng Internet là yêu cầu tất yếu trong thời đại công nghệ hiện nay. Các công việc phải giải quyết qua hệ thống mạng như thư điện tử, hệ thống quản lý văn bản, đến các ứng dụng chat – trao đổi công việc, hay gọi điện video call, hội nghị trực tuyến,…



Nguy cơ – hiểm họa

- Mạng Internet mang lại nhiều lợi ích song cũng nhiều mối nguy hiểm. Sử dụng thường xuyên trình duyệt mạng sẽ dễ bị lây nhiễm mã độc bởi thao tác quá nhiều trên các trang mạng online.

- Nguy cơ bị lừa đảo, khai thác thông tin cá nhân và các tin tức không đúng sự thật. Điều này gây ảnh hưởng tâm lý, gây hoang mang lo sợ cho chính người sử dụng.

- Qua các lỗ hổng đó, hệ thống có thể bị nghe lén, bị thu thập thông tin dữ liệu người dùng, bị đòi tiền chuộc và mã hóa dữ liệu mà không hề biết.

Biện pháp đề phòng

- Cập nhật hệ điều hành thường xuyên, sử dụng hệ điều hành và các phần mềm có bản quyền và đáng tin cậy.

- Cài đặt các phần mềm diệt virus, phần mềm chống cắm usb,….

- Khi đăng nhập trên trình duyệt không lưu mật khẩu, không cung cấp thông tin cho bên thứ 3, không cung cấp mật khẩu các hệ thống công vụ cho cá nhân khác sử dụng, đặc biệt không chia sẻ thông tin cá nhân lên mạng internet.

-Không cài phần mềm lạ, các toolbar, banner quảng cáo trên trình duyệt web. Chọn chế độ lướt web ở nơi truy cập công cộng.

4. Sử dụng mạng Wifi

Mạng không dây (wifi) ngày nay là hệ thống mạng tiện lợi và tốc độ truy cập khá cao, đảm bao môi trường làm việc qua mạng tại bất kỳ nơi đâu.

Nguy cơ – hiểm họa

- Do mạng không dây được kết nối dễ dàng vì vậy nếu không quản trị tốt, không phụ thuộc vào vị trí vật lý, vì vậy nguy cơ bị truy cập trái phép là rất cao.

- Khi đã đánh cắp được mật khẩu hoặc đã tấn công được vào mạng, hacker sẽ đứng trong mạng nội bộ, có thể tấn công các hệ thống mạng hoặc máy chủ.

Biện pháp đề phòng

- Thiết lập an toàn bảo mật cho thiết bị mạng không dây (WPA2; WPA2-AES, vì nó an toàn hơn WPA/TKIP) sẽ gây khó khăn cho việc chặn bắt dữ liệu hay các truy cập trái phép. Nên sử dụng giới hạn thiết bị đầu cuối truy cập *(ví dụ như sử dụng địa chỉ lọc MAC)* để định danh các thiết bị truy cập vào mạng.

- Hạn chế sử dụng mạng wifi tại nơi công cộng để truy cập vào các ứng dụng, tài khoản nạp rút tiền, tài khoản email, tài khoản ngân hàng,…. nhằm hạn chế tối đa khả năng bị tấn công.

- Sử dụng mật khẩu khó đoán, bao gồm các quy định bảo mật (chữ hoa, chữ thường, số, ký tự đặc biệt) và thường xuyên thay đổi mật khẩu theo định kỳ.

- Nếu phải sử dụng các phương thức thanh toán hoặc các công việc đòi hỏi bảo mật cao, hãy ưu tiên sử dụng 4G hoặc 5G

5. Sử dụng mạng xã hội

Mạng xã hội hiện nay khá phát triển và mang lại lợi ích to lớn cho người sử dụng.

Mạng xã hội giúp tăng cường trao đổi thông tin tri thức bao gồm cả trực tuyến và ngoại tuyến. Khi tham gia mạng xã hội bạn như đang tham gia một xã hội ảo trên mạng Internet với hàng triệu người với nhiều thông tin cả 2 chiều tốt và xấu.

Nguy cơ – hiểm họa

- Mạng xã hội tiềm ẩn rất nhiều vấn đề liên quan đến cá nhân. Khi đã tham gia mạng xã hội, bạn sẽ là một thành viên trong cộng đồng đó, các mỗi quan hệ bạn bè, các thông tin cá nhân (ảnh, videos,…) sẽ có thể không được kiểm soát. Điều này sẽ gây nguy cơ lộ lọt thông tin cho những kẻ muôn sử dụng nó vào mục đích xấu.

- Các hình thức thường thấy là nhờ mối quan hệ để lừa đảo, mượn tiền, cho vay nặng lãi, nạp thẻ điện thoại, thu thập thông tin nhạy cảm nhằm theo dõi, tống tiền, hay thậm chí bắt cóc.

Biện pháp đề phòng

- Bạn cần phải biết quản trị thông tin của chính mình. Các thông tin cá nhân khi bạn cung cấp trên mạng xã hội cần được kiểm soát chặt chẽ, cố gắng hạn chế công khai các thông tin có tính riêng tư. Bạn phải nắm rõ mục đích sử dụng của mạng xã hội của bạn là gì ?

- Thiết lập cài đặt các đối tượng có thể xem được cập nhật của bạn. Thiết lập an toàn cho phép ai được xem các nội dung bạn đăng (bạn bè hay bất kỳ ai).

- Xác nhận danh tính khi chấp nhận kết bạn với ai hoặc khi tham gia nhóm nào?

- Không mở đường link có dấu hiệu bất thường, nhạy cảm, những người không quen biết.

- Không mở các tệp tin lạ có định dạng .rar, .zip, .pdf … từ những người không quen biết

6. Thiết lập máy tính cá nhân an toàn

Máy tính cá nhân là thiết bị không thể thiếu đối với hầu hết cán bộ, người lao động khi làm việc, thực hiện công việc cá nhân. Máy tính cá nhân lưu trữ rất nhiều dữ liệu quan trọng cả trông công việc và đời sống sinh hoạt hằng ngày.

Máy tính cá nhân ở đây bao gồm cả máy tính xách tay (laptop) và máy tính để bàn (desktop)

Nguy cơ – hiểm họa

- Máy tính là thiết bị dễ bị các hacker tấn công nhất. Máy tính thường phải cài đặt rất nhiều phần mềm để thực hiện tác tác vụ thông thường (soạn thảo, truy cập mạng, gửi email, mạng xã hội, các phần mềm khác,…) do đó tiềm ẩn rất nhiều nguy cơ bị tấn công qua các lỗ hổng bảo mật.

- Việc tấn công truy cập trái phép vào máy tính cá nhân có thể làm lộ thông tin cá nhân, các dữ liệu người dùng bị sao chép và mã hóa, các mật khẩu bị thu thập cho mục đích xấu.

- Tấn công máy tính cá nhân còn là bước trung gian để hacker từ đó truy cập vào các máy tính khác, thậm chí máy chủ vì đã chiếm quyền của máy tính đó.

Biện pháp đề phòng

- Thực hiện cài đặt hệ điều hành mới nhất, tùy theo yêu cầu ưu tiên cài đặt hệ điều hành bản quyền hoặc hệ điều hành nguồn mở. Nếu sử dụng hệ điều hành nguồn mở phải tìm hiểu rõ nguồn gốc, có kỹ năng sử dụng.

-Thường xuyên cập nhật bản vá lỗi hệ điều hành hàng tuần/hàng tháng.

- Bật hệ thống tường lửa lửa trên máy tính.

- Tạo mật khẩu mạnh cho tài khoản người dùng (bao gồm chữ hoa, chữ thường, số, ký tự đặc biệt) nhằm bảo vệ máy tính khi người lạ truy cập.

- Gỡ bỏ các phần mềm không cần thiết như các chương trình quảng cáo, các bản dùng thử phần mềm. Càng hạn chế cài đặt các phần mềm thì quản lý máy tính càng đơn giản hơn. Cài đặt phần mềm diệt virus, nên sử dụng phần mềm có bản quyền của các thương hiệu nổi tiếng (Kaspersky, BKAV…)

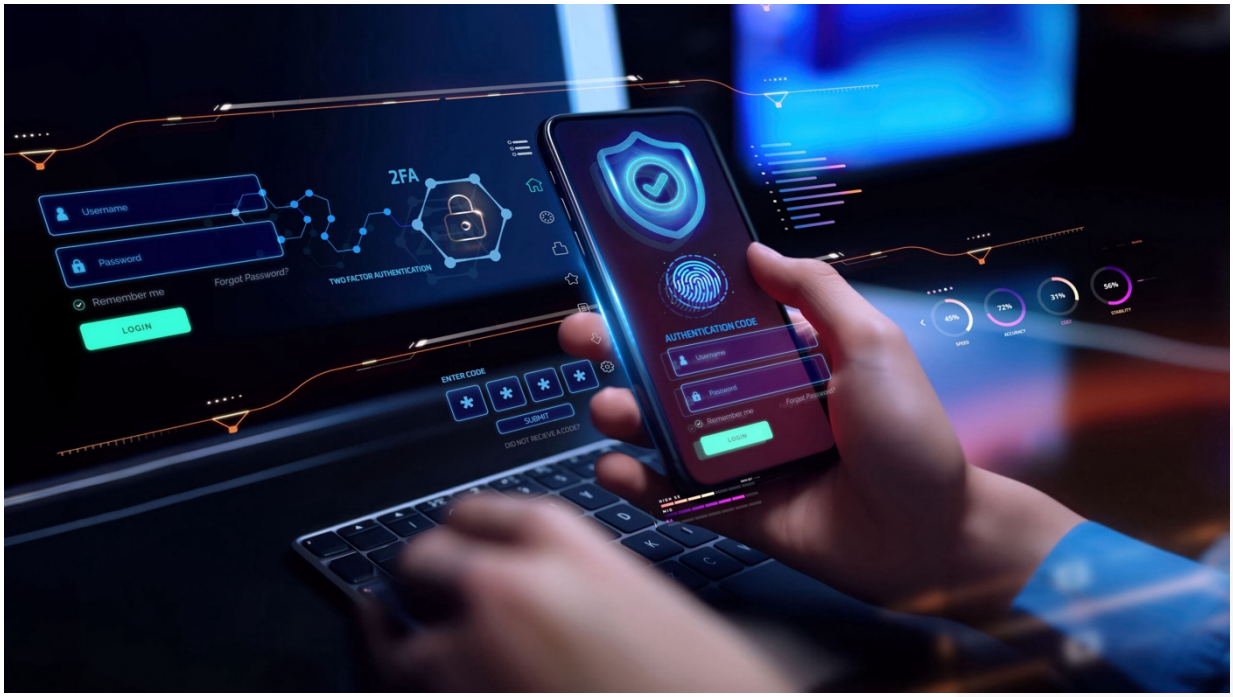
- Không sử dụng các phần mềm OTT gửi nhận dữ liệu công việc như Zalo, Viber, Facebook…

- Thận trọng khi truy cập Internet, không truy cập những trang mạng không chính thống, các đường link quảng cáo hoặc nhận phần thưởng hấp dẫn,…

- Không sử dụng các phần mềm crack *(hay còn gọi là phần mềm bẻ khóa)* các ứng dụng. Khi sử dụng sẽ gây nguy cơ chứa mã độc truy cập vào hệ thống máy tính đang sử dụng.

7. Sử dụng thiết bị di động (Mobile/Tablet)

Điện thoại di động / Máy tính bảng là thiết bị phổ biến và nhu cầu sử dụng ngày càng cao. Thiết bị di động cho phép người dùng truy cập Internet, tải về các phần mềm miễn phí/có phí để thực hiện các tác vụ tương tự như trên máy tính.



Nguy cơ – hiểm họa

- Các mã độc trên điện thoại ngày càng tăng mạnh và tinh vi khi bạn sử dụng thiết bị di động để truy cập mạng Internet.

- Khi tải các ứng dụng không có uy tín, bạn sẽ có nguy cơ lộ thông tin cá nhân đến máy chủ của hacker, yêu cầu bạn lựa chọn những thông tin như cho phép truy cập danh bạ, cho phép truy cập dữ liệu trên máy,…

- Nguy cơ bạn bị mất tài khoản thư điện tử, tài khoản ngân hàng, các tài khoản khác khi hacker đã có quyền truy cập thiết bị của bạn.

Biện pháp đề phòng

- Sử dụng thiết bị di động của nhà phân phối chính hãng phân phối ra thị trường, không nên sử dụng sản phẩm trôi nổi, giá rẻ.

- Thường xuyên cập nhật các phiên bản mới nhất có thể, tùy theo cấu hình của thiết bị di động.

- Quản lý dữ liệu trên thiết bị cá nhân một cách an toàn, có thể đặt mật khẩu dữ liệu. Đặc biệt lưu ý những thông tin địa chỉ, thông tin cá nhân và các dữ liệu nhạy cảm (ảnh, videos).

- Quản lý tốt tài khoản ngân hàng khi sử dụng phần mềm giao dịch trực tuyến qua thiết bị di động, phải sử dụng bảo mật bằng OTP đối với các giao dịch.

- Quản lý danh mục danh bạ người dùng, sao lưu danh bạ thường xuyên và copy sang máy tính cá nhân của mình.

- Trước khi tải phần mềm và cài đặt lên thiết bị di động phải kiểm tra kỹ đặc quyền mà phần mềm yêu cầu (chú ý các quyền cho phép sử dụng máy ảnh, ghi âm, thực hiện tự động kết nối Internet, truy cập danh bạ, truy cập dữ liệu,…)

- Thực hiện tắt wifi hoặc 4G, 5G khi không có nhu cầu sử dụng mạng Internet. Điều này làm giảm khả năng tấn công nếu thiết bị nhiễm mã độc bởi các hacker thu thập thông tin qua môi trường mạng Internet.

- Cập nhật các phiên bản mới của hệ điều hành thiết bị di động.

8. Sử dụng ổ cứng di động

Ổ cứng di động là thiết bị công nghệ để lưu trữ những dữ liệu quan trọng trong quá trình làm việc của cá nhân, thậm chí là cả đơn vị.

Ổ cứng di động thường được sử dụng để lưu trữ dữ liệu từ vài tháng đến hằng năm. Do đó trong ổ cứng có rất nhiều dữ liệu sau thời gian dài sử dụng.

Nguy cơ – hiểm họa

- Nguy cơ ổ cứng bị nhiễm virus và mã độc sau khi kết nối với một hoặc nhiều máy tính cá nhân.

- Nguy cơ nhiễm virus hoặc mã độc vào hệ thống mạng LAN rất lớn nếu không xử kịp thời.

- Nghiêm trọng hơn là việc mất dữ liệu trong ổ cứng, những dữ liệu đã tồn tại theo thời gian dài mà không hề hay biết.

Biện pháp đề phòng

- Sử dụng ổ cứng di động theo đúng mục đích, không kết nối với những máy tính đã nhiễm virus hoặc nghi ngờ nhiễm virus. Hạn chế tối đa việc sử dụng ổ cứng di động khi không cần thiết.

- Bắt buộc phải quét virus trước khi mở ổ cứng di động bằng phần mềm diệt virus tin cậy và có bản quyền, được cập nhật đầy đủ.

- Thực hiện định kỳ sao lưu dự phòng trên nhiều thiết bị khác nhau, chẳng hạn sử dụng 02 ổ cứng di động trong đó 01 ổ cứng làm nhiệm vụ backup, áp dụng các biện pháp an toàn như mã hóa, nén file,…

9.Lừa đảo qua mạng

Là một hình thức lừa gạt người dùng liên quan đến tiền bạc, danh dự khi truy cập mạng Internet hoặc sử dụng dịch vụ mà phải click chuột vào một biểu tượng, đường link hay video trên màn hình.

Nguy cơ – hiểm họa

- Đối tượng thường sử dụng các biểu tượng bắt mắt hoặc những nội dung gây trí tò mò cho người xem, các nội dung hấp dẫn tới từng đối tượng (mua sắm, giảm giá, trúng thưởng, tặng quà,…)

- Nếu click chuột vào các đường link hoặc biểu tượng thường xuất hiện các nội dung yêu cầu nhập thông tin cá nhân, các nội dung liên quan đến trả phí để nhận thưởng, giới thiệu bạn bè để nhận quà tặng,…

- Khi đó các thông tin cá nhân bị khai thác vào mục đích xấu, một số đối tượng sẽ đánh cắp tài khoản, tấn công ip, cài đặt virus và mã độc vào máy tính người dùng.

Biện pháp đề phòng

- Thường các hành vi của đối tượng xấu thường rất tinh vi và thủ đoạn, đầu tiên người dùng phải cảnh giác khi truy cập vào các trang web nghi ngờ.

- Cài đặt phần mềm diệt virus và thường xuyên cập nhật chương trình, cài đặt quét tự động.

10. Tấn công Email có chủ đích

Là việc tấn công bằng cách gửi tmail giả mạo như thể từ một cá nhân hoặc tổ chức quen biết. Email này chứa nội dung đơn giản, nhưng làm cho người dùng thấy quen thuộc gây mất cảnh giác. Đặc biệt email này chứa mã độc kèm theo, các tấn công này thường được ghi nhận với hành vi đánh cắp mật khẩu hoặc lây nhiễm virus vào máy tính nếu máy tính không được bảo vệ

Nguy cơ – hiểm họa

- Cách thức tấn công giả mạo qua email ngày càng phổ biến bởi mối quan hệ của người dùng ngày càng đa dạng. Các đối tượng thường sử dụng sau khi đã thu thập thông tin rõ ràng từ các mối quan hệ của người dùng, mạo danh các quan hệ quen biết để đưa ra các nội dung phù hợp, kèm theo đó là các đường link hoặc tệp đính kèm có mã độc.

- Nếu vô tình mở tệp hoặc đường link thì sẽ kết nối với máy chủ của hacker, tự động cho phép truy xuất vào máy tính cá nhân, các cổng bảo mật sẽ được mở, truy cập sẽ chạy ngầm mà người dùng không thể nhận ra.

Biện pháp đề phòng

- Cẩn trọng khi nhận bất kỳ email nào, kể cả quen biết (đặc biệt những mối quan hệ không thường xuyên, các cá nhân tổ chức quảng cáo,…

- Phải cài đặt phần mềm diệt virus, thường xuyên cập nhật hệ thống

- Sử dụng hệ thống email đáng tin cậy, bật các chế độ bảo vệ của windows

- Khi click vào biểu tượng đó thường sẽ mở ra một trang web khác yêu cầu nhập thông tin, thông tin thanh toán, hãy dừng lại và không phản hồi bất kỳ yêu cầu gì nếu nghi ngờ.

- Khi đã mở email nghi ngờ, hãy bình tĩnh và ngắt mạng và gọi điện quản trị mạng để được tư vấn và hỗ trợ kịp thời.

11. Cảnh báo phát hiện tin giả

Các thông tin trên mạng tràn lan và rất khó kiểm soát và phân biệt đúng sai. Tin giả sẽ gây tác hại xấu đặc biệt trong tình hình hiện nay (chính trị, xã hội,…). Nếu hiểu không rõ sẽ vi phạm pháp luật với hành vi của mình trên mạng xã hội.

Nguy cơ – hiểm họa

-Tin giả có nhiều mục đích, câu view, bán hàng, tuyên truyền. Thao tác trên mạng xã hội đơn giản, nhưng nguy cơ tiềm ẩn rất lớn.

- Người đăng thông tin sai sẽ phạt tiền 10-20 triệu đồng (Nghị định 15/2020 của Chính phủ). Tiết lộ thông tin bí mật Nhà nước sẽ bị truy cứu trách nhiệm hình sự.

Biện pháp đề phòng

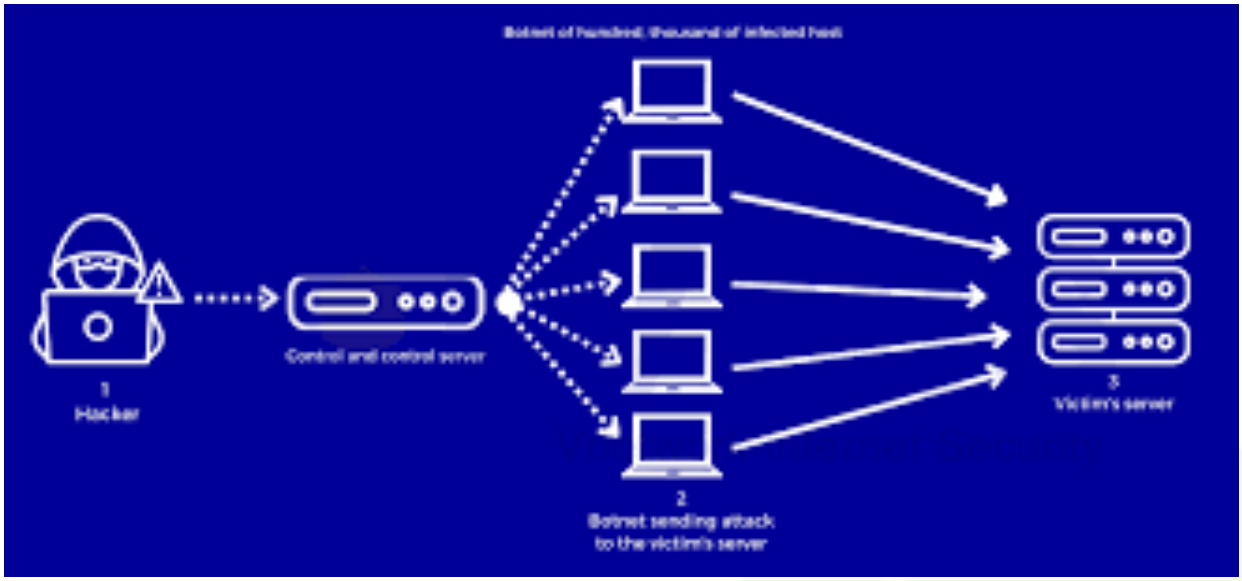
-Xem xét kỹ lưỡng thông tin liên quan, chính thống để đối chiếu, phật biệt rõ là tin thật hay nói đùa, trang web có được quản lý hay không. Tin giả thường có tiêu đề "nóng hổi", "giật gân", chủ đề đang "hot" trên xã hội

- Khi đọc tuyệt đối không chia sẻ bằng bất kỳ hình thức nào (share, chụp ảnh, copy) qua các mạng xã hội Facebook, Zalo, Youtube, TikTok…

- Kiểm tra mức độ tin cậy của trang web, đường dẫn, liên kết,…

12. Tấn công từ chối dịch vụ DDOS

Là kiểu tấn công từ chối dịch vụ phân tán (viết tắt của Distributed Denial of Service) nhằm làm cho người dùng không thể sử dụng tài nguyên của máy tính. Mục tiêu để làm hệ thống mạng không thể sử dụng, hoặc gián đoạn chậm đi đáng kể so với bình thường



Nguy cơ – hiểm họa

- Kẻ tấn công sẽ bí mật cài đặt mã động vào các máy tính, có thể là các máy tính không liên quan và sử dụng máy tính đó để tấn công vào mạng hoặc máy chủ đã định trước.

- Từ máy tính đó kẻ tấn công sẽ thực hiện các tấn công khác như phát tán virus, thay đổi trang web, gửi email rác,…

Biện pháp đề phòng

- Thường xuyên cập nhật phiên bản hệ điều hành mới nhất, cập nhật bản vá lỗi hệ điều hành.

- Cài đặt và thường xuyên cập nhật virus, cài đặt bản virus phù hợp với yêu cầu của hệ thống (bản dành cho client, bản dành cho máy chủ, bản dành cho mail,…).

- Thường xuyên kiểm tra và rà soát lại các ứng dụng trên các máy tính cá nhân và máy chủ trong mạng, gỡ bỏ các ứng dùng nghi ngờ và chạy ngầm (thông báo kỹ thuật hoặc chuyên gia để được hỗ trợ).

Một số lỗi thường gặp

Hướng dẫn sử lý sự cố cơ bản thường gặp trên máy tính, mạng nội bộ,…

1. Máy tính bật không lên

Dấu hiệu

Máy tính đã cắm nguồn nhưng bật không thấy lên tín hiệu, hoặc có lên tín hiệu nhưng không lên màn hình

Khắc phục

Đây là lỗi vô cùng phổ biến khi sử dụng máy tính. Có rất nhiều nguyên nhân của vấn đề này

+ Kiểm tra tất cả dây nguồn của cả cây máy tính và cả màn hình. Nguyên nhân có thể do thiết thiết bị nguồn, dây bị lỏng hoặc cáp giữa máy tính và màn hình có vấn đề.

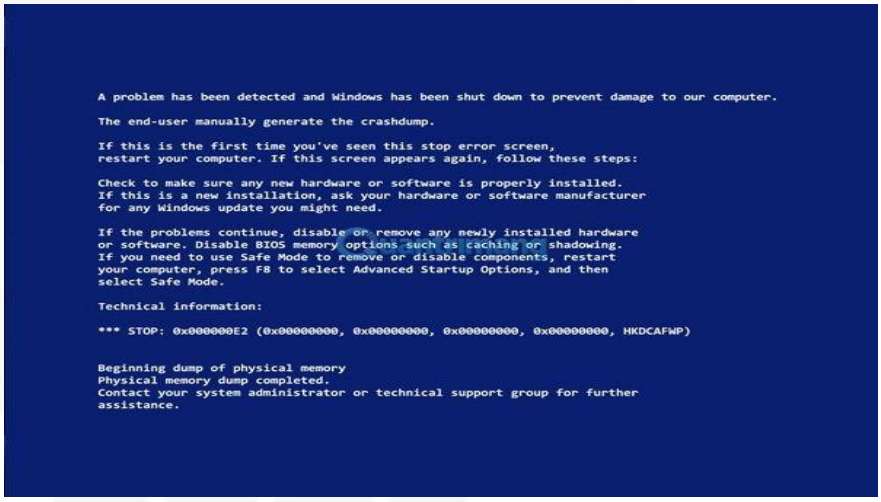
+ Kiểm tra và lưu ý khi bật máy tính có thể nút khởi động (nút power) trên máy tính bị trục trặc không nhạy.

+ Khi bật máy tính có những cảnh báo âm thanh tiếng "bip" báo máy tính hoạt động. Máy tính báo lỗi nếu tiếng "bíp" liên tục, đây là cảnh báo lỗi phần cứng của máy tính. Khi đó cần phải tháo máy tính để kiểm tra các kết nối như RAM, ổ cứng, cáp dữ liệu,…

2. Màn hình máy tính bị lỗi "màn hình xanh"

Dấu hiệu

Máy tính đang sử dụng bình thường bỗng hiện lên màn hình xanh mà không rõ nguyên nhân



Khắc phục

Có nhiều nguyên nhân của màn hình xanh xuất hiện, nhưng về cơ bản đây là lỗi thường thấy, và nguyên nhân là do phần cứng nhiều hơn là do phần mềm

+ Do lỗi hệ điều hành windows. Sau một quá trình sử dụng hệ điều hành, cài đặt nhiều chương trình phần mềm, không thường xuyên cập nhật hệ điều hành, các ứng dụng,… máy tính thường bị lỗi. Có rất nhiều nguyên nhân phát sinh lỗi khó có thể giải thích, như do virus, do xung đột giữa các phần mềm, lỗi cài đặt không tương thích, lỗi bản quyền,…Khi đó chúng ta khắc phục bằng cách: Gỡ bỏ các phần mềm không cần thiết, các phần mềm nghi ngờ là gặp lỗi, xóa bỏ cá tệp rác bằng các phần mềm dọn rác và file tạm để tối ưu hệ thống. Sử dụng đĩa cài đặt để repair để khắc phục Nếu đã làm mọi cách mà không được thì phải cài lại hệ điều hành trước khi bị lỗi nặng hơn.

+ Do lỗi phần cứng máy tính. Kiểm tra tất cả sự kết hợp giữa các phần cứng với nhau như màn hình, bàn phím, chuột, CPU, RAM, ổ cứng, card màn hình, …và các driver nhận diện chúng trong hệ điều hành. Lỗi phát sinh thường thấy là do vấn đề liên quan đến ổ cứng, RAM, các cáp kết nối. Cần phải thường xuyên kiểm tra và bảo dưỡng định kỳ thiết bị.

3. Lỗi ổ cứng

Dấu hiệu

Có nhiều đấu hiệu của lỗi ổ cứng như sau:

+ Xuất hiện lỗi “corrupted” khi truy cập dữ liệu

+ Lỗi không nhận ổ cứng

+ Lỗi xuất hiện tiếng kêu lạ

+ Máy tính liên tục bị treo và xuất hiện màn hình cảnh báo

Khắc phục

Ổ cứng là phần cứng được sử dụng nhiều nhất khi truy cập máy tính. Ổ cứng cũng là quan trọng nhất, chứa toàn bộ dữ liệu người dùng. Do đó cần thường xuyên kiểm tra ổ cứng để có biện pháp chủ động khi sự cố xảy ra

+ Thường xuyên kiểm tra ổ cứng bằng công cụ, một trong số đó là phần mềm CrystalDiskInfo để kiểm tra tình trạng ổ cứng

+ Hạn chế bật tắt đột ngột máy tính (ví dụ như rút nguồn đột ngột), phải sử dụng ổn áp để trách sốc thiết bị, đặc biệt là ổ cứng

+ Thường xuyên backup dữ liệu định kỳ (tùy theo dữ liệu thay đổi nhiều hay ít để có phương án cụ thể: 1 tuần/ 1 tháng/ 3 tháng/ 6 tháng). Có thể sử dụng ổ cứng cắm ngoài chuyên dụng, nén các file để giảm dung lượng và dễ quản lý.

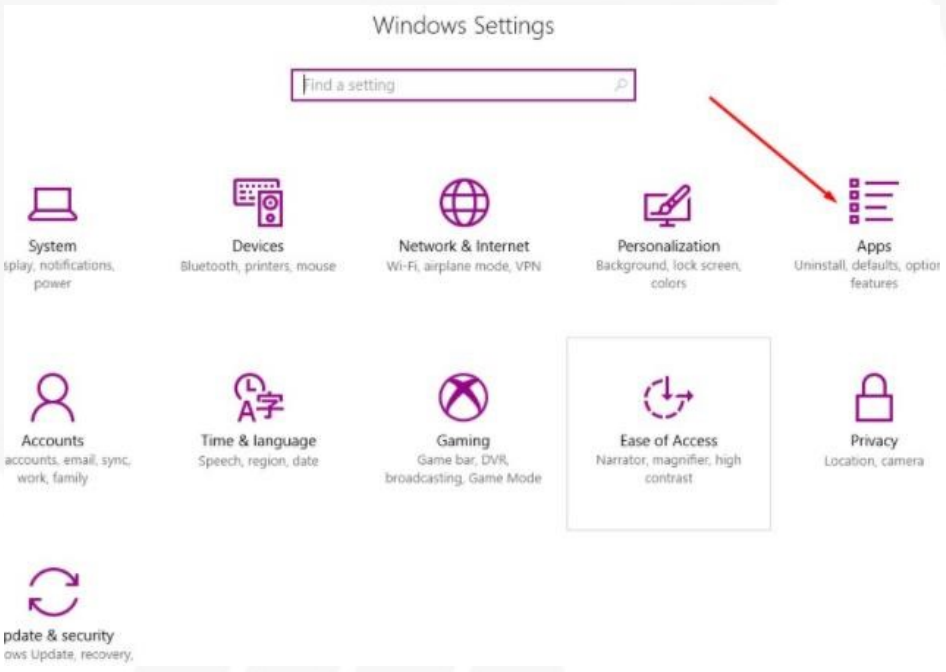
4. Gỡ bỏ ứng dụng

Dấu hiệu

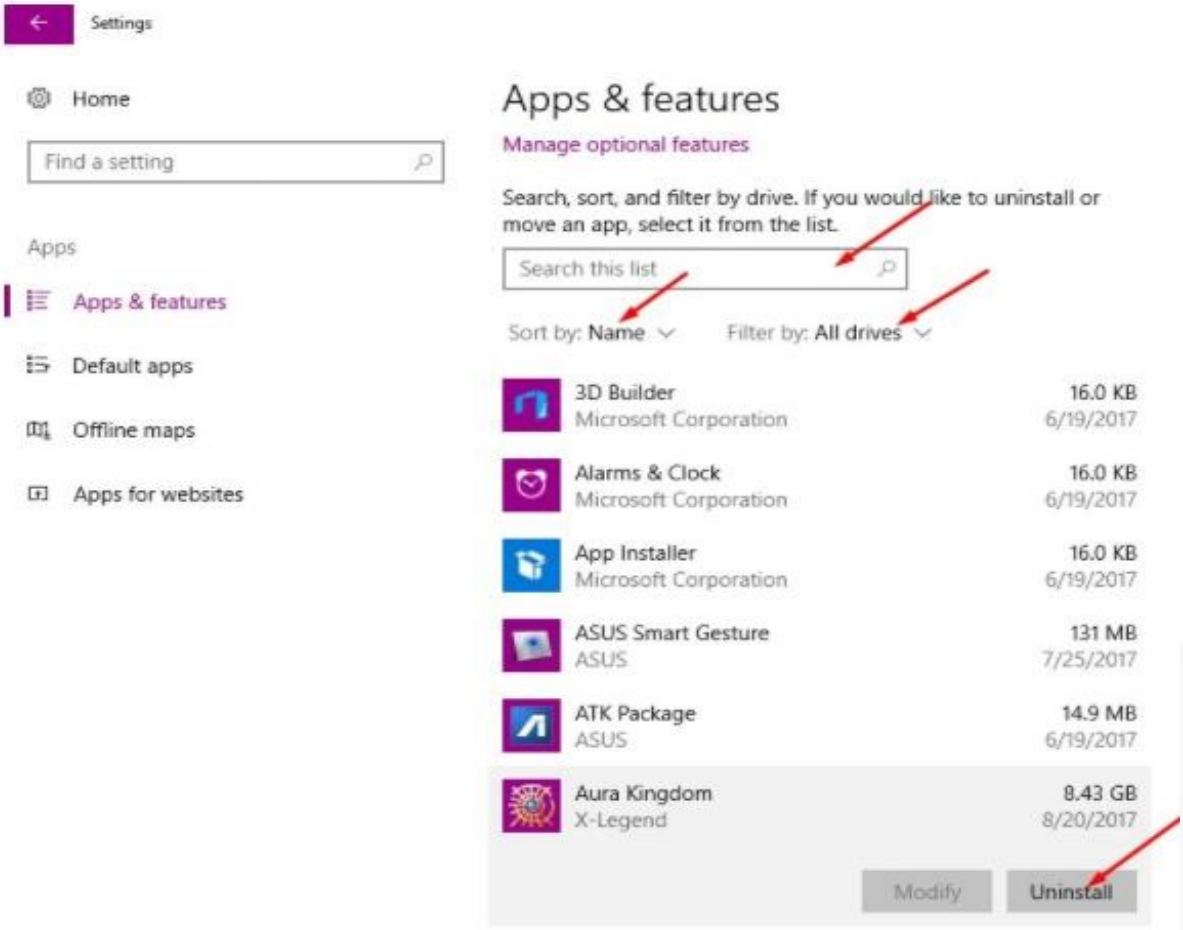
Để quản lý máy tính tốt nhất, chúng ta cần hạn chế cài đặt nhiều ứng dụng không cần thiết. Điều này gây tốn tài nguyên, làm chậm máy tính và tăng nguy cơ mất an toàn an ninh mạng

Khắc phục

Vào Setting >> Apps để **xóa ứng dụng**



Tiếp tục chọn những ứng dụng không cần thiết để gỡ bỏ **(Uninstall)**



5. Máy tính bị chậm/treo

Dấu hiệu

Dấu hiệu của lỗi này là máy tính bị treo/đơ, chuột quay liên tục và thao tác chậm.

Đây là nguyên nhân phổ biến làm người dùng khó chịu, khiến công việc bị ngừng trệ, gây mất thời gian và giảm hiệu quả công việc

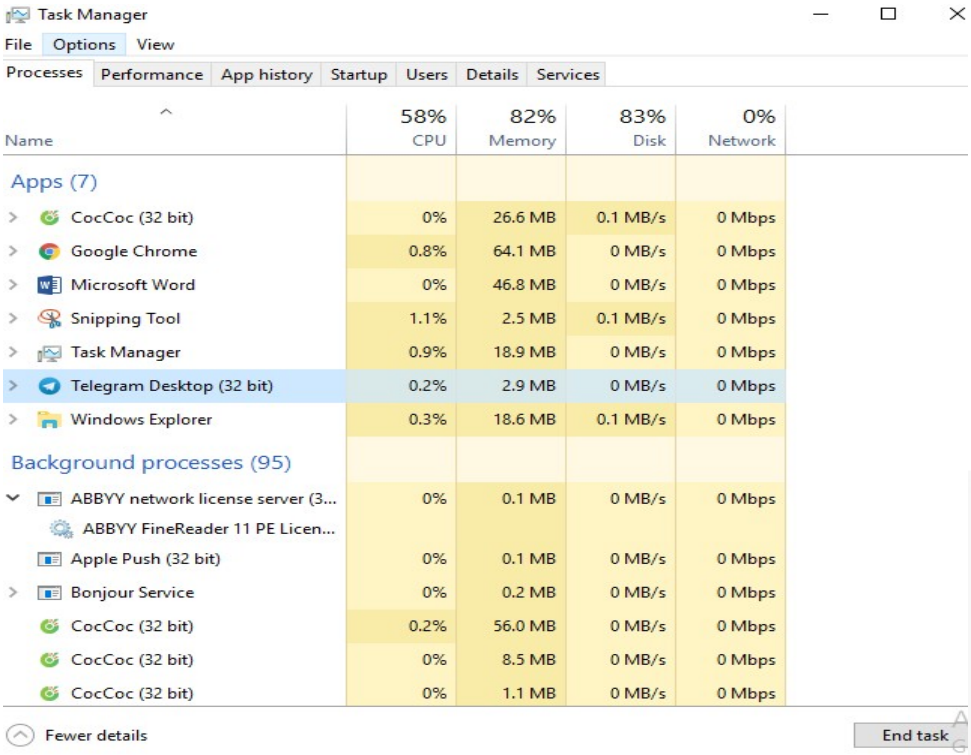
Khắc phục

Có nhiều nguyên nhân khiến máy tính bị chậm, treo

+ Máy tính bị nhiễm virus. Đây là lỗi thường xảy ra và cũng là một trong những dấu hiệu nhận biết máy tính đang có khả năng bị nhiễm virus. Để khắc phục cần phải diệt virus bằng phần mềm chuyên dụng như AVG antivirus, Kaspersky antivirus,…

+ Do phần mềm máy tính xảy ra. Nguyên nhân có thể xuất phát từ phần mềm nào đó quá nặng gây tốn tài nguyên bộ nhớ RAM và CPU làm chậm quá trình xử lý.

Để xử lý bạn hãy ấn tổ hợp phím **Ctr+Alt+Del** để vào Task Manager. Trong Task Manager chọn Processes, tiếp theo ấn chuột vào CPU. Những chương trình đầu tiên chính là nguyên nhân máy bị chậm, treo. Hãy chọn vào chương trình đó vấn End Task để tắt chương trình.



+ Do phần cứng máy tính. Điều này thường xảy ra khi ổ cứng bị lỗi (bad sector), lỗi RAM, lỗi CPU, nguồn máy tính hoặc card màn hình. Do đó hãy kiểm tra lại các thiết bị phần cứng của máy tính.

6. Mất hết biểu tượng icon trên màn hình

Dấu hiệu

Không còn nhìn thấy các biểu tượng icon trên màn hình máy tính để sử dụng

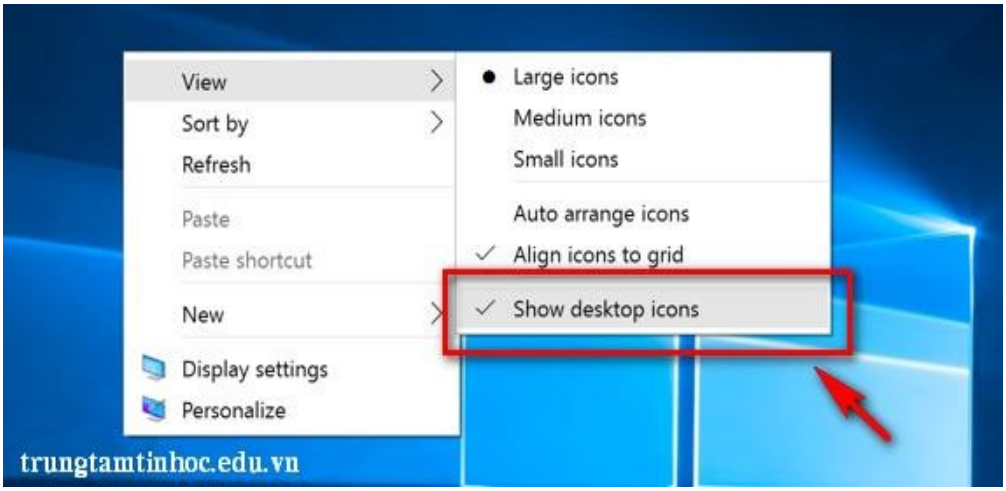
Khắc phục

Rất đơn giản, chỉ cần thao tác click chuột phải và chọn view >> Show desktop icons.

Tại đây có thể thao tác một số lựa chọn khác như:

+ Chỉnh độ to/nhỏ của các icon sử dụng

+ Sắp xếp theo tên, ngày tháng,…



7. Lỗi màn hình bị xoay hoặc đảo ngược

Dấu hiệu

Màn hình máy tính bị xoay 90 độ hoặc xoay ngược mà không thể sử dụng được

Khắc phục

Nguyên nhân là do bạn đã vô tình bấm vào tổ hợp các phím tắt, làm màn hình bị xoay không theo ý muốn.

+ Tổ hợp phím: **CTRL + ALT + Mũi tên đi lên** (chế đô mặc định)

+ Tổ hợp phím: **CTRL + ALT + Mũi tên đi xuống** (xoay ngươc màn hình 180 độ)

+ Tổ hợp phím: **CTRL + ALT + Mũi tên sang trái** (xoay ngang màn hinh 90 độ về bên trái)

+ Tổ hợp phím: **CTRL + ALT + Mũi tên sang phải** (xoay ngang màn hình 90 đô về bên phải)

8. Máy tính bị mất kết nối mạng Internet

Dấu hiệu

Máy tính xuất hiện **dấu X đỏ** thì chắc chắn máy tính không có kết nối mạng Internet

Có thể kiểm tra tín hiệu đèn tại nút mạng phía sau của cây máy tính, nơi đang cắm dây mạng

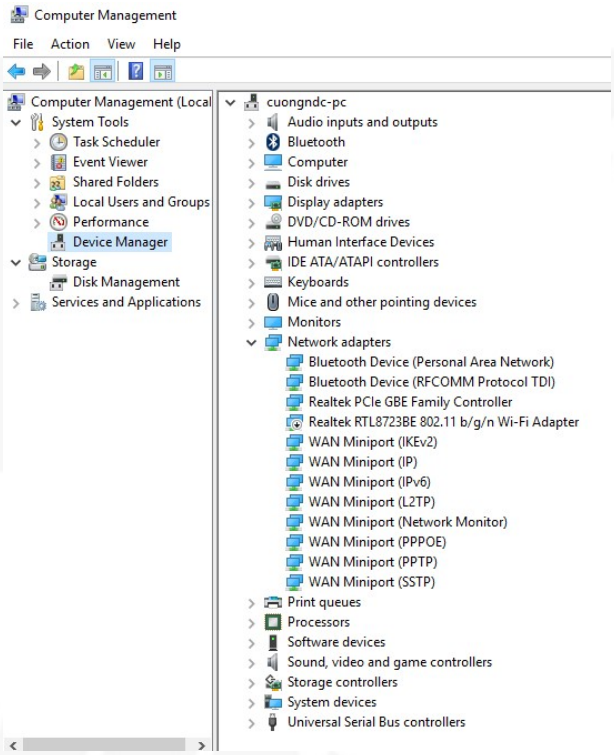
Khắc phục

Kiểm tra lại xem đầu dây mạng có bị lỏng không, kiểm tra tại đầu mạng tại máy tính và đầu còn lại trên tường hoặc trên switch, kiểm tra đèn tín hiệu

Kiểm tra xem dây mạng có bị đứt không, nguồn điện đã cắm trên switch chưa, so sánh với các máy tính khác trong phòng

Cần phải đảm bảo chất lượng cáp mạng để tín hiệu mạng liên tục, không bị hao tổn (kiến nghị sử dụng dây mạng CAT6 hoặc CAT5 loại tốt)

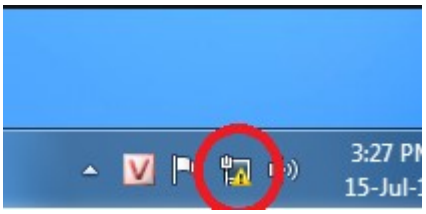
Nếu là lần đầu sử dụng thì cần kiểm tra máy tính đã cài đủ driver mạng chưa. Kiểm tra trong Manager >> Device Manager, nếu thiếu cần phải dùng máy tính khác để tải về cài đặt (lưu ý đúng theo dòng máy tính đang sử dụng)



9. Mạng bị biểu tượng "chấm than"

Dấu hiệu

Cũng giống như mất kết nối mạng, mạng sẽ có biểu tượng **"chấm than"**. Điều này có nghĩa chúng ta sẽ không thể sử dụng mạng Internet



Hiện tượng này xảy ra là do máy tính không thể kết nối được đến máy chủ, không lấy được địa chỉ IP để có thể kết nối mạng. Biểu tượng chấm than là do máy tính đã có kết nối với thiết bị như switch, hub,.. nhưng các thiết bị này không có kết nối được đến máy chủ mạng.

Khắc phục

- Tương tự như lỗi máy tính mất kết nối, chúng ta cần kiểm tra tất cả các tín hiệu, dây mạng kết nối.

- Kiểm tra switch nối đến máy tính đang lỗi mạng, có thể thiết bị bị treo. Rút điện và khởi động lại thiết bị

- Kiểm tra lại dây mạng kết nối từ switch đến thiết bị model, switch access. Tìm dây mạng chính kết nối mạng đến thiết bị switch này và kiểm tra nguyên nhân không có tín hiệu để khắc phục (như thay dây, xác định lỗi, gọi hỗ trợ).

10. Lỗi không in qua mạng được

Dấu hiệu

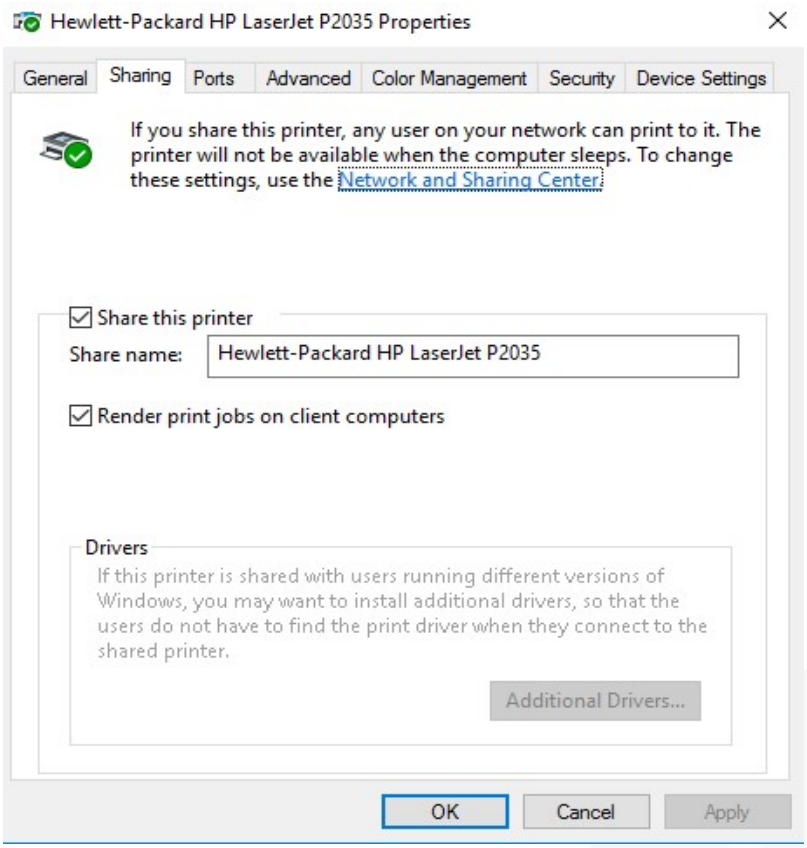
- Máy tính không thể in được văn bản, trong khi đó máy in hoạt động hoàn toàn bình thường.

- Máy báo tín hiệu không in được, thông báo lỗi in ấn trên máy tính

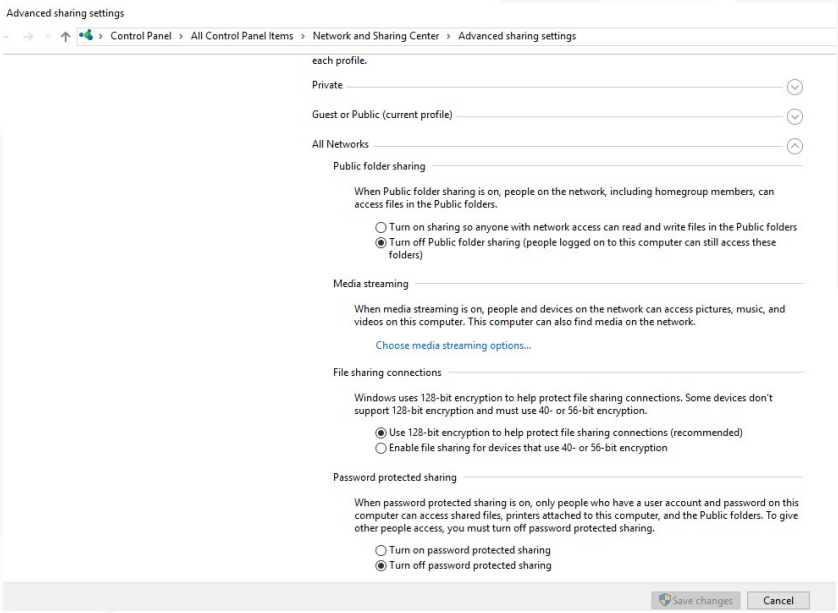
Khắc phục

- Xác định máy in đang được cài trên máy nào (hay còn gọi là máy chủ đang cài đặt trực tiếp máy in) hoặc máy in qua mạng

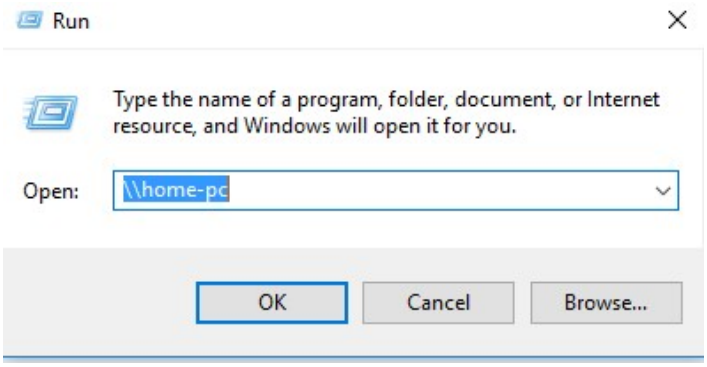
Thiết lập chia sẻ máy in trên máy chủ



Lưu ý cấu hình chế độ share và **tắt mật khẩu** để kết nối máy tính khác



Kết nối máy tính cần in vào máy chủ bằng cách gõ tên máy tính hoặc địa chỉ ip của máy chủ.



11. Lỗi font chữ trên máy tính

Dấu hiệu

Việc lỗi font chữ trên máy tính khiến việc soạn thảo và đọc văn bản khó khăn, không tương thích khi mở các file văn bản word (2003,2007,2010,2013,…)

Khắc phục

+ Đầu tiên hãy kiểm tra xem máy tính đã cài đặt bộ gõ Unikey chưa (link tải bộ gõ tiếng việt tại http://unikey.vn/vietnam/). Cài đặt và để chế độ V để gõ tiếng việt.

+ Tiếp theo nếu lỗi không đọc được chữ tiếng việt nghĩa là bạn đang thiếu font chữ. Bạn phải tải bộ font chữ tiếng việt đầy đủ tại http://fontchu.com/ và giải nén, copy vào đường dẫn "C:\Windows\Fonts".