

ỦY BAN NHÂN DÂN TỈNH LAI CHÂU
SỞ KHOA HỌC VÀ CÔNG NGHỆ

CHUYÊN ĐỀ 6

**BẢO VỆ DỮ LIỆU CÁ NHÂN VÀ QUYỀN RIÊNG TƯ TRÊN
KHÔNG GIAN MẠNG; BẢO VỆ SỨC KHỎE THỂ CHẤT VÀ TINH
THẦN TRONG KHÔNG GIAN MẠNG VÀ CÔNG NGHỆ SỐ**
(Tài liệu nội bộ)

Lai Châu, tháng 02 năm 2026

MỤC LỤC

PHẦN MỞ ĐẦU	4
1. Mục đích.....	4
1.1. Bảo vệ dữ liệu cá nhân và Quyền riêng tư	4
1.2. Bảo vệ sức khỏe thể chất và tinh thần	4
2. Yêu cầu	4
3. Đối tượng tập huấn	5
PHẦN NỘI DUNG.....	6
I. BẢO VỆ DỮ LIỆU CÁ NHÂN VÀ QUYỀN RIÊNG TƯ TRÊN KHÔNG GIAN MẠNG	6
1. Khái niệm cơ bản.....	6
1.1. Dữ liệu cá nhân là gì?	6
1.2. Dữ liệu cá nhân cơ bản	6
1.3. Dữ liệu cá nhân nhạy cảm.....	7
1.4. Quyền riêng tư.....	8
1.5. Tầm quan trọng của bảo vệ dữ liệu cá nhân	9
2. Cách sử dụng và chia sẻ thông tin cá nhân một cách an toàn trên không gian mạng.....	10
2.1. Mật khẩu và xác thực hai yếu tố	10
2.2. Cần trọng khi chia sẻ thông tin cá nhân.....	10
2.3. Bảo vệ dữ liệu cá nhân trên điện thoại an toàn	11
2.4. Cần trọng trong việc mua sắm trực tuyến.....	12
2.5. Kiểm tra chính sách quyền riêng tư.....	13
3. Rủi ro khi chia sẻ thông tin trên không gian mạng	14
4. Tác hại của việc mất dữ liệu cá nhân.....	15
5. Các biện pháp bảo vệ dữ liệu cá nhân và quyền riêng tư cá nhân trên internet....	16
5.1. Khi chia sẻ thông tin, không nên chia sẻ nhiều hơn mức cần thiết.....	16
5.2. Kiểm tra các cài đặt ứng dụng trên các thiết bị kỹ thuật số của bạn	17
5.3. Sử dụng chế độ ẩn danh hoặc riêng tư khi sử dụng trình duyệt.....	18
5.4. Sử dụng kết nối an toàn	19
II. BẢO VỆ SỨC KHỎE THỂ CHẤT VÀ TINH THẦN TRONG KHÔNG GIAN MẠNG VÀ CÔNG NGHỆ SỐ	21
1. Rủi ro ảnh hưởng đến sức khỏe thể chất và biện pháp phòng tránh.	21
1.1. Rủi ro sức khỏe thể chất	21
1.2. Tư thế đúng khi sử dụng thiết bị số.....	23
1.3. Biện pháp phòng tránh khi sử dụng thiết bị số	24
2. Rủi ro ảnh hưởng đến sức khỏe tinh thần và biện pháp phòng tránh.....	27

2.1. Rủi ro ảnh hưởng đến sức khỏe tinh thần.....	27
2.2. Biện pháp phòng tránh và giảm thiểu.....	28
3. Lừa đảo trên không gian mạng.....	29
4. Cách bảo vệ dữ liệu cá nhân và người khác khỏi nguy cơ rủi ro trên không gian mạng.....	30
4.1. Mật khẩu và xác thực hai yếu tố	30
4.2. Cảnh trọng khi chia sẻ thông tin cá nhân.....	31
4.3. Bảo vệ điện thoại an toàn.....	31
4.4. Cảnh trọng trong việc mua sắm trực tuyến.....	32
TÀI LIỆU THAM KHẢO	34

PHẦN MỞ ĐẦU

1. Mục đích

1.1. Bảo vệ dữ liệu cá nhân và Quyền riêng tư

Mục đích chính là xây dựng "hàng rào bảo vệ" cho danh tính số của mỗi cá nhân:

Nâng cao nhận thức về giá trị dữ liệu: Giúp người dân hiểu rằng thông tin cá nhân (họ tên, số điện thoại, địa chỉ, dữ liệu sinh trắc học...) là tài sản quý giá cần được bảo mật.

Trang bị kỹ năng tự bảo vệ: Hướng dẫn cách thiết lập bảo mật (MFA, mật khẩu mạnh), nhận diện các hình thức lừa đảo (phishing), và kiểm soát việc chia sẻ thông tin trên mạng xã hội.

Phổ biến các quy định pháp lý Nghị định 13/2023/NĐ-CP để người dùng biết quyền lợi của mình và các tổ chức biết trách nhiệm trong việc xử lý dữ liệu.

Ngăn ngừa rủi ro tội phạm mạng: Giảm thiểu nguy cơ bị đánh cắp danh tính, lừa đảo tài chính hoặc bị tống tiền dựa trên thông tin cá nhân bị rò rỉ.

1.2. Bảo vệ sức khỏe thể chất và tinh thần

Mục đích là hướng tới một lối sống số lành mạnh và bền vững:

Về thể chất: Cảnh báo về các bệnh lý do lạm dụng công nghệ (cận thị, hội chứng ống cổ tay, các vấn đề về cột sống). Khuyến khích việc cân bằng thời gian sử dụng thiết bị (screen time) và vận động thể chất.

Về tinh thần: Phòng chống bạo lực mạng trang bị tâm thế ứng phó với tin giả, bắt nạt trực tuyến (cyberbullying) và những tác động tiêu cực từ áp lực đồng lứa trên mạng xã hội; Giảm thiểu hội chứng tâm lý ngăn ngừa tình trạng lo âu, trầm cảm hoặc hội chứng "sợ bỏ lỡ" (FOMO) do so sánh bản thân với những hình ảnh ảo trên mạng; Xây dựng văn hóa số văn minh hình thành thói quen sử dụng mạng xã hội có trách nhiệm, biết chọn lọc thông tin và duy trì sự kết nối thực tế với cộng đồng.

2. Yêu cầu

Dữ liệu & Riêng tư: Thành thạo các kỹ năng bảo mật (mật khẩu, 2FA), cẩn trọng tuyệt đối khi chia sẻ thông tin và nắm vững quyền pháp lý để tự bảo vệ trước các rủi ro mạng.

Sức khỏe thể chất: Duy trì tư thế làm việc đúng chuẩn, thực hiện các khoảng nghỉ ngắn và kiểm soát thời gian sử dụng thiết bị để tránh các bệnh lý về mắt, cột sống.

Sức khỏe tinh thần: Xây dựng tâm lý vững vàng trước tin giả, chủ động phòng chống bắt nạt mạng và duy trì sự cân bằng giữa cuộc sống thực và thế giới ảo.

Đạo đức số: Hình thành thói quen ứng xử văn minh, tôn trọng quyền riêng tư của người khác và có trách nhiệm với mọi hành vi trên không gian mạng.

3. Đối tượng tập huấn

Chuyên đề hướng tới đối tượng là cán bộ, công chức, viên chức, người lao động và người dân thuộc mọi độ tuổi, đặc biệt là những người thường xuyên sử dụng internet để học tập, làm việc trên môi trường số. Chương trình nhằm hỗ trợ người tham gia sử dụng không gian mạng an toàn, có trách nhiệm và hiệu quả để bảo vệ dữ liệu cá nhân, quyền riêng tư và sức khỏe thể chất, tinh thần khi sử dụng công nghệ số. Đồng thời, định hướng mỗi cá nhân tự học, tự cập nhật và phát triển kỹ năng số theo nhu cầu riêng, góp phần hình thành công dân số chủ động và thích ứng tốt trong thời đại chuyển đổi số.

PHẦN NỘI DUNG

I. BẢO VỆ DỮ LIỆU CÁ NHÂN VÀ QUYỀN RIÊNG TƯ TRÊN KHÔNG GIAN MẠNG

1. Khái niệm cơ bản

1.1. Dữ liệu cá nhân là gì?

Dữ liệu cá nhân là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự trên môi trường điện tử gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể. Dữ liệu cá nhân bao gồm dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm.

Theo khoản 1, Điều 2 Nghị định 13/2023/NĐ-CP

Dữ liệu cá nhân rất quan trọng và đảm bảo 3 yếu tố của dữ liệu:

Tính duy nhất: Dữ liệu cá nhân là "chìa khóa" để mở ra danh tính của bạn. Nếu mất chìa khóa này, kẻ xấu có thể đóng giả bạn để thực hiện các hành vi phạm pháp.

Giá trị kinh tế: Trong kỷ nguyên số, dữ liệu là "dầu mỏ mới". Các công ty quảng cáo khao khát dữ liệu của bạn để biết bạn thích gì, đang ở đâu và muốn mua gì.

Quyền sở hữu: Bạn là chủ sở hữu dữ liệu của mình. Bạn có quyền biết ai đang giữ nó, họ dùng làm gì và bạn có quyền yêu cầu họ xóa đi.

Ví dụ thực tế: Khi bạn chụp ảnh căn cước công dân đăng lên mạng mà không che số ID hay ngày sinh, bạn đã vô tình cung cấp "dữ liệu cá nhân nhạy cảm" cho cả thế giới, tạo cơ hội cho các khoản vay "ma" hoặc lừa đảo chiếm đoạt tài khoản.

1.2. Dữ liệu cá nhân cơ bản

- a) Họ, chữ đệm và tên khai sinh, tên gọi khác (nếu có);
- b) Ngày, tháng, năm sinh; ngày, tháng, năm chết hoặc mất tích;
- c) Giới tính;
- d) Nơi sinh, nơi đăng ký khai sinh, nơi thường trú, nơi tạm trú, nơi ở hiện tại, quê quán, địa chỉ liên hệ;
- đ) Quốc tịch;
- e) Hình ảnh của cá nhân;

g) Số điện thoại, số chứng minh nhân dân, số định danh cá nhân, số hộ chiếu, số giấy phép lái xe, số biển số xe, số mã số thuế cá nhân, số bảo hiểm xã hội, số thẻ bảo hiểm y tế;

h) Tình trạng hôn nhân;

i) Thông tin về mối quan hệ gia đình (cha mẹ, con cái);

k) Thông tin về tài khoản số của cá nhân; dữ liệu cá nhân phản ánh hoạt động, lịch sử hoạt động trên không gian mạng;

l) Các thông tin khác gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể không thuộc quy định tại khoản 4 Điều này.

Theo khoản 3, Điều 2 Nghị định 13/2023/NĐ-CP

Ví dụ 1: Đăng thông tin lên Facebook: Chị A đăng bài bán hàng và công khai: họ tên đầy đủ, số điện thoại, địa chỉ nhà. Sau đó chị liên tục nhận cuộc gọi quảng cáo, thậm chí có người mạo danh đặt hàng rồi “bom hàng”. Chỉ từ họ tên + số điện thoại + địa chỉ (dữ liệu cơ bản), người xấu có thể khai thác để quấy rối hoặc lừa đảo.

Ví dụ 2: Làm mất giấy tờ photo: Anh B photo CCCD để làm hồ sơ xin việc. Bản photo bị thất lạc. Vài tháng sau, anh phát hiện thông tin của mình bị dùng để đăng ký tài khoản vay online. Họ tên, ngày sinh, số CCCD là dữ liệu cơ bản nhưng nếu bị lộ có thể gây rủi ro tài chính.

Lưu ý: Dữ liệu cá nhân cơ bản không “vô hại”; Càng công khai nhiều, nguy cơ càng cao; Chỉ cung cấp thông tin khi thật sự cần thiết và cho tổ chức đáng tin cậy.

1.3. Dữ liệu cá nhân nhạy cảm

Dữ liệu cá nhân nhạy cảm là dữ liệu cá nhân gắn liền với quyền riêng tư của cá nhân mà khi bị xâm phạm sẽ gây ảnh hưởng trực tiếp tới quyền và lợi ích hợp pháp của cá nhân gồm:

a) Quan điểm chính trị, quan điểm tôn giáo;

b) Tình trạng sức khỏe và đời tư được ghi trong hồ sơ bệnh án, không bao gồm thông tin về nhóm máu;

c) Thông tin liên quan đến nguồn gốc chủng tộc, nguồn gốc dân tộc;

d) Thông tin về đặc điểm di truyền được thừa hưởng hoặc có được của cá nhân;

đ) Thông tin về thuộc tính vật lý, đặc điểm sinh học riêng của cá nhân;

e) Thông tin về đời sống tình dục, xu hướng tình dục của cá nhân;

g) Dữ liệu về tội phạm, hành vi phạm tội được thu thập, lưu trữ bởi các cơ quan thực thi pháp luật;

h) Thông tin khách hàng của tổ chức tín dụng, chi nhánh ngân hàng nước ngoài, tổ chức cung ứng dịch vụ trung gian thanh toán, các tổ chức được phép khác, gồm: thông tin định danh khách hàng theo quy định của pháp luật, thông tin về tài khoản, thông tin về tiền gửi, thông tin về tài sản gửi, thông tin về giao dịch, thông tin về tổ chức, cá nhân là bên bảo đảm tại tổ chức tín dụng, chi nhánh ngân hàng, tổ chức cung ứng dịch vụ trung gian thanh toán;

i) Dữ liệu về vị trí của cá nhân được xác định qua dịch vụ định vị;

k) Dữ liệu cá nhân khác được pháp luật quy định là đặc thù và cần có biện pháp bảo mật cần thiết.

Theo khoản 4, Điều 2 Nghị định 13/2023/NĐ-CP

Ví dụ 1: Lộ thông tin tài khoản ngân hàng: Ông A nhận cuộc gọi tự xưng công an yêu cầu xác minh tài khoản. Ông cung cấp số tài khoản, mã OTP gửi về điện thoại. Chỉ 5 phút sau, tiền trong tài khoản bị chuyển đi. Số tài khoản + mã OTP là dữ liệu tài chính cực kỳ nhạy cảm.

Nguyên tắc: Tuyệt đối không cung cấp OTP cho bất kỳ ai.

Ví dụ 2: Lộ thông tin sức khỏe: Chị B chia sẻ hồ sơ bệnh án, kết quả xét nghiệm lên nhóm mạng xã hội để hỏi ý kiến. Sau đó, thông tin bệnh lý của chị bị lan truyền, ảnh hưởng đến công việc và tâm lý. Thông tin sức khỏe là dữ liệu nhạy cảm vì liên quan đến danh dự, quyền riêng tư và cơ hội nghề nghiệp.

Lưu ý: dữ liệu nhạy cảm có thể ảnh hưởng đến tài sản, danh dự và an toàn cá nhân. Không chia sẻ thông tin tài chính, OTP, hồ sơ bệnh án, hình ảnh giấy tờ tùy thân lên mạng. Khi nghi ngờ bị lộ thông tin, cần báo ngay ngân hàng hoặc cơ quan chức năng.

1.4. Quyền riêng tư

Quyền riêng tư là khả năng kiểm soát những gì người khác biết về mình, hay nói một cách đơn giản là cách chúng ta xử lý thông tin về bản thân. Các thông tin này có thể bao gồm danh tính, hoạt động, sở thích, thói quen và các khía cạnh khác trong cuộc sống.

<https://binhdanhocvuso.lamdong.gov.vn/bao-ve-du-lieu-ca-nhan-va-quyen-rieng-tu-tren-internet-N26.aspx>

Nội dung của quyền riêng tư bao gồm: quyền bảo mật thông tin cá nhân; Quyền bảo vệ hình ảnh cá nhân; Quyền bảo mật thư tín, điện thoại, tin nhắn; Quyền không bị theo dõi, xâm phạm đời sống riêng tư

Ví dụ:

Tự ý đăng ảnh người khác lên mạng khi chưa xin phép → xâm phạm quyền riêng tư.

Đọc trộm tin nhắn, ghi âm cuộc gọi của người khác → vi phạm pháp luật.

Tiết lộ thông tin bệnh án, tình trạng hôn nhân của người khác → xâm phạm bí mật cá nhân.

Trong thời đại công nghệ, quyền riêng tư không chỉ bảo vệ “đời sống thật” mà còn bảo vệ “cuộc sống số”. Giúp bảo vệ danh dự và nhân phẩm; Hạn chế lừa đảo, chiếm đoạt tài sản; Tạo môi trường số an toàn, văn minh.

Tôn trọng quyền riêng tư của mình và của người khác. Không chia sẻ thông tin, hình ảnh khi chưa được phép. Sử dụng mạng xã hội có trách nhiệm và đúng pháp luật.

1.5. Tầm quan trọng của bảo vệ dữ liệu cá nhân

Bảo vệ dữ liệu cá nhân là hoạt động phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi vi phạm liên quan đến dữ liệu cá nhân theo quy định của pháp luật. *(Theo khoản 5 Điều 2 Nghị định 13/2023/NĐ-CP)*

Việc bảo vệ dữ liệu cá nhân là rất quan trọng để đảm bảo quyền riêng tư và các quyền cơ bản khác của mỗi cá nhân. Việc thu thập, xử lý và lưu trữ dữ liệu cá nhân cần được thực hiện một cách có trách nhiệm và tuân thủ các quy định của pháp luật.

Khi thực hiện các hoạt động trên internet, bạn có thể đang tiết lộ thông tin cá nhân của mình thứ mà những người khác có thể dùng để xâm phạm quyền riêng tư của bạn. Các thông tin này có thể là các thông tin như: Họ và tên, ngày sinh, địa chỉ nhà/nơi làm việc, email...

Ví dụ: Khi mua sắm trực tuyến, bạn có thể sẽ phải cung cấp thông tin về thẻ tín dụng và địa chỉ nhà cho các đơn vị cung cấp dịch vụ.

Các trang mạng thường cung cấp dịch vụ miễn phí để được ghi lại những gì bạn làm, bao gồm: Những thông tin bạn tìm kiếm trên trang của họ; Những bài đăng, hình ảnh bạn đăng tải hoặc tương tác trên mạng xã hội; Những sản phẩm bạn mua/lướt xem;

Vì sao cần bảo vệ thông tin cá nhân khi sử dụng Internet:

Những thông tin về bạn xuất hiện trên Internet tạo nên danh tiếng và hình ảnh của bạn trên Internet;

Khi thông tin cá nhân của bạn – bao gồm cả thông tin nhạy cảm – xuất hiện trên Internet, những kẻ xấu có thể sử dụng chúng để thực hiện các hành vi phạm tội, như giả mạo bạn, mở thẻ tín dụng, thẻ ngân hàng hoặc có thể quấy rối, tống tiền bạn...

2. Cách sử dụng và chia sẻ thông tin cá nhân một cách an toàn trên không gian mạng

2.1. Mật khẩu và xác thực hai yếu tố

Để bảo vệ tài khoản của bạn một cách toàn diện, hãy tạo ra những lớp bảo mật vững chắc.

Đầu tiên, hãy xây dựng một mật khẩu mạnh, kết hợp cả chữ cái in hoa, in thường, số và ký tự đặc biệt. Tránh sử dụng những thông tin dễ đoán như ngày sinh hay tên người thân. Ví dụ cụ thể như:

Mật khẩu mạnh: Nph#456@KP#p

Mật khẩu yếu: nhuphuong hoặc 23080000

Thứ hai, đừng quên bật tính năng xác thực hai yếu tố (2FA) cho các tài khoản quan trọng. Với 2FA, ngay cả khi kẻ gian có được mật khẩu, chúng cũng không thể truy cập vào tài khoản của bạn nếu không có mã xác thực được gửi qua điện thoại hoặc ứng dụng. Hiện nay có rất nhiều ứng dụng đã triển khai 2FA nhằm bảo vệ thông tin người dùng, bạn hãy tận dụng tính năng này để tài khoản của mình an toàn nha.

2.2. Cần trọng khi chia sẻ thông tin cá nhân

Cần trọng khi chia sẻ thông tin cá nhân là việc mỗi người cần suy nghĩ kỹ trước khi cung cấp họ tên, số điện thoại, địa chỉ, tài khoản ngân hàng, hình ảnh giấy tờ tùy thân... cho người khác hoặc đăng tải lên mạng.

Trong môi trường số, thông tin có thể bị sao chép, lưu trữ và phát tán rất nhanh. Một khi đã chia sẻ, việc kiểm soát lại gần như không thể.

Nguyên tắc quan trọng: Chỉ chia sẻ khi thật sự cần thiết và đúng đối tượng.

Mạng xã hội là một không gian công cộng, vì vậy hãy cẩn trọng khi chia sẻ thông tin cá nhân của bạn. Để tạo ra một hồ sơ cá nhân an toàn, bạn nên hạn

chế chia sẻ những thông tin quá riêng tư như địa chỉ nhà, số điện thoại. Kiểm tra và điều chỉnh cài đặt quyền riêng tư trên các nền tảng mạng xã hội một cách thường xuyên.

Ngoài ra, hãy luôn cảnh giác với các cuộc tấn công mạng như lừa đảo qua email hoặc tin nhắn. Đừng bao giờ click vào các liên kết lạ hoặc tải xuống các tệp đính kèm từ những người gửi không đáng tin cậy.

Ví dụ 1: Lộ OTP ngân hàng bà A nhận cuộc gọi tự xưng nhân viên ngân hàng yêu cầu cung cấp mã OTP để “xác minh tài khoản”. Sau khi cung cấp, tiền trong tài khoản bị chuyển hết. Bài học không bao giờ cung cấp mật khẩu, mã OTP cho bất kỳ ai.

Ví dụ 2: Đăng ảnh căn cước công dân lên mạng anh B chụp ảnh CCCD mới và đăng lên Facebook để “khoe”. Sau đó, thông tin bị kẻ xấu sử dụng để đăng ký vay tiền online. Bài học không đăng hình ảnh giấy tờ tùy thân lên mạng xã hội.

Ví dụ 3: Điền thông tin vào link lạ: Chị C nhận tin nhắn trúng thưởng, bấm vào đường link và điền họ tên, số điện thoại, số tài khoản. Sau đó chị liên tục bị gọi điện lừa đảo. Bài học kiểm tra kỹ nguồn gửi trước khi cung cấp thông tin cá nhân.

Lưu ý: Thông tin cá nhân là tài sản của mỗi người. Chia sẻ càng nhiều, rủi ro càng cao. Hãy tỉnh táo trước khi bấm “Gửi” hoặc “Đăng”.

2.3. Bảo vệ dữ liệu cá nhân trên điện thoại an toàn

Điện thoại thông minh hiện nay lưu trữ rất nhiều dữ liệu cá nhân như danh bạ, hình ảnh, tin nhắn, tài khoản ngân hàng, mạng xã hội và ứng dụng dịch vụ công. Nếu không được bảo vệ đúng cách, điện thoại có thể trở thành “cửa ngõ” để kẻ xấu đánh cắp thông tin và chiếm đoạt tài sản. Vì vậy, bảo vệ dữ liệu trên điện thoại là bước quan trọng để đảm bảo an toàn trong môi trường số.

Biện pháp bảo vệ cơ bản để bảo vệ dữ liệu cá nhân trên điện thoại của mình, chúng ta cần thực hiện một số biện pháp an toàn như: Cài đặt mật khẩu mạnh, vân tay hoặc nhận diện khuôn mặt. Không chia sẻ mã OTP, mật khẩu cho bất kỳ ai. Chỉ tải ứng dụng từ kho chính thức (CH Play, App Store). Không bấm vào đường link lạ gửi qua tin nhắn, Zalo, Facebook. Thường xuyên cập nhật hệ điều hành và ứng dụng.

Đầu tiên, bạn hãy tiến hành thiết lập một lớp bảo mật vững chắc bằng cách khóa màn hình bằng mật khẩu, mã PIN hoặc vân tay, FaceID,...

Thứ hai, luôn giữ cho thiết bị của bạn được cập nhật bằng cách cài đặt các bản vá bảo mật mới nhất cho hệ điều hành và ứng dụng. Các bản vá này sẽ giúp vá các lỗ hổng có thể bị kẻ xấu lợi dụng để xâm nhập vào thiết bị của bạn. Thường xuyên cập nhật hệ điều hành cũng là một cách bảo vệ an toàn cho điện thoại của bạn đó nha.

Cuối cùng, hãy tạo thói quen sao lưu dữ liệu quan trọng thường xuyên để phòng trường hợp thiết bị bị mất hoặc hư hỏng. Việc sao lưu dữ liệu sẽ giúp bạn khôi phục lại dữ liệu một cách nhanh chóng và dễ dàng nếu chẳng may xảy ra việc ngoài ý muốn.

Ví dụ 1: Mất điện thoại không khóa màn hình: Anh A làm rơi điện thoại nhưng không cài mật khẩu. Người nhặt được truy cập vào ứng dụng ngân hàng và thực hiện giao dịch. Nếu có khóa màn hình và xác thực sinh trắc học, rủi ro sẽ giảm đáng kể.

Ví dụ 2: Cài ứng dụng giả mạo: Chị B tải ứng dụng “vay tiền nhanh” từ đường link trên Facebook. Ứng dụng yêu cầu cấp quyền truy cập danh bạ và hình ảnh. Sau đó chị bị đe dọa, tống tiền bằng hình ảnh cá nhân. Không cài đặt ứng dụng từ nguồn không rõ ràng.

Ví dụ 3: Nhấn vào link lạ: Ông C nhận tin nhắn “Tài khoản của bạn sắp bị khóa”, bấm vào link và đăng nhập. Ngay sau đó tài khoản bị chiếm quyền. Cần kiểm tra kỹ địa chỉ website trước khi đăng nhập.

Lưu ý: điện thoại là “kho dữ liệu cá nhân di động”. Bảo vệ điện thoại chính là bảo vệ tài sản và danh dự của mình. Luôn cẩn trọng trước khi tải, bấm hoặc chia sẻ.

2.4. Cẩn trọng trong việc mua sắm trực tuyến

Mua sắm trực tuyến ngày càng phổ biến vì tiện lợi và nhanh chóng. Tuy nhiên, nếu không cẩn trọng, người dân có thể gặp rủi ro như lừa đảo, mất tiền, lộ thông tin cá nhân hoặc nhận hàng kém chất lượng.

Vì vậy, cần nâng cao cảnh giác khi đặt hàng, thanh toán và cung cấp thông tin trên môi trường mạng.

Mua sắm trực tuyến mang đến nhiều tiện lợi, nhưng cũng tiềm ẩn nhiều rủi ro. Để bảo vệ thông tin cá nhân và tài khoản ngân hàng của mình, bạn cần đặc biệt chú ý đến vấn đề bảo mật khi thanh toán. Hãy luôn kiểm tra xem trang web mua sắm có biểu tượng khóa an toàn (hình ổ khóa nhỏ) và sử dụng giao thức HTTPS trước địa chỉ trang web.

Biểu tượng này cho biết thông tin bạn nhập vào, bao gồm số thẻ ngân hàng và các thông tin cá nhân khác, được mã hóa và truyền đi một cách an toàn, giúp ngăn chặn kẻ gian đánh cắp dữ liệu.

Bảo vệ dữ liệu cá nhân là một bước quan trọng để đảm bảo an toàn và sự riêng tư trong thế giới số hóa ngày nay. Bằng cách áp dụng các biện pháp bảo mật như sử dụng mật khẩu mạnh, cài đặt xác thực hai yếu tố và hạn chế chia sẻ thông tin nhạy cảm, bạn có thể giảm thiểu rủi ro bị tấn công mạng hay đánh cắp danh tính.

<https://www.thegioididong.com/tin-tuc/cach-bao-ve-du-lieu-ca-nhan-an-toan-1569761>

Những điểm cần lưu ý:

- Chỉ mua hàng trên sàn thương mại điện tử, website uy tín.
- Kiểm tra kỹ thông tin người bán, đánh giá sản phẩm.
- Không chuyển tiền trước cho cá nhân không rõ ràng.
- Không cung cấp mã OTP, mật khẩu khi thanh toán.
- Kiểm tra kỹ đường link trước khi đăng nhập tài khoản.

Ví dụ 1: Chuyển tiền đặt cọc rồi mất liên lạc: Chị A thấy quảng cáo bán điện thoại giá rẻ trên Facebook. Người bán yêu cầu chuyển khoản trước 50% để “giữ hàng”. Sau khi chuyển tiền, tài khoản người bán chặn liên lạc. Bài học không chuyển tiền đặt cọc cho người bán không rõ nguồn gốc.

Ví dụ 2: Website giả mạo sàn thương mại điện tử: Anh B nhận tin nhắn khuyến mãi lớn kèm đường link. Trang web có giao diện giống sàn thương mại điện tử quen thuộc. Sau khi đăng nhập, tài khoản bị chiếm quyền và bị trừ tiền. Bài học kiểm tra kỹ địa chỉ website, không bấm vào link lạ.

Ví dụ 3: Nhận hàng không đúng quảng cáo: Ông C mua sản phẩm qua livestream giá rẻ. Khi nhận hàng, chất lượng không đúng mô tả nhưng không thể liên hệ đổi trả. Bài học: Ưu tiên mua trên nền tảng có chính sách bảo vệ người mua.

2.5. Kiểm tra chính sách quyền riêng tư

Là văn bản mà nhà cung cấp dịch vụ (Google, Facebook, Zalo, các app...) dùng để thông báo: Họ thu thập thông tin gì? Họ sử dụng thông tin ra sao? Ai sẽ được chia sẻ thông tin đó? Người dùng có quyền gì với dữ liệu của mình.

Chính sách là căn cứ để hợp pháp hóa việc thu thập dữ liệu. Trách nhiệm khi người dùng đồng ý (tick) trước khi sử dụng dịch vụ.

Ví dụ 1: Khi bạn tạo tài khoản TikTok, bạn đã “chấp nhận” cho phép app truy cập camera, micro, vị trí,...

Ví dụ 2: Mất quyền kiểm soát dữ liệu cá nhân. Khi bạn “đồng ý”, bạn có thể đã cho phép thu thập: Danh bạ, vị trí GPS, lịch sử duyệt web, ảnh, file cá nhân dẫn đến tất cả được dùng mà bạn không hề hay biết!

Ví dụ 3: Chấp nhận các điều khoản bất lợi. Từ bỏ quyền khiếu nại, đồng ý bị theo dõi hoạt động, cho phép trích xuất nội dung riêng tư mà bạn upload.

Lưu ý:

Đừng “click cho nhanh”

Luôn xem mục chính sách quyền riêng tư và điều khoản sử dụng

Ưu tiên ứng dụng có chính sách rõ ràng, minh bạch

Kiểm tra kỹ quyền mà ứng dụng yêu cầu khi cài đặt

3. Rủi ro khi chia sẻ thông tin trên không gian mạng

- Lộ lọt thông tin cá nhân như số điện thoại, CMND/CCCD, địa chỉ, tài khoản ngân hàng, dẫn đến bị lợi dụng để lừa đảo.

- Bị tấn công chiếm đoạt tài khoản (Facebook, Zalo, ngân hàng, email...) nếu chia sẻ quá nhiều thông tin riêng tư hoặc sử dụng mật khẩu yếu.

- Bị lừa đảo qua mạng, mạo danh người quen, cơ quan chức năng để vay tiền, nhờ chuyển tiền hoặc chiếm đoạt tài sản.

- Bị theo dõi, xâm phạm quyền riêng tư, do chia sẻ thông tin vị trí, hình ảnh nơi ở, thói quen sinh hoạt.

- Bị đánh cắp danh tính (identity theft) và sử dụng vào hành vi phạm pháp, vay nợ, mở tài khoản trái phép.

- Bị tấn công mạng như phát tán mã độc, virus, theo dõi hoạt động thiết bị thông qua các liên kết độc hại được chia sẻ.

- Ảnh hưởng uy tín cá nhân nếu đăng tải thông tin nhạy cảm, phát ngôn thiếu kiểm soát hoặc bị kẻ xấu cắt ghép, bóp méo.

- Lan truyền thông tin sai sự thật, dẫn đến vi phạm pháp luật hoặc gây ảnh hưởng tiêu cực đến cộng đồng.

Ví dụ 2: Công khai ngày sinh, số điện thoại. Chị B để công khai ngày sinh, số điện thoại trên trang cá nhân. Đối tượng xấu thu thập thông tin, gọi điện giả danh công an yêu cầu “xác minh tài khoản”. Thông tin cá nhân công khai có thể bị lợi dụng để lừa đảo.

Ví dụ 4: Chia sẻ vị trí theo thời gian thực. Gia đình D đăng bài “đi du lịch 5 ngày” kèm vị trí cụ thể. Kẻ xấu biết nhà không có người và thực hiện trộm cắp. Chia sẻ vị trí, lịch trình công khai có thể gây nguy cơ mất an toàn.

4. Tác hại của việc mất dữ liệu cá nhân

- Bị lợi dụng để lừa đảo, chiếm đoạt tài sản. Khi dữ liệu cá nhân bị rò rỉ như số điện thoại, CCCD, tài khoản ngân hàng, kẻ xấu có thể giả mạo cơ quan Nhà nước, ngân hàng hoặc người quen để lừa chuyển tiền, vay tín dụng hoặc mở tài khoản trái phép. Điều này không chỉ gây thiệt hại kinh tế mà còn khiến nạn nhân rơi vào trạng thái lo lắng, hoang mang.

Ví dụ: Anh A bị lộ số điện thoại và số CCCD khi đăng ký một website không rõ nguồn gốc. Sau đó, anh nhận cuộc gọi tự xưng là nhân viên ngân hàng yêu cầu xác minh tài khoản vì “có giao dịch bất thường”. Do thông tin cá nhân bị lộ nên kẻ lừa đảo đọc đúng họ tên, ngày sinh, địa chỉ → anh A tin tưởng và cung cấp mã OTP. Kết quả mất 80 triệu đồng trong tài khoản chỉ trong vài phút.

- Nguy cơ bị đánh cắp danh tính. Tin tặc có thể dùng thông tin như họ tên, ngày sinh, số định danh, địa chỉ để tạo hồ sơ giả, đăng ký dịch vụ hoặc thực hiện hành vi vi phạm pháp luật dưới danh nghĩa của nạn nhân. Việc “đóng giả” này gây ảnh hưởng lớn tới uy tín, thậm chí khiến nạn nhân bị liên quan đến các vụ việc pháp lý mà bản thân không hề hay biết.

Ví dụ: Chị B phát hiện mình bị đòi nợ từ một công ty tài chính dù chưa từng vay tiền. Điều tra mới biết có người dùng CCCD và thông tin cá nhân của chị để đăng ký vay online. Hậu quả phải làm việc với ngân hàng, công an để chứng minh mình không liên quan. Uy tín bị ảnh hưởng nghiêm trọng.

- Bị theo dõi, xâm phạm đời tư cá nhân. Khi thông tin cá nhân như vị trí, lịch sử truy cập, thói quen sử dụng mạng xã hội bị lộ, nạn nhân có thể bị theo dõi hoặc quấy rối. Đây là mối nguy đặc biệt nghiêm trọng đối với trẻ vị thành niên, phụ nữ hoặc người có vị trí công tác nhạy cảm.

Ví dụ: Một học sinh thường xuyên đăng ảnh check-in, chia sẻ vị trí thời gian thực trên mạng xã hội. Một đối tượng lạ theo dõi và biết chính xác lịch học – giờ về nhà. Nguy cơ bị quấy rối, đe dọa hoặc tiếp cận ngoài đời thực. Trường hợp này đặc biệt nguy hiểm với trẻ em và phụ nữ.

- Tài khoản cá nhân bị chiếm đoạt. Một khi dữ liệu đăng nhập hoặc thông tin xác thực bị rò rỉ, các tài khoản như Facebook, Zalo, Gmail, ngân hàng số... có thể bị chiếm quyền kiểm soát. Hacker từ đó tung tin giả, tống tiền, làm ảnh hưởng danh dự, uy tín và gây thiệt hại tài chính.

Ví dụ: Một giảng viên dùng chung mật khẩu cho email và Facebook. Sau khi email bị rò rỉ trong một vụ lộ dữ liệu, hacker đăng nhập được Facebook, gửi tin nhắn vay tiền hàng loạt cho sinh viên. Thiệt hại tài chính + ảnh hưởng nghiêm trọng đến uy tín nghề nghiệp.

- Bị tống tiền, đe dọa. Nếu thông tin nhạy cảm như hình ảnh riêng tư, lịch sử giao dịch, tài liệu cá nhân bị lấy cắp, kẻ xấu có thể dùng để đe dọa, yêu cầu tiền chuộc hoặc ép buộc thực hiện các hành vi bất chính. Nhiều trường hợp phải chịu áp lực tâm lý kéo dài, gây ảnh hưởng nghiêm trọng đến sức khỏe tinh thần.

Ví dụ: Một người bị hack tài khoản cloud cá nhân chứa hình ảnh riêng tư. Kẻ xấu gửi email yêu cầu chuyển tiền nếu không sẽ phát tán dữ liệu. Nạn nhân chịu áp lực tâm lý lớn, lo sợ, mất ăn mất ngủ trong thời gian dài.

- Doanh nghiệp bị ảnh hưởng uy tín và thiệt hại tài chính. Đối với tổ chức, rò rỉ dữ liệu khách hàng hoặc tài liệu nội bộ có thể dẫn đến mất niềm tin của người dân, bị xử phạt theo quy định pháp luật, thậm chí ảnh hưởng đến hoạt động kinh doanh và thương hiệu. Việc khắc phục hậu quả tốn kém và kéo dài.

Ví dụ thực tế: Năm 2018, vụ rò rỉ dữ liệu của Facebook (Cambridge Analytica) làm lộ thông tin của hàng triệu người dùng. Hậu quả: bị điều tra, phạt hàng tỷ USD, mất niềm tin nghiêm trọng từ người dùng toàn cầu. Hoặc nhiều ngân hàng tại Việt Nam từng bị giả mạo thương hiệu để lừa đảo khách hàng → dù không trực tiếp gây rò rỉ nhưng vẫn ảnh hưởng uy tín.

- Gây nguy cơ mất an toàn cho gia đình và đời sống cá nhân. Khi thông tin về địa chỉ nhà, lịch sinh hoạt, thông tin người thân bị lộ, kẻ xấu có thể lợi dụng để trộm cắp, đột nhập hoặc gây hại. Đây là tác hại rất nguy hiểm vì ảnh hưởng trực tiếp đến an toàn của cá nhân và gia đình.

Ví dụ: Một gia đình đăng đầy đủ thông tin về chuyến du lịch dài ngày trên mạng xã hội (vé máy bay, thời gian, địa điểm). Đối tượng xấu biết nhà đang không có người và thực hiện trộm cắp. Thiệt hại tài sản + nguy cơ mất an toàn cá nhân.

5. Các biện pháp bảo vệ dữ liệu cá nhân và quyền riêng tư cá nhân trên internet.

5.1. Khi chia sẻ thông tin, không nên chia sẻ nhiều hơn mức cần thiết

- Không đăng tải những nội dung mà bạn không muốn công khai. Mạng xã hội không phải “nhật ký riêng”. Một khi đã đăng: Có thể bị chụp màn hình, bị lưu trữ lại, bị chia sẻ ngoài ý muốn, Internet không có nút “xóa hoàn toàn”.

Ví dụ: Một sinh viên đăng bài than phiền về nơi thực tập, kèm hình ảnh nội bộ công ty. Bài viết bị lan truyền, ảnh hưởng cơ hội việc làm sau này. Hoặc đăng ảnh giấy khen có đầy đủ: Họ tên, ngày sinh, mã số... Kẻ xấu có thể dùng để xác thực giả mạo.

- Hạn chế chia sẻ các thông tin chi tiết như địa chỉ nhà/nơi làm việc, số điện thoại. Đây là dữ liệu định danh và dữ liệu vị trí. Khi kết hợp với thông tin khác → tạo hồ sơ cá nhân hoàn chỉnh.

Ví dụ: Đăng bài “Nhà mình ở số 25 đường X, hiện đang đi du lịch 1 tuần”. Tự thông báo nhà đang không có người. Hoặc công khai số điện thoại trên Facebook. Nhận cuộc gọi giả mạo ngân hàng, công an. Khi lộ số điện thoại + họ tên → dễ bị lừa đảo vay tín dụng online.

- Giữ bí mật các thông tin như tên đăng nhập và mật khẩu tài khoản, tài khoản ngân hàng... Thông tin xác thực là chìa khóa hệ thống. Không chỉ không chia sẻ, mà còn: Không lưu công khai, không gửi qua chat, không dùng chung mật khẩu.

Ví dụ: Một giáo viên gửi file Word chứa: Tài khoản: abc@gmail.com Mật khẩu: 123456 Qua nhóm chat lớp để nhờ chỉnh sửa tài liệu. Nếu một người trong nhóm bị hack, toàn bộ tài khoản liên quan có thể bị chiếm đoạt. Hoặc bị lừa cung cấp mã OTP khi giả mạo ngân hàng → mất tiền trong vài phút.

- Khi điền các biểu mẫu, chỉ nên nhập các thông tin bắt buộc – thường được đánh dấu bằng dấu sao màu đỏ (*). Nhiều website thu thập dư thừa thông tin để: Marketing, phân tích hành vi, bán dữ liệu. Thông tin không bắt buộc thì không cần cung cấp.

Ví dụ: Đăng ký nhận tài liệu miễn phí. Biểu mẫu yêu cầu: Email (*), họ tên (*), số điện thoại, nghề nghiệp, địa chỉ. Nếu chỉ email là bắt buộc (*), thì chỉ nên nhập email. Cung cấp thêm số điện thoại → có thể bị spam, phishing cá nhân hóa.

5.2. Kiểm tra các cài đặt ứng dụng trên các thiết bị kỹ thuật số của bạn

Hãy cẩn thận khi cho phép ứng dụng truy cập camera (máy ảnh), micro (mic), vị trí... Bạn có thể xem lại quyền bạn đã cấp cho ứng dụng trên điện thoại di động thông minh của bạn trong mục “Cài đặt”. Camera, micro, vị trí là **dữ**

liệu nhạy cảm vì chúng liên quan trực tiếp đến: Hình ảnh cá nhân, âm thanh cuộc trò chuyện, thói quen di chuyển. Nếu cấp quyền bừa bãi, ứng dụng có thể: Ghi âm nền, theo dõi vị trí liên tục, thu thập dữ liệu hành vi

Ví dụ 1: Một ứng dụng chỉnh sửa ảnh yêu cầu quyền micro. Chức năng chính chỉ là chỉnh ảnh, không liên quan ghi âm. Nếu cấp quyền, ứng dụng có thể thu thập âm thanh nền.

Ví dụ 2: Ứng dụng mạng xã hội được cấp quyền vị trí “luôn luôn”. Mọi di chuyển đều được ghi lại. Có thể xây dựng hồ sơ thói quen sinh hoạt.

- Chỉ cấp quyền liên quan đến chức năng ứng dụng. Nên cho các ứng dụng truy cập các quyền liên quan đến chức năng của chúng. Quyền phải phù hợp với chức năng. Nếu không phù hợp thì nghi ngờ mục đích thu thập dữ liệu.

Ví dụ: ứng dụng thời tiết chỉ cần quyền truy cập vị trí (để dự báo chính xác), không cần cấp quyền truy cập danh bạ, camera, micro.

- Chọn “khi dùng ứng dụng” thay vì “luôn luôn”. Có 3 mức quyền phổ biến: Từ chối, chỉ khi dùng ứng dụng, luôn luôn. Nếu chọn “Luôn luôn” ứng dụng có thể truy cập dữ liệu kể cả khi chạy nền.

Ví dụ: Ứng dụng giao đồ ăn: Chỉ cần vị trí khi đặt hàng. Không cần theo dõi vị trí cả ngày. Nếu để “Luôn luôn” → ứng dụng có thể ghi nhận toàn bộ lịch trình di chuyển. Chuyển sang “Khi dùng ứng dụng” → Giảm thiểu thu thập dữ liệu thừa.

- Xoá ứng dụng khi không còn sử dụng. Nếu không còn nhu cầu sử dụng ứng dụng, nên xoá nó khỏi thiết bị của bạn. Ứng dụng cũ có thể: Chứa lỗ hổng bảo mật, không còn được cập nhật, vẫn giữ quyền truy cập đã cấp. Không dùng nhưng vẫn giữ rủi ro âm thầm.

Ví dụ: Một ứng dụng game cài 2 năm trước. Đã cấp quyền truy cập danh bạ và bộ nhớ. Không còn chơi nhưng chưa xóa. Nếu tài khoản game bị xâm nhập, dữ liệu liên quan vẫn có thể bị khai thác.

5.3. Sử dụng chế độ ẩn danh hoặc riêng tư khi sử dụng trình duyệt

- Khi sử dụng chế độ ẩn danh hoặc riêng tư: Trình duyệt không lưu trữ thông tin bạn truy cập trên Internet. Khi bật chế độ ẩn danh (Incognito/Private): Không lưu lịch sử truy cập, không lưu cookie sau khi đóng cửa sổ, không lưu thông tin đăng nhập tạm thời, không lưu dữ liệu biểu mẫu. Sau khi đóng trình duyệt, người khác mở máy sẽ không xem được bạn đã truy cập gì.

Ví dụ 1: Bạn dùng máy tính ở cơ quan để đăng nhập email cá nhân. Nếu dùng chế độ thường → lịch sử và cookie còn lưu. Nếu dùng ẩn danh → khi đóng cửa sổ, phiên đăng nhập bị xóa.

- Các trang web tạm thời không nhận ra người sử dụng. Do cookie không được lưu lâu dài nên: Website không nhớ bạn là ai, không tự động đăng nhập, không cá nhân hóa nội dung dựa trên lịch sử cũ.

Ví dụ: Bạn tìm kiếm giá vé máy bay nhiều lần. Ở chế độ thường → website ghi nhớ và có thể hiển thị giá cao hơn (do phân tích hành vi). Ở chế độ ẩn danh → website coi như người dùng mới. Hữu ích khi so sánh giá vé, khách sạn.

- Lưu ý: Nhà cung cấp dịch vụ Internet của bạn vẫn có thể biết bạn đang truy cập ở đâu trên Internet. Chế độ ẩn danh không che giấu được: Nhà cung cấp Internet, quản trị viên mạng cơ quan/trường học, Website bạn truy cập. Nếu cần ẩn danh thực sự → phải dùng thêm công cụ chuyên biệt. Bạn bật ẩn danh để truy cập một website. Trình duyệt không lưu lịch sử trên máy. Nhưng nhà mạng vẫn ghi nhận bạn đã truy cập địa chỉ đó.

- Cách sử dụng chế độ ẩn danh hoặc riêng tư trong trình duyệt:

+ Trình duyệt Chrome: Nhấp vào dấu (:) Tùy chỉnh và kiểm soát Google Chrome ở góc trên cùng bên phải màn hình → Nhấp vào Cửa sổ ẩn danh mới hoặc nhấn (Ctrl + Shift + N)



+ Trình duyệt Safari: Nhấp vào biểu tượng Tab ở góc phải màn hình → Chọn tab Riêng tư.

+ Trình duyệt Microsoft Edge: Chọn vào logo Microsoft Edge (tác vụ) → Chọn Cửa sổ riêng tư mới hoặc nhấn (Ctrl + Shift + N).

5.4. Sử dụng kết nối an toàn

Trong an toàn thông tin, kết nối an toàn nghĩa là dữ liệu được truyền đi qua Internet phải được mã hóa và bảo vệ khỏi nghe lén, chỉnh sửa hoặc giả mạo. Nếu kết nối không an toàn, mọi thông tin bạn gửi đi có thể bị “nghe trộm”.

- Sử dụng website có HTTPS thay vì HTTP. HTTP dữ liệu truyền ở dạng gần như “văn bản thường”. HTTPS dữ liệu được mã hóa. Dấu hiệu nhận biết:

Có biểu tượng khoá  trên thanh địa chỉ, bắt đầu bằng https://

Ví dụ 1: Bạn đăng nhập Internet Banking qua một website chỉ có “http://”. Kẻ xấu trong cùng mạng WiFi có thể chặn và đọc dữ liệu.

Ví dụ 2: Bạn mua hàng online trên website có “https://”. Thông tin thẻ ngân hàng được mã hóa trước khi gửi đi. HTTPS giúp bảo mật quá trình truyền dữ liệu, không đảm bảo website là uy tín 100%.

- Cần trọng khi sử dụng WiFi công cộng, sử dụng mạng di động khi giao dịch quan trọng. WiFi miễn phí ở: Quán cà phê, sân bay, khách sạn. Thường không có mã hóa mạnh hoặc có thể bị giả mạo. Nguy cơ: Tấn công, giả mạo điểm phát WiFi, đánh cắp cookie đăng nhập. Mạng di động 4G/5G cá nhân bảo mật hơn Wifi công cộng, ít nguy cơ bị giả mạo điểm truy cập an toàn hơn đáng kể.

Ví dụ: Một người kết nối WiFi “Free Coffee” ở quán. Tin tặc tạo một điểm phát WiFi giả có tên tương tự. Khi người dùng đăng nhập Facebook → hacker có thể thu thập phiên đăng nhập. Không nên thực hiện giao dịch ngân hàng khi dùng WiFi công cộng.

- Kiểm tra chứng chỉ bảo mật website Không chỉ nhìn HTTPS mà còn: Tên miền chính xác, không sai chính tả, không có ký tự lạ.

Ví dụ:

Website giả mạo www.nganhang-abc-security.com

Website thật www.nganhangabc.com.

Lưu ý dù có HTTPS nhưng vẫn có thể là website lừa đảo.

Tình huống và câu hỏi thảo luận:

Tình huống: Lan là sinh viên đại học. Trong chuyến du lịch cùng bạn bè, Lan đăng lên mạng xã hội: Ảnh check-in tại sân bay và khách sạn, ảnh vé máy bay có hiển thị mã QR rõ ràng thời gian khởi hành và điểm đến. Bài đăng nhận được nhiều lượt thích và bình luận. Tuy nhiên, Lan không biết rằng những thông tin này có thể bị khai thác.

Câu hỏi thảo luận:

Trong bài đăng của Lan có những loại dữ liệu cá nhân nào?

Mã QR trên vé máy bay có thể chứa những thông tin gì?

Việc công khai thời gian – địa điểm có được xem là dữ liệu cá nhân không? Vì sao?

II. BẢO VỆ SỨC KHỎE THỂ CHẤT VÀ TINH THẦN TRONG KHÔNG GIAN MẠNG VÀ CÔNG NGHỆ SỐ

Trong kỷ nguyên số, thách thức không chỉ nằm ở bảo vệ dữ liệu mà còn ở bảo vệ chính sức khỏe con người. Công nghệ và thiết bị số giúp nâng cao hiệu suất làm việc, kết nối nhanh chóng và mở rộng tri thức – nhưng nếu sử dụng thiếu kiểm soát, chúng có thể tác động trực tiếp đến cả thể chất lẫn tinh thần.

1. Rủi ro ảnh hưởng đến sức khỏe thể chất và biện pháp phòng tránh.

1.1. Rủi ro sức khỏe thể chất

- Ảnh hưởng đến thị lực (Hội chứng thị giác màn hình). Trong thời đại công nghệ số, máy tính, điện thoại thông minh và máy tính bảng đã trở thành những công cụ không thể thiếu trong học tập, làm việc và giải trí. Tuy nhiên, việc tiếp xúc với màn hình trong thời gian dài đang âm thầm tạo ra nhiều tác động tiêu cực đến sức khỏe thị giác, thường được gọi là Hội chứng thị giác màn hình.

Khi tập trung nhìn màn hình quá lâu, tần suất chớp mắt tự nhiên của con người giảm đáng kể, khiến mắt không được bôi trơn đầy đủ và dễ rơi vào tình trạng khô rát. Đồng thời, mắt phải điều tiết liên tục ở khoảng cách gần trong thời gian dài, làm cơ mắt bị căng thẳng. Bên cạnh đó, ánh sáng xanh phát ra từ các thiết bị điện tử cũng góp phần gây mỏi mắt và làm tăng áp lực lên hệ thần kinh thị giác.

Hậu quả thường gặp bao gồm: khô và đỏ mắt, cảm giác cộm như có dị vật trong mắt, nhức mỏi kéo dài, nhìn mờ tạm thời, đau đầu và giảm khả năng tập trung. Không chỉ dừng lại ở đó, việc giữ nguyên một tư thế khi sử dụng thiết bị trong thời gian dài còn gây đau cổ, vai, gáy và ảnh hưởng đến cột sống.

Nếu không được điều chỉnh kịp thời, tình trạng này có thể làm suy giảm chất lượng công việc, học tập và cuộc sống. Vì vậy, việc sử dụng thiết bị công nghệ một cách khoa học, hợp lý và có thời gian nghỉ ngơi phù hợp là điều hết sức cần thiết để bảo vệ đôi mắt – “cửa sổ tâm hồn” trong thời đại số.

- Rối loạn giấc ngủ: Việc sử dụng điện thoại, máy tính và các thiết bị điện tử vào buổi tối đã trở thành thói quen phổ biến của nhiều người. Tuy nhiên, ít ai

nhận ra rằng ánh sáng xanh phát ra từ màn hình đang âm thầm tác động tiêu cực đến chất lượng giấc ngủ và đồng hồ sinh học của cơ thể.

Ánh sáng xanh có khả năng ức chế quá trình sản sinh melatonin (hormone gây buồn ngủ) – loại hormone đóng vai trò điều hòa giấc ngủ và tạo cảm giác buồn ngủ tự nhiên. Khi melatonin bị suy giảm, cơ thể khó chuyển sang trạng thái nghỉ ngơi, khiến thời gian đi vào giấc ngủ kéo dài hơn. Không chỉ vậy, nhịp sinh học (chu kỳ thức – ngủ) cũng bị rối loạn, làm cho cơ thể mất đi sự cân bằng vốn có.

Hậu quả thường thấy là tình trạng khó ngủ, ngủ chập chờn, không sâu giấc hoặc dễ tỉnh giữa đêm. Sau khi thức dậy, cơ thể thường cảm thấy mệt mỏi, uể oải, thiếu tỉnh táo và giảm khả năng tập trung trong ngày hôm sau. Nếu kéo dài, rối loạn giấc ngủ còn có thể ảnh hưởng đến tâm trạng, hiệu suất học tập, làm việc và sức khỏe tổng thể.

Vì vậy, việc hạn chế sử dụng thiết bị điện tử trước giờ ngủ, điều chỉnh độ sáng màn hình phù hợp và xây dựng thói quen sinh hoạt khoa học là những giải pháp quan trọng để bảo vệ giấc ngủ – nền tảng thiết yếu cho sức khỏe thể chất và tinh thần.

- Bệnh lý lối sống ít vận động: Việc ngồi trong thời gian dài khiến cơ thể tiêu hao ít năng lượng, quá trình trao đổi chất diễn ra chậm hơn, dẫn đến tích tụ mỡ thừa và nguy cơ béo phì. Không chỉ ảnh hưởng đến vóc dáng, tình trạng này còn làm gia tăng nguy cơ mắc các bệnh tim mạch, tăng huyết áp và rối loạn chuyển hóa. Tim phải hoạt động kém hiệu quả hơn khi cơ thể thiếu vận động thường xuyên, làm tăng nguy cơ biến chứng về sau.

Bên cạnh đó, hệ cơ xương khớp cũng chịu nhiều tác động tiêu cực. Ngồi sai tư thế, ít thay đổi vị trí hoặc thiếu các hoạt động giãn cơ có thể gây đau lưng, thoái hóa cột sống, đau vai gáy và suy yếu hệ cơ. Theo thời gian, những tổn thương này có thể trở nên mãn tính, ảnh hưởng đến chất lượng cuộc sống và khả năng lao động.

Lối sống ít vận động không chỉ gây ra các biểu hiện trước mắt mà còn để lại hậu quả lâu dài đối với sức khỏe tổng thể. Vì vậy, việc duy trì thói quen vận động thường xuyên, xen kẽ thời gian làm việc với các bài tập nhẹ nhàng và xây dựng chế độ sinh hoạt khoa học là yếu tố quan trọng để bảo vệ cơ thể một cách bền vững.

- Hội chứng ống cổ tay, đau lưng: Hội chứng ống cổ tay hình thành khi dây thần kinh giữa ở cổ tay bị chèn ép do chuyển động lặp lại và tư thế đặt tay

không phù hợp. Người mắc thường cảm thấy tê bì, đau nhức, yếu lực cầm nắm, thậm chí lan lên cánh tay. Nếu không được điều chỉnh kịp thời, tình trạng này có thể ảnh hưởng trực tiếp đến hiệu suất công việc và khả năng vận động tinh của bàn tay.

Song song đó, thói quen ngồi khom lưng, cúi đầu về phía trước hoặc giữ nguyên một tư thế quá lâu làm tăng áp lực lên cột sống, đặc biệt là vùng thắt lưng và cổ. Hậu quả là đau lưng, đau vai gáy, căng cơ và về lâu dài có thể dẫn đến thoái hóa cột sống hoặc rối loạn tư thế.

Những vấn đề này không xuất hiện ngay lập tức mà tích tụ dần theo thời gian, trở thành “bệnh nghề nghiệp” phổ biến trong thời đại số. Vì vậy, việc điều chỉnh tư thế ngồi đúng chuẩn, bố trí bàn ghế phù hợp, nghỉ giải lao định kỳ và thực hiện các bài tập giãn cơ là giải pháp quan trọng giúp phòng tránh và bảo vệ hệ cơ xương khớp một cách hiệu quả.

1.2. Tư thế đúng khi sử dụng thiết bị số

1.2.1. Khi dùng máy tính

Việc sử dụng máy tính trong thời gian dài với tư thế sai có thể gây ra hàng loạt vấn đề như đau lưng, mỏi cổ, hội chứng ống cổ tay và suy giảm thị lực. Vì vậy, xây dựng và duy trì tư thế đúng khi làm việc với máy tính không chỉ giúp nâng cao hiệu suất mà còn bảo vệ sức khỏe lâu dài.

- Tư thế ngồi chuẩn lưng thẳng, tựa vào ghế, giữ đường cong sinh lý tự nhiên của cột sống. Vai thả lỏng, không gồng cứng. Đầu giữ thẳng, không cúi quá thấp hoặc ngửa quá cao. Hông và đầu gối tạo góc khoảng 90–100 độ. Hai bàn chân đặt phẳng trên sàn, không vắt chéo chân trong thời gian dài. Tư thế ngồi đúng giúp phân bổ đều trọng lực cơ thể, giảm áp lực lên cột sống thắt lưng và hạn chế tình trạng cong vẹo hoặc thoái hóa sớm.

- Vị trí màn hình màn hình đặt ngang tầm mắt hoặc thấp hơn mắt khoảng 5–10 cm. Khoảng cách từ mắt đến màn hình 50–70 cm. Trung tâm màn hình nằm hơi thấp hơn tầm nhìn tự nhiên. Khi màn hình quá thấp, người dùng phải cúi đầu liên tục gây đau cổ; nếu quá cao sẽ làm căng cơ gáy. Khoảng cách hợp lý giúp giảm điều tiết mắt và hạn chế mỏi mắt.

- Bàn phím và chuột cần đặt song song với mặt bàn. Khuỷu tay tạo góc khoảng 90 độ. Cổ tay giữ thẳng, không gập lên hoặc gập xuống. Chuột đặt gần bàn phím để tránh phải với tay quá xa. Tư thế tay sai trong thời gian dài có thể chèn ép dây thần kinh giữa ở cổ tay, dẫn đến hội chứng ống cổ tay. Việc giữ cổ tay trung tính giúp giảm áp lực và phòng ngừa tổn thương.

- Thời gian và vận động sau mỗi 30–60 phút, nên đứng dậy vận động nhẹ 3–5 phút. Áp dụng quy tắc 20-20-20 cho mắt: cứ 20 phút nhìn màn hình, nhìn xa 20 feet (khoảng 6m) trong 20 giây. Thực hiện các động tác giãn cơ cổ, vai, lưng. Cơ thể con người không được thiết kế để ngồi bất động quá lâu. Nghỉ ngắn định kỳ giúp tăng tuần hoàn máu, giảm căng cơ và cải thiện sự tập trung.

1.2.2. Khi dùng điện thoại

Điện thoại thông minh đã trở thành vật bất ly thân trong học tập, làm việc và giải trí. Tuy nhiên, thói quen cúi đầu hàng giờ để nhìn màn hình nhỏ lại đang âm thầm tạo áp lực lớn lên cổ, vai, lưng và cả thị giác. Việc duy trì tư thế đúng khi sử dụng điện thoại không chỉ giúp giảm mỏi tức thì mà còn phòng tránh những tổn thương lâu dài cho hệ cơ xương khớp.

- Giữ đầu và cổ ở tư thế trung tính. Nâng điện thoại lên gần tầm mắt, thay vì cúi gập cổ xuống. Giữ đầu thẳng, tai thẳng hàng với vai. Tránh duy trì tư thế cúi đầu quá 15–20 độ trong thời gian dài. Khi cúi đầu 45–60 độ để nhìn điện thoại, áp lực lên cột sống cổ có thể tăng lên nhiều lần so với tư thế thẳng. Điều này dễ dẫn đến đau cổ, cứng gáy và lâu dài có thể gây thoái hóa đốt sống cổ.

- Tư thế ngồi hoặc đứng đúng. Nếu ngồi: lưng thẳng, tựa vào ghế, hai chân đặt vững trên sàn. Nếu đứng: phân bổ trọng lượng đều hai chân, không dồn một bên. Tránh nằm sấp hoặc nằm nghiêng một bên quá lâu khi dùng điện thoại. Tư thế lệch, vặn mình hoặc nằm sai cách khiến cơ và dây chằng bị kéo căng không đồng đều, làm tăng nguy cơ đau lưng và lệch tư thế.

- Vị trí tay và cổ tay. Giữ cổ tay ở trạng thái tự nhiên, không gập quá mức. Thỉnh thoảng đổi tay cầm để tránh quá tải một bên. Không giữ điện thoại quá thấp khiến vai và cổ phải cúi về trước. Việc giữ điện thoại liên tục trong thời gian dài có thể gây căng cơ bàn tay, tê ngón tay hoặc đau cổ tay do lặp lại thao tác chạm và cuộn màn hình.

- Bảo vệ thị giác. Giữ khoảng cách từ mắt đến màn hình khoảng 30–40 cm. Điều chỉnh độ sáng phù hợp với môi trường xung quanh. Nghỉ mắt định kỳ, áp dụng quy tắc 20-20-20. Màn hình nhỏ khiến mắt phải điều tiết nhiều hơn, dễ gây mỏi mắt và khô mắt nếu tập trung liên tục.

1.3. Biện pháp phòng tránh khi sử dụng thiết bị số

1.3.1. Biện pháp phòng tránh tổn hại cho mắt khi sử dụng thiết bị số

Trong thời đại số, đôi mắt phải làm việc với cường độ cao hơn bao giờ hết. Màn hình máy tính, điện thoại, máy tính bảng... đều phát ra ánh sáng xanh và yêu cầu mắt điều tiết liên tục ở khoảng cách gần. Nếu không có biện pháp

bảo vệ phù hợp, nguy cơ khô mắt, mỏi mắt, nhức đầu và suy giảm thị lực sẽ ngày càng gia tăng. Vì vậy, việc áp dụng các biện pháp phòng tránh là điều cần thiết và mang tính lâu dài.

- Áp dụng quy tắc 20-20-20. Cứ mỗi 20 phút nhìn màn hình, hãy nhìn ra xa khoảng 6 mét trong ít nhất 20 giây. Quy tắc này giúp cơ mắt được thư giãn, giảm co cứng do điều tiết liên tục ở khoảng cách gần. Đây là biện pháp đơn giản nhưng cực kỳ hiệu quả để hạn chế mỏi mắt và nhìn mờ tạm thời.

- Điều chỉnh ánh sáng và độ sáng màn hình. Không sử dụng màn hình trong môi trường quá tối. Điều chỉnh độ sáng màn hình tương đương với ánh sáng xung quanh. Hạn chế ánh sáng chói hoặc phản chiếu trực tiếp vào mắt. Sự chênh lệch ánh sáng lớn giữa màn hình và môi trường khiến mắt phải liên tục thích nghi, làm tăng căng thẳng thị giác. Ánh sáng phù hợp giúp giảm áp lực lên võng mạc và dây thần kinh thị giác.

- Giữ khoảng cách và vị trí màn hình hợp lý. Màn hình máy tính cách mắt 50–70 cm. Điện thoại cách mắt khoảng 30–40 cm. Tâm màn hình hơi thấp hơn tầm mắt. Khoảng cách hợp lý giúp giảm mức độ điều tiết và hội tụ của mắt, từ đó hạn chế tình trạng nhức mỏi kéo dài.

- **Tăng cường chớp mắt và giữ ẩm cho mắt. Chủ động chớp mắt thường xuyên khi làm việc. Có thể sử dụng nước mắt nhân tạo nếu được khuyến nghị. Uống đủ nước mỗi ngày. Khi tập trung cao độ, tần suất chớp mắt giảm đáng kể, làm lớp phim nước mắt bay hơi nhanh và gây khô mắt. Việc chớp mắt đầy đủ giúp bôi trơn và bảo vệ giác mạc.**

- **Hạn chế sử dụng thiết bị trước khi ngủ. Tránh dùng thiết bị ít nhất 30–60 phút trước giờ ngủ. Bật chế độ lọc ánh sáng xanh vào buổi tối. Ánh sáng xanh không chỉ gây căng thẳng thị giác mà còn ức chế hormone melatonin, ảnh hưởng đến giấc ngủ. Hạn chế tiếp xúc vào buổi tối giúp mắt và hệ thần kinh được nghỉ ngơi đúng nhịp sinh học.**

- Chế độ dinh dưỡng và kiểm tra mắt định kỳ. Bổ sung vitamin A, lutein, omega-3 từ thực phẩm tự nhiên. Khám mắt định kỳ để phát hiện sớm các vấn đề về thị lực. Dinh dưỡng đầy đủ giúp duy trì sức khỏe võng mạc và giảm nguy cơ thoái hóa điểm vàng. Kiểm tra định kỳ giúp điều chỉnh kính hoặc phát hiện sớm các bất thường.

1.3.2. Biện pháp phòng tránh đối với giấc ngủ khi sử dụng thiết bị số

Sử dụng thiết bị số không đúng cách có thể làm rối loạn nhịp sinh học, gây khó ngủ, ngủ không sâu và mệt mỏi kéo dài.

- Hạn chế sử dụng thiết bị số trước khi ngủ (ít nhất 60 phút). Ánh sáng xanh từ màn hình ức chế hormone melatonin – hormone điều hòa giấc ngủ. Khi melatonin bị giảm, não hiểu nhầm là “vẫn còn ban ngày”, khiến cơ thể khó đi vào trạng thái nghỉ ngơi. Hạn chế sử dụng thiết bị số trước khi ngủ giúp não chuyển sang chế độ thư giãn tự nhiên, tăng chất lượng giấc ngủ sâu, giảm tình trạng trằn trọc, khó ngủ.

- Sử dụng chế độ lọc ánh sáng xanh (Night Mode). Hầu hết điện thoại, máy tính hiện nay đều có chế độ: Night Shift (iOS), Night Light (Windows), Eye Comfort Shield (Android). Chế độ này làm màn hình ngả vàng, giảm ánh sáng xanh. Giảm kích thích thần kinh, hạn chế rối loạn nhịp sinh học, giảm mất ban đêm.

- Không sử dụng thiết bị số trên giường ngủ. Khi vừa nằm trên giường vừa dùng điện thoại, não sẽ liên kết “giường ngủ” với hoạt động tỉnh táo thay vì nghỉ ngơi. Sử dụng thiết bị số trên giường ngủ gây khó ngủ hơn, giảm phản xạ buồn ngủ tự nhiên, tăng thói quen lệ thuộc thiết bị.

- Thiết lập giờ giới hạn sử dụng thiết bị. Cài đặt chế độ Screen Time (iPhone), Digital Wellbeing (Android). Giúp kiểm soát thời gian dùng ứng dụng giải trí vào buổi tối. Tạo kỷ luật công nghệ, giảm thói quen lướt vô thức, bảo vệ sức khỏe tinh thần.

1.3.3. Biện pháp phòng tránh đối với lối sống khi sử dụng thiết bị số

Trong thời đại công nghệ phát triển mạnh mẽ, thiết bị số đã trở thành một phần không thể thiếu trong học tập, làm việc và giải trí. Tuy nhiên, việc sử dụng thiếu kiểm soát có thể làm thay đổi lối sống theo hướng thụ động, giảm vận động và hạn chế giao tiếp trực tiếp. Điều này dễ dẫn đến lệ thuộc công nghệ và mất cân bằng giữa đời sống thực và môi trường số. Vì vậy, cần xây dựng thói quen sử dụng thiết bị hợp lý, có giới hạn thời gian rõ ràng. Đồng thời, tăng cường hoạt động thể chất và duy trì các mối quan hệ ngoài đời thực. Bên cạnh đó, mỗi người cần hình thành văn hóa ứng xử có trách nhiệm trên không gian mạng. Sự cân bằng giữa “online” và “offline” chính là chìa khóa giúp duy trì một lối sống lành mạnh, tích cực và bền vững trong thời đại số.

1.3.4. Biện pháp phòng tránh đối với tư thế khi sử dụng thiết bị số

Tư thế khi sử dụng thiết bị số ảnh hưởng trực tiếp đến cột sống, cổ, vai gáy và thị lực. Việc ngồi sai tư thế trong thời gian dài có thể gây đau lưng, cong vẹo cột sống và thoái hóa sớm.

Vì vậy, cần duy trì tư thế ngồi thẳng lưng, vai thả lỏng, hai chân đặt vuông góc với mặt sàn.

Màn hình nên đặt ngang tầm mắt và cách mắt khoảng 50–70 cm để tránh cúi gập cổ. Khi sử dụng điện thoại, hạn chế cúi đầu quá lâu, nên nâng thiết bị lên gần tầm mắt.

Bên cạnh đó, cứ mỗi 45–60 phút cần đứng dậy vận động, giãn cơ nhẹ nhàng. Việc bố trí bàn ghế phù hợp chiều cao cơ thể cũng giúp giảm áp lực lên cột sống. Duy trì tư thế đúng không chỉ phòng tránh bệnh lý cơ xương khớp mà còn nâng cao hiệu quả học tập và làm việc lâu dài.

1.3.5. Biện pháp phòng tránh bảo vệ tinh thần khi sử dụng thiết bị số

Thiết bị số không chỉ tác động đến thể chất mà còn ảnh hưởng sâu sắc đến tinh thần và cảm xúc. Việc tiếp xúc liên tục với mạng xã hội, tin tức tiêu cực hoặc áp lực so sánh bản thân có thể gây căng thẳng, lo âu và giảm tự tin. Vì vậy, cần chủ động xây dựng thói quen sử dụng công nghệ lành mạnh.

Trước hết, nên giới hạn thời gian sử dụng mạng xã hội để tránh lệ thuộc và quá tải thông tin. Thứ hai, chọn lọc nội dung tích cực, tránh theo dõi những trang gây cảm xúc tiêu cực hoặc kích động. Bên cạnh đó, không nên so sánh bản thân với hình ảnh “hoàn hảo” trên mạng vì phần lớn đó chỉ là hình ảnh đã được chọn lọc.

Ngoài ra, cần duy trì giao tiếp trực tiếp với gia đình và bạn bè để cân bằng cảm xúc. Khi cảm thấy căng thẳng vì môi trường số, nên tạm ngắt kết nối, vận động hoặc tham gia hoạt động ngoài trời.

Bảo vệ tinh thần trong thời đại số không phải là tránh xa công nghệ, mà là làm chủ nó, sử dụng có chọn lọc và giữ vững giá trị cá nhân. Công nghệ phục vụ con người – chứ không phải điều khiển cảm xúc của con người.

2. Rủi ro ảnh hưởng đến sức khỏe tinh thần và biện pháp phòng tránh

Trong thời đại số, thiết bị công nghệ mang lại nhiều lợi ích nhưng cũng tiềm ẩn không ít rủi ro đối với sức khỏe tinh thần. Nếu không kiểm soát tốt, việc sử dụng quá mức có thể gây căng thẳng, lo âu và lệ thuộc tâm lý.

2.1. Rủi ro ảnh hưởng đến sức khỏe tinh thần

Bắt nạt và bạo lực mạng: Lời nói, hình ảnh xấu lan truyền gây tổn thương tâm lý sâu sắc, dẫn đến tự ti, lo âu, trầm cảm, thậm chí ý định tự tử.

Lo âu và căng thẳng kéo dài, tiếp xúc liên tục với tin tức tiêu cực, áp lực học tập – công việc và dòng thông tin dày đặc dễ khiến não bộ rơi vào trạng thái quá tải.

So sánh xã hội & Áp lực thể hiện: Áp lực "like", "share" và so sánh bản thân với người khác trên mạng xã hội gây căng thẳng, mất cân bằng tinh thần, hình ảnh cơ thể tiêu cực. So sánh bản thân và giảm tự tin, mạng xã hội thường hiển thị hình ảnh thành công, hạnh phúc đã được chọn lọc. Việc so sánh bản thân với hình ảnh “hoàn hảo” đó dễ gây mặc cảm, tự ti. Lệ thuộc mạng xã hội (nghiện thiết bị số), thói quen kiểm tra điện thoại liên tục có thể tạo cảm giác bồn chồn khi không online, ảnh hưởng khả năng tập trung.

Nghiện mạng xã hội & màn hình: Dẫn đến rối loạn giấc ngủ, suy nhược cơ thể, giảm tập trung, ảnh hưởng việc học tập, làm tăng nguy cơ trầm cảm.

Tiếp xúc nội dung độc hại: Lừa đảo, tin giả, nội dung bạo lực, kích động, hoặc các "thử thách" nguy hiểm, gây hậu quả thực tế.

Cô lập xã hội: Dành quá nhiều thời gian online có thể làm giảm kết nối và kỹ năng giao tiếp xã hội thực tế. Cô lập xã hội, giao tiếp qua màn hình quá nhiều có thể làm giảm tương tác trực tiếp, dẫn đến cảm giác cô đơn dù vẫn “kết nối”.

2.2. Biện pháp phòng tránh và giảm thiểu

Nâng cao nhận thức: Hiểu rõ rủi ro, nhận biết hành vi sai trái, và biết cách ứng xử lành mạnh trên mạng.

Quản lý thời gian sử dụng thiết lập giới hạn sử dụng mỗi ngày, đặc biệt với mạng xã hội và trò chơi trực tuyến. Chọn lọc nội dung tích cực theo dõi các kênh học tập, phát triển bản thân; hạn chế tiếp xúc với nội dung gây tiêu cực hoặc tranh cãi. Tạm ngắt kết nối khi cần thiết nếu cảm thấy căng thẳng, nên “digital detox” vài giờ hoặc một ngày để não bộ được nghỉ ngơi.

Tăng cường hoạt động thể chất và giao tiếp trực tiếp. Duy trì hoạt động ngoài đời thực tăng cường thể thao, đọc sách, tham gia hoạt động nhóm để cân bằng cảm xúc.

Bảo vệ thông tin cá nhân: Cẩn trọng khi chia sẻ, chỉ chia sẻ thông tin với nguồn tin cậy.

Kiểm chứng thông tin: Không chia sẻ tin giả, tin sai sự thật.

Ứng xử có trách nhiệm: Tôn trọng người khác, không tham gia bắt nạt mạng, không vi phạm pháp luật và đạo đức.

Trò chuyện và tìm kiếm sự giúp đỡ: Lắng nghe, thấu hiểu con cái; tìm đến chuyên gia tâm lý khi vấn đề nghiêm trọng. Chia sẻ cảm xúc trao đổi với gia đình, bạn bè hoặc người đáng tin cậy khi gặp áp lực từ môi trường sống.

Tận dụng lợi ích: Sử dụng mạng xã hội cho mục đích kết nối tích cực, học hỏi, và tiếp cận thông tin hữu ích.

Ví dụ 1: Một học sinh thường xuyên lướt mạng xã hội vào buổi tối và thấy bạn bè khoe thành tích học tập. Em bắt đầu lo lắng, mất ngủ và nghĩ mình kém cỏi. Biện pháp: Giới hạn thời gian dùng mạng buổi tối, tập trung vào mục tiêu cá nhân và trao đổi với thầy cô để định hướng học tập.

Ví dụ 2: Một người trẻ kiểm tra điện thoại liên tục, cảm thấy khó chịu khi không có thông báo mới. Biện pháp: Tắt thông báo không cần thiết, đặt thời gian “không điện thoại” mỗi ngày và tham gia hoạt động thể thao.

3. Lừa đảo trên không gian mạng

Lừa đảo trên không gian mạng là các hành vi chiếm đoạt tài sản, thông tin cá nhân bằng thủ đoạn tinh vi như mạo danh cơ quan chức năng, nhân viên viễn thông, ngân hàng; dụ dỗ đầu tư tài chính "việc nhẹ lương cao"; hoặc sử dụng AI tạo video/hình ảnh nhạy cảm để tống tiền; hoặc đánh vào tâm lý nhẹ dạ, ham lợi, thiếu cảnh giác. Các hình thức phổ biến gồm: "bảo hiểm" tài khoản Facebook, lừa SIM 4G/5G, "việc nhẹ lương cao", giả mạo email/tin nhắn ngân hàng, đầu tư tiền ảo/đa cấp, tống tiền bằng hình ảnh. Cần cảnh giác, không cung cấp thông tin cá nhân/mã OTP/mật khẩu, không truy cập link lạ, không chuyển tiền cho người không quen biết.

- Các thủ đoạn lừa đảo phổ biến

+ Mạo danh cơ quan chức năng: Giả công an, viện kiểm sát... gọi điện yêu cầu điều tra, cung cấp thông tin để chiếm đoạt tiền.

+ "Bảo hiểm" tài khoản/Fanpage: Nhắn tin hứa hẹn bảo vệ tài khoản Facebook, Fanpage khỏi bị khóa, yêu cầu phí cao hoặc cài app lạ.

+ "Việc nhẹ lương cao": Dụ dỗ làm nhiệm vụ online (như tìm, like, đánh giá sản phẩm) trên các sàn TMĐT để nhận hoa hồng, ban đầu trả lãi nhỏ rồi chiếm đoạt tiền lớn.

+ Lừa SIM 4G/5G: Giả nhân viên nhà mạng yêu cầu nâng cấp SIM, lấy thông tin để chiếm đoạt tài khoản ngân hàng.

+ Lừa đảo đầu tư: Kêu gọi đầu tư tiền ảo, chứng khoán, đa cấp trên các website giả mạo với lợi nhuận khủng, không có thật.

+ Tổng tiền bằng hình ảnh/video: Dùng AI ghép ảnh/video người dùng vào nội dung nhạy cảm để đe dọa, tổng tiền.

+ Giả mạo tin nhắn/email: Gửi tin nhắn trúng thưởng, thông báo thanh toán tiền điện/nước/internet giả mạo.

+ Lừa đảo tình cảm: Dụ dỗ, lừa tiền sau khi xây dựng mối quan hệ tình cảm online.

- Cách phòng tránh:

+ Tỉnh táo: Luôn giữ bình tĩnh, không tin vào những lời hứa hẹn lợi ích cao bất thường.

+ Bảo mật thông tin: Tuyệt đối không cung cấp mã OTP, mật khẩu, thông tin tài khoản ngân hàng, không cấp quyền quản trị cho người lạ.

+ Cảnh giác link lạ: Không truy cập, đăng nhập vào các đường link, website, ứng dụng từ người gửi không xác định.

+ Xác thực thông tin: Khi người quen nhờ chuyển tiền/thông tin, cần gọi điện thoại trực tiếp xác nhận.

+ Không chuyển tiền trước: Tuyệt đối không chuyển cọc hay bất kỳ khoản tiền nào cho người lạ trong mọi trường hợp.

+ Tố giác tội phạm: Báo ngay cho cơ quan Công an, chính quyền địa phương khi phát hiện hành vi nghi ngờ lừa đảo.

4. Cách bảo vệ dữ liệu cá nhân và người khác khỏi nguy cơ rủi ro trên không gian mạng

Bên dưới đây sẽ là 4 cách bảo vệ dữ liệu cá nhân được Hiệp hội An ninh mạng Quốc gia khuyến dùng. Hãy cùng theo dõi và thực hiện để an toàn cho mình cùng cộng đồng bạn nha.

4.1. Mật khẩu và xác thực hai yếu tố

Để bảo vệ tài khoản của bạn một cách toàn diện, hãy tạo ra những lớp bảo mật vững chắc. Đầu tiên, hãy xây dựng một mật khẩu mạnh, kết hợp cả chữ cái in hoa, in thường, số và ký tự đặc biệt. Tránh sử dụng những thông tin dễ đoán như ngày sinh hay tên người thân. Ví dụ cụ thể như:

Mật khẩu mạnh: Nph#456@KP#p

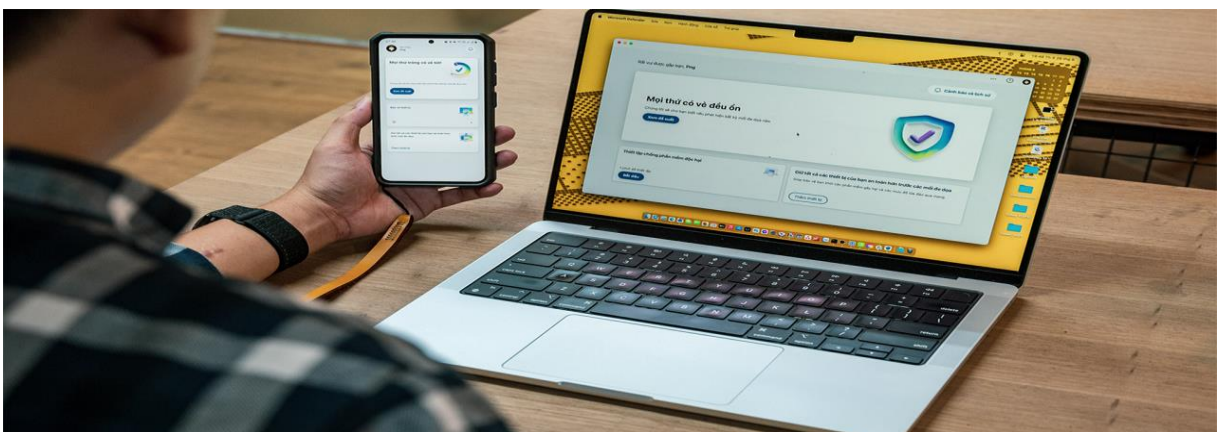
Mật khẩu yếu: nhuphuong hoặc 23080000



Thứ hai, đừng quên bật tính năng xác thực hai yếu tố (2FA) cho các tài khoản quan trọng. Với 2FA, ngay cả khi kẻ gian có được mật khẩu, chúng cũng không thể truy cập vào tài khoản của bạn nếu không có mã xác thực được gửi qua điện thoại hoặc ứng dụng. Hiện nay có rất nhiều ứng dụng đã triển khai 2FA nhằm bảo vệ thông tin người dùng, bạn hãy tận dụng tính năng này để tài khoản của mình an toàn.

4.2. Cảnh trọng khi chia sẻ thông tin cá nhân

Mạng xã hội là một không gian công cộng, vì vậy hãy cẩn trọng khi chia sẻ thông tin cá nhân của bạn. Để tạo ra một hồ sơ cá nhân an toàn, bạn nên hạn chế chia sẻ những thông tin quá riêng tư như địa chỉ nhà, số điện thoại. Kiểm tra và điều chỉnh cài đặt quyền riêng tư trên các nền tảng mạng xã hội một cách thường xuyên.



Ngoài ra, hãy luôn cảnh giác với các cuộc tấn công mạng như lừa đảo qua email hoặc tin nhắn. Đừng bao giờ click vào các liên kết lạ hoặc tải xuống các tệp đính kèm từ những người gửi không đáng tin cậy.

4.3. Bảo vệ điện thoại an toàn

Để bảo vệ dữ liệu cá nhân trên điện thoại của mình, chúng ta cần thực hiện một số biện pháp an toàn. Đầu tiên, bạn hãy tiến hành thiết lập một lớp bảo mật vững chắc bằng cách khóa màn hình bằng mật khẩu, mã PIN hoặc vân tay, FaceID,...

Thứ hai, luôn giữ cho thiết bị của bạn được cập nhật bằng cách cài đặt các bản vá bảo mật mới nhất cho hệ điều hành và ứng dụng. Các bản vá này sẽ giúp vá các lỗ hổng có thể bị kẻ xấu lợi dụng để xâm nhập vào thiết bị của bạn. Thường xuyên cập nhật hệ điều hành cũng là một cách bảo vệ an toàn cho điện thoại của bạn đó nha.

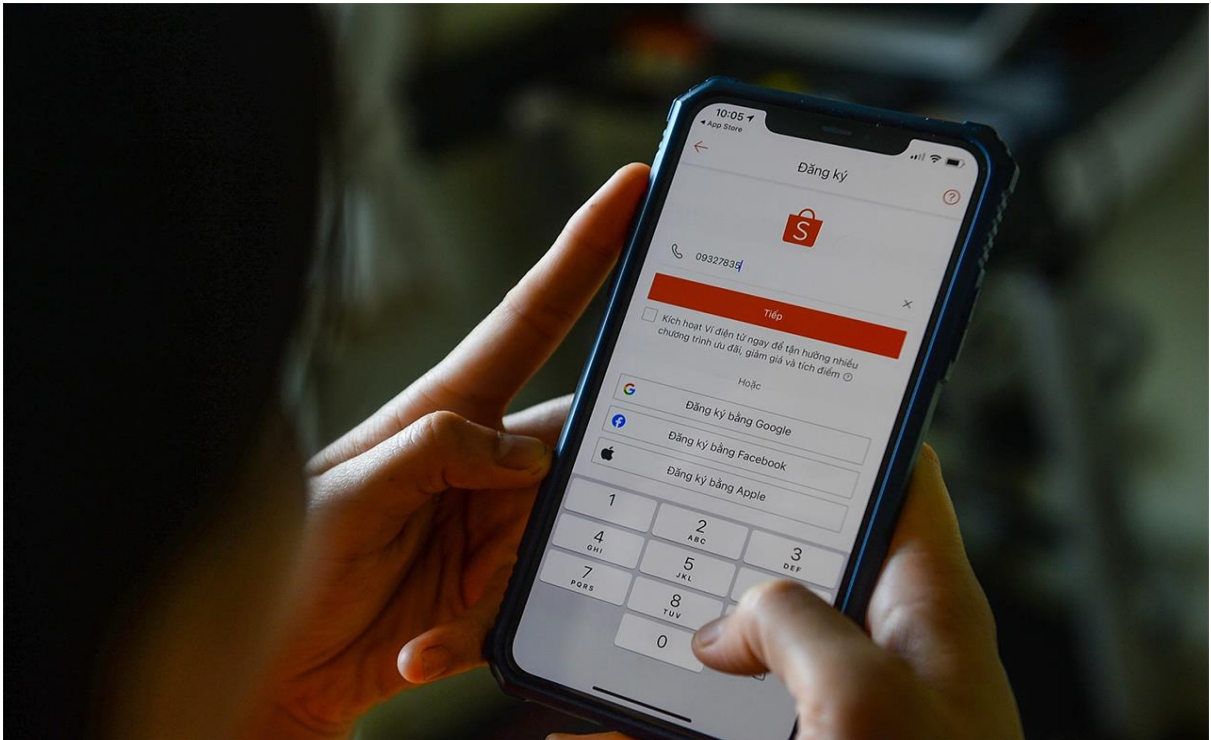


Cuối cùng, hãy tạo thói quen sao lưu dữ liệu quan trọng thường xuyên để phòng trường hợp thiết bị bị mất hoặc hư hỏng. Việc sao lưu dữ liệu sẽ giúp bạn khôi phục lại dữ liệu một cách nhanh chóng và dễ dàng nếu chẳng may xảy ra việc ngoài ý muốn.

4.4. Cảnh trọng trong việc mua sắm trực tuyến

Mua sắm trực tuyến mang đến nhiều tiện lợi, nhưng cũng tiềm ẩn nhiều rủi ro. Để bảo vệ thông tin cá nhân và tài khoản ngân hàng của mình, bạn cần đặc biệt chú ý đến vấn đề bảo mật khi thanh toán. Hãy luôn kiểm tra xem trang web mua sắm có biểu tượng khóa an toàn (hình ổ khóa nhỏ) và sử dụng giao thức HTTPS trước địa chỉ trang web.

Biểu tượng này cho biết thông tin bạn nhập vào, bao gồm số thẻ ngân hàng và các thông tin cá nhân khác, được mã hóa và truyền đi một cách an toàn, giúp ngăn chặn kẻ gian đánh cắp dữ liệu.



Bảo vệ dữ liệu cá nhân là một bước quan trọng để đảm bảo an toàn và sự riêng tư trong thế giới số hóa ngày nay. Bằng cách áp dụng các biện pháp bảo mật như sử dụng mật khẩu mạnh, cài đặt xác thực hai yếu tố và hạn chế chia sẻ thông tin nhạy cảm, bạn có thể giảm thiểu rủi ro bị tấn công mạng hay đánh cắp danh tính.

<https://www.thegioididong.com/tin-tuc/cach-bao-ve-du-lieu-ca-nhan-an-toan-1569761>

Tình huống và câu hỏi thảo luận:

Tình huống: Chị Hương là nhân viên kế toán, làm việc 8–9 tiếng/ngày trước máy tính.

Thói quen của chị: Ngồi hơi trượt người ra trước, lưng không chạm ghế, màn hình đặt thấp hơn tầm mắt, ít đứng dậy vận động, có khi ngồi liên tục 2–3 tiếng. Buổi tối về nhà vẫn dùng laptop làm thêm. Sau 6 tháng, chị bắt đầu: Đau mỏi cổ – vai – gáy kéo dài, đau lưng dưới, mỏi mắt, khô mắt, đôi khi tê bàn tay khi đánh máy lâu. Chị nghĩ rằng đây là “bệnh nghề nghiệp bình thường của dân văn phòng”.

Câu hỏi thảo luận:

Chị Hương đang gặp những vấn đề sức khỏe thể chất nào?

Những dấu hiệu nào cho thấy chị đang ngồi sai tư thế?

Tình trạng tê tay có thể liên quan đến hội chứng gì?

TÀI LIỆU THAM KHẢO

Nghị định 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ về Bảo vệ dữ liệu cá nhân.

<https://binhdanhocvuso.lamdong.gov.vn/bao-ve-du-lieu-ca-nhan-va-quyen-rieng-tu-tren-internet-N26.aspx>

<https://www.thegioididong.com/tin-tuc/cach-bao-ve-du-lieu-ca-nhan-an-toan-1569761>

<https://binhdanhocvuso.lamdong.gov.vn/quy-tac-dat-mat-khau-N25.aspx>