

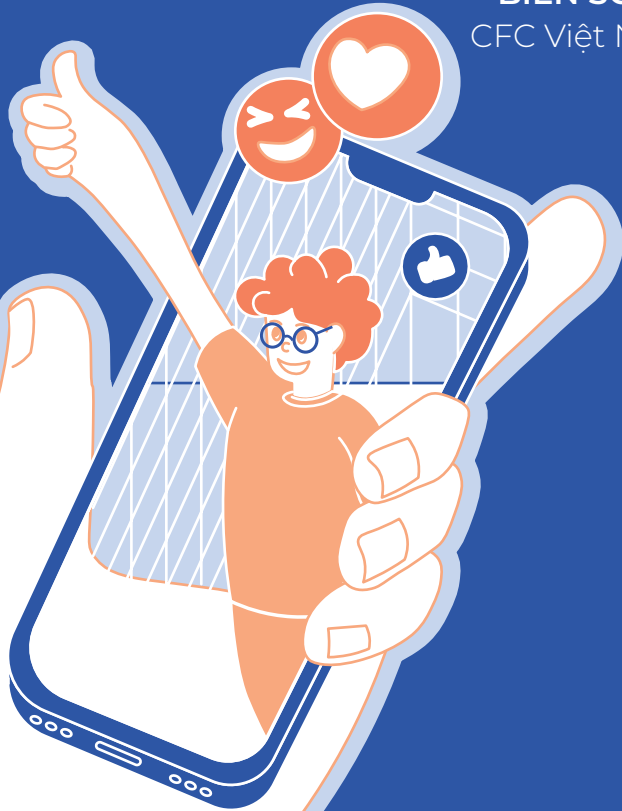
Cẩm nang



CÔNG DÂN SỐ VĂN MINH



BIÊN SOẠN:
CFC Việt Nam



MỤC LỤC

Từ viết tắt và giải thích một số thuật ngữ	3
Lời nói đầu	4
Giới thiệu bộ cẩm nang	6
Mục đích của cẩm nang	8
Nguyên tắc xây dựng cẩm nang	9
NỘI DUNG CẨM NANG	10
Bài 1: Chân dung một “Công dân số văn minh”	10
Bài 2: Quy tắc tôn trọng, tuân thủ pháp luật	22
Bài 3: Quy tắc trách nhiệm	32
Bài 4: Quy tắc an toàn, bảo mật thông tin	50
Bài 5: Quy tắc ứng xử lành mạnh	62
Bài 6: Sống thật trên mạng ảo	76
Bài 7: Quản lý thời gian trên mạng	92
Bài 8: Một số hình thức lừa đảo/mạo danh trên mạng phổ biến	104
Bài 9: Nguyên tắc vàng phòng tránh lừa đảo/mạo danh trên mạng	114
TÀI LIỆU THAM KHẢO	122
Phụ lục	122

Từ viết tắt và giải thích một số thuật ngữ

111	Tổng đài điện thoại quốc gia bảo vệ trẻ em
Block	Chặn
Chat	Tán gẫu
Comment	Bình luận
Email	Thư điện tử
Fake news	Thông tin sai lệch/ Tin giả
Flag	Lưu ý/cảnh báo
Ignore	Lờ đi
Like	Thích (chức năng thể hiện cảm xúc trên mạng xã hội)
Livestream	Truyền trực tiếp
CFC	Trung tâm Sức khỏe Gia đình & Phát triển Cộng đồng
New feed	Bảng tin
Nickname	Biệt danh
Search engine	Công cụ tìm kiếm
Selfie	Ảnh tự chụp/ Chụp ảnh “tự sướng”
Share	Chia sẻ (chức năng chia sẻ thông tin)
Webcam	Thiết bị ghi hình kĩ thuật số được kết nối với máy tính để truyền trực tiếp hình ảnh
Website	Trang điện tử
MXH	Mạng xã hội

LỜI NÓI ĐẦU

Việt Nam là quốc gia có dân số sử dụng Internet tích cực nhất trên thế giới, với 69 triệu người dùng Internet tính đến tháng 1 năm 2021, chiếm **70,3%** tổng dân số. Việt Nam cũng có **72 triệu** tài khoản mạng xã hội. **Do đại dịch covid-19**, với nhiều người làm việc và giao dịch trực tuyến hơn, lừa đảo và gian lận trực tuyến cũng gia tăng. Mọi người chia sẻ tin tức mà chưa có nhận thức và thói quen kiểm tra nguồn thông tin cũng như độ tin cậy, xác thực của thông tin. Trong trường học, nội dung về quyền công dân số nói chung và an toàn trực tuyến nói riêng vẫn chưa được đưa vào chương trình giảng dạy chính thức. Nội dung và video giáo dục, các chương trình về an toàn Internet và trách nhiệm kỹ thuật số hiện có ở Việt Nam còn giới hạn.

Trong bối cảnh đó, **CFC Việt Nam**, tổ chức tiên phong trong đào tạo an toàn trực tuyến và giáo dục kỹ năng an toàn trên mạng với kinh nghiệm đào tạo cho hàng ngàn giáo viên và trường học tại Việt Nam đã khởi động một sáng kiến hướng tới công dân số văn minh cho thanh niên Việt Nam. Dự án được hỗ trợ bởi Google.org và triển khai thực hiện bởi CFC Việt Nam. Mục tiêu của dự án hướng tới:

1. Nâng cao nhận thức về trách nhiệm số cho người dùng Internet tại Việt Nam;
2. Nâng cao kiến thức về ảnh hưởng và dấu ấn kỹ thuật số của người dùng Internet cho thanh niên Việt Nam
3. Giúp người dùng Internet nhận ra tin tức giả mạo và ngăn chặn gian lận và lừa đảo trực tuyến;

Đến cuối năm 2022 dự án kì vọng tiếp cận và nâng cao nhận thức cho 1 triệu người dùng Internet trẻ tuổi, đặc biệt là thanh niên và sinh viên Việt Nam. Dự án sẽ được triển khai thực hiện với 3 nội dung (1) Phòng tránh lừa đảo trên mạng; (2) Ứng xử văn minh trên mạng và (3) Sống thật trên mạng ảo. Các nội dung này được thể hiện qua 3 hoạt động chính là hoạt động đào tạo, tập huấn; tổ chức chiến dịch sáng tạo video clip dài 1 phút với nội dung cổ động thanh thiếu niên Việt Nam thực hiện công dân mạng văn minh và thứ ba là sản xuất và lan tỏa các video clip, bài hát tuyên truyền với các chủ đề nội dung của dự án.

Thông tin về hoạt động dự án, video clip được công bố và cập nhật trên trang web của dự án: <https://congdansovanminh.com/>



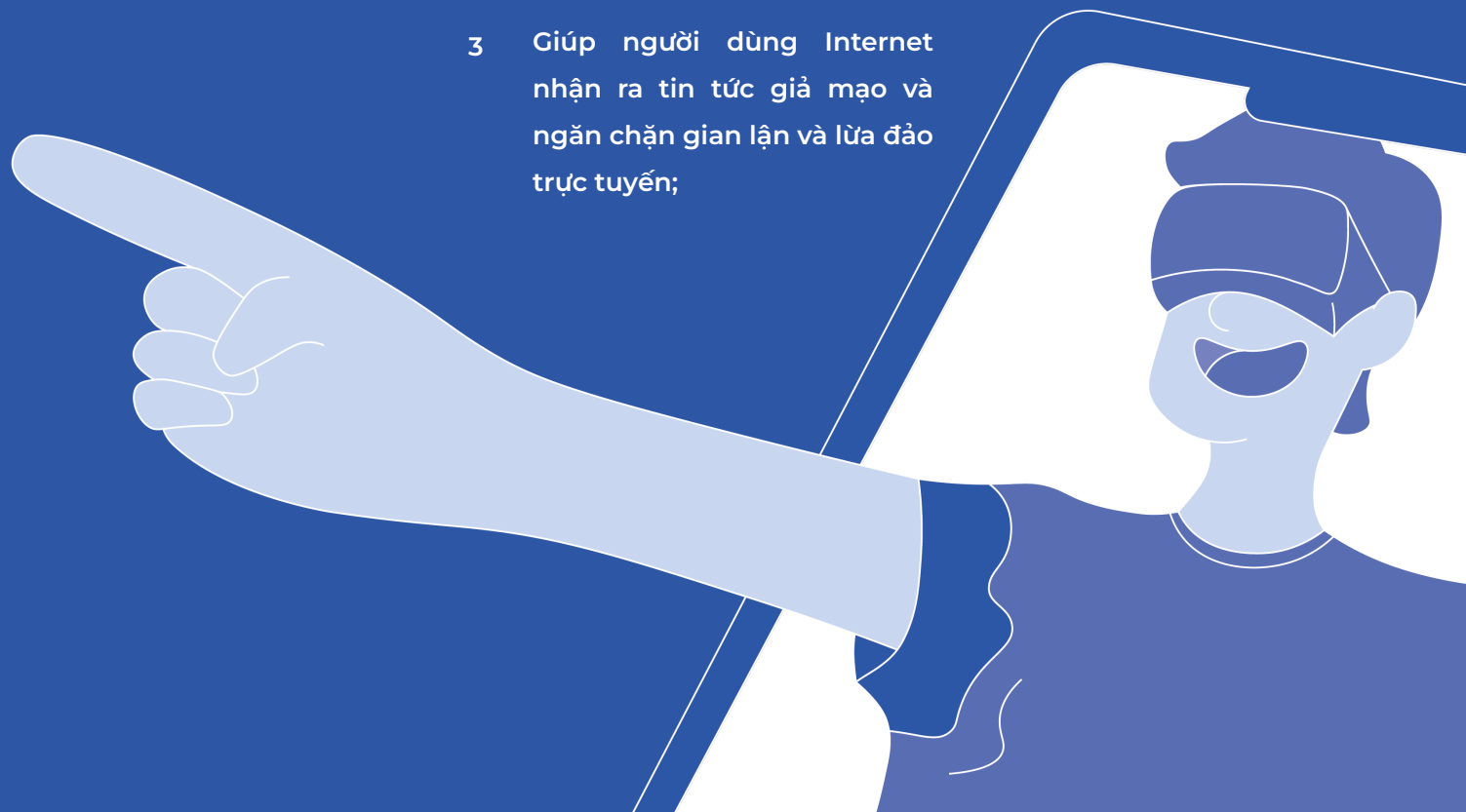
GIỚI THIỆU BỘ CẨM NANG

Mục đích của cẩm nang

Trong khuôn khổ dự án “**Công dân số văn minh**”, với sự tài trợ của Google.org, Trung tâm Sức khỏe Gia đình & Phát triển Cộng đồng (CFC) thực hiện cuốn Cẩm nang “Công dân số văn minh” với mong muốn được chia sẻ và hướng dẫn những kinh nghiệm, bí kíp và cả những khuyến khích để các bạn thanh thiếu niên sẵn sàng, chủ động đối mặt với các thách thức của thời đại công nghệ, và có những trải nghiệm an toàn và tuyệt vời cùng Internet.

Cẩm nang “Công dân số văn minh” tập trung đến đối tượng là các bạn thanh thiếu niên Việt Nam, cung cấp những kiến thức, kĩ năng về bộ quy tắc ứng xử của thanh niên Việt Nam trong thời đại công nghệ kĩ thuật số với mục tiêu hướng tới:

1. Nâng cao nhận thức về trách nhiệm số cho người dùng Internet tại Việt Nam;
2. Nâng cao kiến thức về ảnh hưởng và dấu ấn kĩ thuật số của người dùng Internet cho thanh niên Việt Nam
3. Giúp người dùng Internet nhận ra tin tức giả mạo và ngăn chặn gian lận và lừa đảo trực tuyến;



NGUYÊN TẮC

XÂY DỰNG CẨM NANG

- ✔ Dựa trên Bộ quy tắc ứng xử trên mạng xã hội của Bộ Thông tin và truyền thông.
- ✔ Dựa trên thực tế những vấn đề thường gặp của thanh thiếu niên khi tương tác trên mạng Internet như bị bắt nạt, lừa đảo, sống ảo...
- ✔ Dựa trên những nghiên cứu và tham khảo các tài liệu trong và ngoài nước, những thực hành tốt trên mạng Internet.

NỘI DUNG CẨM NANG

- ✔ Cẩm nang gồm 9 bài về các nội dung xây dựng nên một công dân số văn minh.
- ✔ Nội dung cẩm nang đa dạng, xoay quanh hai phần chính là kiến thức và kỹ năng, được thể hiện qua các phần như Kiến thức chung, Hiểu biết về pháp luật, Ứng xử văn minh trên mạng, Sống thật trên mạng, Phòng tránh lạm bẫy trên mạng và đưa ra một số kiến thức cần biết, tài liệu tham khảo để các bạn thanh thiếu niên có thể có hướng nghiên cứu thêm.

CẤU TRÚC 1 BÀI

GỒM CÓ:

- 1 **Câu hỏi thảo luận**
- 2 **Các định nghĩa/khái niệm chính**
- 3 **Nội dung chính:** gồm phần lý thuyết và/hoặc các bí kíp, kỹ năng, tình huống, câu chuyện
- 4 **Suy ngẫm:** gồm một số câu hỏi tình huống, bài tập vận dụng hay hoạt động gợi ý.

Bài

01

Chân dung một CÔNG DÂN SỐ VĂN MINH

1. Đặt vấn đề

Chuyển đổi số đang là một xu hướng được rất nhiều người quan tâm. Việt Nam cũng nằm trong xu hướng này với mục tiêu chuyển đổi số dựa trên 3 trụ cột: Xã hội số, Kinh tế số và Chính phủ số. Trong đó, xã hội số được hình thành từ những công dân số. Vậy công dân số là gì? Chân dung của một công dân số văn minh sẽ như thế nào?



01 02 03 04 05 06 07 08 09

<https://congdansovanminh.com/>

2. Khái niệm chính

Công dân kỹ thuật số (Công dân số)

Một công dân kỹ thuật số hay công dân số là người có kỹ năng sử dụng công nghệ thông tin để giao tiếp với người khác, tham gia vào các hoạt động xã hội, kinh doanh và chính trị trên nền tảng kỹ thuật số. Công dân số là người có kỹ năng, kiến thức và có thể truy cập Internet thông qua máy tính, điện thoại di động và các thiết bị kỹ thuật số khác để tương tác với cá nhân, tổ chức và cộng đồng.



3. Nội dung

3.1. Các đặc điểm chính của công dân số

Trong một thế giới số, công dân số có thể sử dụng các quyền công dân và thực hiện nghĩa vụ công dân của họ, am hiểu pháp luật và nắm được các quy định được phép hay cấm thực hiện. Không phải bất kì ai sử dụng Internet cũng là công dân số. Đặc điểm để xác định một công dân số được mô tả dưới đây:

a) Đạt trình độ nhất định về Công nghệ



Công dân số chắc chắn là những người hiểu biết về công nghệ. Họ có kiến thức về phần cứng như máy tính, máy tính bảng, điện thoại thông minh và phần mềm, ứng dụng đi kèm cũng như kỹ năng sử dụng thiết bị điện tử. Họ sử dụng công nghệ và Internet hỗ trợ cho các hoạt động học tập và làm việc của mình. Nói đến công dân số là nói đến sự thông minh, hiện đại, cập nhật và hiểu biết công nghệ thông tin trong cuộc sống, từ cấp địa phương đến cấp quốc gia, toàn cầu.

b) Hiểu được thực tế của thế giới ảo và văn hóa số



Nhận thức rằng một thế giới ảo trong đó thế giới thực đang được mô phỏng, văn hóa trong thế giới thực đang được tạo ra và mở rộng trên môi trường số. Công dân số gắn kết với thiết bị di động và luôn có nhu cầu những thiết bị này được tối ưu, ví dụ như nhanh hơn, nhỏ hơn, chính xác hơn, mới hơn, hoàn hảo hơn, thú vị hơn, ít nguy hiểm và sở hữu công nghệ mới hơn. Mọi thứ công dân số tiếp cận trong thế giới thực sẽ tiếp tục được số hóa và được gọi là sản phẩm kỹ thuật số.

c) Có khái niệm sâu rộng về Internet



Internet có nhiều ý nghĩa và chức năng hơn việc là một cánh cổng của một thế giới ảo chỉ giúp làm giảm thời gian thực thi công việc hoặc một nguồn lưu trữ. Môi trường Internet được xác định bởi tốc độ, kết nối, tổ chức, kỹ năng giao tiếp, tương tác, kiểm soát, quản lý, giám sát và thiết kế, chia sẻ với nguồn nội dung đa dạng, phong phú.

Công dân số thường xuyên sử dụng nền tảng kỹ thuật số và cơ sở dữ liệu như tài liệu, thư viện điện tử trong nghiên cứu và học thuật. Phần lớn các nhà nghiên cứu về văn hóa số sẽ làm việc trong các lĩnh vực như Internet, truyền thông xã hội, truyền thông kỹ thuật số, ngoại giao, thương mại và xuất bản. Do đó, Internet được chuyển đổi thành một nền tảng để chia sẻ và truy cập thông tin với nguồn tri thức và dữ liệu vô cùng phong phú, đa dạng.

d) Trách nhiệm và đạo đức thông tin



Đạo đức thông tin bao gồm các quy tắc mà tất cả người dùng Internet và người dùng máy tính cá nhân phải tuân theo. Công dân số cần có đạo đức vì họ tự do lựa chọn sở thích trên môi trường số và có trách nhiệm trong việc lựa chọn hành động của mình như khi tích vào đường dẫn, nhấp vào từng biểu tượng, truy cập từng trang web và nhập mọi mật khẩu của mình trên mạng.

đ) Hiểu biết về luật truyền thông số và cần trọng trong giao tiếp



Công dân số hiểu biết về các phương thức hạn chế truy cập, cấm xuất bản, trình bày và tiêu thụ nội dung bị cấm (nội dung tiêu cực, tin tặc, tài liệu độc hại, v.v.), vi phạm an ninh quốc gia, gây chia rẽ, ngôn từ kích động thù địch, vi phạm quyền lợi và tự do. Công dân số cũng biết về quyền hạn trong thế giới số và thực thi chúng, như là viết blog, bình luận về tin tức, thư từ, phê bình, thực hiện thương mại, được đào tạo, tạo nhóm, trở thành thành viên của nhóm, tạo và đóng tài khoản, đồng thời đảm bảo an toàn cho dữ liệu cá nhân được lấy từ các tổ chức cung cấp dịch vụ lưu trữ.

e) Tích cực với truyền thông xã hội đa phương tiện



Công dân số có các tài khoản mạng xã hội như Twitter, YouTube, LinkedIn, ... nhưng bản chất đặc biệt của công dân số không hẳn là người dùng tích cực trên mạng xã hội, nó tùy thuộc vào phong cách sử dụng mạng xã hội của họ. Tích cực ở đây là một cách thức trong hành động như chú ý đến các vấn đề của địa phương, quốc gia và toàn cầu, đặc điểm chính trị, nghệ thuật, văn học, khoa học ...

Quá trình thực hiện một công việc của công dân số trở thành thông tin, có thể được thêm vào sự nghiệp cá nhân của công dân số và dĩ nhiên là bao gồm cả tiền án, tiền sự. Mạng xã

hội là một phần không thể thiếu của nhận dạng kỹ thuật số và thể hiện bản sắc, tính cách của con người một cách rõ ràng. Khả năng hiển thị và nhận dạng này ít nhiều liên quan đến việc công dân chia sẻ thông tin cá nhân trong thực tế.

g) Nhận thức được sự tôn trọng quyền riêng tư trên mạng



Người đằng sau màn hình, không phải là người ngoài cuộc dù họ là thật hay giả và tất cả họ đều bình đẳng với quyền công dân. Người dùng là thật ngay cả khi tài khoản của họ là giả và Internet vẫn được sử dụng bởi người dùng thực.

Tính chất nhạy cảm và pháp lý của truy vết trên Internet, camera giám sát, điện thoại di động, thiết bị ghi âm giọng nói và ghi âm camera ẩn, giọng nói của một người và màn hình hiển thị có thể được coi là riêng tư đối với người không thích sự giám sát và tất cả các loại ghi âm trái phép. Tất cả những hành vi lăng mạ, xuyên tạc, xúc phạm, truyền tải các dấu hiệu, biểu tượng, ghi âm v.v. cần phải được quy định rõ ràng như trong các quan hệ xã hội thực tế.

h) Ủng hộ việc tham gia xã hội một cách tự chủ



Hai cơ hội tăng cường sự tham gia hoạt động nhà nước đã được tạo ra. Đầu tiên, công dân có thể được thông báo về quyết định đã được thực hiện hoặc sẽ được đưa ra trên mạng xã hội một cách nhanh chóng. Thứ hai, công dân có thể truyền đạt ý kiến của họ về những quyết định đã được thực hiện hoặc sẽ được thực hiện mà không mất nhiều thời gian hoặc phải gặp tận nơi nhà chức trách, theo cách tự do và nhanh chóng hơn. Hai cơ hội này cần đi kèm với các tính chất như tính minh bạch, tính tương tác, giao tiếp tức thì và các kênh phản hồi điện tử được giữ ở chế độ mở.

Giao tiếp thuận lợi hơn khi có cơ hội được đại diện bởi Công nghệ thông tin và truyền thông. Các thủ tục chính thức đã được tự động hóa và do đó ngăn chặn được nhiều sự trùng lặp. Dữ liệu phân tán và khó truy cập trở nên phổ biến hơn và có hệ thống lưu trữ tập trung. Việc bảo lưu, truy cập dữ liệu và thông tin chính thức trở nên dễ dàng. Do đó, tính hiệu quả, năng suất của hành chính công tăng lên. Chính phủ số thông qua Internet để trở nên nhanh hơn, minh bạch hơn, có trách nhiệm hơn đối với hành động của mình.

Các chính phủ sẽ hoạt động hiệu quả hơn khi ghi lại mọi kết quả phát triển kinh tế xã hội, có thể phân tích những chia sẻ và tích lũy trong cơ sở dữ liệu kỹ thuật số (hình ảnh, video, tuyên bố, trích dẫn, ý kiến, lượt thích, trang web đã truy cập, nội dung đã đọc, thời gian trực tuyến, sản phẩm đã tiêu dùng, v.v.) và tìm hiểu các quan điểm chính trị của công dân. Theo dõi và giải thích các dấu vết của công dân số là một phương pháp dự đoán hiệu quả cho chính phủ và nhà đầu tư.

Một công dân số văn minh có đầy đủ đặc điểm của một công dân số và cũng có các quy tắc ứng xử, chuẩn mực đạo đức, hành vi của con người trong môi trường số. Bộ quy tắc chung của một công dân số văn minh bao gồm các tiêu chí sau:

- ✓ Ứng xử văn minh trên mạng
- ✓ Sống thật trên mạng
- ✓ Phòng tránh chàm bẫy trên mạng

Chúng ta sẽ cùng tìm hiểu chi tiết trong các nội dung tiếp theo.

4. Suy ngẫm

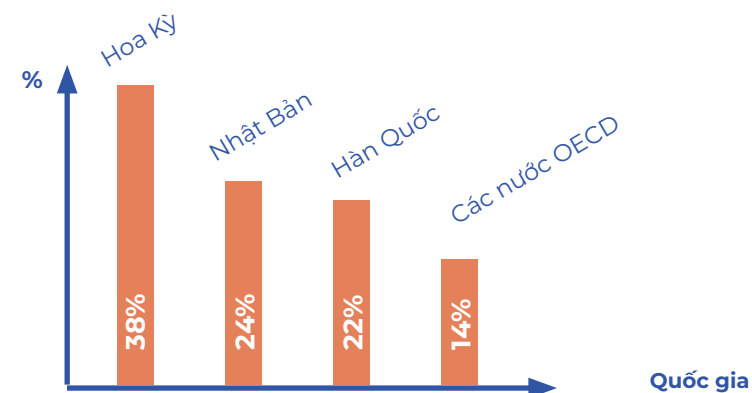
Sinh viên thời đại 4.0 phải nghĩ khác, làm khác.

Tại Đại hội đại biểu Hội Sinh viên Việt Nam TP.HCM năm 2020, vấn đề sinh viên thời 4.0 cần chuẩn bị gì để có thể tham gia vào cuộc cách mạng công nghiệp lần thứ 4, đã được đặt ra như một định hướng quan trọng.

PGS-TS Vũ Hải Quân cho biết: **“Theo dự báo của tổ chức McKinsey công bố năm 2018 đến năm 2030:**

70% công ty khắp thế giới sẽ sử dụng trí tuệ nhân tạo và GDP toàn cầu sẽ tăng 13 nghìn tỷ USD.

Đến năm 2030, tỷ lệ tự động hóa đối với tất cả các công việc ở Hoa Kỳ sẽ là 38%, ở Nhật Bản là 24% và ở Hàn Quốc là 22% và trung bình ở các nước thuộc OECD (Tổ chức hợp tác và phát triển kinh tế) sẽ là 14%.



Tỷ lệ tự động hóa công việc tại các nước (2030)

Điều này có nghĩa là:

“Nhiều việc làm sẽ được tự động hóa, robot hóa, tỷ lệ thất nghiệp sẽ gia tăng”.

Đình Thanh Toàn, sinh viên năm 3 ngành khoa học máy tính, Trường ĐH Công nghệ thông tin – ĐH Quốc gia TP.HCM, đã chia sẻ: “Là sinh viên thì càng không thể đứng ngoài cuộc. Vì thế, ngay từ bây giờ sinh viên tụi em phải chuẩn bị tâm thế để sẵn sàng tham gia vào cuộc cách mạng công nghiệp 4.0. Để không bị tụt lại phía sau, không bị đào thải, em nghĩ mỗi bạn phải tự mình cập nhật thêm những tri thức mới, kỹ thuật, công nghệ mới của nhân loại. Đồng thời để cao tinh thần sáng tạo, tìm tòi, học hỏi để có thể áp dụng được những kiến thức mới đó vào đời sống thực tế”. Bên cạnh đó sinh viên phải năng động, trải nghiệm thật nhiều mới đón nhận và rèn luyện được những kỹ năng mới. Bản thân Toàn tham gia rất nhiều hoạt động thiện nguyện vì cộng đồng như Xuân tình nguyện, Mùa hè xanh... Từ đó, các kỹ năng như làm việc nhóm, quản lý thời gian, xử lý tình huống... được nâng cao rõ rệt. Không những thế còn giúp Toàn nhận ra vai trò của mỗi cá nhân trong cộng đồng và có ý thức trách nhiệm hơn với xã hội.

Nguồn: Sinh viên thời 4.0 phải nghĩ khác, làm khác!

Mỹ Uyên- Báo điện tử Thanhnien.vn



Lật qua để xem nội dung tiếp theo

Bài

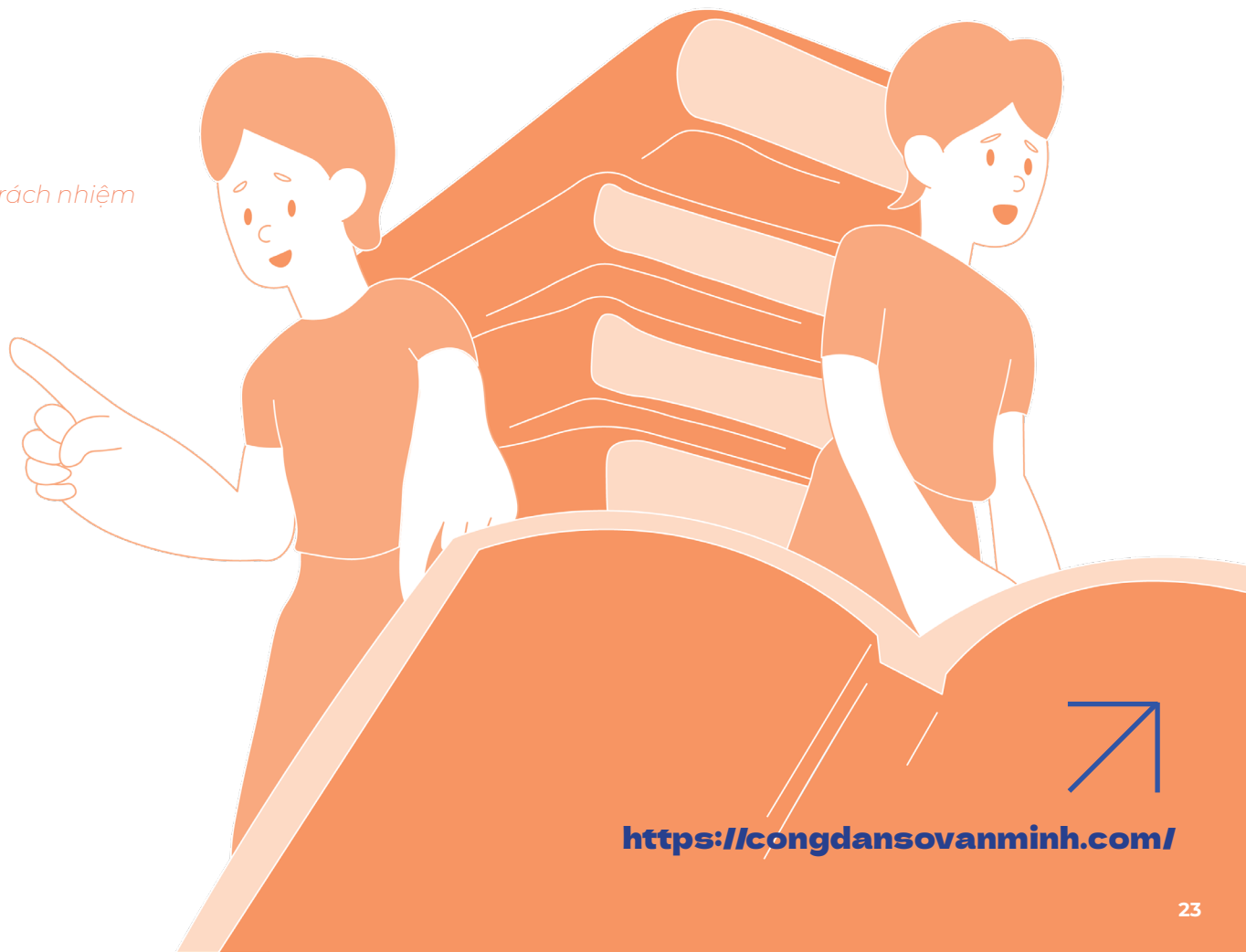
02

QUY TẮC TÔN TRỌNG, TUÂN THỦ PHÁP LUẬT

1. Câu hỏi thảo luận/Đặt vấn đề:

Với vai trò là một công dân số, liệu bạn đã hiểu rõ quyền và trách nhiệm của mình trên môi trường mạng chưa?

Hiểu biết quy định của pháp luật về các hoạt động trên môi trường mạng, tôn trọng và tuân thủ pháp luật về các hoạt động trên môi trường mạng là quy tắc đầu tiên của Ứng xử văn minh trên mạng.



2. Khái niệm chính

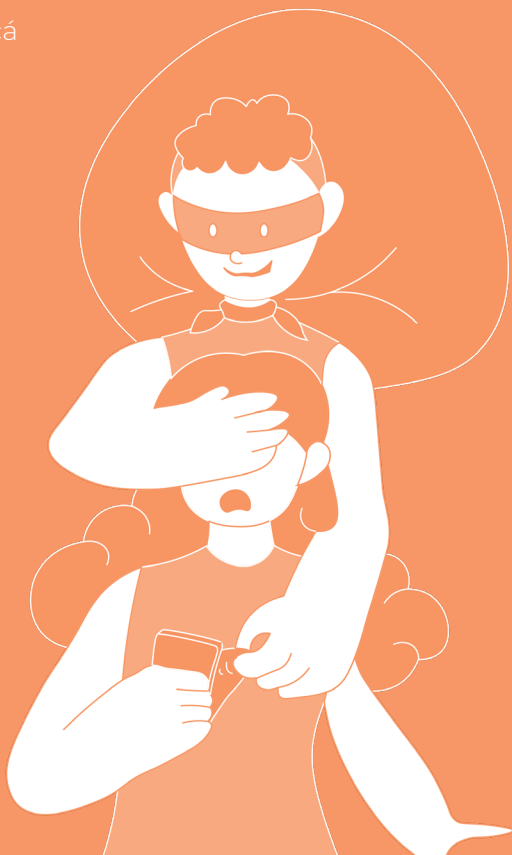
An ninh mạng & Bảo vệ an ninh mạng

2.1. An ninh mạng

An ninh mạng là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2.2. Bảo vệ an ninh mạng

Bảo vệ an ninh mạng là phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng.



3. Nội dung

3.1. Quyền lợi của công dân số

Luật An ninh mạng 2018 với 7 chương, 43 điều quy định cụ thể về việc bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; các biện pháp phòng ngừa, xử lý hành vi xâm phạm an ninh mạng; hoạt động bảo vệ an ninh mạng; các lực lượng trực tiếp tham gia vào việc bảo vệ an ninh mạng; trách nhiệm của các cơ quan, tổ chức, cá nhân và các điều khoản thi hành của Luật an ninh mạng.

Luật An ninh mạng 2018 bảo vệ 06 quyền con người sau đây:



Quyền sống, quyền tự do cá nhân;



Quyền bình đẳng trước pháp luật và được pháp luật bảo vệ;



Quyền không bị can thiệp vào đời tư, gia đình, chỗ ở hoặc thư tín;



Quyền không bị xâm hại danh dự hay uy tín cá nhân;



Quyền tự do tư tưởng, tín ngưỡng và tôn giáo của công dân;



Quyền tự do ngôn luận, tự do biểu đạt của công dân.

Công dân số cần hiểu biết về vấn đề đạo đức, nhận thức và pháp lý do mọi hành động diễn ra trên môi trường số có thể được ghi lại và truy vết.

Công dân số liên tục được khuyến khích, ủng hộ tham gia và được đáp ứng với nhiều cơ hội mới. Tham gia vào mạng xã hội, mạng lưới của tổ chức nào đó, viết ý kiến, đưa ra nhận xét, tham gia một cuộc khảo sát số và bỏ phiếu, v.v. Nhiều công việc khác cũng bắt buộc công dân tham gia thông qua môi trường kỹ thuật số. Môi trường kỹ thuật số được tạo ra và hoạt động diễn ra liên tục với sự tham gia của công dân là tự nguyện. Công dân không cần phải viết đơn và giải thích lý do họ rời đi. Tham gia vào một nhóm hoặc từ bỏ nó là tự nguyện và miễn phí.

3.1. Quyền lợi của công dân số

Công dân số là một thành phần của công dân toàn cầu, họ có quyền tự do lựa chọn trong hành động và do đó chịu trách nhiệm về lựa chọn của mình. Công dân số cần biết rằng họ có thể phải nhận thiệt hại từ người khác và có thể gây tổn hại cho người khác khi đang trực tuyến. Nghĩa vụ pháp lý trong thế giới số thuộc về họ. Luật pháp kỹ thuật số nhất thiết phải được tuân thủ và nguyên tắc đạo đức phải được tuân theo một cách tự nguyện.

Theo Điều 42 Luật An ninh mạng 2018 thì cơ quan, tổ chức, cá nhân sử dụng không gian mạng có trách nhiệm:

- ✔ **Tuân thủ quy định** của pháp luật về an ninh mạng;
- ✔ **Kịp thời cung cấp thông tin** liên quan đến bảo vệ an ninh mạng, nguy cơ đe dọa an ninh mạng, hành vi xâm phạm an ninh mạng cho cơ quan có thẩm quyền, lực lượng bảo vệ an ninh mạng;
- ✔ **Thực hiện yêu cầu và hướng dẫn của cơ quan có thẩm quyền** trong bảo vệ an ninh mạng; giúp đỡ, tạo điều kiện cho cơ quan, tổ chức và người có trách nhiệm tiến hành các biện pháp bảo vệ an ninh mạng.

Bên cạnh đó pháp luật hiện hành của Việt Nam cũng bảo vệ dữ liệu, thông tin cá nhân và quyền riêng tư (Theo Cục Quản lý mật mã dân sự và kiểm định sản phẩm mật mã tổng hợp năm 2020).

Bảng tóm tắt:

STT	Tên văn bản	Năm phát hành	Nội dung liên quan
1	Hiến pháp Việt Nam	2013	Nguyên tắc bất khả xâm phạm về đời sống riêng tư và bí mật cá nhân
2	Bộ luật dân sự	2015	Khái niệm và quyền dân sự được bảo vệ liên quan đến về đời sống riêng tư, bí mật cá nhân và bí mật gia đình.
3	Luật Giao dịch điện tử	2005	Nguyên tắc bảo mật trong của các bên tham gia các giao dịch điện tử, trách nhiệm quản lý nhà nước bảo đảm thực hiện quyền, nghĩa vụ của các bên.
4	Luật Công nghệ thông tin	2006	Chính sách nhà nước, quyền và nghĩa vụ của các bên trong phát triển hạ tầng công nghệ thông tin.

STT	Tên văn bản	Năm phát hành	Nội dung liên quan
5	Luật An toàn thông tin mạng	2006	Quyền, trách nhiệm của các bên trong việc bảo đảm an toàn thông tin mạng; mật mã dân sự; tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin mạng; kinh doanh trong lĩnh vực an toàn thông tin mạng; quản lý nhà nước về an toàn thông tin mạng
6	Luật Viễn thông	2009	Chính sách phát triển hạ tầng viễn thông quốc gia, kinh doanh dịch vụ viễn thông
7	Luật Khám bệnh, chữa bệnh	2009	Bảo vệ bí mật về hồ sơ, thông tin sức khỏe, y tế của công dân.
8	Luật Quản lý thuế	2006	Bảo vệ bí mật tài chính về thu nhập và nộp thuế của công dân.
9	Luật các Tổ chức tín dụng	2010	Bảo vệ bí mật tài khoản và giao dịch tài khoản của công dân.

STT	Tên văn bản	Năm phát hành	Nội dung liên quan
10	Luật Kinh doanh bảo hiểm	2000	Bảo vệ bí mật về hợp đồng bảo hiểm.
11	Luật Bảo hiểm xã hội	2014	Bảo vệ bí mật, chống truy cập dữ liệu bảo hiểm bất hợp pháp.
12	Bộ luật Hình sự	2015	Áp dụng chế tài hình sự đối với tội phạm mạng, tội phạm công nghệ cao, xâm phạm bí mật đời tư.
13	Bộ luật tố tụng hình sự	2015	Quyền của các cơ quan tố tụng trong điều tra tội phạm, yêu cầu cung cấp thông tin thuộc bí mật đời tư, bí mật cá nhân và bí mật gia đình.

4. Suy ngẫm



The image shows a social media post interface. At the top left is a profile picture of a person and the name "user_name" with "now" underneath. To the right of the name are three dots. The main text of the post is in Vietnamese, discussing the impact of the internet on information spread and the importance of digital citizenship. Below the text is a row of six reaction icons: a thumbs up, a heart, a laughing face, a surprised face, a sad face with a tear, and an angry face. At the bottom of the post are three buttons: "Like" with a thumbs up icon, "Comment" with a speech bubble icon, and "Share" with a share icon.

user_name
now

Internet là công cụ giao tiếp quan trọng, lan truyền cả thông tin truyền cảm hứng, tích cực và cả những ý kiến tiêu cực, bình luận gây sốc. Nhưng, Internet lại không có khả năng phân biệt tin tốt và tin xấu. Mà chỉ có người dùng mới có khả năng đó. Hãy suy nghĩ về cách ứng xử trực tuyến của bản thân qua văn bản, bài đăng, bình luận, hình ảnh, và video của mình xem có đang tuân thủ theo các quy định của pháp luật hiện hành và văn minh, phù hợp văn hóa hay chưa?

Like Comment Share



Lật qua để xem nội dung tiếp theo

Bài

03

QUY TẮC TRÁCH NHIỆM

1. Câu hỏi thảo luận/Đặt vấn đề:

Những khái niệm như “dấu chân kỹ thuật số” hay “Danh tiếng trên mạng” có quen thuộc với bạn? Bạn đã thể hiện trách nhiệm trong các hoạt động trên mạng của mình (như đăng tải, chia sẻ hay lan truyền thông tin trên mạng) như thế nào?



2. Khái niệm chính

Dấu chân số, tin giả, danh tiếng và chia sẻ quá mức

2.1. Dấu chân kỹ thuật số (Dấu chân số)

Dấu chân kỹ thuật số của một người là tất cả thông tin về người đó xuất hiện trực tuyến, có thể bao gồm mọi dạng thông tin, từ hình ảnh, âm thanh, video, văn bản cho đến “lượt thích” và bình luận trên trang cá nhân của bạn bè người đó. Tương tự như khi chúng ta đi trên cát, khi hoạt động trên mạng, chúng ta cũng sẽ để lại dấu chân.

2.2. Danh tiếng trên mạng

Danh tiếng trên mạng có thể là danh tiếng của một công ty, cá nhân, sản phẩm hay dịch vụ những yếu tố khác trên Internet và những nền tảng số. Những danh tiếng này bị ảnh hưởng bởi nội dung mà tổ chức đưa ra, những hiệu ứng hay những tương tác với người dùng, những hành động hay mạng xã hội.

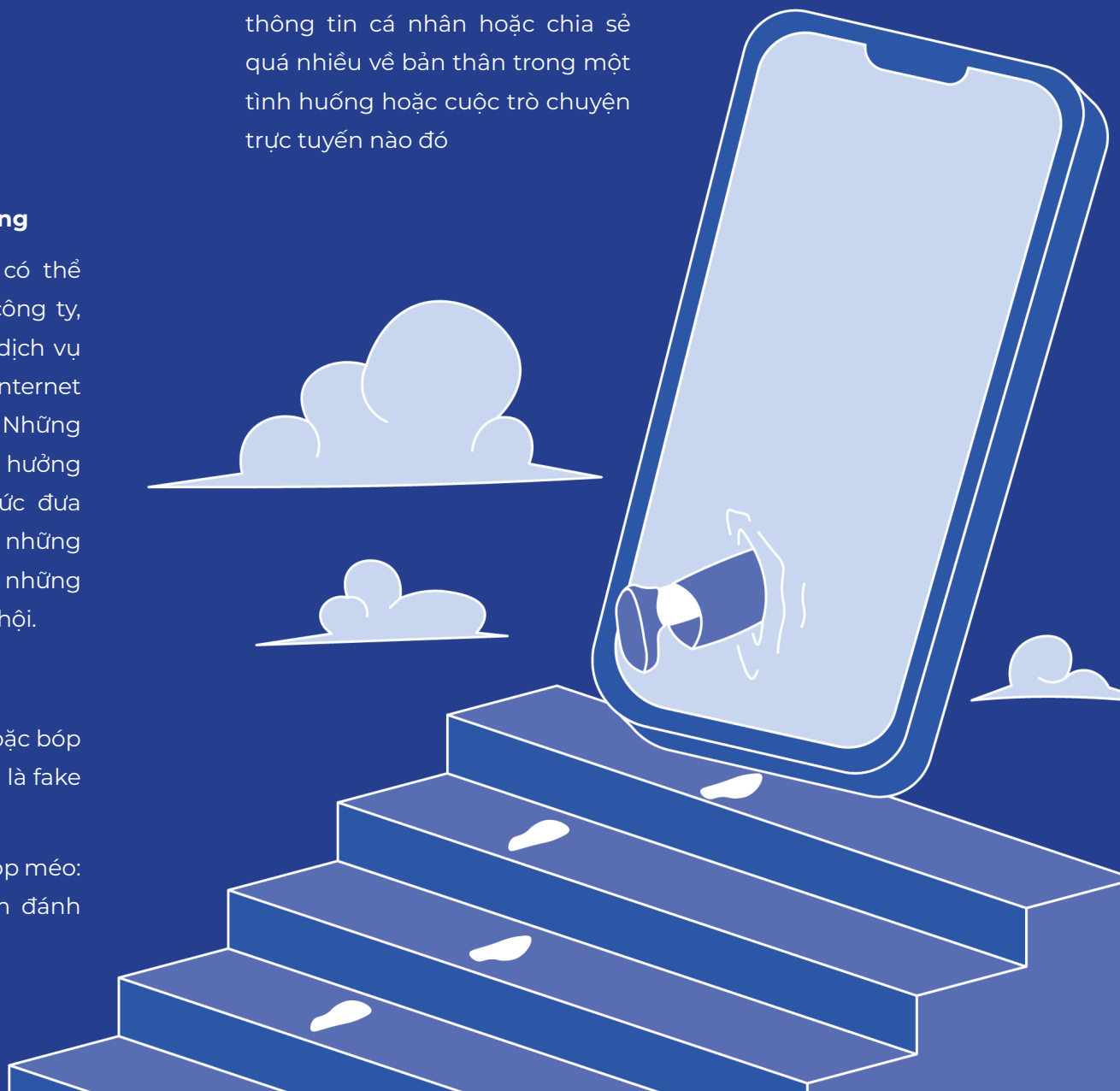
2.3. Tin giả

Tin giả: Tin tức lừa đảo hoặc bóp méo sự thật (hay còn gọi là fake news - tin tức giả mạo).

Thông tin bị xuyên tạc/bóp méo: Thông tin sai lệch nhằm đánh lừa hoặc gây hiểu lầm.

2.4. Chia sẻ quá mức

Chia sẻ quá mức khi trực tuyến - thường là chia sẻ quá nhiều thông tin cá nhân hoặc chia sẻ quá nhiều về bản thân trong một tình huống hoặc cuộc trò chuyện trực tuyến nào đó



3. Nội dung

3.1. Quản lý dấu chân kĩ thuật số & Kiểm soát danh tiếng trên mạng

a) Tầm quan trọng của danh tiếng trên mạng



Danh tiếng trên mạng là rất quan trọng, bởi vì nó có thể ảnh hưởng đến sự tín nhiệm và sống còn của một thương hiệu. Như một thương hiệu chuyên nghiệp, hình ảnh thương hiệu cá nhân có thể tạo ra ảnh hưởng, tương tác tích cực hay tiêu cực tới bạn một ngày nào đó nếu bạn không chú ý. Ngoài ra danh tiếng cá nhân trên mạng cũng có tầm ảnh hưởng quan trọng đến sự sống còn, phát triển nhưng khác ở đây là phạm vi cá nhân.

Những thông tin làm nên danh tiếng của bạn như: giải thưởng, chứng nhận, sự kiện của bạn được lên báo, trang cá nhân trên mạng xã hội của bạn, ... Những điều này có thể xuất hiện dễ dàng dựa vào kết quả tìm kiếm trên Google.

Danh tiếng trên mạng xã hội là vô cùng quan trọng. Những con số sau sẽ minh chứng cho điều này:

70% người quản lý tuyển dụng đã từ chối một ứng cử viên vì một chuyện hay điều nào đó họ tìm thấy trực tuyến (*Cross-Tab*).

97% mọi người đọc các đánh giá trực tuyến khi tìm kiếm một doanh nghiệp địa phương (*BIA Kelsey*)

b) Bảo vệ chính mình và danh tiếng của mình khỏi mối họa trên mạng.



80% Hơn 80% thiệt hại danh tiếng đến từ sự không phù hợp giữa tiếng vang và thực tế (*Digimind*).

2/3 số lượng người khảo sát cho rằng Internet là nguồn thông tin đáng tin cậy nhất về một người hoặc một doanh nghiệp (*Edelman Insights*).

SUY NGHĨ HAI LẦN TRƯỚC KHI ĐĂNG.

Khi dùng mạng Internet/mạng xã hội, phải suy nghĩ kỹ trước khi có tương tác gì là cách phòng thủ tốt nhất. Hãy suy nghĩ theo cách cảm thông, đồng cảm với người khác thậm chí là với người mà bạn không biết. Bằng cách này sẽ hạn chế những hình ảnh xấu như những ngôn từ không phù hợp hay các bài đăng không có cùng quan điểm với người khác mà có thể là sếp tương lai của bạn.

DỌN DỆP NHỮNG NỘI DUNG TRÊN MẠNG XÃ HỘI TRONG QUÁ KHỨ.

Nếu bạn phát hiện bạn có những bài viết cũ và không được tốt, bạn nên chủ động tìm cách xóa chúng ngay. Có rất nhiều công cụ có thể xóa các bài đăng cũ trên Facebook hay Twitter và các Mạng xã hội khác nữa. Ngoài ra còn các công cụ quản lý có thể tự động xóa bài đăng khi các bài đăng đó tới một ngưỡng tuổi nào đó.

SỬ DỤNG CÀI ĐẶT RIÊNG TƯ.

Trên thực tế không thể hiểu hết về một con người qua những gì ta thấy trên mạng về họ, nhưng điều này không ngăn cản những người tuyển dụng, các nhân viên tuyển sinh hay các đối tượng hẹn hò của bạn nhìn vào những gì bạn thể hiện trên mạng và đánh giá nó. Vì vậy hãy sử dụng các cài đặt riêng tư để hạn chế những gì họ có thể xem trên hồ sơ của bạn để chúng không thể tác động lên con người thật của bạn.

3.2. Tác động của việc chia sẻ quá nhiều thông tin

Hiện nay, các ứng dụng mạng xã hội như Whatsapp, Zalo, Viber, Skype, ... là phương tiện tốt để chúng ta giữ liên lạc với mọi người. Tuy nhiên, chúng cũng chứa những rủi ro. Một số người có thể chia sẻ quá nhiều thông tin bản thân với người khác trên mạng.

Khi bạn chia sẻ hình ảnh, video, hay tin nhắn, bạn sẽ không thể kiểm soát chúng sẽ đi về đâu. Ví dụ, nếu bạn đăng một hình ảnh của bạn trên mạng và cài đặt chế độ "Công khai" thì tất cả những người dùng trên ứng dụng/nền tảng này đều có thể thấy hình ảnh đó, họ có thể chia sẻ hình ảnh này với những người khác. Điều này dẫn đến nhiều người biết đến hình ảnh của bạn, dù cho bạn có muốn hay không.

Việc chia sẻ quá nhiều thông tin về bản thân trên mạng có thể khiến chúng ta gặp nguy hiểm, ảnh hưởng đến danh tiếng trên mạng và cho phép những người không quen biết liên lạc hoặc làm phiền chúng ta và có thể tìm thấy chúng ta ngoài đời thực.

Vì sự an toàn,

chúng ta cần suy nghĩ nên hay không nên chia sẻ cái gì, khi nào và chia sẻ cho ai.

3.3. Xây dựng tư duy phản biện trước các thông tin chia sẻ

Không phải mọi thứ trên mạng Internet đều an toàn và đáng tin cậy, hãy dừng lại để suy nghĩ, tìm hiểu, phân tích đánh giá để xác thực thông tin đó có đáng tin hay không trước khi tin tưởng bất cứ thông tin nào hay trước khi tải (hoặc đăng) video, nhạc từ Internet, hay gửi lời bình luận, chia sẻ video, hình ảnh hoặc tin tức. Điều đó sẽ giúp bạn tạo dựng và phát triển tư duy phản biện nhanh nhạy, bảo vệ danh tiếng của bạn trên mạng khỏi những rắc rối trên mạng với bạn bè, thành viên trong gia đình hay với chính quyền.

Đừng quên hỏi thăm, xin ý kiến của những người thân hoặc bạn bè nếu bạn thấy chưa chắc chắn khi đăng tải hay chia sẻ thông tin nào đó trên mạng Internet.

a) Kiểm tra mức độ xác thực của trang web:



Trên mạng có hàng triệu các trang web chứa nhiều thông tin để chúng ta truy cập. Nhưng chúng ta nên luôn luôn nhớ rằng bất cứ ai cũng có thể tạo nội dung trên trang web. Vì vậy, bạn không thể tin tưởng tất cả mọi thứ bạn thấy. Có một vài chiến lược bạn có thể sử dụng để đánh giá xem một trang web có đáng tin cậy hay không.

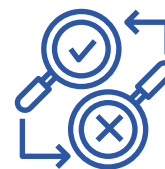
- ✔ **Xem xét loại tên miền:** Tên miền mà trang web được lưu trữ trên có thể cho bạn biết một chút về loại nội dung bạn đang xem.

Đuôi trang web	Loại trang web
.gov	thường là các trang web chính thức của chính phủ .
.edu	thường được xuất bản bởi các tổ chức giáo dục
.org	thường là các trang web của các tổ chức .
.com	các trang web thương mại

Dựa trên loại tên miền, bạn có thể đánh giá mức độ chính xác hoặc sai lệch của nội dung.

- ✔ **Tìm tác giả/bản quyền** của trang web (thường ở phía cuối trang chủ)
- ✔ **Tìm kiếm câu chuyện đó trên Google** để kiểm tra những nguồn thông tin khác
- ✔ Một trang web có thể tin cậy và an toàn hơn khi **bắt đầu bằng “https” và có ổ khóa phía trước**.
- ✔ **Viết đúng chính tả** thường là trang mạng đáng tin cậy hơn
- ✔ **Không có quảng cáo pop-up**, các quảng cáo pop-up có thể cho thấy trang mạng đó ít tin cậy hơn.
- ✔ Trang web đó **có mục Liên hệ với chúng tôi** bao gồm số điện thoại và địa chỉ email

b) Cách nhận biết tin thật và tin giả trên mạng:



Khi việc tiếp cận thông tin ngày càng trở nên dễ dàng thì khả năng nhận biết, đánh giá thông tin trực tuyến là thật hay giả rất cần thiết và quan trọng.

- ✔ **Xem xét nguồn tin:** Kiểm tra trang web/ tài khoản người đăng trên mạng xã hội có thông tin liên hệ rõ ràng không?
- ✔ **Kiểm tra thông tin minh họa, hình ảnh đường liên kết** có thực sự hữu ích hay có mục đích nào khác.
- ✔ **Bẫy định kiến:** Cân nhắc xem bạn có đang định kiến hay thiên vị với đối tượng nào không?

Ví dụ: Nếu bạn tìm thấy một bài báo nói rằng mọi người nên mua áo ấm vì thời tiết rét đậm rét hại và sau đó bạn thấy rằng tác giả của bài viết là một công ty bán quần áo, có khả năng nhà xuất bản của bài viết đang chia sẻ thông tin không khách quan. Thông tin không khách quan không phải lúc nào cũng xấu. Các blogger cá nhân, những người xuất bản bài viết để chia sẻ suy nghĩ những thông tin có giá trị. Tuy nhiên, bạn nên nhận thức được sự thiên vị của bất kỳ tác giả nào và biết khi nào có ý kiến so với thực tế.

1

Kiểm tra tác giả 

bài viết có đáng tin cậy không?

2

Kiểm tra thời gian 

Cẩn thận giữa sự việc hiện tại với tin tức cũ bị đăng lại. Luôn chắc chắn kiểm tra ngày xuất bản của một trang web/ bài viết để xác định xem có thực tiễn và phù hợp với nhu cầu không.

3

Đọc toàn bộ tin tức 

Tiêu đề thường giật tít để thu hút người đọc.

4

Hỏi ý kiến chuyên gia 

hoặc các nguồn đáng tin cậy.

Cuối cùng, hãy nhớ rằng bạn phải luôn kiểm tra nhiều nguồn. Tránh dựa vào một nguồn duy nhất cho tất cả các thông tin của bạn. Càng sử dụng nhiều nguồn, bạn càng dễ xác minh tính chính xác của thông tin mà bạn tìm được.

Hãy ghi nhớ các chiến lược này trong khi bạn duyệt web để đảm bảo thông tin bạn sử dụng là đáng tin cậy và chính xác.

Đồng thời, **khi phát hiện tin giả bạn hãy thông báo về Trung tâm xử lý tin giả Việt Nam** bằng các cách sau:

- * **Website: <http://tingia.gov.vn>**
- * **Email: online.abei@mic.gov.vn**
- * **Điện thoại: 18008108**

3.4. Hành động có trách nhiệm trên mạng

a) 4 chìa khóa giúp hành động có trách nhiệm trên mạng



Một bức ảnh hay một bài đăng mà bạn thấy hài hước và vô hại có thể bị hiểu lầm bởi những người mà bạn chẳng bao giờ nghĩ là sẽ nhìn thấy nội dung đó, cả trong hiện tại và sau này. Cảm xúc có thể bị tổn thương. Những người không hiểu được rằng đó chỉ chuyện đùa cho vui có thể nghĩ là bạn có ác ý vì họ không hiểu thông điệp của bạn.

Người khác có thể suy nghĩ không giống như cách bạn suy nghĩ. Do đó, hành động có trách nhiệm đầu tiên thể hiện qua việc trước khi đăng một nội dung hoặc hình ảnh lên mạng, hãy dừng lại và tự trả lời các câu hỏi sau:

- ? Người khác có thể hiểu như thế nào về thông điệp của tôi? Tôi có chắc chắn là họ sẽ hiểu đúng ý tôi muốn nói hay không?
- ? Liệu người khác có thể hiểu nhầm không?
- ? Bạn cũng nên tự hỏi mình những câu tương tự trước khi bạn bình luận hoặc đăng thông tin: Tôi có chắc chắn là mình hiểu đúng ý họ muốn nói không? Làm sao để biết?

Thứ hai, hành động có trách nhiệm trên mạng thể hiện thông qua việc tôn trọng ý kiến và quyền riêng tư của mình và của người khác mỗi khi muốn chia sẻ điều gì trên mạng, đặc biệt là trước khi chia sẻ, lan truyền thông tin trên mạng.

Chính vì vậy, **4 chìa khóa giúp bạn hành động có trách nhiệm trên mạng đó là:**

- ✔ **SUY NGHĨ:** hãy suy nghĩ trước khi đăng tin, nói chuyện trực tuyến, tải dữ liệu trên mạng Internet. Hãy suy nghĩ những gì bạn đang làm sẽ ảnh hưởng đến danh tiếng của bạn như thế nào, và nó có thể ảnh hưởng gì đến người khác.
- ✔ **HỎI:** hãy tự hỏi liệu những gì bạn đang đăng lên mạng xã hội có làm bạn/ người khác tổn thương.
- ✔ **ĐỐI XỬ:** hãy đối xử với người khác trên mạng giống như cách mà bạn muốn người khác đối xử với bạn.
- ✔ **DỪNG BIỂU TƯỢNG CẢM XÚC:** sử dụng biểu tượng cảm xúc giúp người khác hiểu hơn những gì bạn nói trên mạng.
- ✔ **ĐỜI SỐNG THỰC:** nếu bạn không nói hay làm điều gì trong đời thực, thì đừng nói và làm điều đó trên mạng.

b. Các hành vi thiếu trách nhiệm trên mạng bị xử phạt theo quy định của pháp luật:



Nghị định 15/2020/NĐ-CP quy định rõ các hành vi tung thông tin giả mạo, gây hoang mang dư luận trên mạng xã hội.

- Cung cấp, chia sẻ thông tin giả mạo, thông tin sai sự thật, xuyên tạc, vu khống, xúc phạm uy tín của cơ quan, tổ chức, danh dự, nhân phẩm của cá nhân;
- Cung cấp, chia sẻ thông tin cổ súy các hủ tục, mê tín, dị đoan, dâm ô, đồi trụy, không phù hợp với thuần phong, mỹ tục của dân tộc.
- Cung cấp, chia sẻ thông tin miêu tả tỉ mỉ hành động chém, giết, tai nạn, kinh dị, rùng rợn;
- Cung cấp, chia sẻ thông tin bịa đặt, gây hoang mang trong nhân dân, kích động bạo lực, tội ác, tệ nạn xã hội, đánh bạc hoặc phục vụ đánh bạc;
- Cung cấp, chia sẻ các tác phẩm báo chí, văn học, nghệ thuật, xuất bản phẩm mà không được sự đồng ý của chủ thể quyền sở hữu trí tuệ hoặc chưa được phép lưu hành hoặc; đã có quyết định cấm lưu hành hoặc tịch thu.
- Quảng cáo, tuyên truyền, chia sẻ thông tin về hàng hóa, dịch vụ bị cấm;

c. Hậu quả của việc cung cấp, chia sẻ thông tin giả mạo, sai sự thật



- Cung cấp, chia sẻ hình ảnh bản đồ Việt Nam nhưng không thể hiện hoặc thể hiện không đúng chủ quyền quốc gia;
- Cung cấp, chia sẻ đường dẫn đến thông tin trên mạng có nội dung bị cấm.

- ✓ Rạn nứt các mối quan hệ.
- ✓ Gây ra những phiền toái, phân biệt đối xử, cô lập, xa lánh, ... cho những người liên quan.
- ✓ Ảnh hưởng đến uy tín, danh dự của bản thân và người khác.
- ✓ Tổn thương đến sức khỏe cả về thể chất lẫn tinh thần.
- ✓ Bị phạt tiền hoặc khởi tố hình sự tùy thuộc mức độ nghiêm trọng của sự việc theo quy định của pháp luật.

Chẳng hạn theo điều 101 của Nghị định 15/2020/NĐ-CP quy định phạt tiền từ 10 - 20 triệu đồng đối với hành vi lợi dụng mạng xã hội để cung cấp, chia sẻ thông tin giả mạo, thông tin sai sự thật, xuyên tạc, vu khống, xúc phạm uy tín của cơ quan, tổ chức, danh dự, nhân phẩm của cá nhân; cung cấp, chia sẻ thông tin bịa đặt, gây hoang mang trong nhân dân, kích động bạo lực, tội ác, tệ nạn xã hội, đánh bạc hoặc phục vụ đánh bạc.

3.5 Câu chuyện thực tế



Năm 2021, bà Nguyễn Phương Hằng (Tổng giám đốc Công ty cổ phần Đại Nam) đã có 53 buổi phát sóng trực tiếp xúc phạm 7 nghệ sĩ Hoài Linh, ca sĩ Thủy Tiên, Đàm Vĩnh Hưng, Trấn Thành...

Vào cuộc điều tra, Cơ quan CSĐT Bộ Công an, Công an TP Hồ Chí Minh đã kết luận các nghệ sĩ, ca sĩ không có hành vi gian dối, không chiếm đoạt tiền từ thiện do người dân đóng góp, ủng hộ để cứu trợ đồng bào miền Trung nên không khởi tố vụ án hình sự.

Theo đó, ngày 24/3/2022, Cơ quan Cảnh sát điều tra Công an Thành phố Hồ Chí Minh đã ra Quyết định số 190-01/QĐ về việc khởi tố vụ án hình sự "Lợi dụng các quyền tự do dân chủ xâm phạm lợi ích của Nhà nước, quyền, lợi ích hợp pháp của tổ chức, cá nhân", quy định tại Điều 331 Bộ luật Hình sự đối với bà Nguyễn Phương Hằng. Cụ thể là hành vi lợi dụng sức ảnh hưởng của bản thân, sử dụng chức năng của mạng xã hội trên Internet, tổ chức nhiều buổi phát trực tiếp nội dung thông tin không kiểm chứng, liên quan đến đời tư của người khác; trong đó sử dụng những ngôn từ mang tính chất nhục mạ, xúc phạm danh dự, nhân phẩm của người khác.

Nguồn: Báo điện tử Chính phủ - Chinhphu.vn

4. Suy ngẫm

Bạn suy nghĩ gì?

Bạn hãy suy nghĩ về những trải nghiệm của chính mình khi sử dụng Internet và những cách thức nào bạn đang sử dụng để đảm bảo mình hành động có trách nhiệm và tôn trọng trên mạng. Bạn sẽ làm gì để tránh đăng những điều thô lỗ/không phù hợp trên mạng?



Lật qua để xem nội dung tiếp theo

Bài 04

QUY TẮC AN TOÀN, BẢO MẬT THÔNG TIN

1. Câu hỏi thảo luận/Đặt vấn đề:

"Xin chào anh/chị. Em tên là T, ở công ty chứng khoán XYZ, em có một số báo cáo về thị trường chứng khoán mới nhất muốn gửi đến anh/chị. Anh chị cho em xin địa chỉ email để em gửi thông tin?". Bạn đã từng nhận cuộc gọi nào như thế này chưa? Nếu có thì bạn có cung cấp thông tin của mình cho người gọi không?



2. Khái niệm chính

Thông tin & tài khoản cá nhân

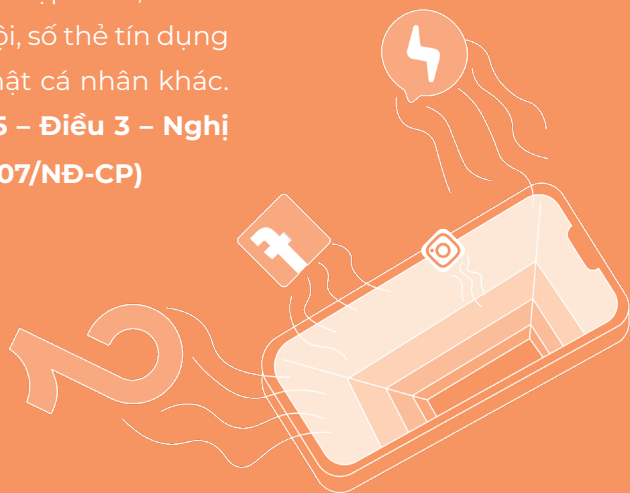
2.1. Thông tin cá nhân

Thông tin cá nhân là thông tin đủ để xác định chính xác danh tính một cá nhân, bao gồm ít nhất nội dung trong những thông tin sau đây: Họ tên, nghề nghiệp, chức danh, địa chỉ liên hệ, địa chỉ thư điện tử, số điện thoại, số chứng minh nhân dân, số hộ chiếu. Những thông tin thuộc bí mật cá nhân gồm có hồ sơ y tế, hồ sơ nộp thuế, số thẻ bảo hiểm xã hội, số thẻ tín dụng và những bí mật cá nhân khác.

(Theo Khoản 5 – Điều 3 – Nghị định số 64/2007/NĐ-CP)

2.2. Tài khoản cá nhân

Tài khoản cá nhân được xem là một cánh cửa để vào một website hay một mạng xã hội nào đó. Tài khoản cá nhân thường được chủ sở hữu lập ra với thông tin cá nhân của chính mình để trao đổi hay thực hiện các hành động trong website hoặc mạng xã hội đó.



3. Nội dung

3.1. Tầm quan trọng của việc bảo mật thông tin cá nhân

Thông tin cá nhân được Pháp luật bảo vệ theo quy định về quyền riêng tư: Đời sống riêng tư, bí mật cá nhân, bí mật gia đình là bất khả xâm phạm và được pháp luật bảo vệ - **Điều 38 Bộ luật dân sự năm 2015**.

Tài khoản cá nhân trên website hoặc MXH được dùng để trao đổi hay thực hiện các hành động trong website hoặc MXH đó. Tài khoản cá nhân thường đi kèm với thông tin cá nhân của chính chủ sở hữu tài khoản do đó việc bảo mật thông tin cá nhân thường sẽ đi kèm với bảo mật tài khoản cá nhân.



Hệ quả khi bị mất mật khẩu:

Khi bị mất mật khẩu tài khoản cá nhân có thể dẫn tới nguy cơ bị giả mạo, kẻ gian lợi dụng tài khoản để đi lừa đảo bạn bè, người thân hoặc đưa ra những thông tin sai lệch làm ảnh hưởng đến hình ảnh của trẻ, mất đi sự kết nối với bạn bè, mất đi nhiều hình ảnh và thông tin quan trọng, có thể bị lộ thông tin cá nhân dẫn tới bị lừa, bắt cóc, xâm hại...

Nguyên nhân có thể bị mất mật khẩu:

- ! Bị mất / bị ăn cắp thiết bị;
- ! Bị hack (lấy cắp) hoặc nhiễm phần mềm độc hại.
- ! Rò rỉ thông tin ngoài ý muốn, do bạn bè / người thân sơ ý, tự cung cấp thông tin cho người khác.

3.2. Một số hướng dẫn an toàn, bảo mật thông tin

✔ **ĐẶT MẬT KHẨU MẠNH:**

Sử dụng mật khẩu khó đoán, có ít nhất 8 ký tự, kết hợp số, chữ in hoa và cả in thường, và ký tự đặc biệt, sử dụng mật khẩu khác nhau cho tài khoản khác nhau, không chia sẻ mật khẩu với người khác, thay đổi mật khẩu ít nhất 6 tháng 1 lần.

✔ **TÍNH NĂNG XÁC THỰC HAI LỚP (HAY BẢO VỆ HAI LỚP):**

Mã xác thực mỗi khi bạn đăng nhập vào tài khoản email hoặc mạng xã hội bằng máy tính mới. Nếu người lạ cố gắng xâm nhập vào tài khoản của bạn, họ sẽ không thể đăng nhập được vì không có mã khóa này.

✔ **THIẾT LẬP CẢNH BÁO ĐĂNG NHẬP:**

Một số ứng dụng email hoặc mạng xã hội có chức năng cảnh báo khi có ai đó khác đăng nhập vào tài khoản của bạn. Cảnh báo này sẽ cho bạn biết thiết bị nào đang cố gắng đăng nhập vào tài khoản cũng như vị trí đăng nhập. Trong trường hợp bạn chưa tự thực hiện được việc đăng ký nhận mã xác thực (nhỏ tuổi, chưa sử dụng email, điện thoại di động) thì có thể sử dụng số điện thoại/ địa chỉ email của người lớn làm địa chỉ nhận mã xác thực.

✔ **ĐĂNG NHẬP AN TOÀN:**

Không nên sử dụng tài khoản Facebook hay Google... để đăng nhập vào nền tảng khác, hạn chế chọn “Lưu mật khẩu” khi đăng nhập, hạn chế sử dụng thiết bị công cộng, hoặc lưu ý đăng xuất khi bạn dùng thiết bị công cộng để truy cập tài khoản. Không truy cập các đường link lạ hoặc tin tưởng người mới quen qua mạng, không cài đặt phần mềm lạ không rõ nguồn gốc.

✔ **CÀI ĐẶT RIÊNG TƯ:**

Quyền riêng tư và tính bảo mật quyền riêng tư trên mạng luôn đi đôi với việc bảo mật trên mạng. Hầu hết ứng dụng và phần mềm đều hỗ trợ chức năng kiểm soát những thông tin chúng ta chia sẻ cũng như cách chia sẻ những thông tin đó. Khi dùng một ứng dụng hoặc trang web, hãy tìm những mục như “Tài khoản của tôi” hoặc “Cài đặt”. Đó là nơi bạn có thể xem những chế độ cài đặt về quyền riêng tư và tính bảo mật giúp bạn quyết định:

- Thông tin mọi người nhìn thấy trên trang thông tin hoặc hồ sơ của mình.
- Những người có thể xem bài đăng, ảnh, video hoặc những nội dung khác mà bạn chia sẻ. Khi học được cách sử dụng những chế độ cài đặt này để bảo vệ quyền riêng tư - và hãy nhớ cập nhật chúng, bạn sẽ quản lý được quyền riêng tư, tính bảo mật và sự an toàn của mình.

Các nguyên tắc bảo mật tài khoản trên mạng với bạn tùy theo lứa tuổi sẽ cần cha mẹ/ người giám hộ hỗ trợ thực hiện các tác vụ yêu cầu xử lý có độ phức tạp nhất định như thiết lập xác thực 2 lớp, cài đặt riêng tư lần đầu: chặn một số trang tin điện tử hoặc nội dung không muốn xem hay không phù hợp với bạn ...

**Mật khẩu mạnh *****

sẽ giúp bạn bảo vệ thông tin cá nhân và khiến những kẻ lừa đảo không thể lấy cắp thông tin của bạn trên mạng

- ✓ Bài hát, bộ phim hoặc trò chơi yêu thích.
- ✓ Mật khẩu mạnh chứa các chữ cái, chữ số và biểu tượng.
- ✓ Đừng bao giờ sử dụng một mật khẩu giống nhau trên nhiều trang web.
- ✓ Hãy tạo ra nhiều phiên bản của cùng một mật khẩu để đặt cho từng tài khoản khác nhau.
- ✓ Đặt mật khẩu sao cho dễ nhớ, nhưng tránh dùng thông tin cá nhân như tên và ngày tháng năm sinh.

**Duy trì bảo mật cho tài khoản**

- ✓ Đặt các mật khẩu dễ nhớ nhưng khó đoán.
- ✓ Đổi mật khẩu 2-3 tháng/lần hoặc ngay lập tức khi bạn cho rằng người khác đã biết mật khẩu.
- ✓ Luôn sử dụng những chức năng khóa màn hình có tính bảo mật cao cho thiết bị của mình.
- ✓ Đặt thiết bị ở chế độ tự động khóa, phòng khi thiết bị rơi vào tay kẻ xấu.
- ✓ Cân nhắc việc sử dụng một ứng dụng quản lý mật khẩu (Dashlane, Keeper..) để ghi nhớ các mật khẩu của mình. Bằng cách này, trẻ có thể đặt một mật khẩu riêng cho mỗi tài khoản và chỉ cần nhớ duy nhất mật khẩu chủ của ứng dụng quản lý mật khẩu.

**Bạn có biết**

Tại sao mật khẩu cần tối thiểu 8 ký tự như chữ cái, chữ số và ký tự đặc biệt không?

Theo nghiên cứu của công ty an ninh mạng Hive Systems (Mỹ), **mật khẩu dễ bị giải mã nhất thường chỉ gồm toàn chữ số, hoặc ít ký tự phức tạp.**

Cụ thể, nếu người dùng đặt mật khẩu chỉ toàn các số, việc giải mã sẽ được thực hiện ngay lập tức, nhất là khi mật khẩu chỉ gồm 4-11 chữ số. Nhưng kể cả khi đặt với 18 số, hacker cũng chỉ mất khoảng ba tuần để giải mã.

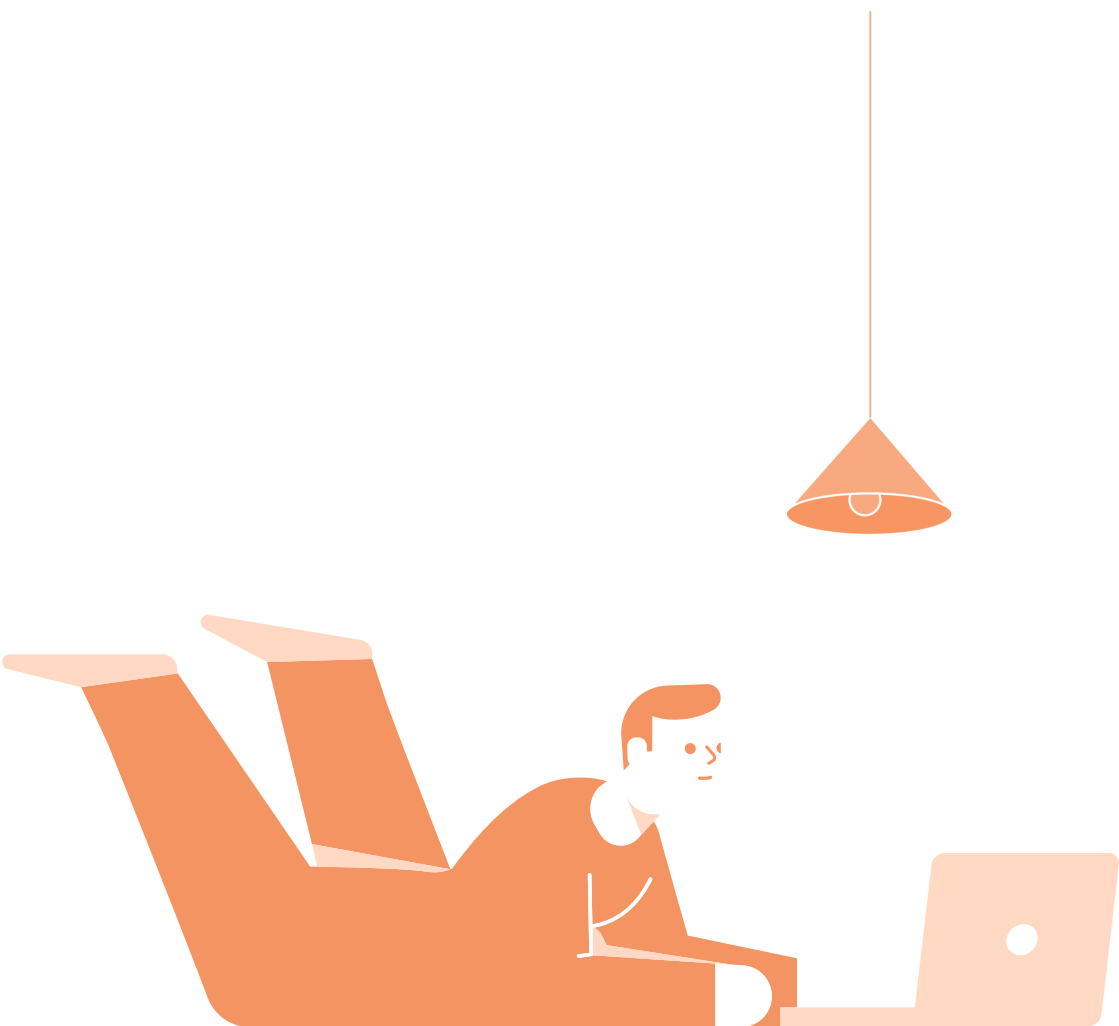
Trong khi đó, **mật khẩu mạnh nhất được đặt gồm số, chữ thường, chữ in hoa và các ký tự đặc biệt.** Hacker có thể giải mã dễ dàng loại mật khẩu này khi chúng từ 4-6 ký tự. Nhưng nếu đặt dài hơn, hacker có thể phải cần từ vài chục phút tới hàng tỷ năm.

Theo các chuyên gia, **mật khẩu ở ngưỡng an toàn nên từ 9 ký tự, gồm số, chữ thường, chữ in hoa và ký tự đặc biệt.** Ở mức này, cần khoảng ít nhất hai ngày để giải mã.

Để xác định thời gian bẻ khóa một mật khẩu, Hive Systems sử dụng dữ liệu từ công cụ HowSecureIsMyPassword của Security.org. Trên blog, nhóm này giải thích rằng đã bắt đầu với cái gọi là “băm” (hashing) - quy trình được điều khiển theo thuật toán mà hầu hết website ngày nay sử dụng để ngăn trang mật khẩu được lưu trữ.

Mật khẩu dạng băm không thay đổi được và cũng không giải mã ngược lại được do dùng thuật toán một chiều. Và khi hacker đột nhập vào trang web thì hacker cũng chỉ thấy những ký tự này. Hacker có thể lập danh sách mọi tổ hợp ký tự có thể có trên bàn phím, sau đó tự

bấm các tổ hợp đó bằng phần mềm thông dụng. Cuối cùng, hacker chỉ cần sử dụng danh sách này, dùng phần mềm chuyên dụng để đối chiếu với tài khoản đánh cắp được, so sánh sự trùng khớp để tìm ra mật khẩu. Thời gian thực hiện quá trình này tùy thuộc vào độ phức tạp của mật khẩu.



Số ký tự	Chỉ có số	Chữ thường	Chữ viết hoa & chữ thường	Số, chữ viết hoa & chữ thường	Số, Chữ hoa, chữ thường, ký tự đặc biệt
4	Ngay lập tức	Ngay lập tức	Ngay lập tức	Ngay lập tức	Ngay lập tức
5	Ngay lập tức	Ngay lập tức	Ngay lập tức	Ngay lập tức	Ngay lập tức
6	Ngay lập tức	Ngay lập tức	Ngay lập tức	Ngay lập tức	Ngay lập tức
7	Ngay lập tức	Ngay lập tức	2 giây	7 giây	31 giây
8	Ngay lập tức	Ngay lập tức	2 phút	7 phút	39 phút
9	Ngay lập tức	10 giây	1 tiếng	7 tiếng	2 ngày
10	Ngay lập tức	4 phút	3 ngày	3 tuần	5 tháng
11	Ngay lập tức	2 tiếng	5 tháng	3 năm	34 năm
12	Ngay lập tức	2 ngày	24 năm	200 năm	3.000 năm
13	2 giây	2 tháng	1.000 năm	12.000 năm	202.000 năm
14	19 giây	4 năm	64.000 năm	750.000 năm	16 triệu năm
15	3 phút	100 năm	3 triệu năm	46 triệu năm	1 tỷ năm
16	32 phút	3.000 năm	173 triệu năm	3 tỷ năm	92 tỷ năm
17	5 tiếng	69.000 năm	9 tỷ năm	179 tỷ năm	7 triệu tỷ năm
18	3 tuần	2 triệu năm	467 tỷ năm	11 triệu tỷ năm	438 triệu tỷ năm

Theo: CNCB

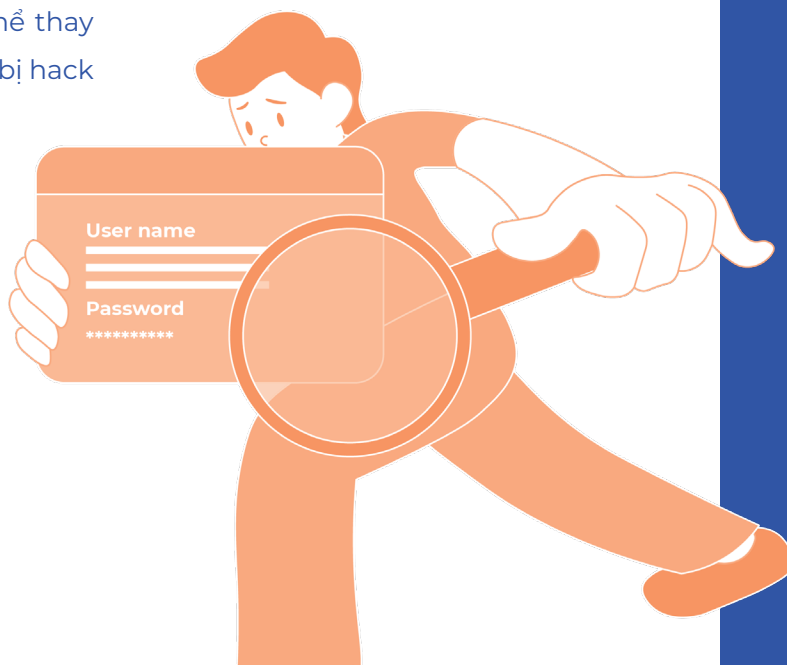
4. Suy ngẫm

Bài tập áp dụng để đánh giá mức độ

An toàn và bảo mật thông tin trên mạng của bạn

Bạn hãy kiểm tra lại xem mật khẩu của mình trên các tài khoản email, tài khoản mạng xã hội, tài khoản ngân hàng ... đã an toàn chưa? Bạn có sử dụng chung một mật khẩu cho nhiều tài khoản không? Nếu có thì hãy thiết lập lại cho an toàn.

Kiểm tra các chức năng bảo vệ hai lớp và cảnh báo đăng nhập đã được bật chưa? Kiểm tra việc đăng xuất tài khoản trên những thiết bị mà bạn đã đăng nhập nhưng không dùng nữa. Nếu bạn chưa đổi mật khẩu trong một thời gian dài (trên 6 tháng) thì có thể thay đổi mật khẩu để tránh bị hack hoặc ăn cắp.



Lật qua để xem nội dung tiếp theo

Bài

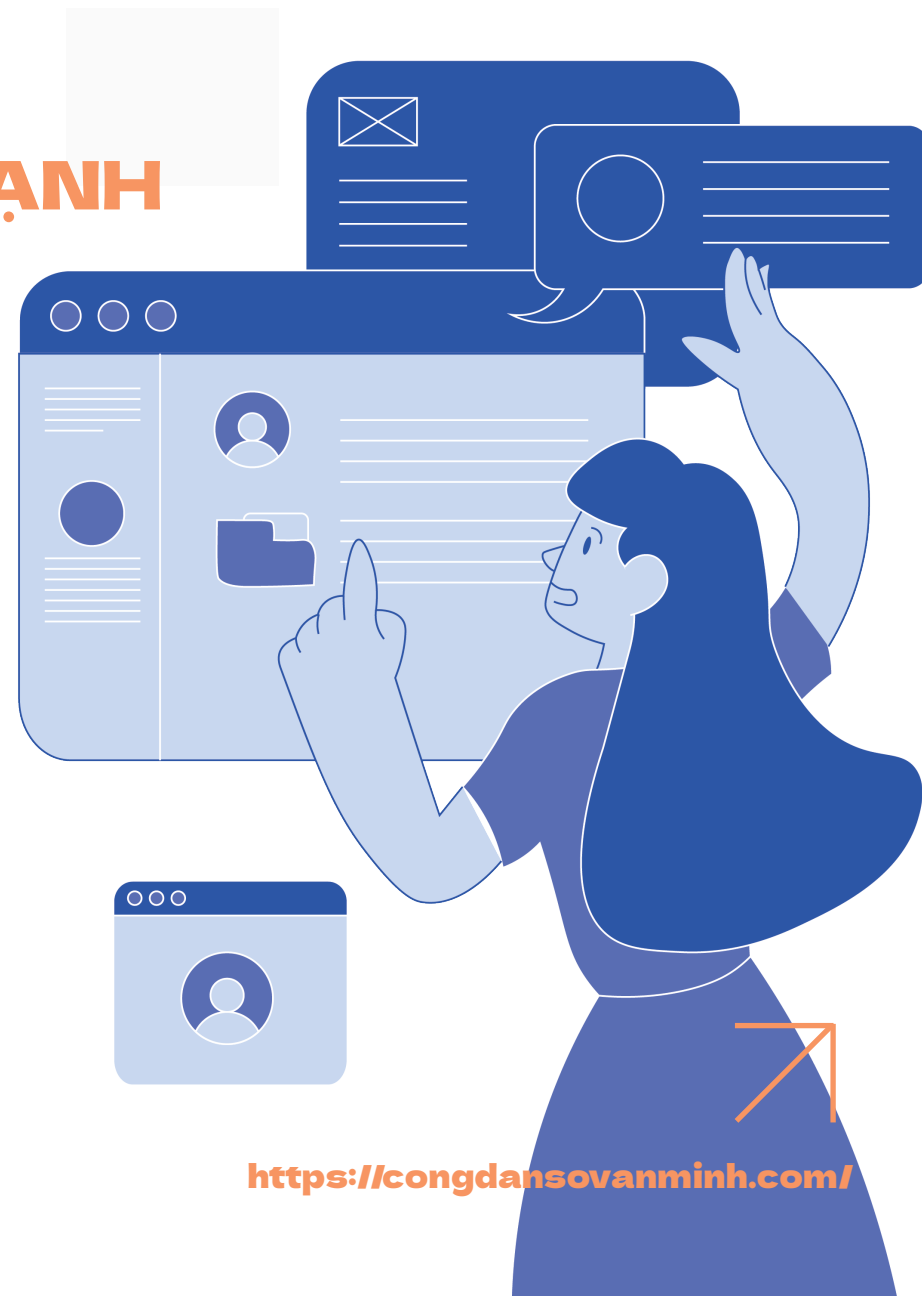
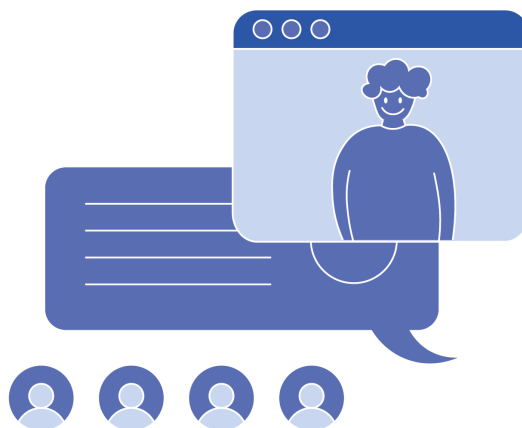
05

QUY TẮC
ỨNG XỬ LÀNH MẠNH

1. Câu hỏi thảo luận/Đặt vấn đề:

Hành vi, ứng xử trên MXH như thế nào là phù hợp với các giá trị văn hóa, đạo đức, truyền thống của Việt Nam?

Khi gặp những thông tin xấu, độc hại bạn sẽ ứng xử như thế nào? Bạn đã bao giờ nghe hoặc trực tiếp chứng kiến một sự việc bắt nạt trên mạng chưa? Nếu gặp tình huống bắt nạt trên mạng bạn sẽ ứng xử như thế nào?



2. Khái niệm chính

Văn hóa mạng

Văn hóa ứng xử trên MXH được hiểu là hệ thống giá trị chi phối nhận thức, thái độ, hành vi ứng xử của cá nhân, cộng đồng trong các mối quan hệ với tự nhiên, xã hội và với chính bản thân khi tham gia MXH, phản ánh trình độ phát triển của cá nhân và cộng đồng.

Văn hóa ứng xử trên MXH bao hàm cả mối quan hệ giữa con người và môi trường xung quanh, biểu hiện ở chỗ mỗi người biết góp phần tuyên truyền trên MXH về bảo vệ môi trường thiên nhiên, tiết kiệm tài nguyên, sống xanh, sạch, đẹp, an toàn, lành mạnh, thân thiện; biết yêu thương, chăm sóc, bảo vệ các loài động vật,... Văn hóa ứng xử trên MXH còn thể hiện trong mối quan hệ với chính bản thân, với các giá trị như sự khiêm tốn, thật thà, dũng cảm, có chính kiến, lập trường, quan

điểm rõ ràng; tinh thần cầu thị, học hỏi, không tự kiêu, tự đại hoặc tâm lý tự ti, thiếu tin vào bản thân...

Bắt nạt trên mạng: là hành vi bắt nạt bằng việc sử dụng công nghệ kỹ thuật số. Nó có thể diễn ra trên phương tiện mạng xã hội, nền tảng nhắn tin, nền tảng chơi game và điện thoại di động. Đó là hành vi lặp đi lặp lại, nhằm mục đích khiến những người bị nhắm mục tiêu sợ hãi, tức giận hoặc xấu hổ.

Hình thức bắt nạt trên mạng - Có rất nhiều hình thức bắt nạt trên mạng trong số đó có một số hình thức phổ biến như sau:

QUẤY RỐI:

Là các hành động như gửi các thông điệp công kích, thô lỗ, và tin nhắn xúc phạm hay đe dọa hành, lạm dụng. Viết những bình luận, bức hình làm khó chịu

hay gây xấu hổ trên các trang MXH. Gây khó chịu rõ ràng cho người chơi khác trên các trang mạng chơi game;

ĐẶT ĐIỀU/PHÍ BÁNG:

Một người gửi các thông tin giả mạo, gây tổn hại và không đúng sự thật về người khác, chia sẻ hình ảnh về một người nào đó với mục đích chế giễu, lan truyền các tin đồn và lời thị phi không đúng sự thật. Điều này có thể diễn ra trên bất cứ trang mạng hay ứng dụng nào. Chúng ta thường chứng kiến những người hay gửi các hình ảnh về người khác và đăng các bài viết lên mạng với mục đích bắt nạt;

MẠO DANH:

Là khi một người nào đó đột nhập vào tài khoản email hoặc mạng xã hội của người khác và sử dụng danh tính trên mạng này để gửi hay đăng các tin

hiêu dâm, hoặc các tài liệu (bài viết, hình ảnh, đoạn ghi âm, video clip...) đáng xấu hổ cho người khác. Nó cũng có thể là việc lập một trang/hồ sơ giả mạo trên các trang mạng xã hội, ứng dụng và những nơi trên mạng khác;

PHÁT TÁN VÀ LỪA ĐẢO:

Là khi một ai đó vô tình hoặc bị lừa chia sẻ các thông tin cá nhân có thể là hình ảnh và video riêng tư. Những thông tin này sau đó có thể bị phát tán và nằm ngoài khả năng kiểm soát;

LOẠI BỎ, CÔ LẬP:

Là khi một ai đó cố ý loại bỏ người khác khỏi nhóm chat hạn như nhóm nhắn tin chung, những ứng dụng trên mạng, các trang mạng chơi game và những hình thức tham gia trên mạng khác.

3. Nội dung

3.1. Hành vi, ứng xử trên MXH phù hợp với các giá trị văn hóa, đạo đức, truyền thống của Việt Nam

Không phải mọi điều phù hợp với pháp luật thì cũng có nghĩa là đã an toàn hoặc không ảnh hưởng đến người khác, bởi trong một số trường hợp, hành vi có thể không vi phạm pháp luật nhưng vẫn không tốt, không hay, tức là không lành mạnh.

Chúng ta hãy lan tỏa

sự tích cực, tốt đẹp phù hợp với văn hóa người Việt Nam thanh lịch, văn minh

Ứng xử lành mạnh trên mạng xã hội nói riêng và Internet nói chung thường gắn với sự “có ích”, “tích cực” hay “truyền cảm hứng”, “lan tỏa điều tốt đẹp”... thông tin, hình ảnh đó không làm người tiếp nhận cảm thấy khó chịu, lo lắng, sợ hãi hay có thể dẫn đến những hậu quả đáng tiếc... hoặc liên quan đến những chủ đề dễ gây mâu thuẫn về giới tính, tôn giáo, văn hóa, đạo đức.... Dù chúng ta biết rằng xã hội luôn tồn tại các mặt tích cực lẫn tiêu cực nhưng mỗi cá nhân cần có ý thức về việc truyền tải thông tin một cách phù hợp như:

- ✔ **Lan tỏa những thông tin tốt đẹp, hình ảnh tốt đẹp** về các hoạt động xã hội, hoạt động vì cộng đồng, phê phán những cái xấu, biểu hiện lệch lạc, hướng tới thông điệp nhân văn, xây dựng văn hóa người Việt thanh lịch, văn minh.
- ✔ **Chia sẻ những thông tin có nguồn chính thống, đáng tin cậy;** có các hành vi, ứng xử phù hợp với những giá trị đạo đức, văn hóa, truyền thống của dân tộc Việt Nam. Khuyến khích sử dụng

mạng xã hội để tuyên truyền, quảng bá về đất nước – con người, văn hóa tốt đẹp của Việt Nam, chia sẻ thông tin tích cực, những tấm gương người tốt, việc tốt.

- ✔ Đồng thời, chúng ta cũng có thể vận động người thân trong gia đình, bạn bè, những người xung quanh **tham gia giáo dục, bảo vệ trẻ em, trẻ vị thành niên sử dụng mạng xã hội một cách an toàn**, lành mạnh thông qua rất nhiều những chia sẻ, thông tin tích cực và có ích.

Những điều này không chỉ góp phần làm cho Mạng xã hội và Internet nói chung trở thành một nơi an toàn và tốt đẹp mà còn giúp cho người trẻ học hỏi và trưởng thành hơn, sống có trách nhiệm hơn.

Giới trẻ làm từ thiện qua

Mạng Xã Hội

Cùng với sự phổ biến của Internet và các mạng xã hội (Facebook, Twitter...), rất nhiều nhiều tổ chức tình nguyện đã sử dụng phương thức kêu gọi bằng cách đưa ra những thông tin cụ thể về chương trình như: Địa điểm thực hiện, thời gian tổ chức và số tài khoản nhận tiền quyên góp cũng như thông tin liên lạc của các thành viên đại diện... lên Fanpage (là trang chia sẻ chuyên nghiệp của một nhóm/tổ chức với nhiều thành viên) của nhóm và trang cá nhân của từng thành viên.



Chính những hoạt động này đã biến những cái “ảo” của Internet thành hành động thiết thực, có ích cho xã hội và cộng đồng.

Ngoài mục đích làm từ thiện và giúp đỡ những số phận kém may mắn thì phong trào mang lại nhiều lợi ích cho các bạn tình nguyện viên tham gia như: Được giao lưu, kết bạn, phát triển kỹ năng giao tiếp, kỹ năng làm việc nhóm...

Hình thức quyên góp được sử dụng nhiều nhất là tiền mặt được chuyển khoản trực tiếp vào số tài khoản của đại diện tổ chức (nhóm). Ngoài ra, tùy theo đặc trưng chương trình (đầu năm học mới, Tết Trung thu, áo ấm mùa đông...) mà các tổ chức sẽ thu nhận các hiện vật khác nhau. Từ bánh nướng, bánh dẻo, kẹo ngọt, đồ chơi, quần áo, giày dép... đến gạo, muối vừng, ruốc... đều được các tổ chức đón nhận.

Mới đây, chương trình “Góp bánh Trung thu tặng trẻ em miền núi” của Câu lạc bộ Tình nguyện trẻ, ngoài bánh, kẹo, đồ chơi thì những bộ quần áo ấm, đôi ủng, muối vừng, cá khô, ruốc... đã được chuyển đến tay các em học sinh xã Pa Ủ, huyện Mường Tè, tỉnh Lai Châu. Những món quà thực sự hữu ích chính là điều các em nhỏ khó khăn mong muốn nhận được từ các nhà hảo tâm.

Khi hỏi về những khó khăn trong quá trình quyên góp, chị Huyền chia sẻ “Chúng tôi không gặp khó khăn gì khi quyên góp vì tất cả những công việc này đều xuất phát từ tấm lòng

của mọi người. Cảm ơn những tấm lòng, dù không hề quen biết nhau, chỉ đọc theo đường link trên Facebook mà tin tưởng, không ngần ngại chuyển tiền ủng hộ vào tài khoản của nhóm và cùng chúng tôi làm thành một Trung thu ấm áp cho các bé”.

Có thể kể đến Fanpage của “Cơm 5.000 Hà Nội” với hơn 5.000 người theo dõi, đã nhận được sự ủng hộ của rất nhiều tấm lòng từ thiện. Mục đích của chương trình là mang những suất cơm chất lượng với giá 5.000 đồng đến tay người lao động, bệnh nhân và sinh viên nghèo trên địa bàn Hà Nội vào mỗi thứ 4 hằng tuần.

Tuy nhiên, để có thể nhận được sự ủng hộ đến từ các cá nhân trên Internet, ngoài việc đưa ra một bản dự án thuyết phục cũng như mục đích và hoạt động chi tiết thì việc công khai minh bạch các khoản thu chi mà tổ chức nhận được là điều rất quan trọng. Điều này khiến cho người ủng hộ, quyên góp yên tâm vì số tiền của mình được sử dụng đúng mục đích.

(Nguồn: Phan Trang - Báo Điện tử Chính phủ)

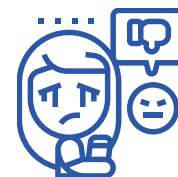
3.2 Có trách nhiệm khi ứng xử với thông tin xấu, độc hại trên mạng Internet

Trên mạng cũng như ở bên ngoài, việc bắt gặp những nội dung xấu như bạo lực, phản cảm, phân biệt chủng tộc là hoàn toàn có thể xảy ra. Có thể bạn sẽ gặp bối rối hay vô tình có những hành xử gây ra hậu quả đáng tiếc và rất khó khắc phục như là vô tình chia sẻ tin giả, gây ảnh hưởng đến người khác, nội dung nhạy cảm xuất hiện trên điện thoại khi ở chỗ đông người.. Để hạn chế những tác động không mong muốn đối với những nội dung trên, chúng ta có thể tìm hiểu và thực hành theo một số nguyên tắc ứng xử khi tham gia mạng Internet:

- ✔ **Sử dụng ngôn ngữ lịch sự**, không sử dụng ngôn từ phản cảm, vi phạm thuần phong mỹ tục; bảo vệ sự trong sáng của Tiếng Việt, không sử dụng ngôn ngữ tục tĩu, cá biệt, có tính bạo lực, phân biệt vùng miền, giới tính, tôn giáo.
- ✔ Đặc biệt, **không được lập nhóm, hội để nói xấu**, công kích lẫn nhau; không đăng tải, chia sẻ thông tin có thể gây xúc phạm, làm mất uy tín, danh dự cá nhân; không theo đám đông khi chưa hiểu rõ về vụ việc đó, hoặc không có căn cứ, gây ảnh hưởng đến trật tự an toàn xã hội...
- ✔ **Dùng chức năng báo cáo (Report) nội dung xấu**, tiêu cực và phản cảm cho các nhà quản trị mạng hoặc cao hơn nữa là báo cho cơ quan chức năng với các vi phạm ảnh hưởng tới cuộc sống ngoài đời thực.

3.3 Có trách nhiệm khi ứng xử với hành vi bắt nạt trên mạng Internet

a) Một số dấu hiệu gợi ý một người có thể đang bị bắt nạt trên mạng:



Khi một người bị bắt nạt trên mạng, người đó có thể xuất hiện một hoặc một vài ảnh hưởng về thể chất cũng như tinh thần. Điều này có thể dẫn tới hậu quả lâu dài, rất nhiều bạn trẻ sau khi bị bắt nạt đã không dám chia sẻ với gia đình, người thân hay bạn bè dẫn tới rất nhiều hậu quả đáng tiếc, thậm chí tử vong. Việc chú ý đến những biểu hiện của người bị bắt nạt trên mạng có thể hỗ trợ rất nhiều trong việc khắc phục hậu quả, chúng ta có thể tham khảo một vài biểu hiện sau:

Đột ngột ngừng sử dụng thiết bị truy cập mạng Internet;

Trở nên bí mật bất thường, đặc biệt là khi đề cập đến các hoạt động trực tuyến;

Né tránh các cuộc thảo luận về những gì người đó đang làm khi trực tuyến

Có những câu nói liên quan đến việc tự sát hoặc ý nghĩa tiêu cực của cuộc sống;

Trở nên xa lánh, thu mình một cách bất thường với bạn thân hoặc các thành viên trong gia đình;

Khó ngủ hoặc không ngủ đủ.

Câu chuyện thực tế:

Em Bùi Q.H, học sinh một trường THCS tại Yên Bái, ngày 19-9-2016, em H bị một nhóm người chặn trước cổng trường, dùng tuýp cao su đánh và ép phải quỳ lạy xin tha thứ trước sự chứng kiến của nhiều học sinh khác. Nhiều học sinh chứng kiến đã dùng điện thoại quay lại clip rồi tung lên mạng xã hội.

Sau khi bị đánh, H rơi vào trạng thái hoảng loạn tâm lý. Gia đình đã đưa H đến điều trị và nằm viện 1 tuần tại Bệnh viện 103 (Yên Bái). Sau khi bị đánh đập, làm nhục, trong thời gian điều trị tại bệnh viện, H được các bác sĩ chẩn đoán có dấu hiệu chấn động về tâm lý. “Trong thời gian nằm viện, H thường xuyên nói với tôi "mẹ ơi con sợ lắm, con xấu hổ lắm khi bị bắt quỳ trước cổng trường rồi đánh đập, con không đi học nữa đâu"- mẹ H cho biết.

Sau đó, ngày 25-9-2016, H đã treo cổ tự tử tại nhà.

(Nguồn: Nguyễn Hưởng - Báo điện tử Người lao động)

b) Phòng ngừa và ứng phó bắt nạt trên mạng

“Phòng bệnh hơn chữa bệnh”, mỗi người cần kiểm soát hành vi của mình có trách nhiệm để ngăn ngừa các tình huống có thể tạo điều kiện cho bắt nạt trên mạng diễn ra cũng như không vô tình trở thành kẻ bắt nạt:

- ✔ **Đặt mật khẩu mạnh:** Bảo mật thông tin cá nhân của mình không để kẻ xấu lợi dụng giả mạo. Tham khảo Bài 5: Quy tắc an toàn, bảo mật thông tin.
- ✔ **Cài đặt giới hạn bạn bè, người tiếp cận** thông tin liên quan đến cá nhân chia sẻ trên MXH. Khi xảy ra tình trạng bắt nạt trên mạng tài khoản MXH của bạn nên được đặt về chế độ riêng tư chỉ mình bạn có thể xem.
- ✔ **Suy nghĩ kỹ trước khi chia sẻ thông tin của mình và người khác lên MXH.** Không chia sẻ các thông tin cá nhân có thể bị người khác lợi dụng như ngày sinh, số điện thoại, Căn cước công dân, địa chỉ nhà riêng, nơi làm việc, trường lớp... Đối với thông tin cá nhân của người khác cần tôn trọng quyền riêng tư, không chia sẻ khi chưa có sự đồng ý của người đó.

- ✔ **Tảng lờ:** Mục đích của kẻ bắt nạt là muốn người bị nhắm mục tiêu sợ hãi, tức giận hoặc xấu hổ do đó hướng dẫn trẻ không nên phản hồi lại bắt nạt trên mạng khiến cho kẻ bắt nạt đạt được mục đích và tiếp tục lặp lại hành động bắt nạt;
- ✔ **Chặn:** Chặn (block) hoặc báo cáo vi phạm (report) người bắt nạt mình nếu hiện tượng bắt nạt tiếp diễn;
- ✔ **Chụp màn hình:** Chụp lại màn hình những tình tiết bắt nạt trên mạng làm bằng chứng phục vụ cho việc trình báo với các cơ quan chức năng;
- ✔ **Khi thấy hành vi bắt nạt trên mạng** Internet chúng ta không nên tham gia cổ vũ dưới bất kỳ hình thức nào, thay vào đó chúng ta nên **sử dụng chức năng báo cáo vi phạm (report)** với nhà quản trị mạng để xử lý các nội dung này. Trong trường hợp việc bắt nạt diễn ra liên quan đến cuộc sống thực, chúng ta có thể báo cáo với cơ quan chức năng để có can thiệp kịp thời. Ví dụ khi thấy bạn cùng lớp bị đe dọa trên mạng và cả ở ngoài trường học/ công sở từ cùng một hoặc một nhóm đối tượng, chúng ta có thể báo với nhà trường, công an...để nhận được sự hỗ trợ.



Lật qua để xem nội dung tiếp theo

Bài

06

SỐNG THẬT TRÊN MẠNG ẢO

1. Câu hỏi thảo luận/Đặt vấn đề:

- Xu hướng sống ảo của giới trẻ hiện nay như thế nào?
- Tại sao thanh thiếu niên lại thích sống “ảo”?
- Liệu sống “thật” trên mạng có mang lại niềm vui, lợi ích hơn sống “ảo”?



2. Khái niệm chính

Hình ảnh cá nhân trên mạng xã hội

Hình ảnh cá nhân trên MXH: gắn với đặc điểm của từng người thể hiện qua các hành vi: Bạn đăng trạng thái ra sao, thể hiện cái tôi cá nhân như thế nào, ngôn từ bạn thể hiện trên MXH phù hợp hay chưa phù hợp? Bạn tham gia vào hội nhóm nào? Thích hay theo dõi gì trên MXH... Các hành vi này tạo dựng nên ấn tượng đối với một cá nhân của những người cùng tham gia MXH do đó, các cá nhân này có thể vô tình hoặc cố ý chủ động tạo ra những hình ảnh cá nhân không giống với đời thực.

Sống ảo:

được biết đến như một hành động, việc làm cập nhật trên MXH khác với thực tế, tự tạo niềm vui cho mình bằng cách đăng ảnh hay trạng thái của mình lên chia sẻ hoặc bằng những lượt tương tác trên MXH như thả tim, thích, theo dõi, có xu hướng tạo ra hình ảnh về một người/ cuộc sống mà họ mong muốn.



3. Nội dung

3.1. Một số biểu hiện của sống ảo phổ biến trong giới trẻ hiện nay



NGHIỆN “LIKE”:

là một hiện tượng rất phổ biến hiện nay. Họ cập nhật trạng thái ở mọi lúc mọi nơi, dù là đang gặp chuyện vui hay những nỗi buồn, những hoạt động cá nhân đều được đưa lên mạng xã hội để thu hút sự quan tâm của mọi người. Thậm chí, họ còn kêu gọi số lượt like để thực hiện một việc, để cứu sống một ai đó,...



CHỤP ẢNH CHECK IN:

Họ luôn cầm điện thoại chụp hình tự sướng ở khắp mọi nơi. Sau đó, sẽ đầu tư rất nhiều thời gian để chọn ra những tấm hình đẹp nhất, photoshop, viết caption và đăng lên mạng xã hội. Họ luôn để ý những bình luận khen chê của người khác trên mạng xã hội, đến mức ảnh hưởng đến công việc, cuộc sống đời thực của họ.



LUÔN DÍNH CHẶT VỚI ĐIỆN THOẠI:

Những người sống ảo thường coi điện thoại là vật bất ly thân, luôn luôn cầm điện thoại dù bất cứ đâu.



SỐNG KHÁC VỚI ĐIỀU KIỆN CỦA BẢN THÂN:

Những người sống ảo thường rất thích khoe trên mạng xã hội. Thường thấy nhất là việc khoe sắm được những món đồ đắt tiền, có những người điều kiện gia đình không tốt nhưng vẫn sắm những món đồ đắt tiền để khoe cho “bằng bạn bằng bè”.

3.2. Hệ quả của sống ảo



LƯỜI GIAO TIẾP, THỤ ĐỘNG, DỄ DẪN ĐẾN TRẦM CẢM:

Do ấn náu mình sau bàn phím sẽ khiến người trẻ ngày càng có xu hướng không muốn sống trong cuộc sống thật, với danh tính thật khi cuộc sống bên ngoài khác xa và không đem lại sự thỏa mãn như với cuộc sống trên mạng.



SỐNG ẢO ĐEM LẠI NHỮNG MỐI QUAN HỆ ẢO:

Khi quá phụ thuộc vào các kết nối ảo, người tham gia mạng xã hội sẽ giảm bớt kết nối với các mối quan hệ thật.



MẤT NHIỀU THỜI GIAN:

Để phục vụ việc tạo dựng hình ảnh hoàn hảo ở trên mạng, người trẻ sẽ mất rất nhiều thời gian và công sức trong việc lướt web, từ việc chỉnh sửa ảnh, nghĩ ra các nội dung ẩn tượng, tìm kiếm các xu hướng hấp dẫn hay dành quá nhiều thời gian để theo dõi tương tác của các bài viết.



SUY NGHĨ TIÊU CỰC, KHÁC XA VỚI THỰC TẾ:

Việc được tung hô trên mạng cũng góp phần khiến người tham gia MXH có cái nhìn ảo tưởng về bản thân, sinh ra so sánh và cảm thấy mình không được coi trọng trên thực tế dễ sinh ra chán nản.



THÍCH ĐƯỢC CHÚ Ý:

Sau một thời gian dài sử dụng, bạn dễ rơi vào trạng thái thích được đăng tải nhiều điều trong cuộc sống hơn và nhận lại lượt thích. Đôi khi bạn có thể cảm thấy những cái like “ảo” trên mạng là điều cần thiết mỗi khi bạn đăng bất cứ điều gì.



KHIẾN BẠN TRỞ NÊN TỰ TI:

Mạng xã hội góp phần tăng sự ganh đua, sự cạnh tranh không ngừng nghỉ để tìm kiếm những cái like ảo. Người dùng có thể rơi vào trạng thái tự ti chỉ vì bài đăng ít “like”. Còn đối với người xem, những gì người khác khoe khoang trên mạng không hẳn là con người thật của họ. Tuy nhiên, khi nhìn thấy những hình ảnh bạn bè với các chuyến du lịch khắp nơi có thể khiến bạn so sánh mình với người khác và cảm thấy ganh tị, tự ti về bản thân.

3.3. Sống thật trên mạng ảo

Thể hiện những hình ảnh chân thật thay vì cố gắng tạo ra một “cuộc sống lý tưởng” trên mạng xã hội là cách để có một tinh thần khỏe mạnh hơn. Trong một thế giới có vẻ như tràn ngập tin tức giả và cuộc sống giả tạo trên mạng xã hội, sống thật trên mạng ảo không chỉ tốt cho sức khỏe tinh thần của bạn mà còn là điều khiến bạn nổi bật giữa đám đông và tạo được dấu ấn. Các nhà nghiên cứu đã chỉ ra rằng việc đăng tải nội dung chân thật sẽ có lợi hơn cho sức khỏe tinh thần của người dùng. Công trình xuất bản trên Tạp chí Khoa học Nature Communications hôm 6/10/2020.

Nhóm các chuyên gia tại Trường Kinh doanh Columbia và Trường Quản lý Kellogg, Đại học Northwestern, Mỹ, cho biết

Phát hiện của chúng tôi chứng minh rằng

tất cả cá nhân, bất kể đặc điểm tính cách, đều có thể hưởng lợi từ việc thể hiện hình ảnh thật trên mạng xã hội

Sự thay đổi từ “cuộc sống hoàn hảo” sang “cuộc sống thực sự trông như thế này” đang là xu thế và chắc chắn sẽ tiếp tục ảnh hưởng đến cách mọi người thể hiện bản thân trên các nền tảng mạng xã hội và mạng Internet nói chung. Nhưng chia sẻ sự thật về góc học tập bừa bãi hay căn phòng lộn xộn của bạn, khuôn mặt ngái ngủ buổi sáng thì cũng không phải là ý hay. Vậy sống thật trên mạng ảo như thế nào cho phù hợp, vừa tốt cho mình vừa hữu ích với các “khán giả” hay cộng đồng mạng? Những bí kíp đơn giản dưới đây sẽ giúp bạn cách để thể hiện bản thân mình một cách chân thật và kết nối với mọi người trên khắp thế giới.

a) Hiểu chính mình.

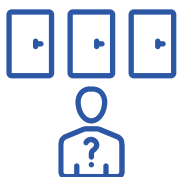


Bạn đã sống bao nhiêu năm với chính mình rồi? Bạn hẳn sẽ hiểu những điểm mạnh, điểm yếu của mình, thói quen, sở thích và cảm xúc của mình. Hãy chia sẻ nó nếu bạn thấy sẵn sàng. **Hãy LÀ con người đích của mình và thể hiện điều đó chứ không phải là điều mà người kì vọng bạn trở thành.** Bạn cũng có thể chia sẻ những trải nghiệm, câu chuyện của mình và bài học của bạn khi trải qua những chuyện đó.

Có người nghĩ rằng hướng dẫn viên thể hình phải là người có cơ thể hoàn hảo, săn chắc. Nhưng một hướng dẫn viên thể hình can đảm chia sẻ hình ảnh thừa cân, béo phì của bản thân trước đây là hành trình người đó có cơ thể khỏe mạnh như bây giờ, chắc chắn câu chuyện sẽ được rất nhiều người quan tâm.

Hay một học sinh, sinh viên giỏi xuất sắc, luôn xuất hiện đầy năng lượng chia sẻ về trải nghiệm mình đã từng trải qua những ngày căng thẳng, khó khăn ra sao mỗi khi kì thi tới. Khi bạn có thể nhìn thấy vẻ đẹp của những trải nghiệm và bài học của mình, và chia sẻ nó, mọi người cũng sẽ nhìn thấy được vẻ đẹp chân thật của bạn.

b) Thử các cách thể hiện khác nhau



Bạn biết mình là ai và bạn đang muốn nói gì, bây giờ bạn **cần tìm ra cách tốt nhất để truyền tải thông điệp của mình**. Có người thể hiện bản thân tốt nhất bằng cách viết các bài chia sẻ, viết blog, nhưng cũng có người giỏi làm những video, hay thu âm giọng nói, hay kể những câu chuyện hài hước. Có rất nhiều những nền tảng, ứng dụng khác nhau để hỗ trợ bạn, vấn đề là tìm ra cách tốt nhất để bạn giao tiếp và truyền tải thông điệp cũng như con người thật của bạn trước mọi người.

Ngay cả khi bạn đã tìm ra cách thể hiện hiệu quả nhất, hãy thử thay đổi cách bạn truyền tải thông điệp của mình.

Ví dụ, bạn thích viết và trên trang cá nhân, bạn viết những bài chia sẻ hay những câu chuyện dài tới 2.000 từ, nhưng nhận ra rằng không

có ai đang đọc chúng, chẳng mấy ai tương tác với bạn. Điều đó không có nghĩa là bạn ngừng viết, mà hãy thử chuyển sang viết những đoạn ngắn hơn, hoặc chia sẻ dần từng phần bài viết dài của bạn, hoặc chia sẻ kèm theo hình ảnh. Thử nghiệm các cách khác nhau để truyền tải thông điệp của mình và trên các nền tảng khác nhau để khám phá những gì bạn thấy thoải mái nhất VÀ mọi người phản hồi, tương tác với bạn nhiều nhất về.

c) Làm những điều khiến bạn hào hứng.



Nếu có một bí quyết nào đó chung của tất cả những người thành công và giàu có trên thế giới thì đó là “làm những điều khiến bạn thấy hào hứng”. Nếu bạn là một cô gái và thích khoa học, sửa chữa máy móc, đừng ngại làm điều mình thích và chia sẻ chúng. Hay nếu bạn là một cô nàng “bánh bèo” thích một thế giới toàn màu hồng, cũng đừng ngại là chính mình và thể hiện con người chân thật của mình. Không có một công thức chung nào cho mọi người, cũng không có một rào cản nào có thể ngăn bạn sống chân thật cả.

Bạn đam mê điều gì mà không cần phải được thúc giục? Đó là cách tương tác trực tuyến đích thực của bạn, hãy tiếp tục!

d) Hỗ trợ những người xung quanh bạn



Ai cũng muốn được sống thật với chính mình. Nếu bạn đã làm được thì hãy **ủng hộ những người bạn của mình cũng làm điều tương tự và giúp họ tỏa sáng ánh sáng chân thật của mình**. Giới thiệu bạn bè và tạo nên một vòng tròn cộng đồng kết nối chân thành. Mọi người thích thấy những người khác hỗ trợ lẫn nhau thay vì nói xấu hay chỉ trích nhau. Lòng tốt chân thành của bạn không chỉ được đánh giá cao và được xem như một luồng gió mới mà còn thu hút người khác tìm hiểu thêm về bạn

đ) Liên tục đầu tư vào sự phát triển của chính mình



Con người đích thực của bạn không phải là một người bị “mắc kẹt” hay dậm chân tại chỗ mà bạn nên phát triển và thay đổi như thế giới xung quanh bạn. Tương tự như điện thoại hay máy tính được các nhà sản xuất liên tục nâng cấp và đưa ra những phiên bản mới hơn, hấp dẫn và thú vị hơn. Bạn của thời đại 4.0 cũng như vậy! **Hãy tìm cách liên tục đầu tư “nâng cấp” bản thân** bằng các khóa học mới về tư duy, kỹ năng cá nhân hoặc bất cứ điều gì sẽ giúp bạn khám phá chính mình và chinh phục những tầm cao mới.

Đừng ngại chia sẻ những điều bạn mới học được hay sự thực tập ban đầu còn vụng về của mình với bạn bè hay cộng đồng theo dõi trực

tuyến của bạn. Hãy chia sẻ và giới thiệu những gì đã giúp trở thành phiên bản mới tốt hơn của mình và truyền cảm hứng cho mọi người.

Đó thậm chí có thể không phải là các lớp học, hay khóa học bài bản mà đơn giản có thể là các công cụ để giao tiếp với mọi người tốt hơn. Có thể bạn có một chiếc máy ảnh mới để tạo video trên YouTube tốt hơn hoặc bạn đã chuyển trang web của mình sang một nền tảng mới để kết nối với khán giả theo một cách mới, giúp cộng đồng trực tuyến của bạn cùng nhau phát triển và học hỏi.

e) Tập trung vào những gì khiến bạn thoải mái và cảm thấy an toàn



Mặc dù bạn nên ra khỏi vùng an toàn của mình một chút khi ở trên mạng và thử những điều mới, **hãy đảm bảo rằng bạn đang làm điều đó trong khả năng và điều kiện cho phép của mình**, những điều khiến bạn cảm thấy thoải mái!

Trông đẹp là một điều tốt, nhưng chỉ khi bạn cảm thấy hài lòng với những gì bạn đang thể hiện, khi bạn cảm thấy thoải mái, những người xung quanh bạn cũng sẽ cảm thấy thoải mái. Nhưng điều này đặt trong môi trường mạng thì sẽ như thế nào? Khi bạn tạo một trang web, có một trang web được thiết kế hiện đại

theo xu hướng mới có thể thu hút được nhiều người nhưng nếu bạn không cảm thấy thoải mái với một trang web như vậy, bạn cảm thấy trang web đó không phù hợp với bạn mà thích phong cách cổ điển hơn. Hãy chọn phong cách cổ điển, tiếp tục với phong cách thiết kế đó và biến nó thành của riêng bạn! Chắc chắn sẽ có những người giống như bạn tìm đến với bạn.

Hãy thoải mái với hình ảnh mà bạn đang chia sẻ với mọi người và đừng cảm thấy áp lực phải làm ra một điều gì đó khác biệt hay theo kì vọng của mọi người. Về dài hạn, mọi người sẽ đánh giá cao cách làm trung thực và khác biệt của bạn đơn giản vì đó là con người chân thật của bạn.

g) Tập trung vào những gì khiến bạn thoải mái và cảm thấy an toàn



Bạn có tiếng nói của mình, bạn đang làm việc để tạo ra uy tín và xây dựng hình ảnh chân thật của mình với mọi người, bạn đang tiếp tục phát triển và đảm bảo rằng bạn cảm thấy thoải mái trên các nền tảng bạn đang sử dụng và cách bạn chia sẻ thông điệp của mình. Điều quan trọng nữa là hãy cam kết với việc bạn đang làm.

Thể hiện bản thân thực sự và được người khác chấp nhận, quan tâm và phản hồi. Đây có lẽ là phần khó nhất của việc sống thật trên mạng ảo.

Với nhiều người, đây là cuộc đấu tranh lớn nhất

của chính họ với thương hiệu của riêng mình. Nhiều người cảm thấy xấu hổ khi “nói chuyện” với “toàn bộ cộng đồng mạng” và bạn bè và gia đình của họ nhìn thấy con người thật của mình. Liệu có bị chê cười? có bị phán xét? Có được chấp nhận và yêu thương hay không? Nhưng khi bạn thể hiện bản thân một cách chân thành và thật sự, bạn sẽ ngạc nhiên khi thấy bạn bè và gia đình ủng hộ và chấp nhận bạn. Dù khi bắt đầu, điều này có thể không thoải mái, và cần nhiều can đảm, nhưng hãy cam kết thực hiện và kiên trì thực hiện! Dần dần, việc này sẽ trở nên dễ dàng hơn và bạn sẽ thấy rằng mọi người luôn ở đó để hỗ trợ bạn thể hiện con người thật của mình trên mạng!



NỠ RỘ

CÁC TRÀO LƯU TIÊU CỰC



Mạng xã hội facebook xuất hiện tại Việt Nam, đã tạo thành một “cơn sốt” đối với giới trẻ và trở thành nơi trú ẩn những “hỉ, nộ, ái ố” của mọi người. Theo đó, nút like (thích) cũng trở nên quen thuộc với mọi người dùng khi nó thể hiện sự hưởng ứng, đồng tình, đồng cảm của mình đối với mỗi cập nhật trạng thái của bạn bè trên facebook. Sẽ chẳng có gì để nói nếu như nó được sử dụng đúng mục đích, thế nhưng nhiều người lại sử dụng nút like khá tùy tiện, lệch lạc thậm chí có người phát cuồng. Để “câu like”, một cô gái 13 tuổi ở tỉnh Khánh Hòa đăng trên dòng trạng thái (status) nội dung nếu đạt mức 1.000 lượt like cô sẽ đốt trường. Sự việc sau đó được cộng đồng mạng chia sẻ “chóng mặt” và chỉ sau một đêm, status đó đã vượt 1.000 like khiến cô gái lo sợ, tìm cách lẩn trốn bạn bè. Tuy nhiên, **do sức ép của “nút like” từ bạn bè, cộng đồng mạng mà cô gái này đã phải thực hiện bằng hành động mang xăng vào đốt trường như đã tuyên bố.** Hoặc gần đây, trào lưu “nói và làm của thanh niên Việt Nam” cũng đang nở rộ theo tuyên bố của một thanh niên sống tại Thành phố Hồ Chí Minh. Theo đó, nam thanh niên này đã tuyên bố hùng hồn trên facebook rằng “nói và làm, cần 40.000 like để tự thiêu, nhảy cầu Tân Hóa” và thanh niên này đã thực hiện thật với sự chứng kiến của hàng trăm “tín đồ” facebook tò mò.

(Theo báo Hà Nội Mới)



Lật qua để xem nội dung tiếp theo



Bài

07

QUẢN LÝ THỜI GIAN TRÊN MẠNG

1. Câu hỏi thảo luận/Đặt vấn đề:

- Tại sao cần quản lý thời gian trên mạng?
- Việc dành quá nhiều thời gian trên mạng xã hội, Internet gây ra ảnh hưởng gì? Có tác hại như thế nào đến cuộc sống của bạn?
- Làm thế nào để có thể quản lý thời gian trên mạng?



2. Khái niệm chính

Nghiện Internet

Nghiện Internet: Từ năm 1996, nhà tâm lý học Kimberly S.Young tại Hoa Kỳ đã tiến hành nghiên cứu đầu tiên và đưa ra khái niệm ‘nghiện Internet’ (Internet Addiction). Theo bà đề xuất, tình trạng ‘nghiện Internet’ có thể được xác định dựa trên 8 tiêu chí sau đây:

- ✔ Bạn tâm với Internet khi luôn nghĩ về hoạt động online của mình ở lần trước hay các lần sắp tới.
- ✔ Nhu cầu gia tăng thời gian sử dụng Internet.
- ✔ Nhiều lần thất bại khi cố gắng kiểm soát, giảm bớt hoặc ngưng sử dụng Internet.
- ✔ Bồn chồn, ủ rũ, buồn phiền hoặc dễ cáu kỉnh khi cố gắng giảm hoặc ngưng sử dụng Internet.
- ✔ Online trên mạng Internet trong thời gian nhiều hơn so với dự định ban đầu.
- ✔ Hủy hoại hoặc nguy cơ mất mối quan hệ quan trọng, mất việc làm, mất cơ hội học tập hoặc đề bạt vì Internet.
- ✔ Nói dối những người trong gia đình, nhà trị liệu hoặc những người khác để che giấu mức độ bị cuốn hút vào Internet.
- ✔ Sử dụng Internet như một cách thức để tạm tránh đối diện với những vấn đề khó khăn trong cuộc sống hay những cảm xúc khó chịu như lo lắng, thất vọng, mặc cảm...

Nếu một người

có từ 5/8 dấu hiệu kể trên trở lên,

có thể họ đang cần sự hỗ trợ từ gia đình, nhà chuyên môn cho vấn đề nghiện Internet của mình.

Tuy lệ thuộc Internet không có cơ chế giống nghiện chất kích thích nhưng nơi người nghiện vẫn xuất hiện các dấu hiệu hết sức đặc trưng tình trạng ‘nghiện’. Đó là việc gia tăng thời lượng sử dụng ngày càng nhiều (dung nạp), có sự trăn trở bận tâm và tìm kiếm xoay quanh chủ đề Internet và những phản ứng khó chịu khi tìm cách giảm sử dụng (triệu chứng cai).

Thông thường, những người ‘nghiện Internet’ sẽ có thời gian sử dụng hơn 38 giờ/ tuần cho mục đích không liên quan đến học tập hay làm việc và gây ra ra những hậu quả tiêu cực cho bản thân.

(Nguồn: Đơn vị tâm lý, Bệnh viện nhi đồng)



3. Nội dung

3.1. Tại sao cần quản lý thời gian trên mạng?

Một kết quả khảo sát của báo Dân trí[1] thực hiện năm 2019 cho thấy, thời lượng sử dụng mạng xã hội trong một ngày của giới trẻ Việt Nam trung bình là 7 giờ, khá cao so với khu vực và thế giới. Một bộ phận giới trẻ dành quỹ thời gian cho mạng xã hội rất lớn, gây nên tình trạng “nghiện” mạng xã hội ngày càng phổ biến.

Mục đích sử dụng mạng xã hội của giới trẻ rất đa dạng, trong đó, 5 mục đích chiếm tỷ lệ cao nhất gồm: Tìm kiếm, cập nhật thông tin xã hội; làm quen với bạn mới, giữ liên lạc với bạn cũ; liên lạc với gia đình, bạn bè; chia sẻ thông tin hình ảnh, video, status và để giải trí.

Việc sử dụng Internet để chơi game trực tuyến, mua sắm trên mạng, nói chuyện với bạn bè hay truy cập mạng xã hội, nghe nhạc, xem video lành mạnh thì không vấn đề gì, nhưng cần đảm bảo rằng những hoạt động này không ảnh hưởng đến cuộc sống của mình. Việc dành quá nhiều thời gian trên mạng có thể làm cho thanh thiếu niên sao nhãng những mối quan hệ với bạn bè, gia đình trong cuộc sống thực cũng như ảnh hưởng đến thời gian học tập, nghiên cứu, vận động thể chất nhà. Dành quá nhiều thời gian trên mạng cũng ảnh hưởng tiêu cực đến sức khỏe cả về thể chất và tinh thần.

Một số dấu hiệu về thể chất, tinh thần cho thấy một người đang dành quá nhiều thời gian trên mạng:

- ! Trở nên căng thẳng hơn, dễ cáu gắt, nhạy cảm với tiếng ồn, tiếng động mạnh.
- ! Trở nên rất lo lắng nếu họ không thể tìm hoặc kiểm tra được điện thoại, tài khoản mạng xã hội.
- ! Liên tục mở hay nhìn vào điện thoại không có chủ đích cụ thể.

- ! Đau đầu, đau mắt, khô mắt...
- ! Gặp vấn đề với giấc ngủ.
- ! Học tập lơ đãng, kết quả học tập giảm sút.
- ! Dành ít thời gian tương tác với bạn bè, gia đình ngoài đời thực.
- ! Gặp khó khăn để dừng các hoạt động trực tuyến như chơi game, “lướt” mạng xã hội...

3.2. Những tác hại của việc dành quá nhiều thời gian trên mạng Internet:

a) Não không có thời gian nghỉ ngơi:



Khi sử dụng dành quá nhiều thời gian, hay bất cứ khi nào rảnh rỗi lại lướt mạng Internet khiến bạn mất đi khoảng thời gian để não được thư giãn và nghỉ ngơi thực sự, gây ra căng thẳng kéo dài, mất ngủ, giảm trí nhớ.

b) Gây nghiện



Internet luôn có những trò chơi trực tuyến gây nghiện, mạng xã hội, các trang web mua sắm, xem phim trực tuyến... đều được thiết kế để thu hút người sử dụng dành nhiều thời gian hơn. Có thể nói, đây chính là một tác hại lớn của Internet đối với trẻ và cả người lớn. Một khi bị nghiện, Internet sẽ chiếm hết thời gian trong ngày thay vì các hoạt động bổ ích khác. Tệ hơn nữa là khiến người nghiện ở một mức độ cực đoan, ảnh hưởng nghiêm trọng đến chất lượng cuộc sống và công việc.

c) Giảm tương tác trực tiếp:



Hiện nay, tình trạng bạn bè dán mắt vào điện thoại thay vì nhìn vào mắt và trò chuyện trực tiếp với nhau khá phổ biến. Khi dành quá nhiều thời gian trên mạng Internet, bạn sẽ không thể tập trung vào cuộc sống thật. Đặc biệt, khi nghiện mạng xã hội khiến bạn sống “ảo” nhiều hơn sống “thật”. Thời gian cho người thật việc thật bị giảm. Điều này có thể khiến các mối quan hệ của bạn bị rạn nứt.

d) Khiến bạn lơ là mục tiêu sống:



Khi bạn quá chú tâm vào mạng xã hội và các trang web trên mạng Internet thì bạn sẽ quên đi các nhiệm vụ, mục tiêu mà bạn muốn hoàn thành. Thời gian dành cho việc phát triển bản thân, học hỏi thì bạn lại lãng phí vào việc lướt mạng và đọc các thông tin không cần thiết. Bạn sẽ dễ rơi vào trạng thái chán nản, mệt mỏi khi quá sa đà vào mạng xã hội và dẫn đến việc học sa sút, thiếu kỹ năng cần thiết cho công việc, chất lượng sống mỗi ngày giảm đi.

5. Ảnh hưởng đến sự phát triển thể chất:



Thanh thiếu niên là độ tuổi cần phát triển cả thể chất lẫn tinh thần trong môi trường giáo dục, gia đình. Chỉ dành hàng giờ để tham gia vào các mạng xã hội, chơi các trò chơi điện tử trực tuyến sẽ có hại. Việc này có thể ức chế sự phát triển thể chất của thanh thiếu niên.

3.3. Quản lý thời gian sử dụng mạng Internet.

Quản lý thời gian sử dụng mạng Internet cũng giống như việc quản lý thời gian nói chung, đó là một kĩ năng cần được thực tập thường xuyên cho tới khi trở thành một thói quen tốt của bạn.

Mạng Internet được sinh ra để làm việc cho chúng ta và được kì vọng làm tăng suất của chúng ta. Tất cả các tiện ích, ứng dụng, trí tuệ nhân tạo... để có chung mục đích làm cho cuộc sống của chúng ta dễ dàng hơn.

NHƯNG THỰC TẾ CÓ PHẢI NHƯ VẬY?

Nếu chúng ta không biết quản lý thời gian và quản lý việc sử dụng công nghệ, Internet của chính mình thì chúng sẽ chiếm lấy cuộc sống của chúng ta, trở thành sợi “dây xích” kéo chúng ta làm việc và gián đoạn cuộc sống thường ngày bất cứ khi nào, bất cứ ở đâu.

Hầu hết mọi người khó tập trung được hơn một hoặc hai phút mà không bị phân tâm bởi các thông báo như “bạn có một email mới”, “ca sĩ Y. mới đăng một status mới”, “diễn viên Z. mới đăng một bức hình/ cập nhật trạng thái”.... có vô số điều đang thu hút sự chú ý của chúng ta.

Thật ra bản thân Internet đều không xấu. Giống như bất kì một công cụ, dụng cụ nào,

TỐT XẤU LÀ DO NGƯỜI SỬ DỤNG.

Dưới đây là một số cách để chúng ta có thể khai thác được những ưu điểm của Internet đồng thời quản lý thời gian sử dụng mạng Internet của mình một cách hiệu quả, cân bằng cuộc sống “thật” và “ảo”.

✔ **HÃY CÓ MỘT DANH SÁCH VIỆC CẦN LÀM.**

Đây là điều rất quan trọng cho việc quản lý thời gian nói chung và Internet nói riêng. Danh sách việc cần làm bao gồm các nhiệm vụ, các việc cần hoàn thành với các thứ tự ưu tiên để từ đó bạn tập trung vào công việc. Sự tập trung này giúp bạn tránh được việc thay vì mở máy tính lên soạn thảo email hay làm bài tập thì lại “lạc trôi” sang một trang web mua sắm, thời gian hay một tài khoản mạng xã hội của ai đó.

✔ **ĐẶT LỊCH HẸN VỚI CÔNG VIỆC VÀ VỚI CHÍNH MÌNH.**

Bạn có thể sử dụng ứng dụng Lịch Google để cung cấp các lời nhắc nhở và các thông tin quan trọng như hẹn với ai, mấy giờ, địa điểm hẹn ở đâu, hẹn online hay offline. Bạn nên dành lịch trình cho công việc, việc học tập và các cuộc hẹn của chính mình trước khi thêm vào các yêu cầu của người khác, và trước khi bị “cuốn đi” bởi các chương trình truyền hình, các video trên mạng hay một bộ phim dài tập nào đó “ngốn” hết thời gian của bạn. Khi bạn điền vào lịch các ưu tiên và công việc của bản thân, bạn sẽ thấy rằng có những ngày ít bận rộn hơn, và bạn cũng có thể dành nhiều thời gian cho những gì là quan trọng với mình như những buổi hẹn ăn tối với gia đình, người thương, các sự kiện vui chơi, giao lưu cùng bạn bè, kế hoạch du lịch... Hãy làm chủ cuộc sống của bạn, đừng để Internet, mạng xã hội hay bất kì điều gì làm chủ cuộc sống của bạn thay bạn.

✔ **KIỂM TRA THỜI GIAN SỬ DỤNG CÁC ỨNG DỤNG TRÊN ĐIỆN THOẠI THÔNG MINH**

Bạn biết chương trình theo dõi việc sử dụng các ứng dụng trên điện thoại chứ? Hãy kiểm tra xem ứng dụng nào “hút” hết thời

gian của bạn? Liệu bạn có sử dụng ứng dụng đó một cách có mục đích và nằm trong tầm kiểm soát của bạn không? Nếu để ý thấy bản thân đang dành thời gian quá nhiều cho một ứng dụng nào đó như Twitter, Tiktok hay Youtube? Hãy đặt ra nguyên tắc cho mình: Sử dụng điện thoại có chủ đích cụ thể, chứ đừng dùng nó cho qua thời gian.

✔ **XÓA BỚT ỨNG DỤNG VÀ DỌN DẸP MÀN HÌNH CHÍNH.**

Tôi đã thử xóa ứng dụng Facebook trong vòng một tháng và cảm thấy vô cùng thoải mái, tận hưởng cuộc sống và không hề có ý định cài lại nó vào điện thoại. Tôi chỉ thỉnh thoảng mở trên website khi mình sử dụng laptop và cần cập nhật tin tức từ bạn bè, công việc. Bạn cũng có thể thử điều này. Xóa các ứng dụng mà bạn không cần hoặc không mang lại giá trị cho cuộc sống của bạn. Bên cạnh đó, hãy đảm bảo màn hình chính của bạn chỉ chứa các ứng dụng quan trọng, phục vụ cho việc học tập, công việc và giúp bạn tăng chất lượng cuộc sống.

✔ **TẮT TẮT CẢ CÁC THÔNG BÁO.**

Đây cũng là điều tôi luôn làm. Nhờ đó, tôi không bị làm phiền bởi thông báo có một email công việc đến khi đang ăn cơm với gia đình mình. Rõ ràng là bạn không cần biết ngay lập tức rằng có ai đó “tag” bạn vào một bài đăng trên mạng xã hội của họ hay có thể kiểm chế được sự tò mò phải kiểm tra ngay email vừa mới tới có nội dung gì. Dù các thông báo chỉ cách bạn 1 cái “chạm” là có thể đọc được ngay, nhưng hãy thực tập cách **DỪNG LẠI**. Hãy kiểm soát thời gian của chính mình.

SỰ LÃNG PHÍ THỜI GIAN VÀO TRUYỀN THÔNG XÃ HỘI

Dữ liệu cho thấy **hầu hết người trưởng thành đang dùng phương tiện truyền thông xã hội hơn một giờ mỗi ngày.**

Không cần bàn cãi về giá trị của hoạt động này, có một sự lãng phí thời gian để duy trì hoạt động trên mạng xã hội của bạn.

Ít nhất 1 giờ/ngày, nghĩa là 7 giờ/tuần hoặc 365 giờ một năm. Thậm chí có thể nhiều hơn.

Nghĩa là ít nhất hơn **15 ngày trong một năm bạn đã bị mất đi cho phương tiện truyền thông.** Mãi mãi.

Thời gian của bạn đáng giá ra sao? Và những gì bạn có thể thực hiện thêm với 2 tuần mỗi năm?

(Theo sách 21 quy tắc cơ bản để quản lý thời gian - Craig Jarrow, Thái Minh Trí dịch)

[1] Nguồn tham khảo: Bài “Giới trẻ Việt Nam sử dụng mạng xã hội 7 giờ mỗi ngày” - Tác giả Thế Kha trên Báo điện tử Dân trí ngày 06/11/2019



Lật qua để xem nội dung tiếp theo

Bài

08

MỘT SỐ HÌNH THỨC LỪA ĐẢO
TRÊN MẠNG PHỔ BIẾN

1. Câu hỏi thảo luận/Đặt vấn đề:

- Thế nào là lừa đảo, lừa đảo trên mạng là gì?
- Các hình thức lừa đảo trên mạng phổ biến hiện nay là gì?
- Làm thế nào để báo cáo các hành vi có dấu hiệu lừa đảo trên mạng?



2. Khái niệm chính

Lừa đảo & lừa đảo trên mạng

Lừa đảo là gì

Lừa đảo là hành vi gian dối để làm người khác tin nhằm thực hiện những mục đích vụ lợi, trái pháp luật. Trong đó động cơ của người thực hiện hành vi lừa đảo là nhằm chiếm đoạt tài sản của người khác hoặc làm cho người khác do hiểu sai sự thật mà tin tưởng ủng hộ sản phẩm/dịch vụ gây ra thiệt hại về tài sản.

Lừa đảo trên mạng là gì?

Lừa đảo trên mạng là hành vi lợi dụng mạng máy tính, mạng viễn thông, phương tiện điện tử nhằm mục đích vụ lợi, trái pháp luật như chiếm đoạt tài sản hoặc làm cho người khác hiểu sai sự thật mà tin tưởng sử dụng ủng hộ sản phẩm/dịch vụ gây ra thiệt hại về tài sản hoặc thiệt hại khác. .



3. Nội dung

3.1. Các hình thức lừa đảo trên mạng phổ biến

Lừa đảo qua hình thức mạo danh là hình thức lừa đảo phổ biến nhất trên mạng. Đối tượng lừa đảo này thường bắt đầu bằng một email, một tin nhắn trên mạng xã hội, một cuộc gọi điện thoại bất ngờ thông báo tin trúng thưởng; tin xấu hoặc tin sự cố kỹ thuật hoặc tin mời chào kiếm tiền nhanh chóng, hấp dẫn hoặc quảng cáo sản phẩm/dịch vụ tốt.

Một số hình thức lừa đảo trên mạng phổ biến:

a) Lừa đảo thông báo trúng thưởng



Đối tượng lừa đảo có thể lợi dụng mạng xã hội và các ứng dụng chuyện trò phổ biến để thông báo bạn trúng thưởng một phần quà có giá trị như xe máy, điện thoại hoặc suất học bổng hoặc voucher ưu đãi. Tuy nhiên đối tượng yêu cầu cung cấp thông tin cá nhân hoặc đặt cọc hoặc thanh toán lệ phí trước để được nhận quà tặng.

b) Lừa đảo cơ quan chức năng đang thực hiện công tác điều tra



Đối tượng lợi dụng tin nhắn hoặc cuộc gọi để thông báo tới người dùng tin xấu hoặc tin sự cố kỹ thuật. Thông thường đối tượng sẽ mạo danh cơ quan nhà nước có uy tín như cơ quan công an, thanh tra giao thông, tòa án, viện kiểm soát, điện lực,... để thông báo người dùng có vi phạm chưa được giải quyết hoặc có khoản nợ đã quá hạn nhưng không được thanh toán đúng ngày. Đối tượng sẽ yêu cầu

c) Lừa đảo nhận quà, nhận tiền từ nước ngoài



người dùng cung cấp thông tin cá nhân để được cung cấp các bằng chứng liên quan đến xử phạt, sau đó sẽ yêu cầu bị hại chuyển tiền vào các tài khoản ngân hàng do đối tượng cung cấp với lý do để phục vụ công tác điều tra rồi chiếm đoạt.

Các đối tượng lừa đảo tự giới thiệu là người nước ngoài, kết bạn, liên lạc để tạo mối quan hệ với nạn nhân thông qua mạng xã hội. Sau một thời gian trò chuyện, đối tượng cảm thấy đã tạo được lòng tin ở đối phương, sẽ thông báo muốn gửi tiền, quà từ nước ngoài về Việt Nam. Sau đó, yêu cầu người bị hại phải nộp tiền để nhận quà với các lý do khác nhau như cước vận chuyển, thuế, phí... vào các tài khoản ngân hàng do các đối tượng cung cấp rồi chiếm đoạt.

Đối tượng cũng có thể lợi dụng hoạt động bán hàng online để yêu cầu đặt mua một số lượng hàng hóa lớn và gợi ý chuyển tiền trước cho người bán thông qua dịch vụ chuyển tiền quốc tế Western Union hoặc sử dụng tài khoản đã chiếm đoạt, lừa đảo người quen để nhờ gửi tiền về cho người thân qua dịch vụ Western Union.

d) Lừa đảo là tổ chức ngân hàng, tổ chức tín dụng



- 1 Đối tượng sẽ giả lập hóa đơn chuyển tiền quốc tế từ Western Union
- 2 Gửi ảnh hóa đơn chứng từ cho bị hại, nhằm làm cho bên bán tưởng rằng phía mua hàng đã thực hiện xong lệnh chuyển tiền.
- 3 Đối tượng sẽ gửi đường dẫn giả mạo Western Union cho người bán hàng online ở Việt Nam để làm thủ tục rút tiền, trong đó có yêu cầu người bán nhập các thông tin cá nhân của ngân hàng như user, mật khẩu và mã OTP.
- 4 Ngay khi người bị hại cung cấp đầy đủ thông tin cá nhân, đối tượng sẽ chiếm đoạt toàn bộ tài khoản của người bị hại.

Đối tượng lợi dụng tin nhắn mạo danh thương hiệu các ngân hàng để gửi tin nhắn thông báo thẻ hoặc tài khoản đang tiêu dùng ở nước ngoài với khoản chi tiêu lớn, yêu cầu người dùng đăng nhập vào các links đính kèm để hủy giao dịch. Ngay khi người dùng đăng nhập, cung cấp thông tin cá nhân, mật

khẩu OTP,..đối tượng lừa đảo có thể lợi dụng để chiếm đoạt chiếm tiền trong tài khoản.

Ngoài ra đối tượng lừa đảo cố ý “chuyển nhầm” một khoản tiền đến tài khoản ngân hàng. Tiếp đó, yêu cầu người dùng trả lại số tiền kia như một khoản vay cùng với khoản lãi cắt cổ.

e) Lừa đảo kêu gọi đầu tư tài chính, tiền ảo



Các đối tượng lập ra các website đầu tư tài chính, các ứng dụng có giao diện tương tự đầu tư tài chính quốc tế rồi sử dụng nhiều thủ đoạn khác nhau để thu hút, lôi kéo nhiều người tham gia. Các sàn tiền ảo, đầu tư tài chính này cam kết người chơi sẽ được hưởng mức lãi suất cao nhưng lại an toàn, có thể rút vốn bất kỳ lúc nào, không cần đầu tư trí tuệ, thời gian.

Sau một thời gian, các sàn giao dịch thông báo dừng hoạt động để bảo trì hoặc lỗi không truy cập được, khách hàng sẽ không thể đăng nhập để rút tiền trong tài khoản.

f) Lừa đảo tuyển dụng



Lợi dụng tình hình dịch bệnh khó khăn và nắm bắt nhu cầu tìm việc làm thêm tại nhà, hiện nay một số các đối tượng xấu đã lợi dụng liên tục đăng tải tin tuyển dụng nhân viên trên các website hoặc facebook cá nhân để

lừa đảo những người tìm việc “nhẹ dạ cả tin”. Các đối tượng xấu sẽ “vẽ ra một công việc như mơ”, từ đó yêu cầu người tìm việc phải nộp phí đặt cọc, phí giữ chỗ hay phí bảo lãnh để đăng ký làm việc.

g) Lừa đảo quảng cáo sản phẩm/dịch vụ hấp dẫn



Đối tượng tung tin giả về các sản phẩm không rõ nguồn gốc nhưng lại có khả năng phòng ngừa vi rút Covid-19 hoặc chữa các bệnh nan y khiến nhiều người cả tin mua hàng.

Đối tượng có thể lợi dụng phương thức vay tiền dễ dàng qua mạng yêu cầu người dùng nộp tiền đặt cọc hoặc thanh toán chi phí duyệt hồ sơ để lừa đảo người dùng.

3.2 Báo cáo các hành vi có dấu hiệu lừa đảo trên mạng

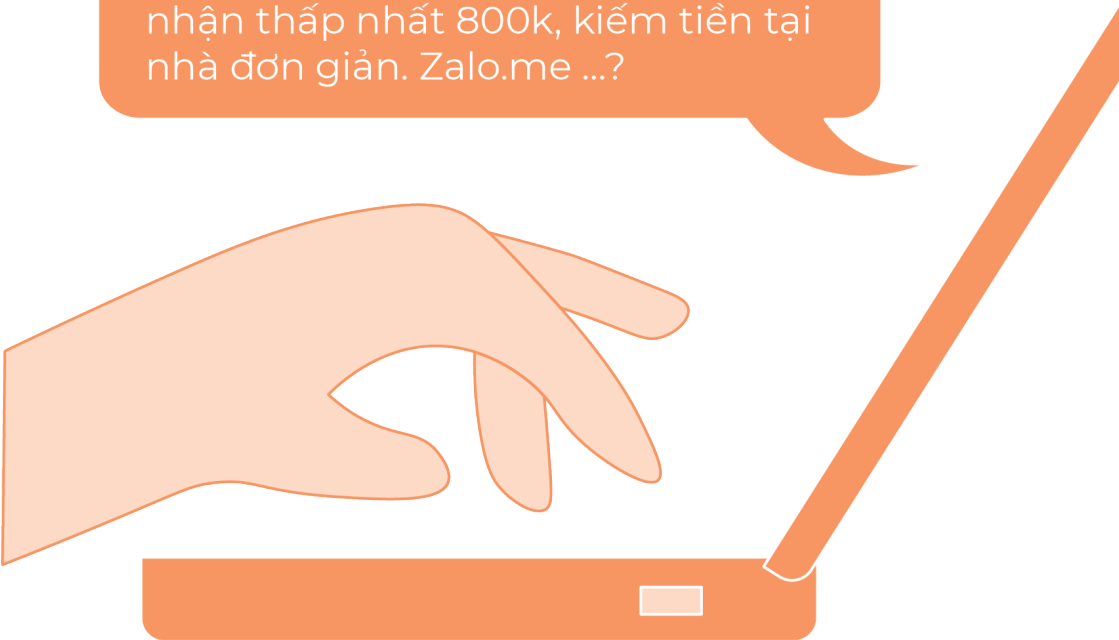
Nếu gặp phải các hành vi có dấu hiệu lừa đảo trên mạng hãy báo cáo tới các địa chỉ dưới đây để được hỗ trợ sớm nhất:

- Đường dây nóng 113 hoặc cơ quan công an nơi gần nhất;
- Đường dây nóng Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao: 069.219.4053;
- Địa chỉ <https://canhbao.ncsc.gov.vn/#/> - Trang cảnh báo an toàn thông tin Việt Nam do Trung tâm Giám sát không gian mạng – Cục An toàn thông tin vận hành.

4. Suy ngẫm

Hoạt động: “Với mức lương 6tr-36tr mỗi tháng với công việc hoàn toàn hợp pháp đảm bảo thu nhập. Mỗi ngày bạn nhận thấp nhất 800k, kiếm tiền tại nhà đơn giản. Zalo.me ...?”. Bạn đã từng nhận tin nhắn nào như thế này chưa? Bạn đã làm gì khi nhận được tin nhắn này?

Với mức lương 6tr-36tr mỗi tháng với công việc hoàn toàn hợp pháp đảm bảo thu nhập. Mỗi ngày bạn nhận thấp nhất 800k, kiếm tiền tại nhà đơn giản. Zalo.me ...?



Lật qua để xem nội dung tiếp theo

Bài

09

NHỮNG NGUYÊN TẮC VÀNG

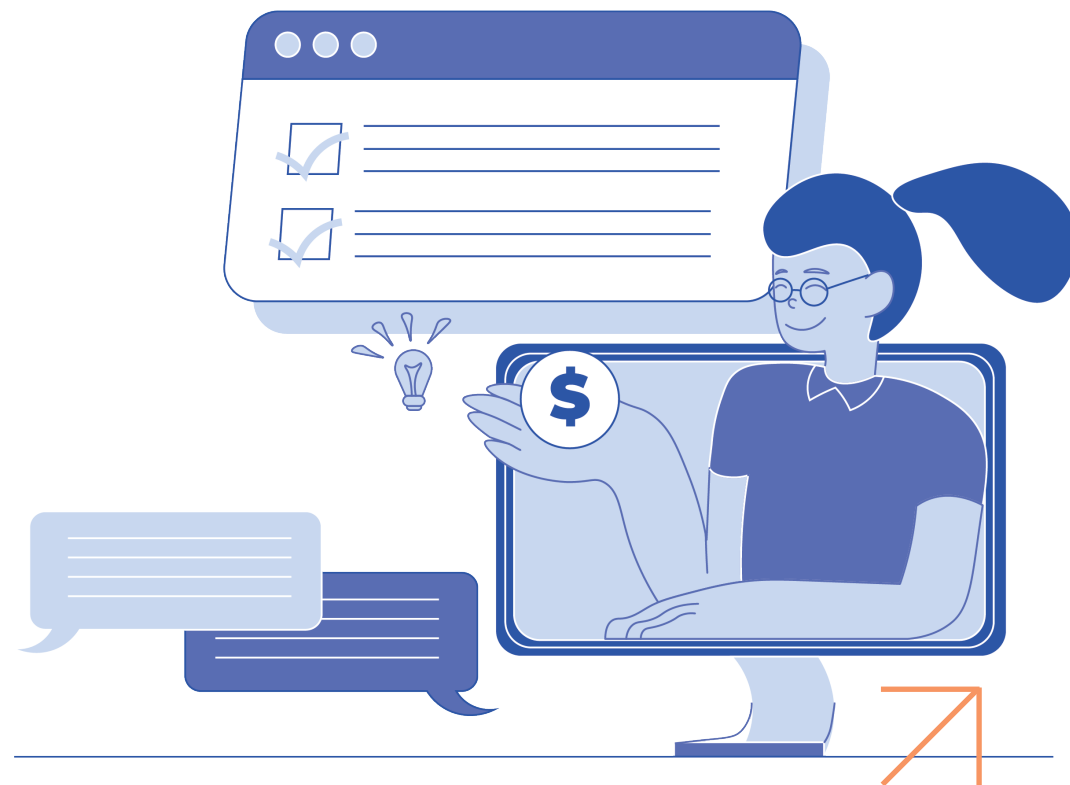
PHÒNG TRÁNH LỪA ĐẢO, MẠO DANH TRÊN MẠNG



1. Câu hỏi thảo luận/Đặt vấn đề:

Những kẻ lừa đảo kỳ vọng sẽ sử dụng các cách thức lừa đảo để đánh cắp thông tin, đánh cắp lòng tin và đánh cắp tài sản của người dùng.

Nội dung chính ở đây đưa ra 2 phương pháp cơ bản đó là Nguyên tắc 3 bước “**Chậm lại – Kiểm tra - Không gửi**” và nguyên tắc **4C**: “Cập nhật-
Cẩn trọng – Câu hỏi – Chia sẻ”.



2. Nội dung

2.1. Các hình thức lừa đảo trên mạng phổ biến

a) Chậm lại

Những kẻ lừa đảo thường tạo ra cảm giác cấp bách để chúng có thể vượt qua khả năng nhận định của bạn. Hãy dành thời gian và đặt câu hỏi để tránh bị dẫn vào tình huống xấu.

b) Kiểm tra

Tìm hiểu thêm để xác thực thông tin bạn đang nhận được. Nếu bạn nhận được một cuộc gọi không mong muốn, hãy tra cứu số ngân hàng, cơ quan, hoặc tổ chức đang gọi đến và liên hệ lại trực tiếp.

c) Dừng lại! Không gửi

Không một cá nhân hoặc cơ quan nào yêu cầu thanh toán ngay tại chỗ. Vì vậy, nếu bạn cảm thấy giao dịch này không đáng tin, hãy dừng lại vì nó có thể là như vậy đấy

2.2. Áp dụng Nguyên tắc 3 bước vào tình huống thực tế

a) Chậm lại

Kẻ lừa đảo đưa ra đề nghị: *Bạn phải hành động nhanh. Nếu bạn không thực hiện chuyển tiền bây giờ, chúng tôi buộc phải tiến hành các thủ tục tố tụng đối với bạn hoặc người thân của bạn.*

Bạn nên làm gì?

HÃY TỰ ĐẶT CÂU HỎI KHI NHỮNG THÔNG BÁO KHẨN CẤP HIỆN LÊN - Tin nhắn hiện lên có vẻ rất khẩn cấp. Tuy nhiên, các cảnh báo và tin nhắn bảo mật thực sự sẽ không bao giờ yêu cầu bạn phải thực hiện một cuộc điện thoại. Nếu bạn cho rằng có sự cố với thiết bị

b) Kiểm tra

của mình, hãy cập nhật phần mềm bảo mật và quét vi-rút.

Kẻ lừa đảo có thể đưa ra đề nghị: *Đây là cuộc gọi từ Tổng Cục Thuế. Chúng tôi đã không nhận được thanh toán thuế của bạn trong năm qua. Bạn đang vướng vào một vấn đề vi phạm pháp luật nghiêm trọng.*

Bạn nên làm gì?

ĐIỀU TRA CÔNG TY - Tìm kiếm tên đơn vị, tổ chức, doanh nghiệp hoặc số điện thoại kèm những từ khóa như “lừa đảo” hoặc “khiếu nại”. Nếu bạn đang tìm kiếm hỗ trợ về mặt kỹ thuật, hãy tìm hiểu một địa chỉ có uy tín mà bạn biết và tin tưởng.

c) Dừng lại! Không gửi

Kẻ lừa đảo có thể đưa ra đề nghị: *Hãy gửi chúng tôi mã thẻ cào điện thoại mệnh giá 200K hoặc 500K. Tôi cần 20 thẻ mỗi loại.*

Bạn nên làm gì?

TRÁNH CÁC PHƯƠNG THỨC THANH TOÁN BẤT THƯỜNG - Các đơn vị, tổ chức, doanh nghiệp hỗ trợ công nghệ hợp pháp sẽ không yêu cầu thanh toán dưới dạng thẻ quà tặng, chuyển khoản ngân hàng, ứng dụng chuyển tiền hoặc tiền mã hóa. Những hình thức thanh toán này chỉ nên được sử dụng với gia đình và bạn bè.

3. Nguyên tắc 4C

NGUYÊN TẮC 4C

Cập nhật

kỹ năng, kinh nghiệm sử dụng internet an toàn;

Câu hỏi

Báo cáo hành vi lừa đảo ngay lập tức. Chia sẻ các thủ đoạn, hình thức lừa đảo tới người thân, bạn bè để cùng cảnh giác

Cẩn trọng

Bảo mật thông tin cá nhân: Không nên tiết lộ thông tin cá nhân qua mạng hoặc qua điện thoại. Không truy cập vào các đường link gắn kèm trong nội dung tin nhắn lạ; không thực hiện thao tác trên điện thoại theo các cú pháp được hướng dẫn bởi người lạ. Kiểm tra địa chỉ e-mail và các đường dẫn cẩn thận trước khi cung cấp thông tin.

Chia sẻ

Kiểm tra, đặt câu hỏi cho mọi vấn đề

Ngoài ra, hãy lưu ý nếu phát hiện hành vi đó có dấu hiệu lừa đảo, hãy thực hiện việc báo cáo tới các địa chỉ uy tín như chúng tôi đã đề cập tới trong Bài số 8.

Nguyên tắc Chậm lại - Kiểm tra - Không gửi hay Nguyên tắc 4C đều là những bộ nguyên tắc hướng tới việc phòng tránh lừa đảo, mạo danh trên mạng. Bạn hãy lựa chọn nguyên tắc phù hợp và để áp dụng với mình nhé.

4. Suy ngẫm

Cơ quan Cảnh sát điều tra Công an tỉnh Quảng Ninh vừa tiến hành khởi tố vụ án **“Lừa đảo chiếm đoạt tài sản”**, quy định tại **Điều 174 Bộ luật Hình sự năm 2015** và đang tích cực điều tra để làm rõ.

Nạn nhân trong vụ án này là chị P.T.H (TP. Cẩm Phả, tỉnh Quảng Ninh) bị lừa đảo chiếm đoạt tài sản với số tiền hơn 822 triệu đồng.

Trước đó, ngày 3/1/2022, trong quá trình truy cập ứng dụng Facebook, chị H thấy có thư mục quảng cáo hiện thị “Tuyển dụng 2” cùng dòng chữ “Gửi tin nhắn”. Do đang có nhu cầu tìm việc làm nên chị H đã kích vào mục trên để tìm hiểu và nhận được tin nhắn qua ứng dụng Messenger với nội dung **“Tuyển dụng nhân viên bán hàng online”**.

Chị H chủ động để lại số điện thoại, sau đó tài khoản Zalo tên “Nguyễn Thùy Dung” kết bạn và tự giới thiệu là chuyên viên tư vấn của Shoppe yêu cầu chị H cung cấp thông tin cá nhân, trong đó tài khoản ngân hàng.

Dung đã cấp cho chị H một mã cộng tác viên ký hiệu là A688 rồi gửi các đường link (mỗi đường link mà Dung gửi tương ứng với một sản phẩm, các sản phẩm này đều thuộc trang web Shoppe.vn) và bảo chị H nhấp vào đường link này sẽ thấy mã sản phẩm kèm giá tiền.

Ngoài ra, Dung còn cung cấp một tài khoản ngân hàng Techcombank mang tên **“PHAM THU HA”** và hướng dẫn chị H thực hiện thao tác mua sản phẩm có trong đường link rồi thanh toán bằng cách chuyển tiền đến số tài khoản trên.

Khi đã chuyển tiền qua ứng dụng Banking, khoảng 10 phút sau tài khoản chị H nhận được số tiền đã mua sản phẩm cùng với 10% hoa hồng giá trị sản phẩm, Dung cho biết đây là hình thức kích cầu cho gian hàng để tăng doanh số bán hàng.

Với cách trên, lần đầu Dung gửi cho chị H đường link của mã sản phẩm có giá 340.000 đồng, chị H chuyển tiền đặt mua sản phẩm này và nhận lại 374.000 đồng, tiếp đó, đối tượng này gửi đường link của mã sản phẩm có giá 220.000 đồng và một mã sản phẩm có giá 639.000 đồng, kết quả chị H nhận lại được tổng là 944.900 đồng.

Do ham lợi nhuận, chị H tiếp tục bị các đối tượng lừa đảo, dẫn dắt mua bán lòng vòng, chị H đã chuyển số tiền lớn cho các đối tượng hơn 822 triệu đồng.

(Nhật Nam - Báo chính phủ điện tử - chinhphu.vn)



Theo bạn

trong câu chuyện trên có những dấu hiệu lừa đảo nào nếu chị H. biết có thể phòng tránh được? Khi phát hiện bị lừa đảo, chị H. có thể trình báo cho những đơn vị nào để được hỗ trợ?

Bạn hãy áp dụng những nguyên tắc được nêu ra trong bài vào trường hợp này như thế nào? Hãy chia sẻ để mọi người cũng biết và phòng tránh nhé.

Tài liệu tham khảo

1. Bộ Quy tắc ứng xử trên mạng xã hội, ban hành kèm theo Quyết định số 874/QĐ-BTTTT của Bộ Thông tin và Truyền thông.
2. Luật An ninh mạng 2018 - Luật số: 24/2018/QH14 ngày 12/6/2018
3. <https://scamspotter.org/scams/>
4. <https://aita.gov.vn/ki-nang-can-thiet-de-tro-thanh-cong-dan-so>
5. <https://thanhvien.vn/sinh-vien-thoi-4-0-phai-nghi-khac-lam-khac-post1023993.html>
6. <https://namdinh.gov.vn/portal/Pages/2021-3-22/Trai-nghiem-truc-tuyen-tai-Viet-Nam-ngay-cang-tot-7spwgt.aspx>
https://news.microsoft.com/vi-vn/2021/02/19/nghien-cuu-cua-microsoft-trai-nghiem-truc-tuyen-tai-viet-nam-cai-thien-ro-ret-trong-dai-dich/#_ftn2
7. <https://www.mic.gov.vn/phapdien/Pages/TinTuc/115687/dieu-3.2.LQ.16.-Truyen-dua-thong-tin-so.html>
8. <https://nacic.gov.vn/nghien-cuu-trao-doi/-/view-content/214123/phap-luat-hien-hanh-cua-viet-nam-ve-bao-ve-du-lieu-thong-tin-ca-nhan-va-quyen-rieng-tu>
9. <https://www.reputationdefender.com/what-online-reputation-management>
10. <https://www.Internetmatters.org/hub/expert-opinion/helping-young-people-express-themselves-authentically-online-to-improve-wellbeing/>
11. <https://www.edutopia.org/discussion/6-rules-being-transparent-teens-authentic-relationships-lead-engagement>
12. <https://educateempowerkids.org/is-your-teenager-a-phoney-four-steps-to-creating-authenticity-on-and-off-social-media/>
13. <https://www.wavoto.com/blog/entry/online-authenticity-starts-by-knowing-you/>
14. <https://repeller.com/how-to-be-your-most-authentic-self-online/>
15. <https://www.forbes.com/sites/forbescoachescouncil/2019/08/26/14-ways-to-discover-and-project-your-authentic-self-online-and-offline/?sh=7ab3cc197d08>
16. <https://www.scientificamerican.com/article/the-benefits-of-being-yourself-online/>
17. <http://giadinh.bvhttdl.gov.vn/ky-nang-ung-xu-van-hoa-tren-mang-xa-hoi/>



ĐỊA CHỈ CUNG CẤP CÁC THÔNG TIN HỖ TRỢ VÀ GIÚP ĐỠ NGAY LẬP TỨC

Liên hệ với cơ quan Công an các cấp hoặc gọi Đường dây nóng của Công an 113.

Đường dây nóng Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao: 069.219.4053.

Tổng đài bảo vệ trẻ em: 111

Liên hệ với cơ quan LĐ-TBXH các cấp & chính quyền địa phương.



Đơn vị hỗ trợ phát hành:

AT SCHOOL TRƯỜNG HỌC TRỰC TUYẾN

Địa chỉ: Ngõ 120 Hoàng Quốc Việt, Cầu Giấy, Hà Nội

Hotline: 034 9875 146

Email: atschool.vn@gmail.com

Website: www.atschool.vn

CẨM NANG CÔNG DÂN SỐ VĂN MINH



9 786043 812381