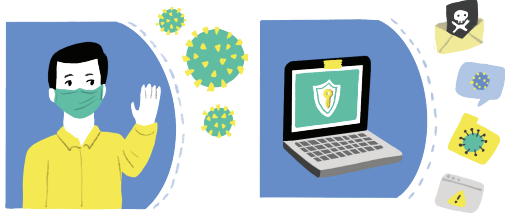


9 cách để giữ an toàn khi trực tuyến trong thời COVID-19

1 Giữ vệ sinh “số” như đeo khẩu trang



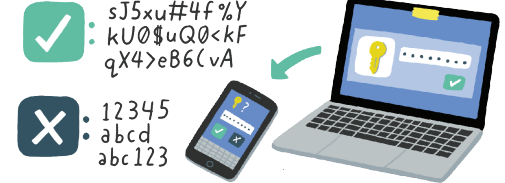
Thường xuyên cập nhật máy tính, điện thoại và chương trình diệt vi-rút. Che máy ảnh trên các thiết bị của bạn bằng băng dính chống nhìn trộm để ngăn người lạ điều khiển máy ảnh của bạn từ xa.

2 Đặt mật khẩu cho các thiết bị số của bạn



Điều này khiến người khác khó truy cập thiết bị của bạn khi không được cho phép.

3 Thay đổi mật khẩu thường xuyên



Sử dụng mật khẩu mạnh khi bạn tạo tài khoản trực tuyến cho ứng dụng hoặc khi dùng dịch vụ. Mật khẩu mạnh cần có cả chữ cái, số và biểu tượng (ví dụ @, -, #, ...). Một số tài khoản có hình thức “Xác minh 2 bước” để tăng tính bảo mật. Với hình thức này, để đăng nhập bạn cần nhập đúng cả mật khẩu và một mã xác minh dùng một lần mà hệ thống gửi đến. Cách an toàn nhất là dùng ứng dụng hoặc khóa token để nhận mã, hoặc có thể qua tin nhắn điện thoại (SMS).

4 Cố gắng ẩn danh khi trình duyệt web



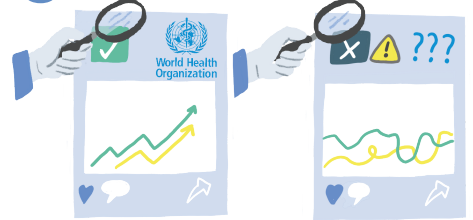
Mọi hoạt động trực tuyến của bạn đều được ghi lại. Điều này giúp lướt web dễ dàng hơn, nhưng cũng đồng nghĩa với việc các công ty có thể theo dõi những gì bạn làm. Những trình duyệt như Chrome và Safari (hoặc có thể chính trình duyệt mà bạn đang dùng) thu thập các thông tin về sở thích và vị trí của bạn để có thể gửi cho bạn quảng cáo có mục đích. Trong thời kỳ COVID-19, cách thức này đã được dùng để bán các phương pháp chữa bệnh giả. Bạn có thể sử dụng trình duyệt ở “chế độ ẩn danh” hoặc dùng trình duyệt an toàn như **Tor Browser**.

5 Nghĩ trước khi ‘nhấp link’



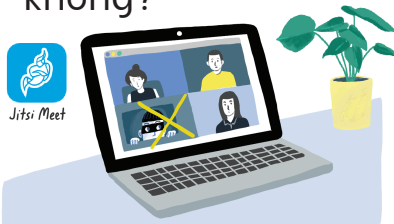
Đây có thể là thể một trò lừa đảo! Những đường link trong thư điện tử, tin nhắn trên các ứng dụng và tin nhắn điện thoại (SMS) với nội dung như cung cấp các thông tin khẩn cấp về COVID-19 hoặc thông báo rằng bạn đã trúng thưởng, hoặc yêu cầu bạn đặt lại mật khẩu tài khoản của bạn đều có thể do một người nào đó gửi đi nhằm ăn cắp thông tin cá nhân và mật khẩu của bạn. Hành vi này được gọi là tấn công giả mạo (phishing).

6 Tin thật hay Tin giả?



Không phải tất cả các thông tin về COVID-19 đều đúng và chính xác. Trước khi chia sẻ lại bất cứ thông tin gì trên mạng xã hội, bạn cần kiểm chứng lại với các nguồn đáng tin cậy như Bộ Y tế hoặc Tổ chức y tế thế giới.

7 Có nên gọi điện trực tuyến (Videochat) hay không?



Hội nghị trực tuyến đang ngày càng phổ biến trong bối cảnh đại dịch nhưng hiện nay cũng có rất nhiều kẻ nghe trộm. Zoom là một ứng dụng rất phổ biến và bạn có thể dùng nó một cách an toàn hơn bằng cách mở Zoom trên trình duyệt Chrome thay vì cài đặt phần mềm vào điện thoại/máy tính cá nhân. Ngoài ra, bạn cũng có thể sử dụng các công cụ khác như Skype, Google Meet và Microsoft Teams. Nếu bạn thực sự quan tâm đến bảo mật, hãy thử ứng dụng **Jitsi Meet**.

8 Sử dụng tin nhắn an toàn



Các ứng dụng tin nhắn như Facebook Messenger, Viber, WhatsApp và Telegram (hoặc có thể chính ứng dụng mà bạn hay dùng) đã bị lợi dụng để phát tán các “tin giả” về COVID-19. Nếu có thể, bạn nên sử dụng các ứng dụng trò chuyện được mã hóa (như **Signal** hoặc **Session**) để ngăn chặn những kẻ nghe lén.

9 Thư điện tử và quyền riêng tư



Mặc dù các dịch vụ email phổ biến như Gmail cung cấp một số tính năng bảo mật, các dịch vụ của Gmail và các bên khác vẫn có thể xem trộm thư điện tử của bạn để thu thập thông tin về bạn. Nếu bạn lo ngại về quyền riêng tư, bạn có những lựa chọn như **Riseup** và **Proton-mail**, đây là những dịch vụ miễn phí và cung cấp đầy đủ dịch vụ email được mã hóa để ngăn chặn xem trộm, tuy nhiên để sử dụng bạn cần đăng ký tài khoản.

2021

Tháng 1

CN	T2	T3	T4	T5	T6	T7
				1	2	
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Tháng 2

CN	T2	T3	T4	T5	T6	T7
		1	2	3	4	5
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28						

Tháng 3

CN	T2	T3	T4	T5	T6	T7
		1	2	3	4	5
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

Tháng 4

CN	T2	T3	T4	T5	T6	T7
			1	2	3	
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Tháng 5

CN	T2	T3	T4	T5	T6	T7
					1	
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

Tháng 6

CN	T2	T3	T4	T5	T6	T7
			1	2	3	4
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Tháng 7

CN	T2	T3	T4	T5	T6	T7
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Tháng 8

CN	T2	T3	T4	T5	T6	T7
		1	2	3	4	5
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Tháng 9

CN	T2	T3	T4	T5	T6	T7
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

Tháng 10

CN	T2	T3	T4	T5	T6	T7
				1	2	
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Tháng 11

CN	T2	T3	T4	T5	T6	T7
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

Tháng 12

CN	T2	T3	T4	T5	T6	T7
				1	2	3
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Giấy phép và Khuyến cáo:

Ấn phẩm này được cấp phép theo giấy phép CC BY-SA 4.0 (Ghi công-Chia sẻ tương tự). Sáng kiến phát triển mã Việt Nam không đại diện hay chịu trách nhiệm, cả về khía cạnh thực tế và luật pháp, về tính chính xác, toàn vẹn và tương thích của dữ liệu và tài liệu được công bố hoặc tham chiếu.

Ấn phẩm này được thực hiện với sự hỗ trợ của SPIDER. Các quan điểm và ý kiến được trình bày trên ấn phẩm này không nhất thiết phản ánh quan điểm của SPIDER.

