Câu hỏi thường gặp của bệnh nhân – Chăm sóc ảo về bảo mật

1. Làm cách nào để biết lượt truy cập video của tôi sẽ được bảo mật?

Bảo vệ quyền riêng tư của khách hàng trong cuộc gọi video bởi nhà cung cấp là vấn đề rất được quan tâm. Một trong những vấn đề mà "Đạo luật về trách nhiệm giải trình và cung cấp thông tin bảo hiểm y tế" (HIPAA) rất chú trọng đó là bảo vệ và xử lý an toàn một số thông tin nhất định, được gọi là "Thông tin sức khỏe được bảo vệ". Ví dụ: nhà cung cấp dịch vụ chăm sóc sức khỏe của bạn phải có sẵn các hệ thống để đảm bảo rằng chỉ những cá nhân được ủy quyền mới có quyền tiếp cận thông tin về sức khỏe của bạn, cho dù đó là thông tin được ghi chép lại trên các tài liệu hay được lưu trữ trong hệ thống máy tính. Các quy định của HIPAA cũng áp dụng cho bất kỳ thông tin nào được truyền qua internet, bao gồm cả các lượt truy cập video.

Để tuân thủ HIPAA, nhà cung cấp dịch vụ chăm sóc sức khỏe của bạn phải sử dụng giải pháp ảo đáp ứng các tiêu chuẩn nghiêm ngặt của HIPAA. Vui lòng liên hệ với nhà cung cấp dịch vụ chăm sóc sức khỏe của bạn nếu có bất kỳ câu hỏi hoặc thắc mắc nào về quyền riêng tư và bảo mật của thông tin được chia sẻ trong phiên chăm sóc sức khỏe từ xa của bạn.

---

2. Các biện pháp bảo vệ của chăm sóc ảo là gì?

HIPAA yêu cầu các nhà cung cấp tích hợp mã hóa và các biện pháp bảo vệ khác vào tương tác của họ với bệnh nhân. Tất cả các chuyên gia y tế hoặc tổ chức chăm sóc sức khỏe cung cấp dịch vụ từ xa cho bệnh nhân tại nhà của họ hoặc tại các trung tâm cộng đồng phải tuân thủ các nguyên tắc của HIPAA. Các quy định về quyền riêng tư và bảo mật của HIPAA cung cấp các biện pháp bảo vệ cho thông tin sức khỏe có thể nhận dạng được. Quy tắc quyền riêng tư của HIPAA thiết lập các giới hạn đối với việc sử dụng và tiết lộ thông tin sức khỏe có thể nhận dạng và Quy tắc bảo mật của nó thiết lập các biện pháp bảo vệ kỹ thuật, vật lý và hành chính để bảo vệ thông tin sức khỏe điện tử có thể nhận dạng được. Ví dụ: mã hóa dữ liệu trên thiết bị lưu trữ và khi truyền là một "đặc tả triển khai có thể giải quyết được" theo Quy tắc bảo mật. Điều này có nghĩa là các dữ kiện được sẽ được mã hóa theo quy định của HIPAA, trừ khi các dữ kiện đó không "hợp lý và phù hợp". Ngoài ra, quy định nêu rõ rằng các nhà cung cấp được yêu cầu về việc áp dụng các giao thức quản lý danh tính và kiểm soát truy cập.

---

3. Những rủi ro khi sử dụng Wi-Fi công cộng trong quá trình khám sức khỏe từ xa của tôi là gì?

Truy cập Wi-Fi trong quán cà phê, thư viện, sân bay, khách sạn và các địa điểm công cộng khác rất thuận tiện, nhưng thường không an toàn. Việc bạn phải nhập mật khẩu để đăng nhập không có nghĩa là các hoạt động trực tuyến của bạn đã được mã hóa. Wi-Fi công cộng có thể tiềm ẩn rất nhiều rủi ro vì những lý do khác nhau.

Do dó, một số mạng không dây thường sử dụng giao thức mã hóa. Cũng cần lưu ý đến điểm phát sóng Wi-Fi giả mạo. Không nên sử dụng các điểm truy cập Wi-Fi công cộng để thực hiện các cuộc thăm khám sức khỏe qua mạng. Ban nên cân nhắc về việc sử dụng dữ liệu di động của bạn thay cho Wi-Fi. (Lưu ý: Bạn có thể bị tính phí cho việc sử dụng dữ liệu này, phụ thuộc gói cước di động của bạn).

4. Một số mối đe dọa bảo mật phổ biến

- **Lừa đảo**

  Lừa đảo xảy ra khi kẻ tấn công giả vờ là một liên hệ đáng tin cậy, người dùng sẽ bị những kẻ lừa đảo dụ dỗ để nhấp vào một đường liên kết độc hại; tải xuống một tệp độc hại; hoặc cung cấp quyền truy cập cho kẻ lừa đảo vào những thông tin nhạy cảm, chi tiết tài khoản hoặc thông tin đăng nhập.

- **Các phần mềm tấn công**

  Phần mềm độc hại bao gồm nhiều mối đe dọa an ninh mạng khác nhau, bao gồm chương trình độc hại Trojan và vi rút. Tất cả đều liên quan đến mã độc mà tin tặc tạo ra để truy cập mạng, đánh cắp thông tin hoặc phá hủy dữ liệu trên máy tính. Phần mềm độc hại thường được tải xuống từ các trang web độc hại, email spam hoặc do thiết bị được kết nối với các thiết khác đã bị tấn công.

- **Phần mềm tống tiền**

  Phần mềm tống tiền là một loại phần mềm độc hại khiến cho thiết bị bị lây nhiễm và bị hạn chế quyền truy cập cho đến khi trả tiền chuộc. Phần mềm tống tiền thường được phát tán thông qua các email lừa đảo và thường khai thác các lỗ hổng của phần mềm.

- **Cuộc tấn công xen giữa "Man in the Middle" (MitM)**

  Trong trường hợp này, kẻ tấn công nằm ở vị trí giữa người gửi và người nhận tin nhắn điện tử và chặn những tin nhắn đó, hoặc có thể thay đổi tin nhắn khi chuyển tiếp cho người nhận. Còn người gửi và người nhận vẫn tin rằng họ đang giao tiếp trực tiếp với nhau.

5. Phần mềm chống vi-rút và chống phần mềm độc hại bảo vệ máy tính như thế nào?

Lợi ích của việc sử dụng phần mềm chống vi-rút và phần mềm chống phần mềm độc hại

- Phát hiện và bảo vệ chống lại phần mềm độc hại, vi-rút và phần mềm có hại khác trong thời gian thực
- Chứa các thành phần phát hiện và phản hồi chống lại các phần mềm tống tiền và chống khai thác chủ động
- Ngăn chặn các nỗ lực xâm nhập và lừa đảo
- Hoạt động linh hoạt với các chế độ quét thủ công và theo lịch trình
- Cung cấp các phương pháp tiếp cận theo lớp để bảo mật máy tính

6. Lợi ích của việc sử dụng tường lửa khi thực hiện khám sức khỏe từ xa

Tường lửa giúp bảo vệ chống lại những kẻ tấn công mạng bên ngoài bằng cách bảo vệ máy tính hoặc mạng khỏi lưu lượng mạng độc hại hoặc không cần thiết. Tường lửa cũng có thể ngăn phần mềm độc hại truy cập vào máy tính hoặc mạng thông qua internet. Tường lửa có thể được định cấu hình để chặn dữ liệu từ một số vị trí nhất định (ví dụ: địa chỉ mạng máy tính), các ứng dụng hoặc cổng và cho phép dữ liệu liên quan, cần thiết đi qua.

---

7. Phần mềm độc hại là gì và làm cách nào để loại bỏ nó?

Phần mềm độc hại (Malware) là viết tắt của *malicious software*, tức phần mềm được tin tặc sử dụng để làm suy yếu chức năng của thiết bị, đánh cắp dữ liệu hoặc thậm chí giành quyền kiểm soát chính thiết bị đó. Thông thường, phần mềm độc hại được tải xuống vô tình khi người dùng mở một tệp bị nhiễm hoặc truy cập một trang web bị nhiễm phần mềm độc hại. Khi phần mềm độc hại ở trên máy tính, nó sẽ khởi động một loại tấn công cụ thể dựa trên thiết kế của nó. Ví dụ: “keylogger” ghi lại từng lần gõ phím và báo cáo thông tin này cho tin tặc, những người đang tìm kiếm tên của người dùng, mật khẩu và các thông tin đăng nhập nhạy cảm khác. “Trojan” thường giả mạo là phần mềm hữu ích hoặc lành tính, ví dụ: phần mềm diệt vi-rút hoặc trò chơi giả mạo. Điều này lừa người dùng mở Trojan, cấp quyền truy cập vào các tệp hệ thống cho phần mềm độc hại này hoặc tạo điều kiện cho việc tải xuống nhiều phần mềm độc hại hơn.

Bạn có thể bảo vệ máy tính của mình khỏi phần mềm độc hại bằng cách cài đặt phần mềm chống vi-rút và thực hiện quét vi-rút định kỳ. Nếu máy tính của bạn đang chạy chậm hoặc thực hiện các hành động bất thường (chẳng hạn như "nhắc nhở" bạn tải xuống phần mềm lạ), thì có nghĩa là nó có thể đang bị nhiễm phần mềm độc hại. Hãy thực hiện quét diệt vi-rút để kiểm tra, xác định và xóa phần mềm độc hại khỏi thiết bị của bạn.

---

8. Tại sao mật khẩu mạnh lại quan trọng và cách tạo mật khẩu mạnh

Tạo mật khẩu mạnh đóng vài trò cực kì quan trọng, bạn nên tạo mật khẩu độc nhất cho tất cả các thông tin đăng nhập và tài khoản trực tuyến của bạn, chứ không chỉ những mật khẩu được sử dụng cho việc khám sức khỏe từ xa. Mật khẩu mạnh đóng vai trò rất quan trọng trong việc giữ an toàn cho các tài khoản trực tuyến và thông tin cá nhân khỏi tội phạm mạng. Việc bật xác thực hai yếu tố sẽ cung cấp một lớp bảo mật bổ sung cho tài khoản.

Các bước để tạo mật khẩu mạnh:

Bước 1: Sử dụng năm từ khác nhau liên quan đến một kỷ niệm là duy nhất đối với bạn. (ví dụ: Learntorideabikeatfive)

Mật khẩu càng dài thì càng khó đoán. Không sử dụng thông tin cá nhân như tên, số chứng minh thư nhân dân/căn cước công dân/hộ chiếu, ngày sinh hoặc thông tin khác có thể dễ dàng có được thông qua tìm kiếm trực tuyến.

Bước 2: Sử dụng chữ in hoa và chữ thường, số hoặc ký hiệu để làm cho việc bẻ khóa trở nên khó khăn hơn. (ví dụ: LearnttoRIDEabikeat5)

Hãy đảm bảo rằng mật khẩu của bạn không thể dự đoán được theo mẫu. Điều này có nghĩa là người khác khó có khả năng đoán ra mật khẩu, ngay cả khi có sự trợ giúp của các công cụ đặc biệt. Một số ví dụ về các mẫu mật khẩu dễ đoán bao gồm:

- Sử dụng các cụm từ phổ biến (ví dụ, maytheforcebewithyou)
- Viết hoa chữ cái đầu tiên của mật khẩu (ví dụ, Livelongandprosper)
- Thêm một số ở cuối mật khẩu (ví dụ, qwerty1)
- Thay thế một chữ cái bằng một số hoặc ký hiệu (ví dụ, p@ssw0rd)

Sau khi tạo thành công một mật khẩu mạnh, hãy bật 2FA. 2FA là viết tắt của xác thực hai yếu tố, là chức năng sẽ bổ sung thêm một lớp bảo mật cho tài khoản của bạn.

---

9. Cách cập nhật trình duyệt internet bảo vệ máy tính

Việc cập nhật trình duyệt internet sẽ cung cấp khả năng bảo vệ vượt trội chống lại các chiêu trò gian lận, vi-rút, Trojan, các cuộc tấn công lừa đảo và các mối đe dọa khác. Nó cũng có thể giải quyết các lỗ hổng bảo mật có trong trình duyệt hiện tại của bạn. Nhiều bản cập nhật trình duyệt được phát hành để chống lại những vấn đề này. Để đảm bảo an toàn và bảo mật tối ưu khi sử dụng internet, hãy luôn chạy phiên bản mới nhất của trình duyệt bạn đã chọn, được hệ điều hành của bạn hỗ trợ.

---

11. Những chiêu trò lừa đảo nào cần biết?

Không mở tệp đính kèm đáng ngờ hoặc nhấp vào liên kết bất thường trong tin nhắn. Chúng có thể xuất hiện trong email, mẩu tin, bài đăng, quảng cáo trực tuyến, tin nhắn hoặc tệp đính kèm. Đôi khi chúng cũng được ngụy trang thành những nguồn được biết đến và đáng tin cậy.

Biết cách thức và thời điểm bạn sẽ được liên hệ để khám sức khỏe từ xa hoặc để có được bất kỳ thông tin theo dõi nào. Nếu bạn nhận được một cuộc gọi hoặc email đáng ngờ về việc theo dõi sức khỏe từ xa của mình, hãy liên hệ với nhà cung cấp dịch vụ chăm sóc sức khỏe của bạn. Phòng cháy hơn chữa cháy.

---

12. Lừa đảo qua mạng là gì và cách phòng tránh

Lừa đảo là bất kỳ loại thông tin liên lạc kỹ thuật số hoặc điện tử nào được thiết kế cho các mục đích xấu. Đây là một kiểu tấn công kỹ thuật xã hội sử dụng mạo danh và các mánh khóe, thường là thuyết phục nạn nhân cung cấp thông tin cá nhân như thông tin đăng nhập, tài khoản ngân hàng thông tin, số an sinh xã hội hoặc dữ liệu nhạy cảm khác.

Mục tiêu của tội phạm mạng là sử dụng những thông tin này để lừa đảo nạn nhân theo một cách nào đó, ví dụ như: ăn cắp tiền, chiếm một hoặc nhiều tài khoản, tạo tài khoản mới lừa đảo hoặc sử dụng tín dụng. Trong một số trường hợp, mục tiêu cuối cùng của kẻ tấn công là chiếm đoạt thiết bị của nạn nhân bằng phần mềm độc hại. Mục tiêu của thủ phạm cũng có

thể là lấy quyền truy cập (thông qua nạn nhân) vào các tài nguyên có giá trị khác bao gồm mạng doanh nghiệp, hệ thống, dữ liệu hoặc tài sản trí tuệ.

Khuyến nghị cho cá nhân:

- Hãy thận trọng với tất cả các email và tin nhắn văn bản không mong muốn.
- Di chuột qua các liên kết được nhúng (không nhấp vào) để hiển thị URL thực tế và so sánh nó với liên kết được hiển thị.
- Không bao giờ nhấp vào liên kết được nhúng, ngay cả khi bạn cho rằng chúng đáng tin cậy. Thay vào đó, hãy sử dụng trình duyệt để tìm kiếm URL chính xác.
- Không bao giờ mở tệp đính kèm dưới bất kỳ hình thức nào trong email nếu bạn không biết chắc. Trong email từ những người gửi đã biết, hãy xác minh riêng các tệp đính kèm trước khi mở chúng.
- Vui lòng liên hệ với nhà cung cấp dịch vụ chăm sóc sức khỏe của bạn về email hoặc tin nhắn văn bản có liên kết nhúng hoặc tệp đính kèm để xác thực thông tin này và đảm bảo rằng quyền riêng tư của bạn được bảo vệ.
- Sử dụng phần mềm chống vi-rút và phần mềm chống phần mềm độc hại trên các thiết bị cá nhân của bạn và luôn cập nhật chúng
- Sử dụng xác thực đa yếu tố trên mọi tài khoản có cung cấp chức năng này. Điều này giúp ngăn chặn tội phạm mạng truy cập vào tài khoản của bạn.

13. Tôi nên sao lưu dữ liệu của mình như thế nào?

Bạn có thể tạo và lưu trữ các bản sao lưu thường xuyên của tất cả thông tin có giá trị trên thiết bị của mình bằng cách sử dụng phương tiện bên ngoài hoặc dịch vụ dựa trên ứng dụng web qua internet. Quá trình này có thể được đơn giản hóa và tự động hóa bằng cách sử dụng ứng dụng sao lưu của bên thứ ba. Đảm bảo việc mã hóa bản sao lưu của bạn để bảo vệ tính bảo mật và toàn vẹn của thông tin của bạn. Sao lưu dữ liệu quan trọng để giảm thiểu các hậu quả nếu dữ liệu bị mất, bị hỏng, bị nhiễm độc hoặc bị đánh cắp.

14. Tôi nên xóa những mục nào trước khi tiến hành khám sức khỏe từ xa?

Trước khi bắt đầu cuộc trò chuyện với nhà cung cấp dịch vụ chăm sóc sức khỏe của bạn, hãy đảm bảo rằng bạn đã loại bỏ các mục không cần thiết để thảo luận về các mối quan tâm về sức khỏe của bạn. Các thiết bị công nghệ không được sử dụng để liên hệ với nhà cung cấp dịch vụ chăm sóc sức khỏe của bạn nên được gỡ bỏ để tránh sự thu thập thông tin nhạy cảm tiềm ẩn. Ví dụ như camera an ninh gia đình hoặc trợ lý ảo.