

9. Làm thế nào sử dụng điện thoại di động một cách an toàn nhất

Điện thoại di động đã trở thành một phương tiện liên lạc thiết yếu hàng ngày của chúng ta. Hầu hết các máy điện thoại di động đều có khả năng thoại và gửi tin nhắn. Với kích thước nhỏ gọn, giá thành khá rẻ và tính ứng dụng cao khiến những thiết bị này rất hữu ích cho các nhà hoạt động trong hoạt động liên lạc và tổ chức.

Điện thoại di động ngày càng được trang bị thêm nhiều tính năng. Chúng có thể được tích hợp thiết bị định vị vệ tinh [GPS](#)^[1], khả năng đa phương tiện (ảnh, phim, ghi âm và truyền dữ liệu), xử lý dữ liệu và truy cập Internet. Tuy nhiên, phương thức hoạt động của mạng di động và cơ sở hạ tầng về cơ bản có nhiều khác biệt so với mạng Internet. Điều này nảy sinh thêm vấn đề về an ninh, bảo mật riêng tư người dùng và sự toàn vẹn thông tin và liên lạc.

Tình huống Cơ bản

Borna và cậu con trai Delir đều là công nhân trong một nhà máy và họ đang giúp đỡ tạo lập một hiệp hội công nhân. Những nỗ lực của họ đang gặp phải sự cản trở của những ông chủ nhà máy, những kẻ có sự hậu thuẫn của chính quyền địa phương. Người đốc công của Borna đã cảnh báo ông rằng ông có thể đang nằm trong sự theo dõi của bản quản lý nhà máy và cần đề phòng với các mối liên hệ. Borna vừa mua một chiếc điện thoại cho mục đích công việc của hiệp hội. Delir hướng dẫn cha mình sử dụng chiếc điện thoại mới này một cách an toàn trong công tác tổ chức hoạt động.

Những điều bạn có thể học được trong chương này

- Vì sao việc liên lạc và lưu dữ liệu trên điện thoại di động là không an toàn
- Những bước cần thực hiện để tăng cường an ninh trong việc sử dụng điện thoại di động
- Làm thế nào để giảm thiểu nguy cơ bị nghe trộm hoặc theo dõi qua điện thoại di động
- Làm thế nào để tăng cường tối đa việc ẩn danh khi sử dụng điện thoại di động

9.1 Điện thoại di động và vấn đề an ninh bảo mật

Chúng ta cần có những quyết định khôn ngoan khi sử dụng điện thoại di động nhằm bảo vệ bản thân, các đối tác liên lạc và dữ liệu của mình. Phương thức mạng di động và cơ sở hạ tầng hoạt động có thể ảnh hưởng rất lớn tới khả năng bảo đảm an toàn thông tin, tính riêng tư và bảo mật truyền thông của người dùng.

- Mạng di động thường là các mạng riêng được sở hữu và vận hành bởi các nhân tố thương mại, có thể nằm dưới sự kiểm soát độc quyền của chính quyền. Nhân tố thương mại này (có thể là chính quyền), thực tế có quyền tối đa truy cập thông tin và liên lạc của khách hàng cũng như khả năng truy cập, can thiệp các cuộc gọi, tin nhắn hay giám sát vị trí của thiết bị liên lạc (nghĩa là vị trí người sử dụng thiết bị đó)
- Bản thân các Hệ điều hành dùng cho điện thoại di động cũng được nhà sản xuất thiết kế riêng hoặc thay đổi theo yêu cầu của các nhà cung cấp dịch vụ viễn thông để sử dụng trên mạng di động của họ. Kết quả là những Hệ điều hành này có thể chứa nhiều tính năng ẩn cho phép nhà cung cấp dịch vụ giám sát chặt chẽ hơn một thiết bị liên lạc bất kỳ nào đó.
- Số lượng các tính năng mới cho điện thoại di động tăng mạnh trong vài năm trở lại đây. Những chiếc điện thoại di động mới thực chất là những chiếc máy tính bỏ túi có thể kết nối Internet có tính năng điện thoại.

Để có thể vạch ra những mảng cần được bảo vệ trong quá trình truyền thông của mình, bạn cần tự đặt ra một số câu hỏi cho bản thân: Nội dung của những cuộc gọi hay nhắn tin của mình là gì? Mình liên lạc với ai, vào lúc nào? Mình gọi điện từ đâu? Thông tin thường dễ bị xâm phạm bởi nhiều cách:

- **Thông tin có khả năng bị xâm phạm khi được gửi từ một chiếc điện thoại di động**
Ví dụ: Một nhà cung cấp dịch vụ viễn thông có thể truy cập toàn bộ các tin nhắn và thoại được truyền trên mạng của họ. Các nhà cung cấp dịch vụ viễn thông hầu hết các nước thường buộc phải ghi lại tất cả các cuộc liên lạc trong mạng. Ở một số quốc gia, dịch vụ viễn thông nằm dưới sự kiểm soát độc quyền của chính quyền sở tại. Các cuộc gọi và tin nhắn cũng có thể bị nghe trộm bởi một kẻ thứ ba trong vùng lân cận gần gần nơi gọi sử dụng các thiết bị không hề đắt tiền.
- **Thông tin dễ bị xâm phạm trong điện thoại của cả người nhận lẫn người gửi**
Ví dụ: Điện thoại di động có thể được dùng để lưu trữ đủ loại thông tin: nhật ký cuộc gọi, tin nhắn đã gửi và nhận, thông tin địa điểm liên lạc, ảnh, các đoạn phim, tệp văn bản. Những dữ liệu này để lộ mạng lưới liên lạc và thông tin cá nhân của bạn và các đồng nghiệp. Bảo mật những thông tin này rất khó, thậm chí với nhiều loại điện thoại điều này là không thể. Các điện thoại di động đời mới thường là những chiếc máy tính-bỏ túi. Càng có nhiều tính năng mức độ rủi ro bảo mật càng cao. Hơn nữa, điện thoại kết nối vào Internet cũng chính là những điểm yếu bảo

mật của mạng máy tính và của mạng Internet.

- **Điện thoại để lộ vị trí của bạn**

▮ Ví dụ: Một phần trong quá trình hoạt động, mọi điện thoại đều tự động và thường xuyên gửi thông tin xác định vị trí của nó về cho nhà cung cấp dịch vụ. Hơn thế nữa, nhiều điện thoại ngày nay có tích hợp tính năng GPS ^[1], và các thông tin vị trí chính xác có thể được nhúng vào trong các dữ liệu khác như ảnh, tin nhắn SMS và các yêu cầu gửi vào mạng Internet gửi từ điện thoại.

Cách mạng về công nghệ mang lại nhiều tính năng mới đồng thời nhiều rủi ro mới.

Borna: Này con trai, ba vừa quyết định từ bây giờ sẽ chỉ sử dụng cái điện thoại di động này để tổ chức các cuộc họp, vì ba nghĩ họ có thể theo dõi điện thoại tại nhà máy và có thể cả ở nhà nữa.

Delir: Cha à, thật tuyệt là cuối cùng ba cũng có một chiếc điện thoại di động, nhưng bố có biết chiếc điện thoại này có thể và không thể làm gì không?

Borna: Tất nhiên rồi: đây là một chiếc điện thoại! Con gọi ai đó, con nói với họ và họ nói với con. Con có thể gọi từ bất kỳ đâu. VÀ, con còn có thể dùng điện thoại để gửi tin nhắn cho những người khác, và những tin gửi cho con sẽ hiện lên trên điện thoại này.

Delir: Tất cả các điều đó là chính xác nhưng đó không phải là tất cả. Có rất nhiều điều ba có thể làm được với chiếc điện thoại này. Nhưng hãy trao đổi một chút về nguy cơ và cảnh báo an toàn đặc biệt là khi ba cho rằng có ai đó đang cố gắng tìm hiểu xem cha đang liên lạc với những ai và đang trao đổi những gì.

Các phần tiếp theo sẽ thảo luận một số bước đơn giản bạn cần thực hiện nhằm giảm các mối nguy cơ an ninh khi sử dụng các thiết bị di động.

9.2 Di động và nguy cơ mất an toàn thông tin

Nhiều người thường xuyên mang theo mình những chiếc điện thoại di động có chứa các thông tin nhạy cảm. Nhật ký cuộc gọi, tin nhắn văn bản, tin nhắn thoại, thông tin liên lạc, lịch biểu, ảnh và rất nhiều các thông tin hữu ích khác trong điện thoại có thể trở nên nguy hiểm nếu chiếc điện thoại hoặc những dữ liệu đó bị thất lạc hoặc mất cắp. Thông tin lưu trữ trong điện thoại có thể xác định chủ nhân sử dụng chiếc điện thoại đó cùng với những người khác trong danh bạ liên lạc, hộp thư chứa tin nhắn, sổ ảnh, vv.

Khi những chiếc điện thoại di động kết nối vào mạng Internet sẽ có những nguy cơ mất an toàn liên quan tới Internet và máy tính, như được thảo luận trong các chương khác của cuốn sách này về an toàn bảo mật thông tin, ẩn danh, dò rỉ thông tin, mất dữ liệu, ăn cắp và nghe trộm thông tin.

Để có thể giảm thiểu những nguy cơ bảo mật này, người dùng cần luôn cảnh giác với những nguy cơ mất an toàn tiềm tàng đối với những chiếc điện thoại di động của họ và những tùy chọn cài đặt trong đó. Khi bạn đã hiểu rõ về các vấn đề có thể xảy ra, bạn có thể cơ chế bảo vệ và có các biện pháp phòng ngừa.

Borna: Một lợi điểm của điện thoại di động là họ sẽ không thể biết được địa điểm chúng ta tổ chức trao đổi sử dụng điện thoại di động trong khi đi lại trong khu chợ thay vì sử dụng điện thoại thông thường khiến họ có thể nghe lén chúng ta.

Delir: Vâng, có phải cha đã từng nói rằng họ có quan hệ với công ty điện thoại?

Borna: Có ai đó đã thông báo rằng họ đang nhờ các kỹ thuật viên thông tin lấy thông tin đàm thoại.

Delir: Nếu cha đăng ký điện thoại sử dụng tên và địa chỉ của mình, họ có thể truy ra cha và các thời điểm cha gọi điện, các thông tin lưu trữ sẽ kết nối thông tin đăng ký điện thoại với danh tính của cha. Cha có đăng ký bằng số chứng minh thư của mình không đấy?

Borna: Không, cha lấy chiếc điện thoại cũ này từ cửa hàng của chú con; chú ấy đảm bảo nó được làm sạch và an toàn. Chú ấy cũng giúp cha mua một thẻ điện thoại trả trước để cha có thể dùng.

Delir: Vâng, đấy là một cái thẻ SIM card ^[2]. Công ty điện thoại theo dõi từng cuộc gọi hay trao đổi dữ liệu liên quan tới số điện thoại, cũng như số mã nhận dạng thẻ SIM cũng như mã số nhận dạng điện thoại. Nếu họ biết số điện thoại của cha, hoặc mã số nhận dạng điện thoại, hoặc mã nhận dạng thẻ SIM của cha, họ có thể sử dụng các mối quan hệ để tìm hiểu về hành vi sử dụng điện thoại của cha đấy.

Borna: Vậy cha cho rằng họ có thể nghe lén tất cả các cuộc hội thoại thậm chí từ máy điện thoại di động của cha?

Delir: Trong trường hợp của cha, nhờ chú con, điện thoại của cha không được đăng ký dưới tên cha và cái thẻ SIM này cũng không có liên hệ gì tới cha cả. Do vậy ngay cả khi họ theo dõi vị trí của chiếc SIM và cả điện thoại này họ cũng không biết gì về mối liên hệ giữa chúng và cha cả.

9.2.1 Những điều nên thực hiện để đảm bảo an toàn thông tin điện thoại

Cũng như các loại thiết bị khác, việc đầu tiên bảo đảm an toàn thông tin trong điện thoại của bạn là bảo vệ chiếc điện thoại và thẻ SIM ^[2] trong đó khỏi bị mất hoặc bị xâm nhập trực tiếp.

- Luôn giữ chiếc điện thoại của bạn bên mình. Không bao giờ để điện thoại ở nơi không thể quan sát. Tránh thể hiện điện thoại của bạn nơi công cộng.
- Luôn khóa máy với mật mã an ninh hoặc Mã Xác định Cá nhân (PINs) và lưu chúng một cách bí mật (không để lộ cho người khác biết). Thay đổi các thông tin mã khóa an ninh mặc định của nhà sản xuất.
- Đánh dấu nhận biết (vẽ, gạch) những ký hiệu đặc trưng và không dễ nhận ra đối với người lạ (tạo một dấu nhỏ, hình vẽ, ký hiệu hay số hoặc sử dụng bút đánh dấu siêu cực tím không hiển thị dưới ánh sáng thường) lên thẻ SIM, thẻ nhớ, pin và điện thoại của mình. Dán tem bảo vệ chống mở máy hoặc dán các vùng nối ghép của điện thoại. Những việc này sẽ giúp bạn dễ dàng nhận ra nếu một trong các thành phần trên bị xâm nhập hoặc thay thế (ví dụ nếu tem dán bị lệch hoặc để lại dấu vết cạy mở).
- Đảm bảo rằng bạn biết rõ về các thông tin được lưu trên thẻ SIM, trên các thẻ nhớ và trên bộ nhớ trong của điện thoại. Không lưu thông tin nhạy cảm trên điện thoại. Nếu bạn cần phải lưu trữ những thông tin nhạy cảm, hãy cân nhắc việc lưu chúng vào một thẻ nhớ ngoài để có thể dễ dàng tháo ra khi cần – không lưu thông tin nhạy cảm này trên bộ nhớ trong của điện thoại.
- Giữ gìn bảo vệ thẻ nhớ SIM và các thẻ nhớ (nếu điện thoại của bạn có thẻ nhớ) vì chúng có thể chứa các thông tin quan trọng nhạy cảm như thông tin đối tác liên lạc, tin nhắn SMS. Ví dụ, chắc chắn rằng bạn không để chúng lại cửa hàng sửa chữa điện thoại khi cần sửa điện thoại.
- Khi vứt bỏ một chiếc điện thoại, hãy chắc chắn rằng bạn không để lại bất cứ thông tin gì lưu trữ trên máy hay thẻ SIM hoặc thẻ nhớ (ngay cả khi điện thoại hoặc thẻ nhớ bị hỏng hoặc hết hạn). Khi muốn vứt bỏ, tốt nhất hãy hủy thẻ SIM. Nếu bạn định cho ai đó, đem bán hay tái chế điện thoại của mình thì hãy đảm bảo rằng mọi thông tin trên đó đã được xóa sạch.
- Chỉ sử dụng dịch vụ của những người bán điện thoại và cửa hàng sửa chữa điện thoại đáng tin cậy. Điều này giúp giảm nguy cơ mất an toàn dữ liệu khi mua một điện thoại cũ hay khi cần sửa chữa điện thoại. Xem xét việc chọn mua điện thoại của hãng nhưng chọn ngẫu nhiên một cửa hàng cung cấp – điều này giúp bạn giảm khả năng chiếc điện thoại của bạn được chuẩn bị trước cho bạn với các phần mềm gián điệp được cài đặt sẵn.
- Hãy sao lưu thông tin trong điện thoại thường xuyên vào máy tính. Lưu bản sao lưu này một cách an toàn và bảo mật (tham khảo [chương 4. Làm thế nào để bảo vệ các thông tin nhạy cảm trên máy tính](#) ^[3]). Việc sao lưu giúp bạn khôi phục dữ liệu trong trường hợp bị mất điện thoại. Việc này cũng giúp bạn xác định được những thông tin nào có thể bị lộ (trong trường hợp bị thất lạc hay mất điện thoại), và sẽ có các hành động thích hợp.
- Dãy 15 số Mã điện thoại hay số IMEI giúp bạn xác định điện thoại của mình và có thể xem số này bằng cách nhấn ***#06#** trên đĩa số điện thoại, hay trên điện thoại phía dưới viên pin hoặc xem trong mục thiết đặt trên máy. Hãy ghi lại dãy số này ở một nơi khác ngoài điện thoại vì nó có thể giúp bạn theo dõi và chứng nhận sự sở hữu một cách nhanh chóng trong trường hợp điện thoại bị mất cắp.
- Cân nhắc các điểm lợi và bất lợi của việc đăng ký điện thoại di động của bạn với nhà cung cấp dịch vụ. Nếu bạn thông báo việc mất điện thoại, nhà cung cấp dịch vụ có thể dừng cung cấp dịch vụ cho điện thoại đó giúp tránh việc điện thoại bị lạm dụng. Tuy nhiên việc đăng ký cũng đồng nghĩa với việc chiếc điện thoại đó có liên hệ tới danh tính của bạn.

9.2.2 Các tính năng cơ bản, theo dõi và ẩn danh

Để điện thoại của bạn có thể gửi và nhận các cuộc gọi hay liên lạc, các cột thu phát sóng gần vị trí bạn nhất sẽ được điện thoại của bạn thông báo vị trí của nó. Các thông báo định vị này sẽ giúp nhà cung cấp dịch vụ viễn thông biết vị trí địa lý chính xác của chiếc điện thoại của bạn tại mọi thời điểm.

Borna: Còn điều gì về chiếc điện thoại này mà cha nên biết?

Delir: Con nghĩ là còn, nhưng cũng còn tùy thuộc xem liệu cha có nghi ngờ rằng họ đang cố gắng theo dõi cha hay không.

Borna: Cha không cho là như vậy, nhưng liệu họ có thể làm điều đó không?

Delir: Vâng, có đấy, nếu điện thoại của cha được bật, VÀ những kỹ thuật viên kia có thể truy cập mạng điện thoại, VÀ họ phải biết được cha đang sử dụng chiếc điện thoại nào.

Borna: Điều này không thể xảy ra vì cha đâu có gọi cuộc điện thoại nào từ máy di động khi đi đến đó.

Delir: Cha có gọi điện hay không thì cũng vậy thôi. Chỉ cần cha mang theo điện thoại di động bên mình, nếu điện thoại được bật nó sẽ liên lạc với các trạm thu phát sóng ở gần nhất, đây đơn giản là cách hoạt động của điện thoại di động. Do đó bất kỳ thời điểm nào vị trí của cha sẽ được xác định ở đâu đó gần cột thu phát sóng điện thoại gần nhất trong mạng di động.

Borna: Vậy thì cha nên tắt điện thoại cho đến khi đến chỗ gặp mặt?

Delir: Vâng, nếu có thể thì tốt nhất cha không nên mang theo điện thoại bên mình. Nếu không thì cha nên tắt điện thoại VÀ tháo pin ra khỏi máy trước khi đi, và không nên bật điện thoại cho đến khi quay về.

Borna: Vậy cơ à? Chỉ tắt máy thôi cũng không được sao?

Delir: Để đảm bảo tuyệt đối an toàn, cha nên tháo pin khỏi điện thoại, và lý do là: đây là thiết bị phát sóng và chùng nào còn có pin, có khả năng cho dù nhỏ rằng ai đó bằng cách nào đó sẽ bật điện thoại của cha lên mà cha không hề hay biết.

Về tính Ẩn danh

Nếu bạn đang thực hiện các cuộc gọi hay nhắn tin SMS với thông tin nhạy cảm, hãy cảnh giác với những 'tính năng' theo dõi được đề cập phía trên của mọi điện thoại di động. Cần nhắc tìm hiểu và thực hiện các bước sau:

- Thực hiện các cuộc gọi ở những địa điểm khác nhau, và chọn các địa điểm không có mối liên hệ tới bạn.
- Tắt máy điện thoại, tháo pin và đến địa điểm được chọn sau đó bật máy thực hiện việc liên lạc xong sẽ tắt máy và tháo pin. Hãy tạo thói quen thực hiện các bước này mỗi khi cần thực hiện một cuộc gọi, điều này sẽ giúp bạn tránh bị theo dõi vị trí bởi nhà cung cấp dịch vụ.
- Hãy thường xuyên thay đổi điện thoại và thẻ SIM [4]. Trao đổi chúng với bạn bè hoặc tại các cửa hàng điện thoại cũ.
- Sử dụng các thẻ SIM trả trước không cần đăng ký nếu có thể. Tránh sử dụng thẻ tín dụng cá nhân để trả tiền mua điện thoại hay thẻ SIM vì điều này có thể tạo một mối liên hệ giữa những thứ này với danh tính của bạn.

Borna: Con đang nói rằng điện thoại của cha có thể vẫn liên lạc với các cột thu phát sóng để xác định vị trí của cha ngay cả khi nó có vẻ đã được tắt?

Delir: Vâng, và đó là trường hợp tồi tệ nhất

Borna: Oh?

Delir: Vâng, người ta có nói về một số chương trình được cài đặt trên điện thoại có thể bí mật bật điện thoại từ xa và thực hiện một cuộc gọi mà người sử dụng không hề hay biết. Khi đó, nếu cha đang trong buổi họp, nó sẽ hoạt động như một máy ghi âm và truyền đi.

Borna: Không thể nào! Có thật như vậy không?

Delir: Vâng, về mặt công nghệ thì điều này được thực hiện khá dễ dàng. Nhưng sẽ là không thể nếu pin được tháo ra, và cha sẽ được an toàn.

Borna: Vậy cha cho rằng để hết sức cẩn thận cha không nên mang theo điện thoại di động. Nhưng liệu cha có nên sử dụng điện thoại di động nữa hay không?

Delir: Ôi con xin cha, Cha thường dạy bảo con không nên sợ những điều mới lạ. Điện thoại di động cũng vậy, cha cần hiểu rõ những lợi ích và các rủi ro có thể xảy ra. Chỉ cần hết sức cẩn thận. Nếu cha hiểu rõ các nguy cơ thì có thể thực hiện các hành động để tránh được chúng.

Về việc nghe lén

Điện thoại của bạn có thể được thiết lập để ghi và truyền bất kỳ âm thanh nào trong phạm vi hoạt động của chiếc micro-phôn tích hợp trong đó mà bạn không hề hay biết. Một số điện thoại có thể được bật từ xa và được điều khiển theo cách này ngay cả khi chúng trông như đang bị tắt.

- Không bao giờ để những người bạn không tin tưởng mượn điện thoại; đây là cách phổ biến nhất để cài đặt phần mềm gián điệp lên máy của bạn.
- Nếu bạn cần thực hiện các cuộc họp quan trọng, bí mật, hãy tắt điện thoại của bạn và tháo pin khỏi điện thoại. Hoặc không mang theo điện thoại nếu bạn có thể để chúng ở một nơi an toàn.
- Hãy đảm bảo những đối tác liên lạc của bạn cũng áp dụng những biện pháp an toàn được đề cập ở đây.
- Thêm nữa, đừng quên rằng việc sử dụng điện thoại công cộng, hoặc ở những nơi bạn không tin tưởng có thể khiến bạn đối mặt với nguy cơ bị nghe lén theo cách truyền thống hoặc bị đánh cắp điện thoại.

Vấn đề nghe lén đường truyền

Thông thường, việc mã hóa đường truyền thoại (và tin nhắn) qua liên lạc bằng điện thoại di động là khá kém. Có những thiết bị công nghệ không đắt tiền được những kẻ thứ ba sử dụng để lấy trộm thông tin trong trường hợp tin nhắn hoặc nghe trộm các cuộc gọi, nếu những kẻ này ở đủ gần khu vực bạn sử dụng điện thoại thì chúng có thể thu sóng phát ra trực tiếp từ điện thoại. Và tất nhiên là nhà cung cấp dịch vụ mạng của bạn có thể truy cập toàn bộ thoại và tin nhắn liên lạc của bạn. Hiện tại, việc mã hóa các cuộc gọi để tránh bị nghe trộm rất tốn kém và gặp vấn đề kỹ thuật – tuy nhiên những công cụ mã hóa này sẽ sớm trở nên rẻ tiền và phổ biến. Để thực hiện việc mã hóa, trước hết bạn cần cài đặt phần mềm mã hóa vào điện thoại của mình cũng như của đối tác liên lạc. Sau đó hai bên có thể sử dụng phần mềm này để trao đổi các cuộc gọi và/hoặc tin nhắn. Phần mềm mã hóa hiện tại chỉ được hỗ trợ trên một số mẫu máy mới gọi là điện

thoại 'thông minh'.

Các cuộc hội thoại giữa Skype và điện thoại không được mã hóa bởi tại một thời điểm nào đó tín hiệu sẽ được chuyển vào mạng di động nơi mà việc mã hóa KHÔNG được thực hiện.

9.2.3 Liên lạc qua nhắn tin – SMS / tin nhắn văn bản

Bạn không nên dùng dịch vụ tin nhắn để gửi các thông tin nhạy cảm quan trọng. Các tin nhắn được trao đổi dưới dạng văn bản thuần khiến chúng không phù hợp với các giao dịch bảo mật.

Borna: Nếu cha không bao giờ dùng điện thoại di động để gọi mà chỉ gửi và nhận các tin nhắn ngắn. Họ không thể nghe thấy gì nếu ta không dùng thoại, và liên lạc như vậy cũng rất nhanh chóng đúng không?

Delir: Cha đợi đã. Những tin nhắn này rất dễ dàng bị đọc trộm, và bất kỳ kẻ nào có thể xâm nhập mạng điện thoại hoặc ngay cả những kẻ được trang bị thiết bị thích hợp có thể thu và đọc những tin nhắn này khi chúng được truyền qua mạng dưới dạng văn bản thuần, và được lưu từ trạm thu sóng này đến trạm thu sóng khác.

Borna: Thật là ngu ngốc. Vậy cha phải làm gì đây? Sử dụng mật mã như là trong chiến tranh?

Delir: Vâng, đôi khi đôi giày cũ nhất lại là vừa chân nhất đấy cha.

Gửi tin nhắn SMS có thể bị nghe trộm bởi người vận hành mạng hoặc bởi những kẻ lạ với những thiết bị không quá đắt tiền. Những tin nhắn này có chứa thông tin số điện thoại của người gửi cũng như người nhận và nội dung trao đổi. Hơn thế nữa, tin nhắn SMS có thể bị thay đổi hoặc giả mạo dễ dàng bởi một bên thứ ba.

Hãy xem xét khả năng thiết lập một hệ thống mật mã giữa bạn và các đối tác liên lạc. Mật mã có thể giúp việc liên lạc trở lên bảo mật hơn và cũng là một cách để xác thực danh tính đối tác liên lạc. Hệ thống mật mã cần được bảo mật và thay đổi thường xuyên.

Tin nhắn SMS vẫn tồn tại sau khi liên lạc:

- Ở nhiều quốc gia, luật pháp (hoặc các ảnh hưởng khác) bắt buộc nhà mạng phải lưu trữ các bản ghi tin nhắn của khách hàng trong một thời gian dài. Hầu hết các trường hợp tin nhắn SMS được các nhà mạng lưu giữ và sử dụng vào mục đích thương mại, kế toán hoặc bằng chứng.

*Các tin nhắn được lưu lại trong máy điện thoại của bạn có thể được truy cập dễ dàng bởi bất kỳ ai có điện thoại của bạn trong tay. Hãy cân nhắc xóa những tin nhắn đã gửi và nhận ngay lập tức

- Một số điện thoại có thể tắt tính năng lưu lịch sử cuộc gọi và tin nhắn. Tính năng này rất hữu ích đối với những công việc có tính chất nhạy cảm cần bảo mật. Bạn cũng cần chắc chắn mình hiểu rõ những tính năng của chiếc điện thoại mình sử dụng. Hãy đọc kỹ hướng dẫn sử dụng!

9.2.4 Các tính năng khác ngoài thoại và tin nhắn

Những chiếc điện thoại di động giờ đã trở thành các máy tính bỏ túi, với hệ điều hành riêng cũng như các ứng dụng có thể tải về nhằm đáp ứng các loại dịch vụ đa dạng cho người dùng. Kết quả tất yếu là các loại vi rút, phần mềm gián điệp cũng xâm nhập vào thế giới di động. Vi rút có thể được cấy vào trong điện thoại của bạn hoặc lây nhiễm trong các ứng dụng, nhạc chuông hay các tin nhắn đa phương tiện được bạn tải về từ mạng Internet.

Cho dù những mẫu điện thoại đời cổ có ít tính năng và không thể truy cập Internet, vẫn rất cần thiết khi bạn tìm hiểu những nguy cơ trên đối với tất cả các loại điện thoại để đảm bảo rằng thiết bị mình sử dụng không bị xâm nhập mà không hề hay biết. Một số cảnh báo trên có thể chỉ dành cho các loại điện thoại thông minh nhưng một điều rất quan trọng là bạn cần xác định và hiểu rõ những tính năng của chiếc điện thoại mình sử dụng để có thể chắc chắn rằng bạn có các hành động phòng vệ thích hợp:

- Không lưu các tệp tin, hình ảnh bảo mật trên điện thoại di động. Hãy chuyển chúng, càng nhanh càng tốt vào một nơi an toàn, như được hướng dẫn tại Chương 4, [Làm thế nào để bảo vệ Dữ liệu trên máy tính của bạn](#) [5].
- Định kỳ xóa các nhật ký cuộc gọi, tin nhắn, các mục thông tin liên lạc và hình ảnh, vv.
- Nếu bạn sử dụng điện thoại để truy cập Internet, hãy tạo các thói quen truy cập an toàn như khi sử dụng máy tính (ví dụ: luôn sử dụng các kết nối được mã hóa bảo mật như [HTTPS](#) [6]).
- Chỉ kết nối điện thoại vào máy tính khi chắc chắn rằng máy tính không bị nhiễm vi rút. Hãy tham khảo Chương 1. [Làm thế nào để bảo vệ máy tính của bạn khỏi phần mềm độc hại và tin tặc](#) [7].
- Không chấp nhận và cài đặt các chương trình có nguồn gốc không rõ ràng và chưa được kiểm tra lên máy điện thoại của bạn, bao gồm nhạc chuông, hình nền, ứng dụng Java hay bất kỳ phần mềm nào từ các nguồn không rõ ràng hoặc không mong muốn. Chúng có thể chứa vi rút, phần mềm độc hại hay gián điệp.
- Quan sát theo dõi hoạt động của điện thoại để phát hiện các biểu hiện và tính năng bất bình thường. Tìm hiểu các chương trình, tiến trình đang chạy không rõ nguồn gốc, các tin nhắn lạ và các hành vi bất bình thường. Nếu bạn

không biết hoặc không sử dụng một số tính năng hay ứng dụng trên điện thoại của mình, hãy tắt hoặc gỡ bỏ chúng nếu có thể.

- Hãy để phòng khi kết nối vào các điểm kết nối không dây không bảo mật (không yêu cầu mật khẩu truy cập), cũng như khi bạn sử dụng máy tính kết nối vào mạng không dây. Điện thoại di động thực sự giống như một máy tính vì vậy cũng bị các khả năng bị xâm nhập và kém bảo mật giống như máy tính và Internet.
- Hãy tắt và vô hiệu hóa các kênh kết nối như Hồng ngoại (IR) ^[8], Bluetooth ^[9] và Không dây (WiFi) trên điện thoại khi không sử dụng. Chỉ bật chúng lên khi bạn có nhu cầu. Chỉ sử dụng các kênh kết nối này tại các địa điểm và trong các tình huống an toàn. Tránh sử dụng Bluetooth vì kênh kết nối này rất dễ bị nghe lén. Thay vào đó hãy sử dụng các cáp kết nối từ điện thoại tới tai nghe hoặc máy tính.

9.3 Đọc thêm

- Bộ Hướng dẫn về Thiết bị Di động ^[10] được xuất bản bởi Tactical Technology Collective. Cùng với các tài liệu khác, tài liệu này bao gồm các mô tả và hướng dẫn kỹ lưỡng về bảo mật cho điện thoại di động ^[11] cũng như các công cụ đa dạng với các ví dụ hướng dẫn sử dụng.
- An ninh cho Các Nhà hoạt động – Cẩm nang Thực hành An ninh dành cho các Nhà hoạt động và các Chiến dịch ^[12].
- Hướng dẫn Điện thoại Di động – Hướng dẫn ngắn gọn, dành cho các nhà hoạt động, cách sử dụng điện thoại di động an toàn và bảo mật ^[13].
- Hướng dẫn Bảo mật với Điện thoại di động dành cho các Nhà báo Công dân ^[14] xuất bản bởi MobileActive.org
- Sơ lược về An toàn Tin nhắn trong MIDP – hướng dẫn dành cho các nhà phát triển của Nokia ^[15]
- Sử dụng điện thoại như các thiết bị gián điệp ^[16]

URL nguồn (được tìm thấy vào ngày 30/06/2014 - 07:10): <https://www.securityinabox.org/vi/chuong-9>

Các liên kết:

- [1] <https://www.securityinabox.org/vi/glossary#GPS>
- [2] https://www.securityinabox.org/vi/glossary#SIM_card
- [3] <https://www.securityinabox.org/vi/chuong-1>.
- [4] https://www.securityinabox.org/en/glossary#SIM_card
- [5] <https://www.securityinabox.org/vi/chuong-4>
- [6] <https://www.securityinabox.org/vi/glossary#SSL>
- [7] <https://www.securityinabox.org/vi/chuong-1>
- [8] <https://www.securityinabox.org/vi/glossary#IrDA>
- [9] <https://www.securityinabox.org/en/glossary#Bluetooth>
- [10] http://wiki.mobiles.tacticaltech.org/index.php/Main_Page
- [11] <http://wiki.mobiles.tacticaltech.org/index.php/Security>
- [12] <http://www.activistsecurity.org/>
- [13] http://www.freebeagles.org/articles/mobile_phones.html
- [14] <http://mobileactive.org/mobilesecurity-citizenjournalism>
- [15] http://sw.nokia.com/id/5274b81c-12d0-43bb-8d89-26f6a1ae111f/A_Brief_Introduction_to_Secure_SMS_Messaging_in_MIDP_en.pdf
- [16] <http://www.mysecured.com/?p=127>