CHUYÊN MỤC CHUYỂN ĐỔI SỐ:

Bài: Làm thế nào để an toàn trong môi trường số và mỗi người dân cần chuẩn bị cho mình những gì?

I. Nhạc hiệu.

II. Lời chào:

Xin kính chào quý vị và các bạn. Mời quý vị và các bạn đón nghe bản tin về Chuyển đổi số của đài truyền thanh thị trấn Sao Vàng. Bản tin hôm nay xin mời quývị và các bạn lắng nghe nội dung: **Làm thế nào để an toàn trong môi trường số và mỗi người dân cần chuẩn bị cho mình những gì?**

Kính thưa quý vị, thưa toàn thể nhân dân!

Mỗi người dân tự có ý thức bảo vệ mình trong môi trường số như bảo vệ mình trong môi trường thực, bảo vệ tài sản vô hình của mình, chẳng hạn thông tin cá nhân, như bảo vệ tài sản hữu hình khác. Chiếc điện thoại thông minh giờ đây trở thành vật bất ly thân với nhiều người, và vì thế, là điểm yếu nhất.

Điện thoại thông minh đã trở thành gián điệp như thế nào?

Điện thoại thông minh với quá nhiều tiện ích, với camera chụp hình, microphone, xác định vị trí, kết nối mạng không dây và nhiều chức năng khác. Thật đáng tiếc, sự riêng tư và bảo mật lại không phải là mối quan tâm hàng đầu đối với hầu hết nhà sản xuất, vì họ quan tâm tới sự tiện lợi và giá thành để cạnh tranh nhiều hơn.

Tất cả điều đó đã biến điện thoại thông minh thành các thiết bị vô cùng lý tưởng để theo dõi, nghe lén, lấy vị trí, dữ liệu nhạy cảm, thậm chí mạo danh để nhắn tin tới các điện thoại khác.

Nếu một ai đó khống chế được chiếc điện thoại thông minh của bạn, có thể người đó còn hiểu về bạn hơn chính bạn.

Hacker xâm nhập vào điện thoại thông minh bằng cách nào?

Có nhiều cách, từ dễ đến khó, được hacker sử dụng. Dễ nhất, không cần có trình độ công nghệ, mà chỉ cần có các mánh khóe lừa đảo, giả mạo. Hacker có thể thu thập thông tin công khai trên mạng, chẳng hạn mạng xã hội, Internet, để xây dựng các nội dung lừa đảo với thông tin đáng tin cậy dành riêng cho mỗi cá nhân, thường là đánh vào lòng ham muốn riêng của mỗi cá nhân.

Cao cấp hơn, hacker có thể tạo ra các phần mềm, có thể là phần mềm độc hại, hoặc phần mềm độc hại núp bóng một ứng dụng thông thường, chẳng hạn ứng dụng xem phim, nghe nhạc để dụ người dùng cài đặt và sử dụng.

Cao cấp hơn nữa, hacker chuyên nghiệp tấn công khai thác các lỗ hổng, điểm yếu của điện thoại hoặc của các ứng dụng chính thống để từ đó xâm nhập.

Dấu hiệu nào cho thấy điện thoại thông minh đã bị "hack"?

Điện thoại thường xuyên bị nóng dù không sử dụng, pin của điện thoại bị "hao hụt" thường xuyên hay giảm tuổi thọ mặc dù ít sử dụng ứng dụng, vì các phần mềm độc hại xâm nhập chạy ngầm sẽ làm tiêu tốn tài nguyên điện thoại để quét thiết bị và truyền thông tin trở lại máy chủ điều khiển của hacker.

Điện thoại bỗng nhiên trở nên thường xuyên bị treo, hoặc tạm dừng, hoặc ứng dụng thường xuyên bị tắt đột ngột, thậm chí, đôi khi điện thoại bị khởi động lại. Điều này có thể là do phần mềm độc hại đang làm quá tải tài nguyên hoặc xung đột với các ứng dụng khác.

Dữ liệu sử dụng hàng tháng cao hơn nhu cầu hoặc bỗng nhiên tăng đột biến, dẫn đến cước phí dữ liệu phải trả tăng cao. Điều này có thể là do dữ liệu từ máy bị chuyển lên máy chủ điều khiển của hacker thông qua kết nối mạng.

Ứng dụng lạ, không phải do mình cài, bỗng xuất hiện, rất có thể đây là một phần mềm độc hại hoặc phần mềm gián điệp.

Vì sao an toàn mạng đơn giản như rửa tay bằng xà phòng?

Chỉ cần có ý thức và thói quen đúng, mỗi người đã tự có thể bảo vệ mình, hạn chế đến 80% nguy cơ, rủi ro, 20% còn lại thì chỉ có những kẻ tấn công chuyên nghiệp, bỏ ra một nguồn lực rất lớn, mới có thể đe dọa được.

Mỗi người hãy tự hiểu rõ các ứng dụng mà mình đã cài trên điện thoại thông minh của mình như chính cơ thể mình. Điện thoại thông minh cho phép người dùng kiểm soát, cấp quyền phù hợp cho từng ứng dụng theo nhu cầu chức năng sử dụng. Bạn hãy xóa các ứng dụng mà mình không dùng, tự mình phân quyền cho các ứng dụng mình cần một cách hợp lý, ví dụ, ứng dụng "Lịch vạn niên" thì không cần đến quyền truy cập vào Danh bạ hay Định vị bạn, không cần cấp cho ứng dụng này quyền đó. Hãy chỉ cài đặt ứng dụng từ các kho chính thức, với iPhone là Apple Store và với các điện thoại dùng Android là Google Play Store. Hạn chế tối đa việc cài các ứng dụng trôi nổi không rõ nguồn gốc.

Hãy thiết lập cho mình mật khẩu mạnh khi sử dụng điện thoại và các ứng dụng, hãy luôn cập nhật lên bản mới nhất của hệ điều hành và ứng dụng.

Hãy cài đặt các ứng dụng bảo mật cho chiếc điện thoại thông minh của mình, giống như trang bị thêm khóa cho tài sản của mình. Việt Nam có những ứng dụng rất tốt, chẳng hạn như phần mềm bảo mật điện thoại thông minh của BKAV, CMC hay Viettel.

Nếu gặp sự cố thì hỏi ai?

Hãy liên hệ Trung tâm Giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin của Bộ Thông tin và Truyền thông để được tư vấn, hỗ trợ.

Địa chỉ trực tuyến tư vấn, hỗ trợ cho người dân tại: https://khonggianmang.vn/

Mỗi người dân cần chuẩn bị cho mình những gì?

Không ngừng học hỏi, không ngừng nâng cao nhận thức, mỗi ngày mỗi người tự học cho mình những điều mới. Khi đã 76 tuổi, Bác Hồ vẫn nói':' Tự tôi, ngày nào cũng học. Nếu có điều chưa biết, hãy tìm hiểu, học hỏi và học từ những người xung quanh, từ những gì đã có sẵn, được chia sẻ từ những địa chỉ tin cậy. Nếu có điều gì đã biết, đã tâm đắc, hãy hướng dẫn, chia sẻ với những người xung quanh. Người trẻ hướng dẫn người già và trẻ em. Người biết nhiều hướng dẫn người biết ít, người biết ít hướng dẫn người chưa biết. Việc hướng dẫn, chia sẻ với mọi người kỹ năng số là giúp cho chính mình có một thế giới số an toàn, lành mạnh và tốt đẹp hơn.

I. Lời chào: Quý vị và các bạn vừa nghe xong bản tin tuyên truyền về Chuyển đổi số của đài truyền thanh thị trấn Sao Vàng. Xin chào và hẹn gặp lại quývị và các bạn vào chương trình lần sau.

(Nhạc hiệu)

Phát thanh viên

Phạm Thị Huyền

Duyệt lãnh đạo

Mạc Văn Tỉnh