|  |  |
| --- | --- |
| UBND XÃ QUẢNG BÌNH  **Đài truyền thanh** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**  **Độc lập - Tự do - Hạnh phúc**  *Quảng Bình, ngày 17 tháng 8 năm 2024* |

**TUYÊN TRUYỀN**

**LÀM SAO ĐỂ AN TOÀN TRONG MÔI TRƯỜNG SỐ**

*Kính thưa toàn thể nhân dân!*

“Môi trường sống nào thì cũng đều không an toàn. Đó là bản chất của cuộc sống. Chúng ta sống trong thế giới thực đã hàng chục nghìn năm rồi, thể chế, pháp luật, bộ máy nhà nước đã hoàn thiện hàng nghìn năm nay mà vẫn có những nguy cơ, vẫn không an toàn tuyệt đối, vẫn có trộm cắp, giết người. Chuyển đổi số tạo ra một không gian sống mới, gọi là không gian mạng hoặc môi trường số. Cuộc sống đã và đang vào môi trường số nhanh hơn so với hệ thống pháp luật và bộ máy thực thi pháp luật và vì vậy, các nguy cơ là không nhỏ. Nhưng cái may mắn là, cả thế giới đang cùng đối mặt những thách thức này, các nước đang hoàn thiện hệ thống pháp luật trên môi trường số. Chúng ta có thể học hỏi. Ví dụ về bảo vệ dữ liệu cá nhân thì châu Âu đã ban hành luật và được nhiều nước coi như chuẩn; các mạng xã hội lớn như Facebook, Twitter, Google cũng đã được các nước quản lý thông qua các luật về thị trường và dịch vụ số. Việt Nam chúng ta cũng đang học hỏi để hoàn thiện thể chế, bộ máy trên môi trường số. Nhưng chúng ta sẽ luôn phải đương đầu với các nguy cơ trên môi trường số. Ngoài luật lệ thì mỗi chúng ta vẫn phải trang bị các kỹ năng số để sinh sống an toàn trong môi trường số. Tai nạn, sự cố an ninh mạng vẫn sẽ xảy ra, nhưng đó cũng là cách để môi trường số ngày một an toàn hơn. Vì không thể có rủi ro bằng 0 nên cách tiếp cận sẽ là quản lý rủi ro, tối thiểu rủi ro, khi rủi ro xảy ra thì khả năng hồi phục là quan trọng nhất. Việt Nam sẽ phải thịnh vượng trên không gian mạng, bởi vậy, Việt Nam phải trở thành cường quốc về an toàn, an ninh mạng để bảo vệ sự thịnh vượng của mình trên không gian mạng. Cường quốc về an toàn, an ninh mạng thì cũng như cường quốc về quân sự trong thế giới thực. 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 riêng tư, 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. 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 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 bỗng xuất hiện, không phải do mình cài, 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 của 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 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/./.

*(Nguồn tham khảo: cẩm nang chuyển đổi số)*

**ĐÀI TRUYỀN THANH XÃ**