ĐÀI TRUYỀN THANH XÃ HOẰNG HỢP
CHUYÊN MỤC CHUYỂN ĐỔI SỐ
NỘI DUNG: Bảo vệ an toàn trên môi trường mạng
Phát ngày: 09/3/2023 đến ngày 10/3/2023

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 xã Hoằng Hợp.

Kính thưa quý vị, thưa toàn thể nhân dân xã Hoằng Hợp!

Ngày nay việc sử dụng internet là nhu cầu hàng ngày của nhân dân. Để bảo vệ an toàn trước những hiểm họa trên môi trường mạng, Đài truyền thanh xã giới thiệu 10 biện pháp sau. Đề nghị nhân dân lắng nghe và thực hiện.

1. Không nhấp vào các đường link lạ

Đôi khi bạn sẽ gặp tình trạng nhận được các đường link lạ từ tin nhắn, hoặc Gmail nhưng không tài nào phân biệt liệu đó có phải là đường link an toàn không, nhất là đối với những người ít có kinh nghiệm sử dụng máy tính. Việc vô tình truy cập vào các đường link lạ này sẽ có thể tạo cơ hội cho kẻ gian đánh cắp lấy thông tin của bạn. Để đảm bảo tính an toàn trước khi truy cập vào một đường link nào, bạn có thể thực hiện kiểm tra tên miền trước trên công cụ tìm kiếm của Google nhằm biết được xếp hạng uy tín của đường link này. Ngoài ra, còn một đặc điểm để nhận biết link lạ đó là thường có tiêu đề giật gân và nếu bạn cảm thấy bản thân bị cuốn hút một cách tức thời thì bạn nên cẩn thận với kiểu đường link này.

2. Sử dụng mật khẩu khó đoán

Đây có lẽ là sai lầm thường thấy khi nhiều người thường chọn các mật khẩu khá phổ biến như 123456 hay abcdef để cho dễ nhớ. Việc làm này đã tạo điều kiện cho tội phạm có thể dễ dàng tiếp cận đến các tài khoản mạng xã hội hay nguy hiểm hơn là thẻ tín dụng chỉ qua vài thao tác tấn công đơn giản. Hãy cố gắng đặt mật khẩu có chứa cả từ in hoa, chữ in thường, ký hiệu và chữ số nhằm nâng cao tính bảo mật cho mật khẩu của bạn. Nếu bạn sợ mình đãng trí thì có thể ghi chú lại trong sổ, hoặc một mảnh giấy và cất vào ví để tránh trường hợp quên mất.

3. Thay đổi mật khẩu định kỳ

Việc thay đổi mật khẩu thường xuyên sẽ giúp hạn chế rủi ro kẻ gian đoán được mật khẩu của bạn. Mẹo ở đây dành cho bạn đó là bạn nên có một vài mật khẩu, sau đó thay đổi qua lại với tần suất 3 tháng/1 lần giữa những mật khẩu đó.

4. Không tin tưởng người quen biết thông qua mạng

Đối với những tin nhắn "mời gọi" từ những người mà bạn mới quen biết từ trên mạng, bạn nên cảnh giác với họ, và tuyệt đối không bao giờ được cung cấp bất kỳ thông tin cá nhân gì của mình cho họ. Và kể cả với những người thân quen, nếu họ có những biểu hiện khác thường, và đòi hỏi thông tin gì đó từ bạn thì bạn cũng nên đề cao cảnh giác bởi có thể tài khoản của họ đang bị điều khiển bởi một kẻ xấu nào khác.

5. Không chia sẻ thông tin cá nhân bừa bãi

Nhiều người thường vô ý đăng tải các hình ảnh về thông tin cá nhân của mình trên các nền tảng mạng xã hội, chẳng hạn như thông tin về chuyến bay, tài khoản ngân hàng,... Nếu buộc phải gửi hay đăng tải những hình ảnh đấy, bạn nên che mờ trước khi đăng.

6. Luôn kiểm tra website cung cấp dịch vụ

Hiện nay có một số trang web giả danh trên nền môi trường mạng nhằm chiếm lấy thông tin và quyền truy cập vào các dữ liệu quan trọng của bạn như tài khoản mạng xã hội. Vì vậy, bạn có thể kiểm tra lại bằng Google Tìm Kiếm để biết liệu đây có phải website chính chủ hay không.

7. Nhớ thực hiện đăng xuất

Khi thực hiện đăng nhập sử dụng các dịch vụ trên mạng, hay liên kết với các tài khoản ngân hàng để thực hiện giao dịch với thiết bị công cộng, bạn nên đăng xuất sau khi sử dụng xong. Việc duy trì kết nối có thể biến bạn trở thành nạn nhân của tội phạm công nghệ thông qua các lỗ hổng bảo mật.

8. Không cài đặt phần mềm lạ, không rõ nguồn gốc

Tuyệt đối không bao giờ được cài đặt các phần mềm không gõ nguồn gốc trên Internet, và tốt nhất thì bạn nên cài đặt thông qua các chợ ứng dụng, hoặc ít nhất là thông qua các trang web chính chủ. Đồng thời trên các thiết bị điện thoại, trên các phiên bản hệ điều hành Android và iOS mới thì bạn có thể tùy chỉnh được quyền truy cập dữ liệu trên thiết bị của bạn.

9. Đọc kỹ các điều khoản trước khi sử dụng

Đây có lẽ là việc mà nhiều người thường bỏ qua nhất vì họ cho rằng đây là một việc không cần thiết phải thực hiện. Tuy nhiên, điều này rất quan trọng bởi bạn sẽ nhận thức được có bao nhiêu loại dữ liệu mà bên cung cấp ứng dụng đang thu thập từ bạn, đồng thời có quyền từ chối sử dụng nếu các điều khoản này vi phạm vào quyền bảo mật thông tin của c hính bạn.

10. Sử dụng công cụ diệt virus uy tín

Nếu có điều kiện, bạn hãy đầu tư các phần mềm diệt virus trên thiết bị máy tính/laptop của bạn. Việc này sẽ giúp bạn phát hiện nhanh các mã độc (malware) đang hoạt động trong thiết bị của bạn, đồng thời sẽ có phương hướng giải quyết tiếp theo nhanh chóng./.

Duyệt phát thanh
TRƯỞNG BAN BIÊN TẬP

PHÓ CHỦ TỊCH
Nguyễn Quang Công