

Biện pháp phòng tránh chiêu trò giả mạo trang thông tin điện tử cơ quan, doanh nghiệp

19:39 15/07/2023

Cùng với sự phát triển mạnh mẽ của công nghệ thông tin, các đối tượng xấu có thể thực hiện việc giả mạo một trang web khi có các kiến thức như một lập trình viên.



Ảnh minh họa

Để tránh bị đánh cắp thông tin qua các trang web giả mạo, theo Cục An toàn thông tin, Bộ Thông tin và Truyền thông, người dân cần lưu ý:

- Kiểm tra địa chỉ URL: Luôn kiểm tra URL của trang web trước khi cung cấp thông tin cá nhân. Hãy chắc chắn rằng địa chỉ URL chính xác và tương ứng với trang web mà bạn mong muốn truy cập.
- Sử dụng trình duyệt an toàn: Sử dụng trình duyệt web có tính năng bảo mật cao và cập nhật phiên bản mới nhất. Các trình duyệt như Google Chrome, Mozilla Firefox và Safari thường có các cơ chế bảo mật tích hợp giúp ngăn chặn truy cập vào trang web độc hại.

- Kiểm tra kết nối an toàn: Khi truy cập vào các trang web yêu cầu cung cấp thông tin nhạy cảm, hãy đảm bảo rằng kết nối là an toàn bằng cách kiểm tra xem trang web có chứng chỉ SSL hợp lệ hay không. Biểu tượng ổ khóa và "https" ở đầu URL là một dấu hiệu của kết nối an toàn.
- Cẩn thận với email và liên kết: Tránh nhấp vào liên kết trong email không xác định hoặc không mong muốn. Kiểm tra nguồn gốc của email và đảm bảo rằng nó là đáng tin cậy trước khi tiếp tục. Nếu có liên kết, hãy kiểm tra xem địa chỉ URL có khớp với trang web mục tiêu hay không.
- Hạn chế cung cấp thông tin cá nhân: Chỉ cung cấp thông tin cá nhân nhạy cảm trên các trang web đáng tin cậy và an toàn. Tránh cung cấp thông tin cá nhân như mật khẩu, số thẻ tín dụng, mã OTP hoặc tài khoản ngân hàng trên các trang web không xác định hoặc không đáng tin.
- Sử dụng phần mềm bảo mật: Cài đặt và duy trì phần mềm diệt virus, phần mềm chống độc, tường lửa và các công cụ bảo mật khác trên thiết bị của bạn. Cập nhật chúng thường xuyên để bảo vệ chống lại các mối đe dọa mới nhất.
- Đào tạo và nhận biết: Hãy tự trang bị kiến thức về các phương pháp tấn công phishing và nhận biết các dấu hiệu nhận biết trang web lừa đảo qua tinnhiemmang.vn hoặc ncsc.gov.vn. Theo dõi và cập nhật các thông tin, tình huống, dấu hiệu về lừa đảo trực tuyến tại Cổng không gian mạng quốc gia (khonggianmang.vn)
- Giữ tỉnh táo và cảnh giác: Luôn giữ một tinh thần cảnh giác khi truy cập vào các trang web và giao dịch trực tuyến. Hãy tin vào cảm giác của bạn và không bao giờ cung cấp thông tin cá nhân nếu bạn có bất kỳ nghi ngờ nào về tính xác thực của trang web đó.
- Kiểm tra đánh giá và phản hồi: Trước khi thực hiện giao dịch hoặc cung cấp thông tin cá nhân, hãy kiểm tra các đánh giá và phản hồi từ người dùng khác về trang web đó. Nếu có nhiều phản hồi tiêu cực hoặc cảnh báo về lừa đảo, hãy tránh truy cập vào trang web đó.
- Sử dụng các phương pháp xác thực bổ sung: Nếu có sẵn, hãy sử dụng các phương pháp xác thực bổ sung như xác thực hai yếu tố hoặc sử dụng mã OTP (One-Time Password) để bảo vệ tài khoản của bạn. Điều này làm tăng cường bảo mật và khó khăn hơn đối với kẻ tấn công phishing.
- Đừng dễ tin vào thông báo đột xuất: Cẩn thận với các thông báo đột xuất yêu cầu cập nhật thông tin cá nhân hoặc yêu cầu thay đổi mật khẩu. Kẻ tấn công phishing thường sử dụng chiêu này để lừa đảo người dùng. Luôn truy cập vào

trang web chính thức của dịch vụ và thực hiện các thay đổi thông qua đó, thay vì truy cập qua liên kết trong email hoặc thông báo không xác định.

- Báo cáo các trang web phishing: Nếu bạn phát hiện một trang web phishing, hãy báo cáo cho nhà cung cấp dịch vụ trực tuyến hoặc cơ quan chức năng có thẩm quyền để họ có thể đối phó với tình huống đó và ngăn chặn người khác trở thành nạn nhân tiếp theo.

Hà Trần