

Đừng để “sập bẫy” trước làn sóng lừa đảo trực tuyến

13:48 05/10/2025

Việc tuyệt đối không cung cấp OTP hay mật khẩu, không bấm vào các đường link lạ và luôn kiểm tra thông tin qua kênh chính thức đã trở thành những “nguyên tắc sống còn” khi làn sóng lừa đảo trực tuyến ngày càng trở nên tinh vi.

Sự biến tấu không ngừng từ các kịch bản lừa đảo trực tuyến

Theo cảnh báo từ cơ quan chức năng, lừa đảo trực tuyến đang có xu hướng gia tăng đột biến. Thay vì tấn công ngẫu nhiên, giờ đây chúng xây dựng những kịch bản lừa đảo tinh vi, nhắm thẳng vào từng nạn nhân cụ thể với mục đích rõ ràng.

Chúng tấn công vào điểm yếu lớn nhất là tâm lý con người, dàn dựng những vở kịch phức tạp để đánh vào lòng tin, sự sợ hãi và cả lòng tham, giống lên hồi chuông cảnh báo khẩn cấp về an toàn trên không gian mạng.



Các đối tượng dễ bị nhắm tới nhất bao gồm sinh viên, người lao động có nhu cầu vay tiêu dùng, nhân viên văn phòng thường xuyên giao dịch và đặc biệt là người lớn tuổi ít am hiểu công nghệ. Các hình thức lừa đảo diễn ra vô cùng đa dạng, không chỉ gói gọn trong một phương thức mà đã mở rộng ra toàn bộ các giao dịch tài chính số.

Kịch bản phổ biến và nguy hiểm nhất là giả mạo nhân viên ngân hàng, ví điện tử uy tín (VNPay, ZaloPay, Momo,...) hoặc thậm chí là các cơ quan chức năng như công an, viện kiểm sát, tòa án. Các đối tượng lừa đảo thường gọi điện thông báo tài khoản của nạn nhân đang gặp sự cố, bị khóa, hoặc có liên quan đến một vụ án nào đó, sau đó dùng lời lẽ đe dọa hoặc thuyết phục để yêu cầu cung cấp ngay lập tức mật khẩu và mã OTP.

Trước thủ đoạn tinh vi này, Ngân hàng TMCP Phương Đông (OCB) khẳng định tuyệt đối không yêu cầu khách hàng cung cấp thông tin đăng nhập, mật khẩu, hay mã xác thực OTP qua các cuộc gọi, tin nhắn hoặc bất kỳ đường dẫn nào. Ngân hàng cam kết bảo mật và không cung cấp thông tin khách hàng ra bên ngoài. Mọi thông báo và hoạt động của OCB đều được truyền thông công khai trên các phương tiện chính thống như website, fanpage, Zalo và các cuộc gọi qua đầu số cố định đã đăng ký.

Và bên cạnh đó, một chiêu thức khác cũng rất phổ biến là chiếm đoạt tài khoản mạng xã hội rồi giả danh người thân để dựng lên các tình huống khẩn cấp, nhờ chuyển tiền hoặc vay mượn. Với cả hai hình thức này, nhiều người dùng đã mất cảnh giác và bị chiếm đoạt toàn bộ tài sản chỉ trong vài phút.

Tinh vi hơn nữa là hình thức tấn công giả mạo (Phishing) thông qua việc phát tán các tin nhắn, email chứa đường link độc hại. Tội phạm tạo ra các trang web có giao diện giống hệt màn hình đăng nhập của ngân hàng hoặc trang ví điện tử lớn rồi dụ dỗ người dùng nhấp vào bằng những nội dung hấp dẫn như "Bạn vừa nhận được tiền", "Xác nhận giao dịch để nhận hoàn tiền". Ngay khi người dùng cả tin và điền thông tin, toàn bộ tên đăng nhập và mật khẩu sẽ bị đánh cắp.

Không dừng lại ở đó, những kịch bản lừa đảo đánh vào nhu cầu tài chính cấp bách ngày càng biến tấu. Chúng quảng cáo các dịch vụ hấp dẫn như "xóa nợ xấu CIC", "nâng hạn mức tín dụng nhanh" để lừa nạn nhân trả một khoản phí trả trước.

Tương tự, thủ đoạn "hỗ trợ giải ngân khoản vay" cũng đang bùng nổ, lôi kéo nạn nhân vào các nhóm chat, yêu cầu chuyển tiền liên tục với lý do "xác minh" rồi chiếm đoạt toàn bộ số tiền khi đã đủ lớn. Mục tiêu cuối cùng của chúng đều

là dụ dỗ người dùng cả tin tự nguyện chuyển tiền vào tài khoản của kẻ lừa đảo.

Tuy nhiên, hậu quả của những vụ việc này không chỉ là thiệt hại về tiền bạc mà còn kéo theo vô số rủi ro khi dữ liệu cá nhân bị lộ lọt, có thể bị sử dụng để vay tín dụng đen hoặc trở thành mục tiêu cho các cuộc lừa đảo khác trong tương lai.

Tỉnh táo để phòng khi giao dịch trên không gian số

Trước thực trạng trên, việc nâng cao cảnh giác và chủ động trang bị kiến thức bảo mật là một yêu cầu tiên quyết. Điều này cho thấy tầm quan trọng trong việc mỗi người dùng cần xây dựng cho mình một tuyến phòng thủ vững chắc ngay từ ban đầu. Chính vì vậy, Ngân hàng TMCP Phương Đông (OCB) tiếp tục đưa ra khuyến cáo, trước mọi yêu cầu bất thường qua điện thoại hay tin nhắn, cần tuân thủ nguyên tắc: Không vội tin – Không vội làm – Không tiết lộ và Có kiểm tra – Có cảnh giác – Có bảo mật.

Theo đó, tuyệt đối không cung cấp OTP, mật khẩu, mã xác thực cho bất kỳ ai; không bấm vào đường link lạ; chỉ giao dịch trên ứng dụng và website chính thống; kiểm tra lại thông tin qua số hotline chính thức của ngân hàng, cơ quan; tuyệt đối không chuyển tiền vào tài khoản lạ với lý do “xác minh” hay “tài khoản an toàn”.

Bên cạnh sự tỉnh táo của người dùng, vai trò chủ động từ các định chế tài chính là yếu tố then chốt để xây dựng nên một "lá chắn" bảo mật toàn diện. Nhận thức rõ điều này, OCB tiên phong trong việc tích hợp nhiều lớp bảo vệ mạnh mẽ ngay trên ứng dụng ngân hàng số OCB OMNI.

Chủ thẻ có thể hoàn toàn an tâm giao dịch khi được trao toàn quyền kiểm soát tài chính thông qua 5 tính năng bảo mật thiết thực bao gồm chủ động cài đặt hạn mức giao dịch thẻ; khóa/mở thẻ ngay lập tức khi phát hiện dấu hiệu bất thường; bật/tắt tính năng thanh toán online theo nhu cầu sử dụng; theo dõi lịch sử giao dịch trực tuyến để phát hiện kịp thời các giao dịch lạ hay kích hoạt xác thực giao dịch bằng OTP cho mọi thanh toán online hay.

Với hoạt động hỗ trợ 24/7, OCB cam kết luôn đồng hành, sẵn sàng tư vấn và hỗ trợ khách hàng ngay khi có nghi ngờ phát sinh nguy cơ tiềm ẩn. Trong cuộc chiến không khoan nhượng với tội phạm công nghệ cao, sự kết hợp giữa ý thức cảnh giác cao độ của mỗi cá nhân và các giải pháp công nghệ bảo mật toàn diện từ ngân hàng sẽ tạo nên một tuyến phòng thủ vững chắc nhất, đảm bảo an toàn cho mọi giao dịch trên không gian số.

Trần Mạnh