Kỹ năng nhận biết lừa đảo trên không gian mạng

Việt Nam hiện có hơn 100 triệu dân, với hơn 70 triệu người sử dụng internet. Trong giai đoạn đẩy mạnh và tăng tốc chuyển đổi số như hiện nay, các đối tượng xấu đã lợi dụng sự bùng nổ về công nghệ thông tin, những tiện ích mà công nghệ thông tin mang lại (như tương tác qua mạng xã hội, các ứng dụng nhắn tin OTT...) để thực hiện nhiều vụ lừa đảo trực tuyến, chiếm đoạt tài sản có giá trị cao. Bài viết giới thiệu kỹ năng nhận biết giúp người dùng nắm được những kiến thức cơ bản để kịp thời nhận biết và phòng tránh nguy cơ bị lừa đảo trực tuyến.

(ảnh: naict.tttt.nghean.gov.vn)

Kịch bản chung của các đối tượng thường là giả mạo danh tính hoặc sử dụng tài khoản mạng xã hội giả mạo để liên hệ với nạn nhân, dẫn dụ khai báo thông tin cá nhân, thông tin tài khoản ngân hàng hoặc nhấp vào đường liên kết, tải về ứng dụng độc hại nhằm chiếm đoạt tài chính của nạn nhân.

Cách tiếp cận

Các đối tượng lừa đảo thường áp dụng các thủ đoạn tác động tâm lý để tiếp cận nạn nhân như: tự nhận/giả mạo là cơ quan công quyền (công an, viện kiểm sát, cán bộ đang làm việc tại các bộ/ngành...), đơn vị cung cấp dịch vụ, các tổ chức tài chính ngân hàng, gia đình bạn bè... để đánh vào nỗi sợ hãi, lòng tham, tình cảm, chủ quan...

Các kênh thường được đối tượng lừa đảo sử dụng để tiếp cận gồm: cuộc gọi qua SIM; tin nhắn (SMS)/thư điện tử (Email); mạng xã hội; nền tảng chat OTT (Ví dụ: Zalo, WhatsApp, Viber, Telegram...). Đôi khi các đối tượng còn sử dụng trực tiếp các kênh OTT này để tiếp cận nạn nhân; Website giả mạo; các ứng dụng giả mạo.

Phương thức lừa đảo

Các phương thức chính được các đối tượng lừa đảo trực tuyến sử dụng bao gồm:

- Dẫn dụ quét mã QR hoặc vào các website lừa đảo để lấy cắp thông tin cá nhân (để hack vào các loại tài khoản) từ đây tiếp tục lừa đảo để lấy các mã OTP, mã xác thực... hoặc hack vào các tài khoản mạng xã hội để làm bàn đạp tiếp tục lừa đảo bạn bè, người thân.

- Hướng kết nối vào các ứng dụng chat OTT để thao túng tâm lý (thường như Zalo sau đó dẫn dụ vào các OTT không được kiểm soát khác như Telegram, Viber, WhatsApp… để từ đây áp dụng các kịch bản lừa đảo khác nhau...).

- Lừa nạn nhân cài các ứng dụng giả mạo hoặc kích hoạt tệp tin có chèn mã độc hại (có đuôi như .pdf, .doc, .xlsx, .bat, .zip, .rar, .html...) để chiếm quyền thiết bị từ đó đánh cắp thông tin cá nhân, lấy tiền trong tài khoản, bôi nhọ danh dự hoặc tống tiền…

- Tác động tâm lý trực tiếp (qua điện thoại) để chiếm đoạt tiền trực tiếp (qua chuyển khoản hoặc ra ngân hàng gửi tiền cho đối tượng lừa đảo) hoặc dẫn dụ nạn nhân nhập cú pháp chuyển sang eSIM để chiếm đoạt số điện thoại của nạn nhân.

Cách thức thực hiện

Đối tượng lừa đảo thường dẫn dụ nạn nhân bằng những cách sau đây:

- *Tạo dựng lòng tin:* Giả danh tổ chức uy tín như ngân hàng, cơ quan chính phủ, hoặc công ty nổi tiếng. Đối tượng sử dụng Email, tin nhắn, hoặc cuộc gọi để tạo dựng lòng tin và yêu cầu thông tin nhạy cảm từ nạn nhân.

- *Kịch bản lừa đảo:* Được biên soạn sẵn một cách chi tiết, và khéo léo để thao túng tâm lý nhằm mục đích dẫn dụ tạo niềm tin và sự đồng cảm từ nạn nhân. Đóng nhiều vai nhân vật khác nhau để tạo ra một câu chuyện hoàn hảo đánh động vào tâm lý của nạn nhân một cách sâu sắc.

Sử dụng biểu mẫu và giao diện giả mạo: Các trang web lừa đảo thường sao chép giao diện của các trang web chính thức, sử dụng biểu mẫu đăng nhập hoặc thanh toán giống như thật để đánh lừa người dùng.

Kích thích tâm lý: Các đối tượng lừa đảo đa phần đánh vào tâm lý: lòng tham, sự sợ hãi, tính hiếu kỳ, tính tò mò và đặc biệt là tình thương, sự thương hại của con người. Đối tượng thường tạo ra cảm giác khẩn cấp để thúc đẩy nạn nhân hành động ngay lập tức mà không suy nghĩ kỹ lưỡng. Ví dụ, họ có thể thông báo rằng tài khoản của bạn sẽ bị khóa nếu không xác nhận thông tin ngay lập tức.

- *Đưa ra phần thưởng hoặc cơ hội hiếm có:* Hứa hẹn giải thưởng lớn, cơ hội đầu tư sinh lời cao, hoặc cơ hội việc làm hấp dẫn để thu hút sự chú ý của nạn nhân.

- *Yêu cầu hành động gấp:* Đối tượng lừa đảo gửi liên kết đến các trang web giả mạo hoặc mã QR, nơi nạn nhân được yêu cầu nhập thông tin cá nhân hoặc tài khoản. Các liên kết này thường được ngụy trang dưới dạng liên kết hợp pháp hoặc phần thưởng.

- *Làm giả thông báo khẩn cấp:* Sử dụng thông báo giả mạo về sự cố bảo mật, viện cớ lý do nguồn tiền đang bị treo vì phải đóng thuế, cơ quan công an điều tra, lỗi tài khoản, hoặc sự kiện khẩn cấp để yêu cầu nạn nhân cung cấp thông tin ngay lập tức.

- *Kích thích sự tò mò:* Gửi Email hoặc tin nhắn về sự kiện, báo cáo, hoặc tài liệu: Đối tượng lừa đảo gửi thông tin về sự kiện nóng hổi, báo cáo quan trọng, hoặc tài liệu hấp dẫn, yêu cầu nạn nhân tải xuống hoặc mở file đính kèm chứa mã độc.

Mục đích của đối tượng lừa đảo

Tại Việt Nam, các đối tượng lừa đảo trực tuyến có 2 mục tiêu chính là lừa đảo tài chính và lừa đảo trực tuyến khác. Trong đó 72,6% là lừa đảo trực tiếp vào tài chính, còn 27,4% là các dạng lừa đảo trực tuyến khác nhau. Tuy nhiên, các hình thức lừa đảo khác đó cũng là bước đệm để tiếp nối cho việc lên kịch bản thực hiện lừa đảo tài chính.

Mục tiêu cuối cùng của đối tượng đều là lừa đảo chiếm đoạt tài sản. Các đối tượng lừa đảo có thể tìm cách đánh cắp tiền từ tài khoản ngân hàng, ví điện tử, hoặc thẻ tín dụng của nạn nhân thông qua các kỹ thuật như

phishing (lừa đảo qua Email và tin nhắn), smishing (lừa đảo qua tin nhắn SMS), hoặc vishing (lừa đảo qua điện thoại).

Các yếu tố mà đối tượng tập trung hướng đến để lợi dụng thực hiện các hành vi lừa đảo là tâm lý nhẹ dạ cả tin, thiếu sự tiếp cận thông tin, thiếu việc làm hoặc thu nhập thấp, đánh vào lòng tham ẩn sâu trong mỗi con người.

Cách thức các đối tượng lừa đảo trực tuyến nhận tiền lừa đảo từ nạn nhân bao gồm: chuyển khoản vào các tài khoản ngân hàng rác, các tài khoản không chính chủ được mua lại từ các đối tượng như sinh viên, hoặc các số tài khoản ngân hàng ảo; chuyển tiền qua các cổng thanh toán trực tuyến (ví dụ như thanh toán mua thẻ điện thoại: cổng Ngân lượng, Bảo kim…); chuyển tiền qua các ví điện tử như Momo, ViettelPay, VNPay…; chuyển tiền thông qua tiền ảo trên các sàn giao dịch.

CT

Nguồn: TẠP CHÍ KHOA HỌC VÀ CÔNG NGHỆ VIỆT NAM.