TẠP CHÍ ĐIỆN TỬ
THƯƠNG HIỆU & CÔNG LUẬN

Chuyển từ điện thoại 2G sang smartphone: Cẩn trọng “bẫy” lừa đảo

15:40 18/09/2026

Việc tắt sóng 2G thúc đẩy hàng triệu thuê bao chuyển sang thiết bị hỗ trợ công nghệ mới. Tuy nhiên, quá trình chuyển đổi từ điện thoại phổ thông sang smartphone cũng đặt ra những rủi ro về an toàn thông tin, đặc biệt đối với người cao tuổi và nhóm người dùng còn hạn chế kỹ năng số.



Ảnh minh hoạ.

Từ điện thoại “cục gạch” đến những rủi ro mới trên smartphone

Lộ trình dừng công nghệ di động 2G là bước chuyển cần thiết nhằm giải phóng tài nguyên tần số, nâng cao chất lượng hạ tầng viễn thông và thúc đẩy phổ cập mạng 4G, 5G.

Một trong những lợi ích đáng chú ý khi công nghệ 2G được loại bỏ là hạn chế nguy cơ từ các trạm BTS giả. Trước đây, các đối tượng có thể lợi dụng hạn chế về cơ chế xác thực của mạng 2G để phát tán tin nhắn giả mạo thương hiệu,

ngân hàng hoặc tổ chức nhằm tiếp cận người dùng.

Tuy nhiên, cùng với quá trình chuyển đổi công nghệ, một vấn đề khác đang đặt ra. Nhiều thuê bao vốn chỉ sử dụng điện thoại phổ thông để nghe, gọi nay bắt đầu chuyển sang smartphone.

Trong nhóm này có không ít người cao tuổi, lao động tự do và người dân ở khu vực nông thôn – những người chưa quen với việc sử dụng ứng dụng, đường link, tài khoản trực tuyến cũng như các biện pháp bảo vệ dữ liệu cá nhân.

Nếu điện thoại phổ thông hỗ trợ 4G chủ yếu phục vụ nghe, gọi và nhắn tin thì smartphone mở ra khả năng truy cập Internet, mạng xã hội, ứng dụng ngân hàng, ví điện tử và nhiều dịch vụ trực tuyến. Đi cùng sự tiện lợi là nguy cơ người dùng tiếp xúc với đường link giả mạo, ứng dụng độc hại và các hình thức lừa đảo trên không gian mạng.

Đây cũng là nhóm đối tượng dễ bị tội phạm công nghệ cao nhắm tới khi chưa có nhiều kinh nghiệm nhận diện những dấu hiệu bất thường.

Mạo danh nhà mạng, công an, ngân hàng để dẫn dụ nạn nhân

Thủ đoạn của các đối tượng lừa đảo ngày càng thay đổi theo hướng trực tiếp tác động vào tâm lý người dùng.

Thay vì chỉ phát tán hàng loạt tin nhắn như trước, các đối tượng có thể gọi điện, nhắn tin, mạo danh cán bộ cơ quan nhà nước, công an, ngân hàng hoặc nhân viên nhà mạng để tạo lòng tin.

Một số kịch bản thường được sử dụng như thông báo thuê bao sắp bị khóa, yêu cầu “cập nhật thông tin 4G”, “chuẩn hóa thuê bao”, “kích hoạt tài khoản định danh” hoặc xử lý một vấn đề bất thường liên quan đến tài khoản ngân hàng.

Sau khi khiến nạn nhân lo lắng, các đối tượng hướng dẫn truy cập đường link, cung cấp thông tin cá nhân, mã OTP hoặc tải ứng dụng, tệp cài đặt không rõ nguồn gốc.

Nếu làm theo hướng dẫn, người dùng có nguy cơ bị đánh cắp thông tin đăng nhập, dữ liệu cá nhân, tài khoản ngân hàng, thậm chí bị cài mã độc nhằm kiểm soát thiết bị và thực hiện các giao dịch trái phép.

Đáng lo ngại, với người mới sử dụng smartphone, giao diện website hoặc ứng dụng giả mạo được thiết kế gần giống ứng dụng thật có thể khiến việc nhận diện trở nên khó khăn hơn.

Hiện nay, nhiều công cụ hỗ trợ nhận diện nguy cơ lừa đảo đã được phát triển. Trong đó, ứng dụng nTrust của Hiệp hội An ninh mạng quốc gia cho phép người dùng tra cứu, cảnh báo các số điện thoại, tài khoản và website có dấu hiệu lừa đảo.

Dù vậy, công cụ kỹ thuật chỉ thực sự phát huy hiệu quả khi người dùng có những kỹ năng số cơ bản. Với người cao tuổi hoặc người lần đầu sử dụng smartphone, các thao tác kiểm tra đường link, tra cứu số điện thoại, thiết lập quyền ứng dụng hay nhận biết những yêu cầu cấp quyền bất thường vẫn có thể là trở ngại.

Gia đình cần trở thành "lá chắn số" cho người lớn tuổi

Để hạn chế nguy cơ lừa đảo trong quá trình chuyển đổi thiết bị, việc bảo vệ người dùng không thể chỉ phụ thuộc vào sự cảnh giác của từng cá nhân.

Các doanh nghiệp viễn thông cần tiếp tục tăng cường giải pháp kỹ thuật, hệ thống lọc và cảnh báo cuộc gọi, tin nhắn có dấu hiệu bất thường; đồng thời phối hợp với cơ quan chức năng cập nhật dữ liệu về số điện thoại, tên miền, tài khoản có dấu hiệu phục vụ hoạt động lừa đảo.

Với người dùng, nguyên tắc quan trọng là không cung cấp mật khẩu, mã OTP hoặc thông tin tài khoản ngân hàng qua điện thoại; không truy cập đường link được gửi từ nguồn không xác định; không tải ứng dụng theo hướng dẫn của người lạ và đặc biệt thận trọng trước những cuộc gọi thúc giục chuyển tiền hoặc yêu cầu thao tác ngay trên điện thoại.

Đối với người cao tuổi mới chuyển sang smartphone, sự hỗ trợ từ người thân có ý nghĩa đặc biệt quan trọng. Các thành viên trong gia đình nên trực tiếp hỗ trợ cài đặt thiết bị, thiết lập các tính năng bảo mật, kiểm soát quyền cài ứng dụng từ nguồn không xác định và hướng dẫn cách xử lý khi nhận cuộc gọi, tin nhắn đáng ngờ.

Một nguyên tắc đơn giản có thể được thống nhất trong gia đình: khi có người lạ gọi điện liên quan đến tiền, tài khoản ngân hàng, công an, nhà mạng hoặc yêu cầu cài ứng dụng, không thực hiện ngay mà cần gọi cho người thân để kiểm tra.

Chuyển đổi từ 2G sang các thế hệ mạng mới là xu hướng tất yếu của quá trình phát triển hạ tầng số. Song song với việc nâng cấp công nghệ, trang bị kỹ năng an toàn số cho những người lần đầu bước vào môi trường smartphone cũng cần được chú trọng, để quá trình chuyển đổi không trở thành cơ hội cho các đối tượng lừa đảo khai thác.

PV