ỦY BAN NHÂN DÂN **XÃ VŨ QUANG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:1032 /UBND V/v tăng cường công tác đảm bảo an toàn, bảo mật trên không gian mạng	*Vũ Quang, ngày11 tháng 5 năm 2026*

Kính gửi:

- Các phòng, ban ngành, đoàn thể cấp xã;
- Các cơ quan, đơn vị đóng trên địa bàn xã;
- Cán bộ, công chức, viên chức, người lao động trên địa bàn xã;
- Các thôn trên địa bàn xã.

Hiện nay trên không gian mạng xuất hiện nhiều chiến dịch tấn công tinh vi và các lỗ hổng nghiêm trọng trên các phầm mềm ứng dụng phổ biến. Các loại virus, mã độc này có thể bị đối tượng tấn công lợi dụng để chiếm quyền điều khiển hệ thống, đánh cắp và mã hoá dữ liệu. Uỷ ban nhân dân xã thông báo thông tin và hướng dẫn một số giải pháp khắc phục như sau:

1. Cảnh báo nguy cơ chiếm quyền Zalo qua "mã QR bình chọn"

Thủ đoạn của người tấn công tạo "Bình chọn cuộc thi" đã được các đối tượng nâng cấp. Thay vì gửi link đăng nhập, đối tượng hiện nay gửi mã QR giả mạo là "mã bình chọn" hoặc "mã nhận quà". Khi người dùng Zalo quét mã này thực chất là đang thực hiện lệnh "Đăng nhập Zalo Web" trên thiết bị của đối tượng tấn công. Ngay khi chiếm được quyền, đối tượng sử dụng công nghệ AI Deepfake để tạo ra các đoạn tin nhắn thoại hoặc hình ảnh cử động giống hệt chủ tài khoản để nhắn tin vay mượn tiền, khiến những người trong danh bạ rất khó phân biệt được thật, giả. Hoặc đối tượng sẽ âm thầm thu thập những dữ liệu tin nhắn, thông tin cá nhân nhạy cảm của người dùng sử dụng cho mục đích xấu.

Thủ đoạn này ảnh hưởng đến tất cả người dùng Zalo, đặc biệt nguy hiểm với những người tham gia các hội nhóm cộng đồng, từ thiện, phụ huynh học sinh…

Giải pháp khắc phục: Tuyệt đối không quét các mã QR lạ được gửi qua tin nhắn để "Bình chọn" hay "Nhận quà". Luôn kiểm tra tài khoản Zalo bằng cách vào "Cài đặt > Tài khoản bảo mật > Lịch sử đăng nhập". Nếu thấy có thiết bị "Zalo Web" lạ là phải bấm "Đăng xuất" ngay lập tức. Thiết lập mã khoá ứng dụng (PIN) để ngăn chặn đăng nhập từ xa.

2. Cảnh báo thủ đoạn thuê SIM "rác" để chiếm đoạt tài khoản từ số điện thoại cũ mà không còn sử dụng

Đây là thủ đoạn mà đối tượng thuê (mua) lại SIM số điện thoại cũ không còn sử dụng mà đã bị nhà mạng thu hồi để phục hồi mật khẩu các loại tài khoản thông qua OTP gửi từ SIM cũ của người dùng đã bỏ nhưng vẫn còn liên kết với Facebook, Zalo, tài khoản Ngân hàng, tài khoản iCloud… Đối tượng sử dụng các số điện thoại này để yêu cầu "Quên mật khẩu" rồi nhận mã OTP từ đó chiếm đoạt toàn bộ tài khoản và dữ liệu nhạy cảm. Ngoài ra các email cũ đã không còn

đăng nhập sử dụng cũng bị các đối tượng dùng phần mềm dò mật khẩu để tìm kiếm thông tin khôi phục tài khoản.

Giải pháp khắc phục: Rà soát ngay mục "Thông tin liên hệ" trên Zalo, Facebook, Ngân hàng… và gỡ bỏ ngay các số điện thoại/ email không còn sử dụng. Chuyển phương thức nhận mã xác thực từ SMS sang các ứng dụng bảo mật chuyên dụng như Google Authenticator hoặc Microsoft Authenticator. Khi thay đổi số điện thoại phải thực hiện thủ tục thay đổi số điện thoại trên tất cả các dịch vụ Ngân hàng và mạng xã hội trước khi bỏ số điện thoại đó.

3. Cảnh báo mã độc "NFC-Steale" đánh cắp thông tin ngân hàng qua ứng dụng giả mạo

Thủ đoạn này lợi dụng quy định về xác thực sinh trắc học và cập nhật thông tin căn cước công dân, đối tượng gửi đường link qua Zalo/SMS giả mạo ứng dụng của Bộ Công an hoặc Ngân hàng. Khi cài đặt mã độc này yêu cầu người dùng áp thẻ Căn cước gắn chip hoặc thẻ Ngân hàng vào mặt sau điện thoại. Mã độc sẽ âm thầm sao chép toàn bộ dữ liệu chip và thông tin thanh toán, đồng thời chiếm quyền điều khiển điện thoại để tự động thực hiện các lệnh chuyển tiền mà người dùng không hề hay biết.

Giải pháp khắc phục: Tuyệt đối không cài đặt ứng dụng qua đường link được gửi từ người lạ hoặc các tệp.APK rời. Chỉ cài đặt ứng dụng từ CH Play hoặc App Store. Cơ quan Công an và Ngân hàng không làm việc qua Zalo hay yêu cầu người dùng tự quét NFC qua ứng dụng lạ. Nếu đã cài đặt lập tức tắt kết nối mạng, tháo SIM và mang điện thoại đến trung tâm bảo mật để quét sạch mã độc hoặc khôi phục cài đặt gốc.

An toàn thông tin mạng là trách nhiệm của toàn xã hội. Mỗi người dân cần nâng cao ý thức cảnh giác, chủ động bảo vệ dữ liệu cá nhân và tích cực tuyên truyền cho người thân, bạn bè về các phương thức, thủ đoạn lừa đảo mới trên không gian mạng.

Đề nghị các cơ quan, đơn vị, tổ chức và toàn thể Nhân dân thường xuyên cập nhật thông tin cảnh báo an ninh mạng. Đồng thời phối hợp chặt chẽ với lực lượng Công an trong công tác phòng ngừa, phát hiện và xử lý các hành vi vi phạm pháp luật trên không gian mạng.

Nơi nhận:
- Như trên;
- TT Đảng Uỷ, HĐND (b/c);
- Chủ tịch, các PCT UBND xã;
- Các cơ quan, đơn vị trên địa bàn xã;
- Các thôn trên địa bàn xã;
- Lưu: VT, UBND.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

U.B.N.D XÃ VŨ QUANG T. HÀ TĨNH

Trần Văn Trà