

Số: / STTTT-TTra

Thái Nguyên, ngày tháng 3 năm 2022

V/v khuyến cáo, phòng tránh rủi ro, lừa đảo
khi sử dụng mạng xã hội zalo

Kính gửi:

- Các Ban đảng;
- Các tổ chức chính trị, tổ chức chính trị xã hội;
- Các tổ chức xã hội nghề nghiệp;
- Các sở, ban, ngành, đoàn thể thuộc tỉnh;
- UBND các huyện, thành phố, thị xã;
- Báo Thái Nguyên;
- Đài Phát thanh – Truyền hình Thái Nguyên;
- Hội Nhà báo tỉnh;
- Tạp chí Văn Nghệ Thái Nguyên;
- Trung tâm Thông tin tỉnh.

Hiện nay, qua công tác quản lý nhà nước, Sở Thông tin và Truyền thông phát hiện trên nền tảng mạng xã hội (facebook, zalo) xuất hiện nhiều đối tượng lừa đảo thông qua mạng xã hội như giả mạo Zalo, đánh cắp tài khoản mạng xã hội nhằm vay mượn tiền và thực hiện hành vi chiếm đoạt. Hình thức của các đối tượng lừa đảo là lập một tài khoản Zalo có tên và sử dụng hình ảnh của người bị hại làm hình đại diện. Sau đó, đối tượng dùng Zalo giả mạo để nhắn tin mượn tiền từ bạn bè, người thân quen trong danh bạ.

Căn cứ chức năng, nhiệm vụ được giao, Sở Thông tin và Truyền thông tỉnh Thái Nguyên đề nghị các cơ quan, đơn vị tuyên truyền, khuyến cáo như sau:

1. Nguyên nhân:

1.1. Lợi dụng lỗ hổng bảo mật (Hacking)

- Kẻ gian có thể đã lấy được nick của người bị hại hoặc giả lập tài khoản Zalo của người bị hại trước đó.

- Đối tượng lừa đảo đã kiểm soát được một tài khoản icloud nào đó của người bị hại.

- Đối tượng đã cài đặt được một ứng dụng/app nào đó lên điện thoại của người bị hại.

- Tài khoản giả mạo chính là người thân quen của người bị hại và đang tham gia một nhóm nào đó cùng người bị hại và có tất cả danh bạ chung trong nhóm.

1.2. Tấn công giả mạo (Phishing)

- Đối tượng giả mạo thành cá nhân lấy ảnh đại diện y hệt người dùng sau đó kết bạn và tìm kiếm thông tin liên quan đến người dùng để lừa đảo.

- Đối tượng giả mạo thành tổ chức, đơn vị uy tín để lừa đảo cung cấp thông tin quan trọng thông qua đường link trong email và trang web.

- Đối tượng giả mạo thành ngân hàng, trang web giao dịch trực tuyến, ví điện tử, công ty thẻ tín dụng để lừa người dùng chia sẻ các thông tin nhạy cảm như: tài khoản & mật khẩu đăng nhập, mật khẩu giao dịch, thẻ tín dụng và các thông tin quan trọng khác thông qua đường link trong email và trang web.

2. Cách thức phòng tránh:

- Không cài đặt ứng dụng (app) lạ và bấm vào đường link khi chưa có thông tin cụ thể.

- Thay đổi mật khẩu email dùng làm icloud, sử dụng chữ in hoa, số và ký tự đặc biệt (@,#,\$...). Tránh không sử dụng ngày tháng năm sinh và số CMND để khởi tạo mật khẩu.

- Khi mua bán trao đổi máy, cần reset máy đưa về tình trạng ban đầu của nhà sản xuất.

- Cảnh giác khi cung cấp những tin tức quan trọng.

- Cảnh giác với người quen khi đã kết bạn với nhau trên mạng xã hội bỗng nhiên vào một ngày tự nhiên lại kết bạn lại.

- Cảnh giác với lời mời kết bạn là những người bạn đã quen biết bằng cách vào kiểm tra lịch sử hoạt động (nhật ký trên tường của người gửi lời mời kết bạn...) nếu người mời kết bạn không có hoạt động nào, hoặc chỉ có 1,2 hoạt động mới đăng là một điều rất nghi ngờ.

- Có kiến thức về an toàn và bảo mật thông tin.

- Không đăng nhập tài khoản vào những thiết bị lạ, nếu buộc phải đăng nhập thì đăng xuất khi hết phiên làm việc.

- Bật chế độ không kết bạn với người lạ trên Zalo.

- Đặt mật khẩu mạnh, thay đổi mật khẩu thường xuyên.

- Đặt mật khẩu bảo vệ thiết bị: PC, máy điện thoại: mã PIN, PassWord, bảo mật vân tay, bảo mật bằng khuôn mặt...

Trên đây là nội dung khuyến cáo, phòng tránh lừa đảo đối với việc sử dụng mạng xã hội Zalo. Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị quan tâm, phối hợp triển khai thực hiện./.

Nơi nhận:

- Như trên;
- UBND tỉnh (b/c);
- Lưu: VT, TTra.

**KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Đào Ngọc Tuất