ỦY BAN NHÂN DÂN **XÃ XUÂN TRÚC**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 183 /TB - UBND	*Xuân Trúc, ngày 31 tháng 10 năm 2024*

THÔNG BÁO
Về việc nhận diện và phòng chống lừa đảo trực tuyến bảo vệ người dân trên không gian mạng năm 2024

Kính gửi: - Toàn thể cán bộ công chức, viên chức, đảng viên và nhân dân;
- Các cơ quan, tổ chức, doanh nghiệp trên địa bàn xã;

Thực hiện công văn số 113/VHTT ngày 29/10/2024 của Phòng Văn hóa và thông tin huyện Ân Thi về việc triển khai Chiến dịch tuyên truyền "Kỹ năng nhận diện và phòng chống lừa đảo trực tuyến bảo vệ người dân trên không gian mạng năm 2024;

Trong thời gian vừa qua, các sự cố lộ lọt thông tin, dữ liệu cá nhân, lừa đảo trực tuyến diễn biến ngày càng phức tạp với nhiều thủ đoạn tinh vi. Một trong những nguyên nhân chính gây ra mất an toàn thông tin được xác định đến từ nhận thức của người sử dụng. Các cuộc tấn công mạng có xu hướng tập trung chủ yếu vào con người thay vì máy móc, thiết bị. Bên cạnh các giải pháp kỹ thuật, việc tuyên truyền, phổ biến, nâng cao nhận thức và kỹ năng nhằm trang bị cho mỗi cá nhân những kiến thức và kỹ năng cơ bản để bảo đảm an toàn thông tin trên không gian mạng là yếu tố then chốt giúp tạo dựng một không gian mạng Việt Nam an toàn, góp phần thúc đẩy nhanh quá trình chuyển đổi số, phát triển hạ tầng kinh tế - xã hội số một cách bền vững.

Để tăng cường nâng cao nhận thức cho người dân giảm thiểu các nguy cơ bị lừa đảo trên không gian mạng, UBND xã thông báo đến toàn thể cán bộ và nhân dân trong xã một số kỹ năng nhận diện lừa đảo trên không gian mạng, nguyên tắc bảo vệ bản thân khỏi lừa đảo trực tuyến, nội dung cụ thể như sau:

1. Cách tiếp cận của các đối tượng lừa đảo

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...), Website giả mạo, Các ứng dụng giả mạo.

2. 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, exe...) 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..

3. Cách thức các đối tượng lừa đảo 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.

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. 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).

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.

4. "Nguyên tắc vàng" bảo vệ bản thân khỏi lừa đảo trực tuyến

- ***Nguyên tắc 1:*** *Hãy chậm lại*

Những đối tượng lừa đảo thường tạo ra cảm giác cấp bách để chúng có thể vượt qua khả năng nhận định của bạn. Những cuộc gọi, tin nhắn... thúc giục phải hành động nhanh như: thời gian khuyến mãi đã hết; nếu không chuyển tiền bây giờ bạn và người thân phải thực hiện các thủ tục tố tụng...

Trong tình huống này, bạn hãy dành thời gian suy nghĩ kỹ và đặt câu hỏi tìm hiểu kỹ nội dung, thông tin để tránh bị dồn vào tình huống xấu.

- ***Nguyên tắc 2****: Kiểm tra tại chỗ*

Tìm hiểu thêm để xác thực thông tin bạn đang nhận được. Nếu bạn nhận được một cuộc gọi không mong muốn, hãy tra cứu số ngân hàng, cơ quan, hoặc tổ chức đang gọi đến và liên hệ lại trực tiếp.

- ***Nguyên tắc 3****: Dừng lại! Không gửi*

Không một cá nhân hoặc cơ quan nào yêu cầu thanh toán ngay tại chỗ. Vì vậy, nếu bạn cảm thấy giao dịch không đáng tin, hãy dừng lại vì có thể đây là dấu hiệu lừa đảo.

5. Quy tắc "6 KHÔNG"

- KHÔNG cung cấp thông tin cá nhân, địa chỉ, số điện thoại, số tài khoản ngân hàng của mình cho đối tượng không quen biết; thận trọng rà soát và kiểm tra kỹ thông tin trước khi thực hiện các giao dịch chuyển tiền.

- KHÔNG kết bạn và nói chuyện với người lạ, đặc biệt là những tài khoản có hình ảnh ngoại hình đẹp và bắt mắt. Tuyệt đối không nhận lời mời tham gia các hội nhóm mà không rõ mục đích đối tượng.

- KHÔNG truy cập, đăng nhập vào các đường dẫn, liên kết, website, ứng dụng hoặc mở tệp đính kèm đến từ người gửi không xác định, không rõ nguồn gốc.

- KHÔNG cán bộ cơ quan nhà nước, bộ công an, viện kiểm sát, tòa án hay đơn vị tài chính… nào gọi điện để điều tra qua điện thoại, yêu cầu phải cung cấp thông tin cá nhân hay đóng tiền.

- KHÔNG thực hiện chuyển khoản trước, tuyệt đối không đặt cọc, chuyển khoản tiền cho các đối tượng lạ trong bất cứ trường hợp nào.

- KHÔNG tham lam những tài sản, món quà không rõ nguồn gốc có thể nhận được một cách dễ dàng, những lợi nhuận "phi thực tế" mà không tốn sức lao động, những lời mời chào, dụ dỗ "việc nhẹ lương cao"...

Người dân Theo dõi và cập nhật các thông tin, tình huống, dấu hiệu về lừa đảo trực tuyến tại kênh thông tin Cổng không gian mạng quốc gia trên các nền tảng mạng xã hội như Facebook, TikTok… hoặc website Khonggianmang.vn.

Vậy UBND xã thông báo đến toàn thể cán bộ công chức, viên chức, đảng viên và nhân dân; Các cơ quan, tổ chức, doanh nghiệp trên địa bàn xã nắm được và tổ chức thực hiện tốt nội dung thông báo trên, cùng đề cao cảnh giác, phòng ngừa các hành vi lừa đảo trên không gian mạng./.

Nơi nhận:
- Đài truyền thanh xã;
- Cổng TTĐT xã;
- Lưu: VT.

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

Ký bởi: Ủy ban nhân dân xã Xuân Trúc
Cơ quan: Tỉnh Hưng Yên

Bùi Đắc Tiến