UBND TỈNH LONG AN
TIỂU BAN AN TOÀN, AN NINH MẠNG

Số: 10934 /TBATANM
V/v tăng cường công tác bảo đảm an toàn, an ninh thông tin, bảo mật tài khoản người dùng trên các hệ thống thông tin

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Long An, ngày 24 tháng 10 năm 2024

Kính gửi:
- Các sở, ban, ngành tỉnh;
- UBND các huyện, thị xã, thành phố.

Qua công tác rà soát, giám sát tình hình bảo đảm an toàn thông tin trên địa bàn tỉnh, Công an tỉnh và Sở Thông tin và Truyền thông đã phát hiện rất nhiều tài khoản, mật khẩu của cán bộ, công chức, viên chức đang sử dụng các hệ thống thông tin dùng chung của tỉnh được "rao bán" công khai trên các diễn đàn, website của nhóm tin tặc trên môi trường mạng, có nguy cơ gây mất an toàn thông tin cho các hệ thống quan trọng của tỉnh, ảnh hưởng nghiêm trọng đến quá trình kết nối và khai thác cơ sở dữ liệu quốc gia về dân cư phục vụ Hệ thống thông tin giải quyết thủ tục hành chính trên địa bàn tỉnh. Nguyên nhân: nhiều khả năng do trong quá trình sử dụng máy tính, cán bộ, công chức, viên chức chưa thực hiện nghiêm các nguyên tắc về đảm bảo an toàn, an ninh thông tin dẫn đến máy tính bị lây nhiễm mã độc đánh cắp tài khoản, dữ liệu.

Thực hiện Công văn số 34/VP-BCĐ ngày 08/8/2024 của Văn phòng Ban Chỉ đạo an toàn, an ninh mạng quốc gia về tăng cường công tác bảo đảm an ninh mạng, phòng, chống tấn công mạng; Công văn số 5722/TCTTKĐA ngày 10/8/2023 của Tổ công tác triển khai Đề án phát triển ứng dụng dữ liệu về dân cư, định danh và xác thực điện tử của Chính phủ (sau đây viết tắt là Tổ công tác triển khai Đề án 06/CP). Để khắc phục tình trạng nêu trên, đảm bảo an toàn thông tin theo yêu cầu của Bộ Công an, Tiểu ban An toàn, an ninh mạng tỉnh đề nghị các sở, ban, ngành tỉnh, UBND các huyện, thị xã, thành phố tập trung thực hiện các nội dung sau:

1. Tiếp tục phổ biến, triển khai, quán triệt Công văn số 5722/TCTTKĐA ngày 10/8/2023 của Tổ công tác Đề án 06/CP đến toàn thể cán bộ, công chức, viên chức để thực hiện nghiêm các quy định có liên quan trong quá trình kết nối, chia sẻ và khai thác thông tin cơ sở dữ liệu quốc gia về dân cư (CSDLQG về dân cư) phục vụ việc tra cứu, kiểm tra, xác thực thông tin công dân để tiếp nhận, xử lý hồ sơ giải quyết thủ tục hành chính cho người dân, doanh nghiệp trên Hệ thống thông tin giải quyết thủ tục hành chính của tỉnh, cũng như các hệ thống chuyên ngành của các đơn vị đã được kết nối với CSDLQG về dân cư.

2. Chỉ đạo công chức phải ***bảo mật, không tiết lộ thông tin dữ liệu cá nhân của công dân*** khi tiếp nhận, xử lý hồ sơ giải quyết thủ tục hành chính cho người dân, doanh nghiệp trên Hệ thống thông tin giải quyết thủ tục hành chính của tỉnh. Trường hợp các cơ quan, đơn vị, địa phương có thay đổi công chức tiếp nhận, xử lý hồ sơ trên Hệ thống thông tin giải quyết thủ tục hành chính của tỉnh, phải có văn bản gửi về Sở Thông tin và Truyền thông (thông qua Trung tâm Công nghệ thông tin và Truyền thông) để kịp thời xóa, cập nhật phân quyền tài khoản cho người dùng.

3. Chỉ đạo các cán bộ, công chức, viên chức thực hiện ***thay đổi mật khẩu*** các tài khoản được cấp đang sử dụng các hệ thống thông tin dùng chung của tỉnh *(Hệ thống giải quyết thủ tục hành chính (phân hệ Một cửa điện tử), Hệ thống Quản lý văn bản và điều hành, Hệ thống Quản lý cán bộ công chức…)* theo đúng quy định, yêu cầu về đảm bảo an toàn thông tin, cụ thể:

- **Kể từ ngày 26/10/2024**, tài khoản cán bộ, công chức, viên chức các hệ thống nêu trên nếu không thay đổi mật khẩu đảm bảo yêu cầu về an toàn thông tin theo hướng dẫn bên dưới sẽ không thể truy cập được vào các hệ thống.

- Độ dài mật khẩu ***tối thiểu từ 8 ký tự trở lên***, bao gồm sự kết hợp đầy đủ giữa: chữ hoa, chữ thường, ký tự số (1,2,3,..) và ký tự đặc biệt (@, #, $, !, %, * , ?, &,…); sử dụng mật khẩu khác nhau cho từng tài khoản để đề phòng việc tin tặc sử dụng một mật khẩu để truy cập vào tất cả các tài khoản.

- Thực hiện thay đổi mật khẩu mặc định ngay khi tiếp nhận tài khoản mới; thường xuyên thay đổi mật khẩu, ít nhất 06 tháng một lần. Tuyệt đối không tiết lộ mật khẩu của cá nhân cho người khác, cũng như giao tài khoản mật khẩu cho người khác sử dụng thay mình.

- Cán bộ, công chức, viên chức hoàn toàn chịu trách nhiệm trong trường hợp để lộ, lọt tài khoản được cấp dẫn đến việc bị lợi dụng sử dụng tài khoản sai mục đính, tấn công gây ảnh hướng đến hoạt động của hệ thống.

4. Khẩn trương triển khai cài đặt phần mềm phòng, chống mã độc quản trị tập trung, trong đó ưu tiên cài đặt cho các máy có sử dụng phần mềm khai thác thông tin cơ sở dữ liệu quốc gia về dân cư; thực hiện rà quét, phát hiện, loại bỏ các phần mềm, ứng dụng mã độc tồn tại trên máy tính; thường xuyên cập nhật các bản nâng cấp phần mềm máy vi tính, thiết bị thông minh.

Thông tin đầu mối liên hệ phối hợp, hướng dẫn: Sở Thông tin và Truyền thông (Trung tâm Công nghệ thông tin và Truyền thông, số điện thoại: 0272 3524 999 hoặc 0946906528 gặp ông Nguyễn Văn Kiệt, 0966452401 gặp ông Phan Quốc Duy); Công an tỉnh (Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, số điện thoại 0272 3989 848 hoặc 0703776688 gặp Đại úy Trần Châu Long).

Theo nội dung trên, đề nghị Thủ trưởng các sở, ban, ngành tỉnh, Chủ tịch UBND các huyện, thị xã, thành phố và Thủ trưởng cơ quan, đơn vị liên quan nghiêm túc quán triệt triển khai thực hiện./.

Nơi nhận:
- TT.TU; TT.HĐND tỉnh (b/c);
- CT, các PCT UBND tỉnh;
- Công an tỉnh;
- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- CVP, các Phó CVP UBND tỉnh;
- Các phòng, ban, trung tâm thuộc VP;
- Lưu: VT, CAT.

TRƯỞNG TIỂU BAN

CHỦ TỊCH UBND TỈNH
Nguyễn Văn Út