

Số: 122/CSĐTNTMT-TCHCKT
V/v tăng cường phòng, chống
tấn công mạng trên hệ thống máy vi
tính và thiết bị CNTT của đơn vị

Sơn La, ngày 12 tháng 4 năm 2024

Kính gửi: Các phòng chuyên môn, điểm vệ tinh

Thực hiện Công văn số 549/ SLĐTBOXH-VP ngày 10/4/2024 của Sở Lao động - Thương binh và Xã hội về việc tăng cường phòng, chống tấn công mạng. Để đảm bảo an toàn hệ thống máy vi tính và thiết bị CNTT của đơn vị, đặc biệt là các dữ liệu lưu trữ đang làm việc. Cơ sở điều trị nghiện ma túy tỉnh yêu cầu các phòng chuyên môn, điểm vệ tinh thực hiện một số nội dung sau :

1. Tuyên truyền, quán triệt

Thường xuyên tuyên truyền, quán triệt đến viên chức, người lao động tại buổi giao ban và hệ thống phát thanh của Cơ sở về năng cao nhận thức, trách nhiệm đối với công tác đảm bảo an ninh, an toàn hệ thống mạng, bảo vệ bí mật nhà nước, thông tin dữ liệu cá nhân trên không gian mạng đặc biệt là đối với các viên chức được phân công sử dụng máy vi tính có kết nối internet để làm việc.

2. Một số biện pháp phòng tránh bị tấn công mạng

- Cài đặt phần mềm phòng chống virus, mã độc theo mô hình quản trị tập trung (đã được phòng Tổ chức – Hành chính – Kế toán hướng dẫn cài đặt).

- Dạng phổ biến tấn công hiện nay File đính kèm email, tệp đính kèm tin nhắn là những công cụ tấn công mạng phổ biến của tin tặc. Do đó cần có tinh thần cảnh giác kiểm tra kỹ các nội dung trên Mail công vụ, Gmail, zalo, hoặc các trang tìm kiếm trên google trực khi mở hoặc truy cập.

- Đối với Gmail, mail công vụ: Luôn kiểm tra địa chỉ, tên người gửi, không download các tệp tin không rõ nguồn gốc

- Đối với sử dụng tìm kiếm trên google : Chỉ thực hiện tìm kiếm nội dung và tải văn bản trên các trang web chính thống uy tín, được xác thực, không tải các phần mềm cài đặt không rõ nguồn gốc.

- Không nên click vào link lạ, trang web đáng ngờ, không tải file đính kèm không rõ nguồn gốc

- Hạn chế sử dụng USB, nếu sử dụng phải quét virus trước khi mở USB.

- Có ý thức, tự chủ động trong việc sao lưu các dữ liệu quan trọng.

3. Tổ chức thực hiện

3.1. Phòng Tổ chức – Hành chính – Kế toán

- Tham mưu tập huấn, bồi dưỡng cho viên chức về kiến thức đảm bảo an toàn thông tin trên không gian mạng.

- Tham mưu bổ sung cơ sở vật chất, trang thiết bị kỹ thuật nhằm đảm bảo an toàn thông tin trên không gian mạng.

- Đôn đốc, hướng dẫn phòng chuyên môn, điểm vệ tinh cài đặt phần mềm phòng chống virut, mã độc theo mô hình quản trị tập trung.

- Liên hệ với Sở Thông tin truyền thông để kiểm tra, đánh giá an toàn, an ninh thông tin an ninh mạng tại đơn vị. Từ đó đưa ra giải pháp để thực hiện.

- Tuyên truyền trên trang thông tin điện tử của Cơ sở.

3.2. Phòng Giáo dục dạy nghề tư vấn hòa nhập cộng đồng

Biên tập tuyên truyền trên hệ thống phát thanh *Cắm nang phòng chống, giảm thiểu rủi ro từ tấn công Ransomware* (có tài liệu gửi kèm).

3.3. Các phòng chuyên môn, điểm vệ tinh

Thực hiện nghiêm túc nội dung mục 1,2 công văn này.

Trong trường hợp phát hiện hoạt động tấn công mạng nghiêm trọng vào hệ thống máy tính cần trao đổi về phòng Tổ chức – Hành chính – Kế toán để phối hợp, hướng dẫn xử lý.

Cơ sở Điều trị nghiện ma túy tỉnh yêu cầu các phòng chuyên môn, điểm vệ tinh nghiêm túc thực hiện./.

Nơi nhận:

- Như trên;
- Ban Giám đốc Cơ sở (B/c);
- Lưu: VT,

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Phùng Đức Sơn