

Số: 584 /SGDDT-VP

Vĩnh Long, ngày 21 tháng 4 năm 2020

V/v cảnh báo nguy cơ mất an toàn thông tin từ phần mềm họp trực tuyến Zoom

Kính gửi:

- Phòng Giáo dục và Đào tạo huyện, thị xã, thành phố;
- Trường THCS&THPT, THPT;
- Trung tâm trực thuộc Sở.

Căn cứ Công văn số 180/STTT-CNTT, ngày 25/3/2020 của Sở Thông tin và Truyền thông tỉnh Vĩnh Long về việc cảnh báo nguy cơ mất an toàn thông tin từ phần mềm họp trực tuyến;

Hiện nay, Zoom đang là phần mềm phổ biến cho học trực tuyến, tổ chức hội họp và làm việc từ xa. Tuy nhiên, phần mềm này tồn tại một số lỗ hổng bảo mật nghiêm trọng như: mã hóa dữ liệu đầu cuối kém, dễ dàng bị dò quét ID cuộc họp, lỗ hổng liên quan đến đường dẫn UNC (Universal Naming Convention).

Đến ngày 14/4/2020, Cục An toàn thông tin - Bộ Thông tin và Truyền thông ghi nhận có hơn 500.000 tài khoản Zoom đã bị lộ lọt thông tin cá nhân của người sử dụng, trong đó bao gồm: email, mật khẩu, đường dẫn URL các cuộc họp và mật khẩu kèm theo.

Để tăng cường công tác bảo đảm an toàn, an ninh mạng, đặc biệt là bảo vệ thông tin cá nhân, bảo vệ quyền và lợi ích hợp pháp của trường, giáo viên và học sinh, Sở Giáo dục và Đào tạo khuyến cáo:

1. Các trường cần nhắc nhở cẩn thận khi sử dụng phần mềm họp trực tuyến Zoom cho các hoạt động dạy học trực tuyến, trao đổi trực tuyến hoặc các tổ chức hội họp khác.

2. Ưu tiên lựa chọn các sản phẩm phần mềm học trực tuyến, tổ chức hội họp và làm việc từ xa do doanh nghiệp uy tín sản xuất, đặc biệt là các sản phẩm do doanh nghiệp uy tín trong nước cung cấp như: Viettel, VNPT,...

3. Đối với giáo viên sử dụng các phần mềm học trực tuyến, tổ chức dạy học và làm việc từ xa:

- Chú ý tải phần mềm từ các nguồn chính thống, thường xuyên cập nhật phiên bản mới nhất của phần mềm (khuyến nghị sử dụng từ phiên bản Zoom 4.9.6 trở lên).

- Không chia sẻ thông tin về phòng họp (ID, mật khẩu) để tránh các trường hợp bị kẻ xấu theo dõi, phá hoại.

- Thiết lập các cấu hình bảo mật cao trên các phần mềm họp trực tuyến. Cụ thể: đặt mật khẩu phức tạp cho các buổi họp; kích hoạt chế độ xét duyệt người tham gia trước khi vào phòng họp; thiết lập các tính năng quản lý việc chia sẻ màn hình

trong buổi họp; hạn chế việc lưu lại nội dung buổi họp trong trường hợp không cần thiết.

- Đối với người dùng đã sử dụng phần mềm Zoom, thực hiện ngay việc đổi mật khẩu phức tạp, tránh sử dụng chung mật khẩu với các tài khoản khác.

- Khi phát hiện nguy cơ, dấu hiệu lộ, lọt thông tin cá nhân của người sử dụng, cần nhanh chóng khắc phục và kịp thời thông báo cho Trung tâm ứng cứu khẩn cấp không gian mạng Việt Nam, Cục An toàn thông tin - Bộ Thông tin và Truyền thông, điện thoại: 086 91003, email: office@vncert.vn và các cơ quan chức năng có thẩm quyền liên quan để phối hợp xử lý kịp thời các vấn đề phát sinh, đồng thời báo về Sở Giáo dục và Đào tạo để nắm thông tin qua số điện thoại 02703.836087, email cntt@vinhlong.edu.vn.

Sở Giáo dục và Đào tạo yêu cầu các đơn vị nghiên cứu thực hiện đúng theo nội dung công văn này./. *Trịnh Văn Ngẫu*

Nơi nhận:

- Như Kính gửi;
- Ban Giám đốc (để BC);
- PA03-Công an tỉnh (để phối hợp);
- Lưu: VT.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**



Trịnh Văn Ngẫu