BỘ CÔNG AN
CÔNG AN TỈNH HƯNG YÊN
Số: 1046/CAT(PA03)

V/v nguy cơ mất an ninh, an toàn thông tin khi sử dụng ứng dụng trực tuyến

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

Hưng Yên, ngày 27 tháng 4 năm 2020

Kính gửi:
- Thủ trưởng các ban, sở, ngành, đoàn thể tỉnh;
- Thường trực huyện ủy, Thành ủy, Thị ủy;
- Chủ tịch UBND các huyện, thành phố, thị xã;
- Thủ trưởng các cơ quan Trung ương đóng trên địa bàn tỉnh.

Theo thông báo của Bộ Công an, qua công tác đảm bảo an ninh mạng, phát hiện các nguy cơ mất an ninh, an toàn thông tin khi sử dụng các ứng dụng trực tuyến, cụ thể.

1. Để ứng phó với tình hình dịch bệnh Covid-19, nhất là trong thời gian cách ly xã hội, nhiều cơ quan, doanh nghiệp, tổ chức, cá nhân đã thực hiện chuyển đổi nhiều hoạt động sang môi trường mạng, sử dụng các ứng dụng online (*như: Zoom cloud Meeting, Microsoft Teams, Googlo Hangout, Facebook Workplace, TrueConf Online, GoToMeeting, Join.me, ClickMeeting, eMeeting.vn…)* với các tính năng chia sẻ nội dung màn hình trên máy tính, cuộc gọi âm thanh/hình ảnh trực tuyến, chia sẻ tài liệu, thuyết trình, lên lịch họp, học tập… để hội họp trực tuyến, học tập trực tuyến… Theo thống kế trước và sau khi phát hiện dịch bệnh Covid-19, chỉ tính riêng ứng dụng Zoom Cloud Meeting số lượng người dùng đã tăng từ 10 triệu lên 200 triệu người, với trên 74.000 khách hàng và 13 triệu người dùng hoạt động hàng tháng, 90.000 trường học trên hơn 20 quốc gia đang sử dụng ứng dựng phục vụ học tập trực tuyến.

Bên cạnh việc gia tăng về số lượng người dùng trong thời gian gần đây, nhiều chuyên gia, hãng bảo mật uy tín… đã liên tiếp đưa ra các cảnh báo, bằng chứng về việc mất an ninh, an toàn thông tin khi sử dụng ứng dụng Zoom Cloud Meeting như: Ứng dụng tự động thu thập và bí mật về chia sẻ dữ liệu người dùng cho Facebook mà không có sự cho phép của người dùng, kể cả những người không sử dụng Facebook; Các tin tặc đăng ký nhiều tên miền giả mạo Zoom nhằm phát tán các tệp tin độc hại giải mạo ứng dụng lừa người dùng tải và cài đặt trên thiết bị của mình; Tồn tại một số lỗ hổng bảo mật cho phép tin tặc có thể đánh cắp thông tin đăng nhập (*thông tin cá nhân của 500.000 tài khoản đã bị lộ, lọt),* chèn các liên kết độc hại, chiếm quyền điều khiển, thay đổi, chèn các nội dung không phù hợp, tấn công kiểm soát micro, camera, đánh cắp các video trực tuyến… (*02 lỗ hổng bảo mật của ứng dụng Zoom Cloud Meeting phiên bản dành cho hệ điều hành Windows và hệ điều hành MacOS đang được tin tặc giao bán).*

2. Từ tình hình trên, để đảm an ninh mạng, an toàn thông tin khi sử dụng các ứng dụng trực tuyến, Công an tỉnh Hưng Yên đề nghị:

- Cần nghiên cứu kỹ trong lựa chọn các ứng dụng, tránh cài đặt, sử dụng các ứng dụng đang bị cảnh báo tồn tại lỗ hổng, điểm yếu bảo mật, tải và cài đặt ứng dụng từ các nguồn chính thống; thường xuyên cập nhật bản vá lỗ hổng của các ứng dụng và hệ điều hành.

- Khi sử dụng các ứng dụng trực tuyến cần sử dụng các kênh, phòng riêng, có mật khẩu bảo vệ, xác thực người tham gia; không chia sẻ các thông tin về phòng họp (*ID, mật khẩu, thời gian…)* Trên không gian mạng; không tải, mở các tệp tin, đường dẫn lạ không rõ nguồn gốc…

- Không sử dụng các ứng dụng trực uyến để trao đổi, gửi, nhận các dữ liệu bí mật nhà nước, bí mật nội bộ.

- Sở Giáo dục và Đào tạo căn cứ Công văn 227/CAT(PA03) ngày 16/4/2020 và Công văn này để đảm bảo an ninh, an toàn cho quá trình dạy, học trực tuyến.

Công an tỉnh trân trọng báo cáo./.

Nơi nhận:
- Đ/c Nguyễn Văn Phóng, Chủ tịch UBND tỉnh;
- Đ/c Nguyễn Duy Hưng, PCT UBND tỉnh;
- Như Kính gửi;
- Lưu CAT, PA03-DCĐ.

GIÁM ĐỐC

(Đã ký)

Đại tá Đỗ Đình Hào