

Số: 158/PA03-Đ1

Nghệ An, ngày 27 tháng 04 năm 2020

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

VĂN PHÒNG UBND TỈNH N.A.  
ĐẾN Số:.....  
Ngày:.....

Kính gửi: Thủ trưởng các cơ quan, đơn vị, trường học, bệnh viện.

Theo thông báo của Bộ Công an, trong thời gian qua, trước diễn biến phức tạp của tình hình dịch bệnh Covid-19, các cơ quan, tổ chức, doanh nghiệp, 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, Google Hangout, Facebook Workplace, TrueConf Online, GoToMeeting, Join.me, ClickMeeting, eMeeting.vn...*) với đầy đủ 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 kê 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 dụng 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 chia sẻ dữ liệu người dùng cho Facebook mà không có sự cho phép của người dùng, kể cả những người dùng không sử dụng Facebook.

- Các tin tặc đăng ký nhiều tên miền giả mạo "Zoom" nhằm phát tán các tệp tin độc hại giả 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 rao bán).

Từ tình hình trên, để đảm bảo an ninh mạng, an toàn thông tin khi sử dụng các ứng dụng trực tuyến, Phòng An ninh chính trị nội bộ - Công an tỉnh Nghệ An đề nghị Thủ trưởng các cơ quan, đơn vị, trường học, bệnh viện chỉ đạo triển khai thực hiện tốt các mặt công tác trọng tâm, cụ thể như sau:

1. Cần nghiên cứu kỹ trong lựa chọn sử dụng các ứng dụng; tránh cài đặt, sử dụng các ứng dụng bị cảnh báo tồn tại lỗ hổng, điểm yếu bảo mật; tải và cài đặt các



ứng dụng từ các nguồn chính thống; thường xuyên cập nhật bản vá, lỗ hổng của các ứng dụng và hệ điều hành.

2. 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.

3. Không sử dụng các ứng dụng trực tuyến để trao đổi, gửi nhận các dữ liệu có nội dung bí mật nhà nước, dữ liệu nội bộ.

Vậy Phòng An ninh Chính trị nội bộ Công an tỉnh thông báo để các cơ quan, đơn vị, trường học, bệnh viện biết, thực hiện./.

**Nơi nhận:**

- Như kính gửi (để ph/hợp);
  - Đ/c Lê Khắc Thuyết (để b/cáo);
  - Phòng PV01, PV05 (để th/dõi);
  - Lưu PA03.
- SL: 130 bản.

**TRƯỞNG PHÒNG**



**Đại tá Dương Đình Văn**