

Số: 17 /TB-BCA-A05

Hà Nội, ngày 17 tháng 4 năm 2020

VP.UBND TỈNH BÌNH PHƯỚC

Số:.....  
**ĐẾN** Ngày: 29/4/2020  
Chuyên:.....  
Lưu hồ sơ số:.....

**THÔNG BÁO**

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

Qua công tác đảm bảo an ninh mạng, Bộ Công an phát hiện các nguy cơ mất an ninh mạng, an toàn thông tin khi sử dụng các ứng dụng trực tuyến, cụ thể như sau:

1. Hiện nay, trong bối cảnh tình hình dịch bệnh Covid-19 diễn biến phức tạp, các 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, Google Hangout, Facebook Workplace, TrueConf Online, GoToMeeting, Join.me, ClickMeeting, eMeeting.vn...) với đầy đủ 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 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: (1) 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; (2) 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; (3) 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), chen các liên kết độc hại, chiếm quyền điều khiển, thay đổi, chen 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).

2. Từ tình hình trên, để đảm bảo an ninh mạng, an toàn thông tin khi sử dụng các ứng dụng trực tuyến, Bộ Công an đề nghị các bộ, ban, ngành, địa phương chủ động thực hiện một số biện pháp sau:

(1) Cần nghiên cứu kỹ trong lựa chọn sử dụng 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.

(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 bí mật nhà nước, dữ liệu nội bộ.

Bộ Công an xin thông báo./.

**Nơi nhận:**

- Đ/c Bộ trưởng Tô Lâm
- Các đồng chí Thứ trưởng BCA
- Văn phòng TW Đảng
- Văn phòng Tổng Bí thư
- Văn phòng Chủ tịch nước
- Văn phòng Quốc hội
- Văn phòng Chính phủ
- Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ
- Tỉnh ủy, Thành ủy, UBND các tỉnh, TP trực thuộc TW
- Tòa án nhân dân tối cao
- Viện kiểm sát nhân dân tối cao
- Kiểm toán nhà nước
- Ngân hàng nhà nước
- Các Cục, Bộ Tư lệnh, đơn vị trực thuộc Bộ
- Công an các tỉnh, thành phố trực thuộc TW
- Lưu: VT, A05(P8).

(để báo cáo);

(để phối hợp);

**TUQ. BỘ TRƯỞNG  
CỤC TRƯỞNG CỤC AN NINH MẠNG  
VÀ PCTP SỬ DỤNG CÔNG NGHỆ CAO**



**Thiếu tướng Nguyễn Minh Chính**

(để thực hiện);