UBND HUYỆN TAM DƯƠNG
PHÒNG GIÁO DỤC VÀ ĐÀO TẠO

Số: 162/PGD&ĐT-CNTT

V/v triển khai áp dụng các biện pháp khẩn cấp phòng chống mã độc lây nhiễm toàn cầu.

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

Tam Dương, ngày 17 tháng 05 năm 2017

Kính gửi: Các trường mầm non, tiểu học, trung học cơ sở

Vào ngày 12/5/2017, trên các phương tiện truyền thông thế giới và Việt Nam đồng loạt đưa tin các nhóm tin tặc sử dụng bộ công cụ đánh cắp được của cơ quan An ninh quốc gia Mỹ để khai thác lỗ hổng MS17-010 trên hệ điều hành Windows của Microsoft, tấn công mã hóa dữ liệu đòi tiền chuộc của các tổ chức, cá nhân.

Tính đến thời điểm hiện tại, đã có khoảng 200.000 máy tính của 150 quốc gia bị lây nhiễm, mã hóa dữ liệu và đòi tiền chuộc, trong đó có Việt Nam, làm tê liệt nhiều hệ thống máy tính, gây ảnh hưởng nghiêm trọng tới nhiều tổ chức, cá nhân.

Mã độc được sử dụng có tên **WannaCry** đã được các tin tặc phát triển liên tục ra nhiều biến thể mới. Cục An toàn thông tin , Bộ Thông tin & Truyền thông và các chuyên gia an ninh mạng nhận định, nguy cơ bùng phát việc lây nhiễm sau ngày 14/5/2017 (sau nghỉ cuối tuần) đối với các các cơ quan, tổ chức chính phủ ở Việt Nam rất lớn.

Ngày 15/5/2017 UBND huyện Tam Dương có Văn bản số 709/UBND-VP về việc triển khai áp dụng các biện pháp khẩn cấp phòng chống mã độc lây nhiễm toàn cầu.

Để phòng tránh nguy cơ lây nhiễm và mất dữ liệu của các nhà trường và khả năng lây nhiễm tới hệ thống máy tính của huyện và các đơn vị. Phòng GD&ĐT Tam Dương yêu cầu Hiệu trưởng các nhà trường chỉ đạo triển khai khẩn cấp một số biện pháp sau đây:

1. Sử dụng hệ thống thư điện tử, quản lý văn bản qua mạng Truyền số liệu chuyên dùng. **Chỉ nối mạng LAN của đơn vị với mạng Internet khi toàn bộ các máy tính trong hệ thống đã cập nhật xong bản vá lỗi.**

2. Đăng nhập vào địa chỉ download bản vá lỗi:
https://blogs.technet.microsoft.com/msrc/2017/04/14/protecting-customers-and-evaluating-risk/

Đối với các hệ điều hành không còn được Microsoft hỗ trợ có thể download tại địa chỉ:

http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

3. Cập nhật ngay các chương trình Antivius đang sử dụng. Đối với các máy tính không có phần mềm Antivirus cần tiến hành cài đặt và sử dụng ngay một phần mềm Antivirus có bản quyền.

4. Cẩn trọng khi nhận được email có file đính kèm và các đường link lạ được gửi trong email, trên các mạng xã hội, công cụ chat…

5. Cần thận trọng khi mở các file đính kèm ngay cả khi nhận được từ những địa chỉ quen thuộc. Sử dụng các công cụ kiểm tra phần mềm độc hại trực tuyến hoặc có bản quyền trên máy tính với các file này trước khi mở ra.

6. Không mở các đường dẫn có đuôi .hta hoặc đường dẫn có cấu trúc không rõ ràng, các đường dẫn rút gọn link.

7. Thực hiện ngay việc lưu trữ (backup) dữ liệu quan trọng ra ổ cứng ngoài.

Trong quá trình thực hiện, nếu có vướng mắc về kỹ thuật hoặc cần hỗ trợ xin liên hệ về phòng GD&ĐT (đ/c Quân – CB phòng GD) hoặc theo địa chỉ Email: quantq.tocntt@vinhphuc.edu.vn để được hỗ trợ./.

Nơi nhận:
- Như kính gửi;
- Lãnh đạo phòng GD;
- Nghiệp vụ các cấp học.
- Lưu: VT.

KT. TRƯỞNG PHÒNG
PHÓ TRƯỞNG PHÒNG

CỘNG HÒA X.H.C.N VIỆT NAM
PHÒNG GIÁO DỤC VÀ ĐÀO TẠO
TAM DƯƠNG - T. VĨNH PHÚC

Trần Văn Thúy