UBND TỈNH BẮC NINH
SỞ GIÁO DỤC VÀ ĐÀO TẠO

Số: 1970 /SGDĐT-GDTH

V/v bảo đảm an toàn thông tin mạng các dịp lễ, Tết trong năm 2022

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

Bắc Ninh, ngày 30 tháng 12 năm 2021

Kính gửi:
- Thanh tra và các phòng thuộc Sở;
- Phòng giáo dục và đào tạo các huyện, thành phố;
- Các đơn vị trực thuộc Sở;
- Các trung tâm GDNN-GDTX cấp huyện.

Căn cứ Quyết định số 21/2019/QĐ-UBND ngày 22/10/2019 của UBND tỉnh ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin (CNTT) của cơ quan nhà nước trên địa bàn tỉnh Bắc Ninh; Công văn số 1101/STTTT-CNTT ngày 27/12/2021 của Sở Thông tin và Truyền thông Bắc Ninh về việc bảo đảm an toàn thông tin mạng các dịp lễ, Tết trong năm 2022;

Để bảo đảm an toàn thông tin mạng, không bị động, bất ngờ với mọi tình huống tấn công mạng vào hệ thống CNTT của các cơ sở giáo dục trên địa bàn tỉnh và phát tán thông tin xấu độc, giảm thiểu các thiệt hại có thể xảy ra nhất là do lỗi của người sử dụng trong các dịp lễ, Tết trong năm 2022, Sở Giáo dục và Đào tạo (GDĐT) hướng dẫn các đơn vị thực hiện một số nội dung như sau:

1. Tăng cường các biện pháp bảo đảm an toàn thông tin đối với các hệ thống CNTT đang quản lý và sử dụng, quán triệt tới cán bộ, công chức, viên chức và người lao động thực hiện tốt theo hướng dẫn trong các tài liệu: Cẩm nang về an toàn thông tin, nhận thức về an toàn thông tin và 10 (mười) biện pháp cơ bản để bảo đảm an toàn thông tin *(các tài liệu được gửi kèm theo Công văn này)*.

2. Quán triệt cán bộ công chức, viên chức, giáo viên, học sinh, sinh viên, học viên sử dụng các trang mạng xã hội (Facebook, Youtube, Twitter, Zalo, Email...) đúng mục đích, tuyệt đối không đăng tải các video clip không lành mạnh, thông tin xấu, làm ảnh hưởng tới uy tín của Ngành, của cán bộ quản lý, giáo viên.

3. Phân công cán bộ phụ trách CNTT của đơn vị trực tiếp theo dõi, bảo đảm an toàn thông tin mạng của đơn vị.

4. Phòng GDĐT các huyện, thành phố hướng dẫn các cơ sở giáo dục thuộc thẩm quyền quản lý triển khai các biện pháp bảo đảm an toàn thông tin nêu trên.

5. Nếu phát hiện sự cố mất an toàn thông tin, các đơn vị kịp thời báo cáo về Sở GDĐT (qua Phòng Giáo dục Tiểu học) theo địa chỉ email: phonggdth@bacninh.edu.vn hoặc gặp ông Nguyễn Văn Đang, Phó Trưởng phòng Giáo dục Tiểu học, điện thoại: 0941006999.

Sở GDĐT yêu cầu các đơn vị thực hiện nghiêm túc nội dung công văn./.

Nơi nhận:
- Như trên;
- Sở TT&TT Bắc Ninh;
- Giám đốc và các Phó GĐ Sở;
- Chủ tịch CĐN;
- Lưu: VT, GDTH.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
TỈNH BẮC NINH

Nguyễn Hữu Bình

Phụ lục

MƯỜI BIỆN PHÁP CƠ BẢN BẢO ĐẢM AN TOÀN THÔNG TIN

(Kèm theo Công văn số 1970 */SGDĐT-GDTH ngày 30 /12/2021 của Sở GDĐT Bắc Ninh)*

I. "NĂM CÓ":

1. **Có** sử dụng mật khẩu mạnh với ít nhất 8 ký tự, có ký tự đặc biệt, có cả chữ thường, chữ HOA và số; định kỳ cần thay đổi mật khẩu; hạn chế việc sử dụng thông tin cá nhân để đặt mật khẩu. Một mật khẩu mạnh sẽ khó bị tấn công, bị dò quét hơn. Ví dụ về mật khẩu mạnh: *1G@3df8*aH*.

2. **Có** thực hiện gỡ bỏ các phần mềm không cần thiết, chỉ cài đặt trên máy tính các phần mềm thật cần thiết và cập nhật thường xuyên vì càng nhiều phần mềm được cài đặt thì càng dễ có nhiều lỗ hổng bảo mật.

3. **Có** sao lưu định kỳ đối với dữ liệu quan trọng, đề phòng trường hợp bị tấn công, xóa hết dữ liệu hoặc bị mã hóa dữ liệu.

4. **Có** cài đặt phần mềm diệt virus, cập nhật phần mềm và thường xuyên quét virus; quét virus đối với các tập tin nhận được từ thư điện tử, tải từ mạng internet, sao chép từ bên ngoài,…Kích hoạt và sử dụng chức năng tường lửa cá nhân để ngăn chặn các kết nối trái phép.

5. **Có** sử dụng chứng thư số khi trao đổi văn bản trên môi trường mạng để xác thực được sự tin cậy của văn bản. Lưu ý: Văn bản điện tử không được ký số theo quy định có thể đã bị thay đổi nội dung so với văn bản gốc.

II. "NĂM KHÔNG":

1. **Không** sử dụng các phiên bản Windows không còn được hỗ trợ, nâng cấp và cập nhật bản vá lỗi Windows và các phần mềm ứng dụng để giảm thiểu nguy cơ bị tấn công qua việc khai thác các lỗ hổng bảo mật.

2. **Không** nên truy cập các Website không tin cậy vì có thể bị cài đặt phần mềm độc hại một cách bí mật lên máy tính.

3. **Không** nên sử dụng phần mềm không bản quyền, không nên tải về, cài đặt phần mềm trên mạng không rõ nguồn gốc vì thường chứa mã độc.

4. **Không** mở thư có tiêu đề nhạy cảm, tập tin đính kèm, liên kết (link) gửi kèm thư điện tử; không cung cấp thông tin cá nhân nếu không rõ nguồn gốc thư điện tử. *Lưu ý: Tên người gửi hoặc địa chỉ thư điện tử của người gửi cũng có thể bị giả mạo.*

5. **Không** nên sử dụng mạng Internet công cộng để đăng nhập vào các hệ thống CNTT, các phần mềm dùng chung (thư điện tử, hệ thống Quản lý văn bản và Điều hành,…) để tránh bị đánh cắp mật khẩu, dữ liệu.