UỶ BAN NHÂN DÂN **PHƯỜNG VẠN PHÚC**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập- Tự do- Hạnh phúc**
Số: 15/UBND-VP V/v phòng ngừa thủ đoạn chiếm quyền truy cập vào hệ thống mạng	*Vạn Phúc, ngày 15 tháng 01 năm 2020*

Kính gửi: Các đơn vị, bộ phận chuyên môn phường.

UBND phường Vạn Phúc nhận được Công văn số 3439/STTTT-CNTT ngày 31/12/2019 của Sở thông tin & truyền thông Hà Nội; Công văn số 115/UBND-VP ngày 14/01/2020 của UBND quận Hà Đông về việc phòng ngừa thủ đoạn chiếm quyền truy cập vào hệ thống mạng các cơ quan, tổ chức; theo yêu cầu của thành phố Hà Nội, quận Hà Đông về việc thông tin một số nội dung cụ thể như sau:

1. Tình hình an toàn thông tin

Theo Công an thành phố Hà Nội, trong khoảng thời gian từ tháng 7/2019 đến tháng 9/2019, Công an thành phố Hà Nội phát hiện 02 vụ việc hacker dùng thủ đoạn lấy cắp thông tin tài khoản quản trị hệ thống mạng, truy cập trái phép vào hệ thống của doanh nghiệp, thực hiện chiếm đoạt tài sản.

Cách thức thực hiện: Qua các thủ đoạn tinh vi (Mua bán thông tin người dùng, trao đổi thông tin với các nhóm hacker...), đối tượng thu được thông tin liên quan đến tài khoản email của nhân viên quản trị mạng, quản trị hệ thống của doanh nghiệp... Từ việc tìm hiểu về hệ thống mạng doanh nghiệp đang sử dụng, đối tượng đã làm email giả mạo và đường dẫn trang web giả mạo (đường link) gửi đến email của nhân viên quản trị mạng, đồng thời yêu cầu người đó nhập tên tài khoản và mật khẩu theo đường dẫn đó để xác thực.

Sau khi chiếm được tài khoản email của quản trị mạng, hacker đã thu nhập được thông tin tài khoản đăng nhập hệ thống thông qua các trao đổi trên email, từ đó truy cập vào hệ thống mạng công ty thu thập thông tin, cài đặt các phần mềm độc hại, nguy hiểm và chiếm đoạt tài sản hoặc thực hiện các hành vi vi phạm pháp luật khác...

Quá trình xác minh, điều tra, Công an thành phố Hà Nội phát hiện trên các máy tính của quản trị mạng doanh nghiệp đều lưu trữ tài khoản/mật khẩu truy cập vào hệ thống, ngoài ra những thông tin này còn được quản trị mạng chia sẻ với nhau, các mật khẩu đều có dạng dễ suy đoán như: tên doanh nghiệp, ký tự, số... đồng thời các máy tính này bị cài đặt mã độc thu thập thông tin và truy cập từ xa.

Nhận thấy hành vi trên có phương thức, thủ đoạn phạm tội tuy không mới nhưng gây hậu quả nghiêm trọng, chúng thường nhằm vào các cơ quan, tổ chức,

doanh nghiệp có quy mô lớn, có tiềm lực kinh tế... Nếu thành công sẽ gây thiệt hại rất lớn cho những đơn vị này.

2. Các đơn vị, bộ phận chuyên môn lưu ý một số vấn đề sau:

- Không nhập tài khoản đăng nhập/mật khẩu vào các đường dẫn (đường link) được cung cấp qua email.

- Không trao đổi thông tin về tài khoản đang nhập/mật khẩu của hệ thống mạng/cơ sở dữ liệu qua email hoặc các phần mềm Chat.

- Tuyệt đối không lưu trữ thông tin về tài khoản đăng nhập/mật khẩu trên máy tính cá nhân hoặc máy được trang cấp.

- Tăng cường công tác giám sát đối với vào/ra hệ thống nhất là ngoài giờ hành chính.

- Đầu tư trang thiết bị an toàn thông tin theo quy định.

- Thường xuyên rà quét virus, mã độc, kiểm tra bất thường trên các máy tính có kết nối với hệ thống máy chủ.

UBND phường Vạn Phúc yêu cầu các đơn vị, cá nhân liên quan nghiêm túc triển khai thực hiện./.

Nơi nhận:
- Như trên;
- TT Đảng ủy, UBND phường
- Lưu: VT.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

U.B.N.D PHƯỜNG VẠN PHÚC Q.HÀ ĐÔNG T.P HÀ NỘI

Nguyễn Văn Dự