

**ỦY BAN NHÂN DÂN
QUẬN BA ĐÌNH**

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

Số: /UBND-VP

Ba Đình, ngày tháng 4 năm 2024

V/v cảnh báo nguy cơ tấn công mạng
gây mất an toàn, an ninh thông tin

Kính gửi:

- Trưởng các Ban Đảng quận ủy; Chánh Văn phòng Quận ủy;
Bí thư Đảng ủy khối doanh nghiệp, Phó Giám đốc TTCT quận;
- Thủ trưởng các phòng, ban chuyên môn thuộc quận;
- Chủ tịch Ủy ban MTTQ và Trưởng các đoàn thể, chính trị - xã hội:
Liên đoàn Lao động quận, Hội Liên hiệp phụ nữ, Hội Cựu chiến binh,
Đoàn TNCS Hồ Chí Minh;
- Thủ trưởng các đơn vị sự nghiệp, hiệp quán, phối quản thuộc quận;
- Bí thư Đảng ủy, Chủ tịch UBND 14 phường;
- Hiệu trưởng các trường Mầm non, Tiểu học, THCS thuộc quận.

Thực hiện Văn bản số 2666/CAHN-PA05 ngày 04/4/2024 của Công an thành phố Hà Nội về việc cảnh báo nguy cơ tấn công mạng gây mất an toàn, an ninh thông tin, để tăng cường đảm bảo an toàn thông tin, tránh lộ lọt mật khẩu đăng nhập các tài khoản của đơn vị và cá nhân trên các phần mềm đang thực hiện tại quận Ba Đình, UBND quận yêu cầu các đơn vị nghiêm túc thực hiện các nội dung sau:

1. Yêu cầu cán bộ, công chức, viên chức, người lao động của đơn vị chủ động, thường xuyên rà soát thay đổi mật khẩu các tài khoản sử dụng các phần mềm: Quản lý hồ sơ và đánh giá CBCCV, Sổ tay Đảng viên, QLVB, dịch vụ công, email công vụ và email cá nhân... Định kỳ thường xuyên 3 tháng thay đổi mật khẩu; không giao mật khẩu tài khoản cho người khác sử dụng; không sử dụng các mật khẩu mặc định đã được cấp, các mật khẩu đơn giản chỉ bao gồm các ký tự và số; Sử dụng mật khẩu đủ mạnh là mật khẩu tổ hợp bao gồm: chữ cái (chữ hoa và chữ thường), số và các ký tự đặc biệt như: @, #, \$, !, ... được mã hóa theo quy tắc của cá nhân người sử dụng.

2. Thường xuyên phổ biến quán triệt đến người sử dụng của đơn vị chấp hành nghiêm các quy định của pháp luật, hướng dẫn về bảo đảm an ninh mạng, bảo vệ bí mật nhà nước. Không truy cập các trang mạng không an toàn, không truy cập các đường dẫn lạ được gửi qua email, mạng xã hội.

3. Rà soát, đổi mật khẩu các tài khoản quản lý các thiết bị camera, không sử dụng mật khẩu mặc định của nhà sản xuất. Không tải và cài đặt trên thiết bị di động

các app không rõ nguồn gốc, không được xác thực trên cửa hàng ứng dụng CH Play, App Store.

4. Rà soát chính sách truy cập, truy cập từ xa máy tính, máy chủ, các hệ thống thông tin. Triển khai các phương án sao lưu dữ liệu được lưu trữ ra thiết bị tách biệt đảm bảo an toàn.

5. Thường xuyên cập nhật các bản vá lỗi, lỗ hổng bảo mật của hệ điều hành và các phần mềm ứng dụng, cài đặt các phần mềm phòng chống mã độc, khi phát hiện các dấu hiệu về tấn công mạng, mất an toàn thông tin lập tức ngắt kết nối mạng, tách máy tính, thiết bị khỏi hệ thống mạng; Thông báo và phối hợp với bộ phận đảm bảo an toàn thông tin của đơn vị để kịp thời khắc phục, giảm thiểu tối đa các nguy cơ mất an toàn, an ninh mạng có thể xảy ra.

UBND quận yêu cầu các đơn vị, UBND 14 phường nghiêm túc thực hiện./.

Nơi nhận:

- Như trên;
- TTQU; TT HĐND quận;
- Đ/c Chủ tịch UBND quận;
- Các Đ/c Phó Chủ tịch UBND quận;
- VPUB: CVP, PCVP, CV;
- Lưu: VT.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Phạm Thị Diễm