HƯỚNG DẪN NHẬN BIẾT EMAIL CÓ DẤU HIỆU BỊ TẤN CÔNG

Tài liệu hướng dẫn nhân viên nhận biết các dấu hiệu bất thường, nghi ngờ tài khoản Email bị tấn công, bị chiếm quyền sử dụng hoặc bị lợi dụng để phát tán mã độc, lừa đảo trong hệ thống doanh nghiệp.

A. Các dấu hiệu nhận biết nghi ngờ bị tấn công Email

1. Tự động gửi Email mà người dùng không thực hiện

- Trong Sent Items xuất hiện email không phải do mình gửi.
- Đồng nghiệp phản ánh nhận được email lạ từ tài khoản của mình.
- Email được gửi hàng loạt đến nhiều địa chỉ không rõ nguồn gốc.

2. Có hoạt động đăng nhập bất thường

- Nhận thông báo đăng nhập từ thiết bị hoặc vị trí lạ.
- Đăng nhập vào thời điểm người dùng không sử dụng.
- Có nhiều lần đăng nhập thất bại liên tiếp.
- Xuất hiện phiên đăng nhập không nhận diện được.

3. Nhận được Email lừa đảo (Phishing)

- Email giả mạo Ban lãnh đạo, ngân hàng, đối tác hoặc bộ phận IT.
- Yêu cầu cung cấp mật khẩu, mã OTP.
- Yêu cầu nhấp vào đường dẫn để xác minh tài khoản.
- Nội dung thúc giục chuyển tiền hoặc cung cấp thông tin nội bộ.

4. Xuất hiện thay đổi cài đặt Email bất thường

- Có quy tắc tự động chuyển tiếp email đến địa chỉ lạ.
- Email bị tự động xóa hoặc di chuyển sang thư mục khác.
- Thay đổi thông tin khôi phục hoặc phương thức xác thực.
- Xuất hiện quyền truy cập hoặc ứng dụng lạ được cấp phép.

5. Email có dấu hiệu bị can thiệp

- Email trong Inbox tự nhiên biến mất.

- Thư đã đọc dù người dùng chưa mở.

- Email gửi đi bị xóa hoặc thay đổi.

- Thư trả lời có nội dung không đúng với nội dung ban đầu.

6. Xuất hiện Email chứa mã độc

- Email đính kèm file lạ như EXE, ZIP, RAR, HTML.

- Có đường dẫn yêu cầu tải phần mềm hoặc tài liệu không rõ nguồn gốc.

- Hệ thống cảnh báo virus, malware hoặc tệp đính kèm nguy hiểm.

B. Các hình thức tấn công Email thường gặp

Hình thức	Mô tả
Phishing	Giả mạo Email để đánh cắp tài khoản, mật khẩu
Spear Phishing	Tấn công có chủ đích vào cá nhân hoặc lãnh đạo
Business Email Compromise (BEC) để lừa chuyển tiền	Giả mạo hoặc chiếm quyền email doanh nghiệp
Brute Force	Thử nhiều mật khẩu để chiếm quyền đăng nhập
Password Spraying	Thử một số mật khẩu phổ biến trên nhiều tài khoản
Malware dẫn	Phát tán mã độc qua file đính kèm hoặc đường
Email Spoofing	Giả mạo địa chỉ người gửi
Account Takeover	Chiếm quyền kiểm soát tài khoản Email

C. Hướng dẫn nhân viên xử lý khi nghi ngờ bị tấn công

Quy trình xử lý ban đầu

1. Không tiếp tục tương tác với Email đáng ngờ

Không nhấp vào liên kết, không mở tệp đính kèm, không trả lời email và không cung cấp mật khẩu, OTP.

2. Thông báo ngay cho bộ phận IT

Cung cấp địa chỉ người gửi, tiêu đề email, thời gian nhận và ảnh chụp màn hình.

3. Nếu đã nhấp link hoặc cung cấp thông tin

Báo IT ngay lập tức. Không tự ý xóa email hoặc xóa dấu vết. Nếu nghi ngờ thiết bị nhiễm mã độc, ngắt kết nối mạng theo hướng dẫn của IT.

4. Nếu nghi ngờ tài khoản bị chiếm quyền

Yêu cầu IT hỗ trợ khóa hoặc thu hồi phiên đăng nhập, đổi mật khẩu an toàn, kiểm tra MFA và rà soát các quy tắc chuyển tiếp email.

5. Phối hợp xử lý và xác minh

Không tự ý khôi phục hoặc tiếp tục sử dụng tài khoản cho đến khi IT xác nhận an toàn.