HƯỚNG DẪN NHẬN BIẾT EMAIL GIẢ MẠO
VÀ EMAIL CHỨA MÃ ĐỘC

Tài liệu hướng dẫn CBNV nhận biết email giả mạo (Phishing Email), email có chứa mã độc (Malware) và các hình thức lừa đảo qua thư điện tử nhằm bảo vệ tài khoản, dữ liệu và hệ thống công nghệ thông tin của doanh nghiệp.

1. Hướng dẫn nhận biết Email giả mạo (Phishing Email)

1. Địa chỉ người gửi bất thường

- Tên hiển thị giống Ban lãnh đạo, đối tác hoặc bộ phận IT nhưng địa chỉ email thực tế khác lạ.
- Tên miền gần giống tên miền chính thức nhưng có thêm ký tự hoặc sai chính tả.
- Email được gửi từ địa chỉ cá nhân không đúng với tổ chức.

2. Nội dung email mang tính thúc giục, đe dọa

- Yêu cầu đổi mật khẩu ngay lập tức.
- Thông báo tài khoản sắp bị khóa.
- Yêu cầu xác minh tài khoản trong thời gian ngắn.
- Yêu cầu chuyển tiền hoặc cung cấp thông tin khẩn cấp.

3. Đường link đăng nhập giả mạo

- Đường link dẫn đến website không chính thức.
- Trang đăng nhập có giao diện giống Microsoft 365 hoặc hệ thống Email của doanh nghiệp.
- Yêu cầu nhập tên đăng nhập, mật khẩu hoặc mã OTP.

4. Nội dung yêu cầu giao dịch bất thường

- Thay đổi số tài khoản ngân hàng của đối tác.
- Yêu cầu thanh toán hóa đơn bất thường.
- Gửi thông tin hợp đồng, báo giá hoặc dữ liệu nội bộ.
- Yêu cầu giữ bí mật và không xác minh qua kênh khác.

2. Hướng dẫn nhận biết Email chứa mã độc (Malware)

1. Tệp đính kèm đáng ngờ

Cảnh giác với các tệp như:

- .exe, .scr, .bat, .cmd
- .js, .vbs, .ps1
- .iso, .img
- .zip, .rar chứa tệp không rõ nguồn gốc.

Đặc biệt cảnh giác với tệp Office yêu cầu bật Macro.

2. Tệp tài liệu có dấu hiệu bất thường

- File hóa đơn, báo giá, hợp đồng không được yêu cầu.
- File PDF yêu cầu tải thêm phần mềm hoặc đăng nhập qua đường link lạ.
- File Word, Excel yêu cầu bật Macro hoặc Enable Content.

3. Đường link tải tệp không rõ nguồn gốc

- Yêu cầu tải phần mềm, bản cập nhật hoặc tài liệu.
- Chuyển hướng qua nhiều website.
- Đường link rút gọn hoặc tên miền lạ.
- Yêu cầu cài đặt ứng dụng để xem tài liệu.

Lưu ý: Không phải tất cả tệp ZIP, PDF, Word hay Excel đều có mã độc. Tuy nhiên, định dạng tệp không đảm bảo an toàn. Không mở tệp nếu không xác minh được nguồn gửi và mục đích gửi.

3. Bảng so sánh Email bình thường và Email giả mạo/mã độc

Tiêu chí	**Email bình thường**	**Email đáng ngờ**
Người gửi	Địa chỉ xác thực	Địa chỉ giả mạo, tên miền lạ
Nội dung	Phù hợp công việc	Thúc giục, đe dọa, bất thường
Đường link	Website chính thức	Website lạ, giả mạo

Tệp đính kèm	Đúng nội dung trao đổi	File lạ, không được yêu cầu
Yêu cầu	Theo quy trình	Yêu cầu mật khẩu, OTP, chuyển tiền
Thời gian	Phù hợp giao dịch	Yêu cầu xử lý bất thường, gấp

4. Hướng dẫn xử lý khi nhận được Email giả mạo hoặc chứa mã độc

Quy trình xử lý dành cho nhân viên

1. Không mở email hoặc tương tác với nội dung đáng ngờ

Không nhấp đường link, không tải tệp đính kèm, không trả lời email.

2. Không cung cấp thông tin tài khoản

Tuyệt đối không cung cấp mật khẩu, mã OTP hoặc thông tin xác thực.

3. Báo cáo ngay cho bộ phận IT

Gửi email nghi ngờ dưới dạng tệp đính kèm nguyên bản (nếu có thể thực hiện an toàn), hoặc báo cáo qua kênh hỗ trợ nội bộ.

4. Nếu đã mở tệp hoặc nhấp đường link

Thông báo ngay cho IT. Nếu đã tải hoặc chạy tệp đáng ngờ, ngắt kết nối mạng của thiết bị theo hướng dẫn IT, không tự ý xóa tệp hoặc cài lại máy.

5. Chờ IT kiểm tra và xác nhận

Chỉ tiếp tục sử dụng tài khoản, thiết bị sau khi bộ phận IT xác nhận an toàn.