INFOGRAPHIC

TRÁNH BỊ LỪA ĐẢO TRỰC TUYẾN

5 bước tự vệ đơn giản cho sinh viên khi dùng tài khoản số

Thông điệp chính: Dừng 10 giây - Kiểm tra nguồn - Không chia sẻ OTP - Bật MFA - Báo cáo khi nghi ngờ

Vì sao cần cảnh giác?

Lừa đảo trực tuyến không chỉ là chuyện "người khác bị"; chỉ cần một đường link giả, tài khoản và tiền có thể mất rất nhanh.

>10.000

tên miền độc hại đã bị hệ thống của Cục ATTT/Bộ TT&TT chặn tính đến 3/2024

>2.700

tên miền lừa đảo trực tuyến nằm trong số tên miền độc hại bị chặn

10,1 triệu

người dùng Việt Nam được bảo vệ trước tấn công lừa đảo, vi phạm trên mạng

12,5 tỷ USD

thiệt hại do người tiêu dùng Mỹ báo cáo vì gian lận trong năm 2024

5 bước tự vệ trước khi bấm, đăng nhập hoặc chuyển tiền

1 **Dừng 10 giây**

Cảnh giác với tin nhắn "khẩn cấp", "trúng thưởng", "xác minh ngay", "chuyển tiền gấp".

2 **Kiểm tra URL & người gửi**

So sánh tên miền, lỗi chính tả, đuôi website; tự vào ứng dụng/trang chính thức thay vì bấm link lạ.

3 **Không đưa OTP/mật khẩu**

Không cung cấp OTP, mật khẩu ngân hàng, mã khôi phục hay ảnh CCCD cho người lạ/kênh không xác thực.

4 **Bật xác thực đa yếu tố (MFA)**

Dùng MFA, mật khẩu mạnh và riêng cho từng tài khoản; ưu tiên trình quản lý mật khẩu.

5 **Báo cáo & khóa ngay**

Khi nghi ngờ: đổi mật khẩu, khóa thẻ/tài khoản, báo ngân hàng/công an và gửi phản ánh website lừa đảo.

Nhớ nhanh: Không vội - Không đưa mã - Không cài app lạ - Luôn kiểm tra nguồn chính thức

Nguồn: Cục ATTT/Bộ TT&TT qua Vietnamnet; FTC; CISA; NIST. Thiết kế: Văn Phúc Đỗ.