Phòng tránh **LỪA ĐẢO** TRỰC TUYẾN

Song hành với sự phát triển của Internet, các mạng xã hội...thì các hình thức lừa đảo trực tuyến đang bùng nổ, trở nên tinh vi, nguy hiểm và có tổ chức hơn. Thiệt hại do các hành động lừa đảo trực tuyến gây ra cho người dùng và xã hội là rất lớn.

04 | Một số hình thức lừa đảo trực tuyến thường được các tội phạm mạng sử dụng phổ biến tại Việt Nam.

- *Tạo các trang web giả mạo giống các website nổi tiếng.*
- *Lừa đảo "trúng thưởng" thông qua các thông báo, quảng cáo, tin nhắn facebook, mail, zalo, sms....*
- *Lừa đảo bán hàng qua mạng, chiếm đoạt tiền.*
- *Hình thức bán hàng đa cấp biến tướng trên Internet: Lừa đảo nạp thẻ trên facebook, diễn đàn mạng...*
- *Lừa đảo đánh cắp thông tin cá nhân.*
- *Lừa đảo đe dọa như: "Bị nhiễm virus", "Cung cấp thông tin phục vụ điều tra"; ...*

Cảnh giác và cẩn thận với những thứ đến quá dễ dàng, hấp dẫn... và may mắn từ Internet.

Với những yêu cầu liên quan tới việc cung cấp thông tin, tài chính thậm chí từ người quen trên Internet thì cần kiểm tra, xác thực lại.

Hãy thực sự tỉnh táo khi bấm vào bất kỳ một liên kết được gửi đến hoặc truy cập vào một website. Kiểm tra kỹ chúng trước khi làm việc gì đó như: Đăng nhập, chuyển tiền,...

BẢO VỆ
THÔNG TIN CÁ NHÂN

Sự phát triển của internet đã kéo theo nhiều hệ quả tất yếu, con người cũng ngày càng lệ thuộc hơn vào công nghệ trong đời sống hằng ngày như phải sở hữu smartphone, máy tính, dùng phương thức thanh toán trực tuyến, chuyển khoản ngân hàng qua mạng...vv... Làm thế nào để có thể luôn an toàn trong thế giới số?

05 | Máy tính cá nhân là nơi tiềm ẩn nhiều các nguy cơ và rủi ro về an toàn thông tin.

Những việc cần làm để bảo mật thông tin cá nhân trên mạng internet

- *Hợp tác với những công ty/trang web đáng tin cậy*
- *Luôn đặt ra những câu hỏi nghi vấn khi tham gia các mạng xã hội*
- *Tránh cung cấp thông tin thẻ tín dụng. Tránh sử dụng thẻ ghi nợ khi mua hàng online.*
- *Bảo vệ mật khẩu nhiều lớp. Luôn sử dụng các mật khẩu khác nhau với các trang mạng xã hội, dịch vụ trực tuyến khác nhau.*
- *Hạn chế chia sẻ thông tin cá nhân trên mạng xã hội*

CỤC AN TOÀN THÔNG TIN
AUTHORITY OF INFORMATION SECURITY

Địa chỉ: Tầng 8 Tòa nhà Cục Tần số vô tuyến điện,
115 Trần Duy Hưng, Cầu giấy, Hà Nội.
Điện thoại: +84 24 3209 6789 * Fax: +84 24 3943 6684
Email: cucattt@mic.gov.vn
Website: https://ais.gov.vn

BỘ THÔNG TIN & TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

NHẬN THỨC
AN TOÀN THÔNG TIN

KỸ NĂNG TỰ ĐẢM BẢO AN TOÀN THÔNG TIN

AIS.GOV.VN

SỬ DỤNG **MẬT KHẨU** ĐÚNG CÁCH?

Để bảo đảm an toàn cho máy tính, thiết bị di động, các hoạt động trên internet...chúng ta cần sử dụng mật khẩu đúng cách. Mật khẩu chính là hàng phòng thủ đầu tiên và quan trọng để chống lại các tội phạm mạng:

- *Sử dụng mật khẩu mạnh.*
- *Sử dụng một mật khẩu duy nhất cho từng tài khoản quan trọng như email, tài khoản ngân hàng...*
- *Giữ bí mật mật khẩu bằng cách nhớ hoặc để ở nơi chỉ mình bạn có thể biết và đọc nó.*
- *Thiết lập các tùy chọn khôi phục mật khẩu và hãy cập nhật chúng một cách thường xuyên.*

01 | Tấn công mật khẩu là một phương pháp tấn công truyền thống và nguy hiểm nhắm vào người dùng.

GỢI Ý CÁCH ĐẶT MẬT KHẨU MẠNH

- *Mật khẩu ít nhất phải có 7 ký tự.*
- *Sử dụng 4 loại ký tự bao gồm: chữ hoa, chữ thường, chữ số và ký tự đặc biệt (@,$,#,%...).*
- *Không dùng các mật khẩu dễ đoán, biết như: họ tên, ngày sinh, ngày đặc biệt.*
- *Sử dụng ít nhất bốn ký tự khác nhau và ngẫu nhiên.*

AN TOÀN CHO **THIẾT BỊ DI ĐỘNG!**

Các thiết bị di động như điện thoại thông minh, máy tính bảng đã vô cùng thông dụng và có hàng triệu ứng dụng trên Internet, không ai có thể đảm bảo chúng hoàn toàn vô hại. Vì vậy chúng ta phải biết cách tự bảo đảm an toàn khi sử dụng thiết bị di động:

- *Luôn luôn thận trọng khi mở các kết nối mạng hay blue- tooth ở những nơi công cộng.*
- *Thường xuyên sử dụng các phần mềm diệt virus để quét, phát hiện mã độc trên hệ thống, các kết nối kém an toàn...*
- *Hạn chế việc bẻ khóa, cài các ứng dụng bên thứ 3, kiểm tra quyền cấp phát khi cài đặt.*
- *Luôn nhớ cập nhật các bản cập nhật của hệ điều hành, các ứng dụng và mật khẩu.*

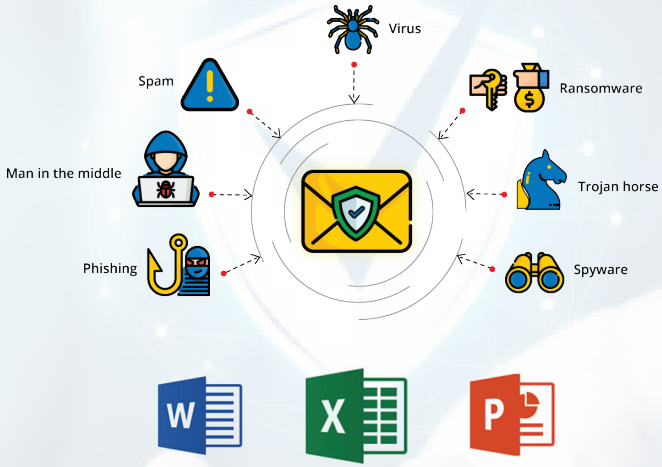
02 | Nguy cơ tiềm ẩn mất An toàn thông tin từ các thiết bị di động là rất lớn.

TẤN CÔNG EMAIL CÓ CHỦ ĐÍCH...

Gần đây, cách thức tấn công có chủ đích thường được thực hiện qua việc gửi các email giả mạo, các email có file đính kèm là mã độc tới người dùng. Khi người dùng tải và mở file đính kèm mã độc sẽ lây nhiễm vào hệ thống. Một số lưu ý khi sử dụng email như:

- *Không nên tin tưởng tên hiển thị trong email.*
- *Bỏ qua các email yêu cầu cung cấp thông tin cá nhân, chuyển tiền, đổi mật khẩu ...*
- *Cẩn trọng với các email có tiêu đề Hấp dẫn - Nhạy cảm- Khẩn cấp.*
- *Cẩn thận, cân nhắc khi tải về các file đính kèm trong email. Tạo thói quen quét virus.*
- *Cân nhắc kỹ lưỡng khi bấm vào liên kết (link) trong email.*

03 | Tấn công Email có chủ đích vào người dùng qua file đính kèm Microsoft Excel



Nếu đã mở một file hay liên kết nghi ngờ là mã độc, hãy ngắt kết nối mạng và liên hệ quản trị mạng của tổ chức hoặc các đơn vị chức năng để được hỗ trợ.