

# Chương II

1

## CÁC MỐI ĐE DỌA ĐẾN AN TOÀN THÔNG TIN (THREATS TO INFORMATION SECURITY)

---

GV: Trần Thị Kim Chi

# NỘI DUNG

---

1. Các khái niệm cơ bản
2. Các mối đe dọa
3. Tấn công và các loại tấn công
4. Mã độc và các phòng chống mã độc
5. CÂU HỎI VÀ BÀI TẬP

Cách phát hiện mã độc #Malware #Virus đào #Bitcoin và hướng khắc phục. - Bing video

Các hình thức tấn công mạng phổ biến hiện nay và cách phòng tránh - ODS

# CÁC KHÁI NIỆM CƠ BẢN

## Lỗ hổng – Mối đe dọa – Rủi ro



# CÁC KHÁI NIỆM CƠ BẢN

## THREAT – MỐI ĐE DỌA



- Mối đe dọa đề cập đến một sự cố mới được phát hiện có khả năng gây hại cho một hệ thống hoặc tổ chức nào đó.
- Là một thuật ngữ, mô tả nơi mà mối đe dọa bắt nguồn và con đường cần để đạt được mục tiêu
- Ví dụ một e-mail lạ có tiêu đề hấp dẫn và có chứa mã độc trong tập tin đính kèm
- **Có ba loại mối đe dọa chính:**
  - Các mối đe dọa tự nhiên (ví dụ: lũ lụt hoặc lốc xoáy),
  - Các mối đe dọa không chủ ý (chẳng hạn như một nhân viên truy cập sai thông tin sai)
  - Các mối đe dọa có chủ ý. (Ví dụ: phần mềm gián điệp, phần mềm độc hại, công ty phần mềm quảng cáo hoặc hành động phá hoại của con người, virus...)

# CÁC KHÁI NIỆM CƠ BẢN

## THREAT – MỐI ĐE DỌA

---

### **Biện pháp phòng tránh**

- Thông báo về các xu hướng hiện tại trong an ninh mạng để họ có thể nhanh chóng xác định các mối đe dọa mới.
- Thực hiện đánh giá mối đe dọa thường xuyên để xác định các phương pháp tốt nhất để bảo vệ hệ thống chống lại một mối đe dọa cụ thể, cùng với việc đánh giá các loại mối đe dọa khác nhau.
- Ngoài ra, kiểm tra các mối đe dọa trong thế giới thực để khám phá các lỗ hổng bảo mật.

# CÁC KHÁI NIỆM CƠ BẢN

## Vulnerability – LỖ HỔNG

- Là một số lỗ hổng hoặc điểm yếu trong phần cứng, phần mềm, con người, các quy trình, thiết kế, cấu hình...tất cả mọi thứ liên quan đến hệ thống thông tin – HTTT) mà kẻ tấn công có thể sử dụng nó để gây thiệt hại cho tổ chức.
- **Ví dụ**, khi một thành viên trong công ty từ chức và bạn quên vô hiệu hóa quyền truy cập của họ, điều này khiến doanh nghiệp của bạn bị cả hai mối đe dọa cố ý và không chủ ý.

# Vulnerability – LỖ HỔNG

---

## **Một số câu hỏi để xác định các lỗ hổng bảo mật của bạn:**

- Dữ liệu của bạn có được sao lưu và lưu trữ ở một địa điểm an toàn bên ngoài trang web không?
- Dữ liệu của bạn có được lưu trữ trên đám mây không? Nếu có, làm thế nào chính xác là nó được bảo vệ khỏi các lỗ hổng trên đám mây?
- Bạn có loại bảo mật mạng nào để xác định ai có thể truy cập, sửa đổi hoặc xóa thông tin từ bên trong tổ chức của bạn?
- Loại bảo vệ chống virus nào đang được sử dụng? Giấy phép có hiện hành không? Nó có chạy thường xuyên khi cần thiết không?
- Bạn có kế hoạch khôi phục dữ liệu trong trường hợp lỗ hổng bị khai thác không?

# CÁC KHÁI NIỆM CƠ BẢN

## RISK – RỦI RO

---

- Rủi ro đề cập đến khả năng mất mát hoặc thiệt hại khi một mối đe dọa khai thác lỗ hổng bảo mật.
- **Ví dụ** về rủi ro bao gồm tổn thất về tài chính do gián đoạn kinh doanh, mất quyền riêng tư, thiệt hại có uy tín, các tác động pháp lý và thậm chí có thể bao gồm mất mạng.

$$\text{RISK} = \text{Threat} + \text{Vulnerability}$$

# CÁC KHÁI NIỆM CƠ BẢN

## RISK – RỦI RO

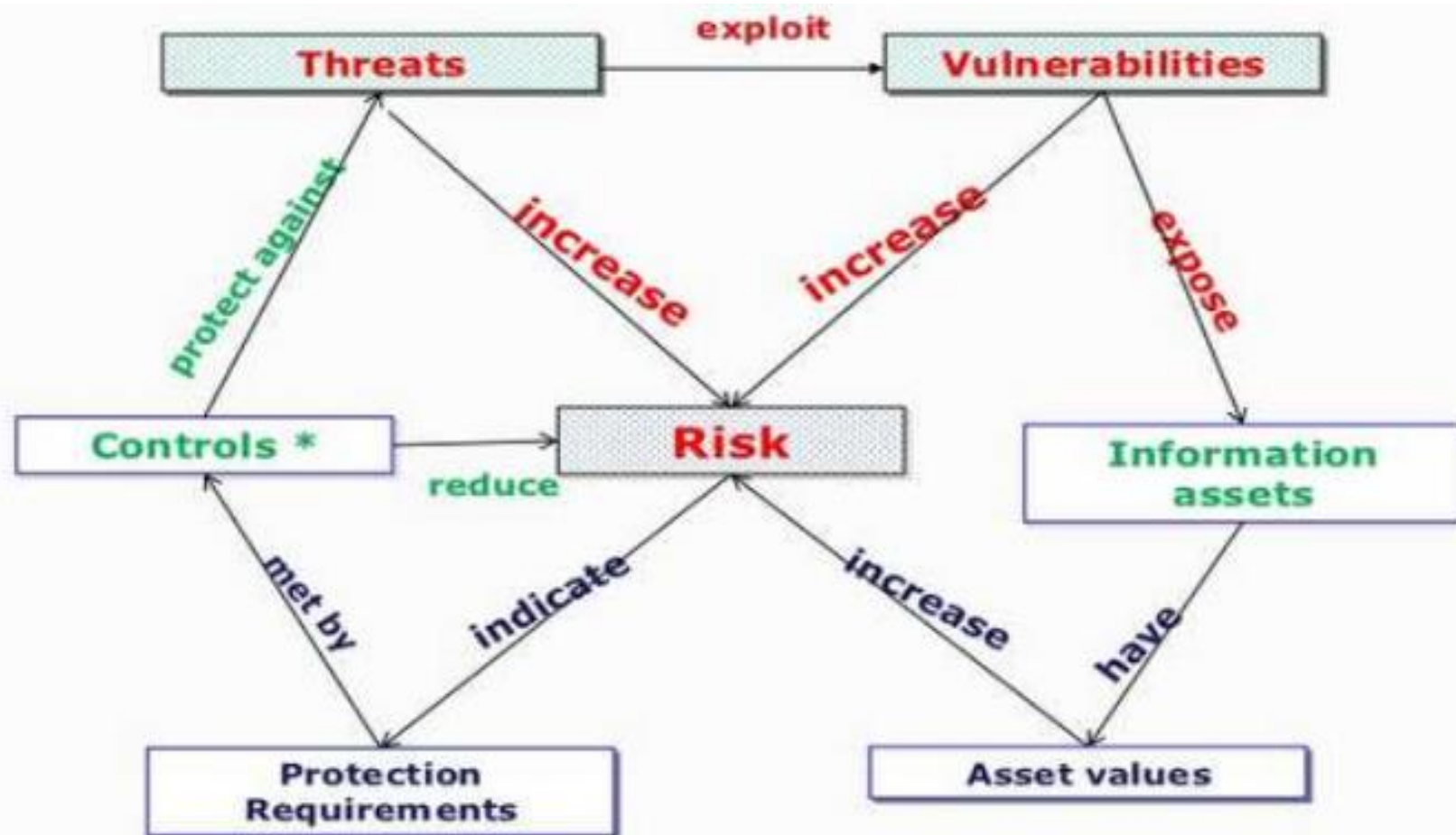
---

**Biện pháp giảm rủi ro: tạo và triển khai một kế hoạch quản lý rủi ro.**

- Đánh giá rủi ro và xác định nhu cầu → phải được thực hiện thường xuyên, định kỳ.
- Bao gồm quan điểm của các bên liên quan (doanh nghiệp, nhân viên, khách hàng, các nhà cung cấp).
- Chỉ định một nhóm nhân viên trung tâm chịu trách nhiệm quản lý rủi ro và xác định mức tài trợ thích hợp cho hoạt động này.
- Thực hiện các chính sách thích hợp và kiểm soát các bên liên quan → đảm bảo người dùng được thông báo về tất cả các thay đổi.
- Giám sát và đánh giá hiệu quả chính sách và kiểm soát.

# CÁC KHÁI NIỆM CƠ BẢN

MỐI TƯƠNG QUAN GIỮA MỐI ĐE DỌA- LỖ HỔNG – RỦI RO



\* Controls: A practice, procedure or mechanism that reduces risk

# Các mối đe dọa đối với một hệ thống và các biện pháp ngăn chặn

---

- **Có 3 hình thức chủ yếu đe dọa đối với hệ thống:**

- ✓ **Phá hoại:** kẻ thù phá hỏng thiết bị phần cứng hoặc phần mềm hoạt động trên hệ thống.
- ✓ **Sửa đổi:** Tài sản của hệ thống bị sửa đổi trái phép. Điều này thường làm cho hệ thống không làm đúng chức năng của nó. Chẳng hạn như thay đổi mật khẩu, quyền người dùng trong hệ thống làm họ không thể truy cập vào hệ thống để làm việc.
- ✓ **Can thiệp:** Tài sản bị truy cập bởi những người không có thẩm quyền. Các truyền thông thực hiện trên hệ thống bị ngăn chặn, sửa đổi.

# Các mối đe dọa đối với một hệ thống và các biện pháp ngăn chặn

---

- **Các đe dọa đối với một hệ thống thông tin có thể đến từ ba loại đối tượng như sau:**
  - ✓ **Các đối tượng từ ngay bên trong hệ thống (insider):** đây là những người có quyền truy cập hợp pháp đối với hệ thống.
  - ✓ **Những đối tượng bên ngoài hệ thống (hacker, cracker):** thường các đối tượng này tấn công qua những đường kết nối với hệ thống như Internet chẳng hạn.
  - ✓ **Các phần mềm** (chẳng hạn như spyware, adware ...) chạy trên hệ thống.

# Các mối đe dọa thường gặp

---

- 1) Lỗi và thiếu sót của người dùng (Errors and Omissions)
- 2) Gian lận và đánh cắp thông tin (Fraud and Theft)
- 3) Kẻ tấn công nguy hiểm (Malicious Hackers)
- 4) Mã độc (Malicious Code)
- 5) Tấn công từ chối dịch vụ (Denial-of-Service Attacks)
- 6) Social Engineering

# Các mối đe dọa thường gặp

---

## 1. Lỗi thiếu sót do người dùng

- Mối đe dọa của hệ thống thông tin xuất phát từ những lỗi bảo mật, lỗi thao tác của những người dùng trong hệ thống.
- Là mối đe dọa hàng đầu đối với một hệ thống thông tin
- Giải pháp:
  - Huấn luyện người dùng thực hiện đúng các thao tác, hạn chế sai sót
  - Nguyên tắc: quyền tối thiểu (least privilege)
  - Thường xuyên back-up hệ thống

# Các mối đe dọa thường gặp

---

## 2. Gian lận và đánh cắp thông tin

- Mối đe dọa này do những kẻ tấn công từ bên trong hệ thống (inner attackers), gồm những người dùng giả mạo hoặc những người dùng có ý đồ xấu.
- Những người tấn công từ bên trong luôn rất nguy hiểm.
- **Giải pháp:**
  - Định ra những chính sách bảo mật tốt: có chứng cứ xác định được kẻ tấn công từ bên trong

# Các mối đe dọa thường gặp

---

## 3. Kẻ tấn công nguy hiểm

- Kẻ tấn công nguy hiểm xâm nhập vào hệ thống để tìm kiếm thông tin, phá hủy dữ liệu, phá hủy hệ thống.
- 5 bước để tấn công vào một hệ thống:
  - Thăm dò (Reconnaissance)
  - Quét lỗ hổng để tấn công (Scanning)
  - Cố gắng lấy quyền truy cập (Gaining access)
  - Duy trì kết nối (Maintaining access)
  - Xóa dấu vết (Cover his track)

# Các mối đe dọa thường gặp

---

## 4. Mã ĐỘC

- Mã độc là một đoạn mã không mong muốn được nhúng trong một chương trình nhằm thực hiện các truy cập trái phép vào hệ thống máy tính để thu thập các thông tin nhạy cảm, làm gián đoạn hoạt động hoặc gây hại cho hệ thống máy tính.
- **Bao gồm:** virus, worm, trojan horses, spyware, adware, backdoor, ...

# Các mối đe dọa thường gặp

---

## 5. Tấn công từ chối dịch vụ

- Là kiểu tấn công ngăn không cho những người dùng khác truy cập vào hệ thống
- Làm cho hệ thống bị quá tải và không thể hoạt động
- DoS: tấn công “one-to-one”
- DDoS(distributed denial of service)
- Sử dụng các Zombie host
- Tấn công “many-to-one”

# Các mối đe dọa thường gặp

---

## 6. Social Engineering

- Social engineering sử dụng sự ảnh hưởng và sự thuyết phục để đánh lừa người dùng nhằm khai thác các thông tin có lợi cho cuộc tấn công hoặc thuyết phục nạn nhân thực hiện một hành động nào đó.

# Các mối đe dọa thường gặp

---

## Có hai loại Social Engineering

- **Social engineering dựa trên con người** liên quan đến sự tương tác giữa con người với con người để thu được thông tin mong muốn
  - Nhân viên gián điệp/giả mạo
  - Giả làm người cần được giúp đỡ
  - Giả làm người quan trọng
  - Giả làm người được ủy quyền
  - Giả làm nhân viên hỗ trợ kỹ thuật

# Các mối đe dọa thường gặp

---

## Có hai loại Social Engineering

- **Social engineering dựa trên máy tính:** liên quan đến việc sử dụng các phần mềm để cố gắng thu thập thông tin cần thiết
  - Phishing: lừa đảo qua thư điện tử
  - Vishing: lừa đảo qua điện thoại
  - Pop-up Windows
  - File đính kèm trong email
  - Các website giả mạo
  - Các phần mềm giả mạo

# Tấn công là gì?

---

- **Định nghĩa chung:** Tấn công (attack) là hoạt động có chủ ý của kẻ phạm tội lợi dụng các thương tổn của hệ thống thông tin và tiến hành phá vỡ tính sẵn sàng, tính toàn vẹn và tính bí mật của hệ thống thông tin.
- Tấn công HTTT là các tác động hoặc là trình tự liên kết giữa các tác động với nhau để phá huỷ, dẫn đến việc hiện thực hoá các nguy cơ bằng cách lợi dụng đặc tính dễ bị tổn thương của các hệ thống thông tin này.

# Tin tặc (Hacker) là gì?

---

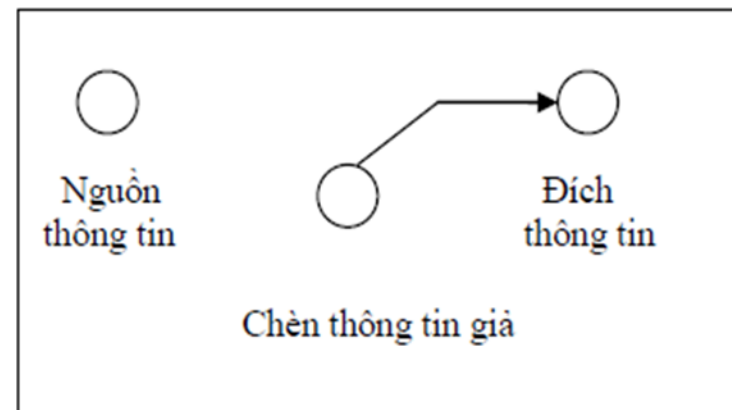
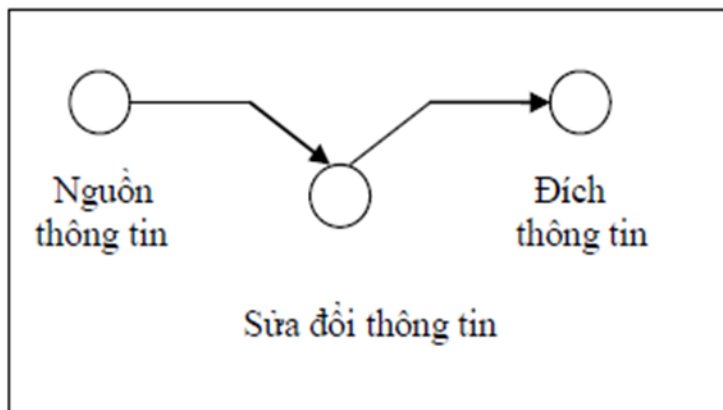
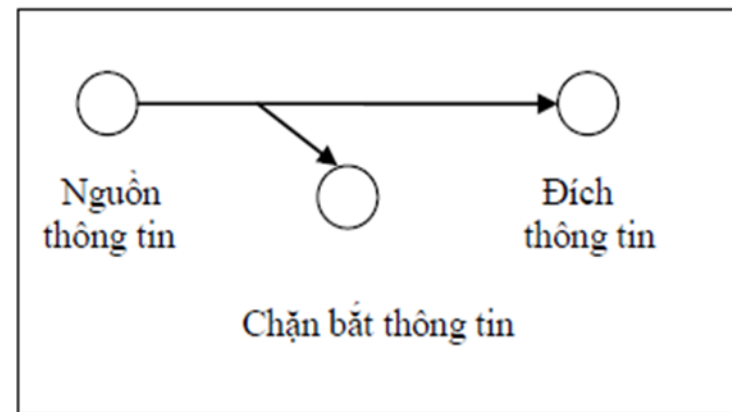
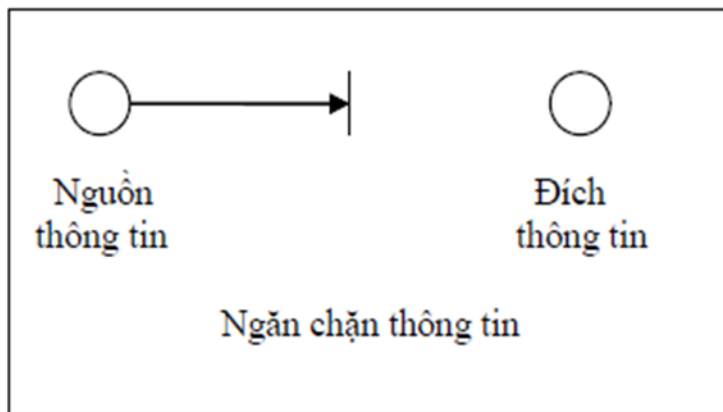
- **Tin tặc (Hacker):** Là một người hay nhóm người sử dụng sự hiểu biết của mình về cấu trúc máy tính, hệ điều hành, mạng, các ứng dụng trong hệ thống... để tìm lỗi, lỗ hổng, điểm yếu và tìm cách xâm nhập, thay đổi hay chỉnh sửa với các mục đích khác nhau (tốt hoặc xấu)

# Các loại Tin tặc (Hacker) phổ biến

---

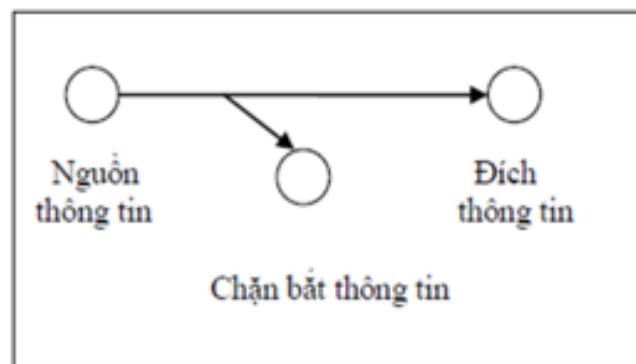
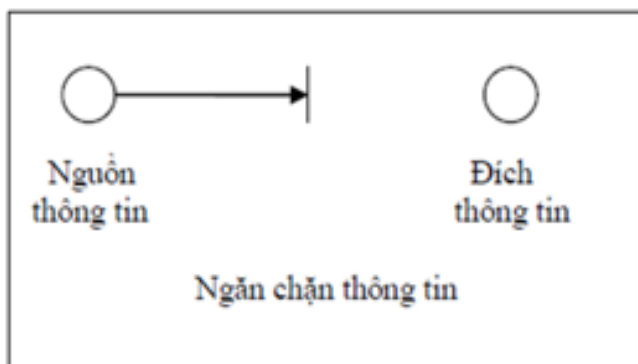
- **Hacker mũ trắng** là những người mà hành động tấn công, xâm nhập và thay đổi, chỉnh sửa hệ thống phần cứng, phần mềm với mục đích tìm ra các lỗi, lỗ hổng, điểm yếu bảo mật và đưa ra giải pháp ngăn chặn và bảo vệ hệ thống chẳng hạn như những nhà phân tích An ninh mạng.
- **Hacker mũ đen** là những người mà hành động tấn công, xâm nhập, thay đổi, chỉnh sửa hệ thống phần cứng, phần mềm với mục đích phá hoại, hoặc vi phạm pháp luật

# Các loại hình tấn công (tiếp)



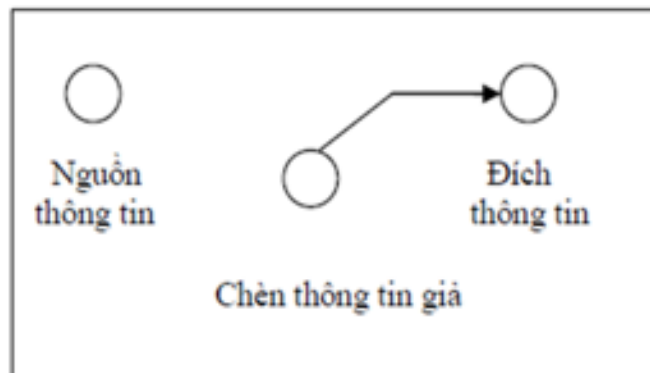
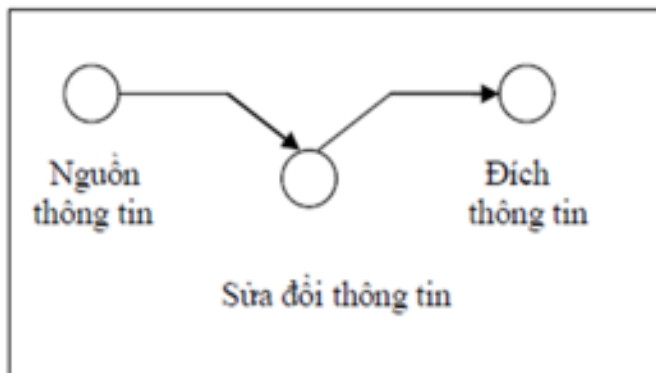
# Các loại hình tấn công (tiếp)

- **Tấn công ngăn chặn thông tin (interruption)**
  - Tài nguyên thông tin bị phá hủy, không sẵn sàng phục vụ hoặc không sử dụng được. Đây là hình thức tấn công làm mất khả năng sẵn sàng phục vụ của thông tin.
- **Tấn công chặn bắt thông tin (interception)**
  - Kẻ tấn công có thể truy nhập tới tài nguyên thông tin. Đây là hình thức tấn công vào tính bí mật của thông tin.

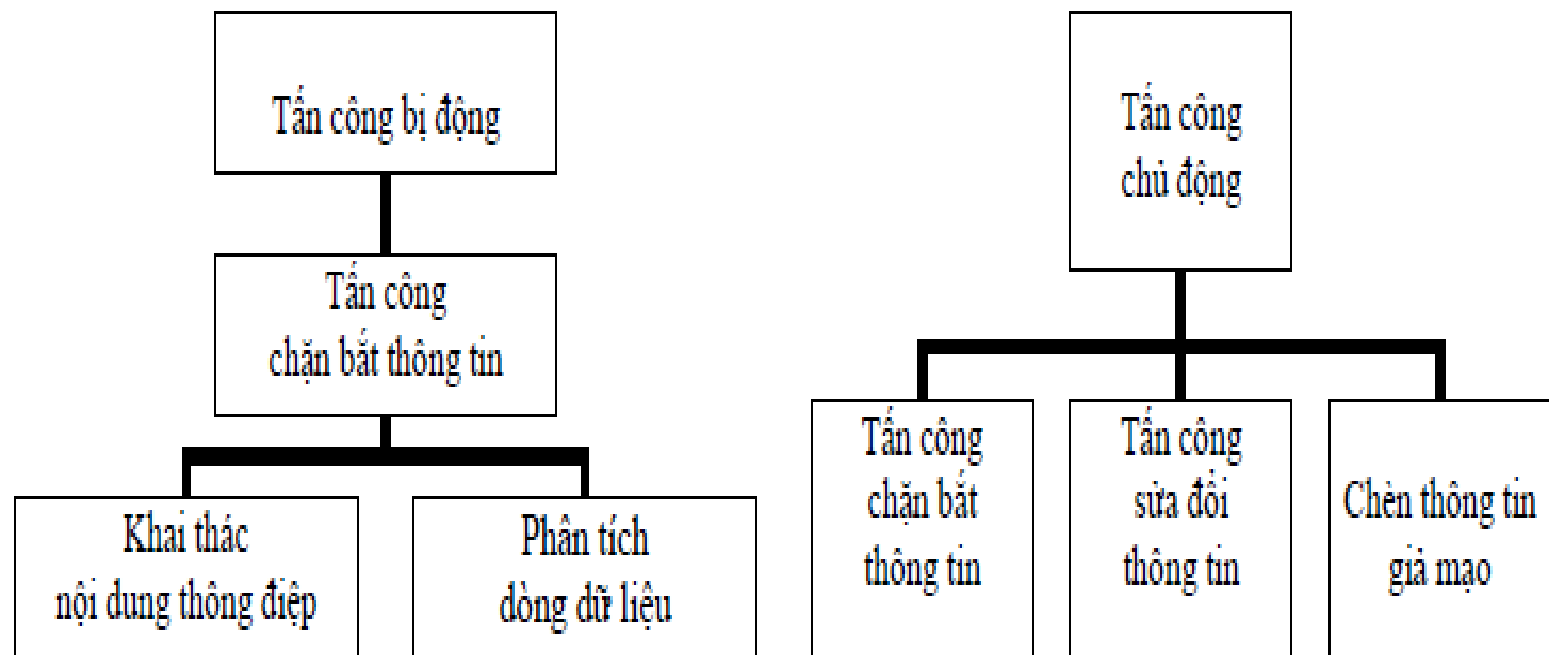


# Các loại hình tấn công (tiếp)

- **Tấn công sửa đổi thông tin (Modification)**
  - Kẻ tấn công truy nhập, chỉnh sửa thông tin trên mạng.
  - Đây là hình thức tấn công vào tính toàn vẹn của thông tin.
- **Chèn thông tin giả mạo (Fabrication)**
  - Kẻ tấn công chèn các thông tin và dữ liệu giả vào hệ thống.
  - Đây là hình thức tấn công vào tính xác thực của thông tin.



# Tấn công bị động và chủ động



# Tấn công bị động (passive attacks)

---

- Mục đích của kẻ tấn công là biết được thông tin truyền trên mạng.
- Có hai kiểu tấn công bị động là **khai thác nội dung thông điệp** và **phân tích dòng dữ liệu**.
- Tấn công bị động rất khó bị phát hiện vì nó không làm thay đổi dữ liệu và không để lại dấu vết rõ ràng. Biện pháp hữu hiệu để chống lại kiểu tấn công này là ngăn chặn (đối với kiểu tấn công này, ngăn chặn tốt hơn là phát hiện).

# Tấn công chủ động (active attacks)

---

- Tấn công chủ động được chia thành 4 loại sau:
  - ❑ **Giả mạo** (Masquerade): Một thực thể (người dùng, máy tính, chương trình...) đóng giả thực thể khác.
  - ❑ **Dùng lại** (replay): Chặn bắt các thông điệp và sau đó truyền lại nó nhằm đạt được mục đích bất hợp pháp.
  - ❑ **Sửa thông điệp** (Modification of messages): Thông điệp bị sửa đổi hoặc bị làm trể và thay đổi trật tự để đạt được mục đích bất hợp pháp.
  - ❑ **Từ chối dịch vụ** (Denial of Service - DoS): Ngăn cấm việc sử dụng bình thường hoặc làm cho truyền thông ngừng hoạt động.

# Một số kỹ thuật tấn công mạng

---

- 1) Tấn công thăm dò.
- 2) Tấn công password
- 3) Tấn công sử dụng mã độc.
- 4) Tấn công xâm nhập.
- 5) Tấn công từ chối dịch vụ.
- 6) Tấn công sử dụng kỹ nghệ xã hội

# Tấn công thăm dò

---

- Thăm dò là việc thu thập thông tin trái phép về tài nguyên, các lỗ hổng hoặc dịch vụ của hệ thống.
- Tấn công thăm dò thường bao gồm các hình thức:
  - Sniffing (Nghe lén)
  - Ping Sweep: Chủ yếu hoạt động trên các mạng sử dụng thiết bị chuyển mạch (switch).
  - Ports Scanning: là một quá trình kết nối các cổng (TCP và UDP) trên một hệ thống mục tiêu nhằm xác định xem dịch vụ nào đang “chạy” hoặc đang trong trạng thái “nghe”. Xác định các cổng nghe là một công việc rất quan trọng nhằm xác định được loại hình hệ thống và những ứng dụng đang được sử dụng.

# Tấn công Password

---

- Password là gì?
- Có 3 dạng tấn công Password phổ biến:
  - **Brute Force Attack** (tấn công vét cạn mật khẩu)
  - **Dictionary Attack** (tấn công từ điển)
  - **Key Logger Attack** (tấn công Key Logger)

# Tấn công Password

---

- **Brute Force Attack** (tấn công dò mật khẩu)
  - Kẻ tấn công sử dụng một công cụ mạnh mẽ, có khả năng thử nhiều username và password cùng lúc (từ dễ đến khó) cho tới khi đăng nhập thành công.
  - VD: đặt mật khẩu đơn giản như 123456, password123, daylamatkhou,... rất dễ bị tấn công brute force.

# Tấn công Password

---

- **Dictionary Attack** (tấn công từ điển)
  - Là một biến thể của Brute Force Attack
  - Tuy nhiên kẻ tấn công nhắm vào các từ có nghĩa thay vì thử tất cả mọi khả năng.
  - Nhiều người dùng có xu hướng đặt mật khẩu là những từ đơn giản và có ngữ nghĩa. VD: motconvit, iloveyou,... Đây là lý do khiến Dictionary Attack có tỉ lệ thành công cao hơn.

# Tấn công Password

---

- **Key Logger Attack** (tấn công Key Logger)
  - Kẻ tấn công lưu lại lịch sử các phím mà nạn nhân gõ, bao gồm cả ID, password hay nhiều nội dung khác.
  - Kẻ tấn công cần phải sử dụng một phần mềm độc hại (malware) đính kèm vào máy tính (hoặc điện thoại) nạn nhân, phần mềm đó sẽ ghi lại tất cả những ký tự mà nạn nhân nhập vào máy tính và gửi về cho kẻ tấn công. Phần mềm này được gọi là Key Logger.
  - Nguy hiểm hơn 2 cách tấn công trên, do việc đặt mật khẩu phức tạp không giúp ích gì trong trường hợp này.

# Tấn công Password

---

- Ngoài ra, kẻ tấn công có thể tấn công gián tiếp thông qua việc:
  - Lừa đảo người dùng tự cung cấp mật khẩu (Tấn công giả mạo Phishing);
  - Tiêm nhiễm Malware
  - Tấn công vào cơ sở dữ liệu – kho lưu trữ mật khẩu người dùng của các dịch vụ...

# Tấn công Password

---

## Cách phòng chống

- **Đặt mật khẩu phức tạp**

- Tuy đơn giản nhưng biện pháp này giúp người dùng phòng tránh được hầu hết các cuộc tấn công dò mật khẩu thông thường.
- Một mật khẩu mạnh thường bao gồm: chữ IN HOA, chữ thường, số, ký tự đặc biệt (ví dụ @\$\*%&#)

- **Bật xác thực 2 bước:**

- Hầu hết dịch vụ cho phép người dùng bật xác thực 2 bước khi đăng nhập trên thiết bị mới. Điều này khiến hacker có hack được mật khẩu cũng không thể đăng nhập được.
- Hiện tại Facebook, Gmail, các ngân hàng, ví điện tử... đều có tính năng này.

# Tấn công Password

---

## Cách phòng chống

- **Quản lý mật khẩu tập trung:**
  - Việc lưu tất cả mật khẩu trên một thiết bị là con dao hai lưỡi. Người dùng cần nhắc khi thực hiện.
- **Thay đổi mật khẩu định kì:**
  - Gây khó khăn cho quá trình hack mật khẩu của tin tặc.
- **Thận trọng khi duyệt web:**
  - Tin tặc có thể hack mật khẩu của bạn bằng cách tạo ra một đường link giả mạo. Link giả thường gần giống trang web chính vì thế, luôn thận trọng với các đường link trước khi đưa thông tin cá nhân

# Tấn công Password

---

## Cách phòng chống

- **Cẩn trọng khi mở email, tải file:**
  - Tuyệt đối không mở file lạ, và luôn kiểm tra địa chỉ email người gửi xem có chính xác không.
  - VD: tên người gửi là Ngọc Luân JSC nhưng địa chỉ email là ngoclunajsc thì chắc chắn có dấu hiệu lừa đảo.

# Tấn công Password

## Bị hack mật khẩu phải làm sao?

- **Ngay lập tức khóa dịch vụ đang sử dụng:**
  - Liên hệ trực tiếp với các nhà cung cấp dịch vụ (ngân hàng, facebook, gmail...) để yêu cầu tạm ngưng dịch vụ cho tài khoản của bạn.
- **Ngắt kết nối với các dịch vụ khác (nếu có):**
  - Nếu bạn bị mất tài khoản Gmail, cần ngắt kết nối với tài khoản facebook, tài khoản ngân hàng bằng cách thông báo cho nhân viên hỗ trợ.
- **Xác nhận danh tính để lấy lại mật khẩu:**
  - Bạn chỉ cần chọn “Forget Password” hoặc “Quên mật khẩu” rồi tiến hành nhập thông tin cần thiết để lấy lại mật khẩu. Mỗi dịch vụ khác nhau yêu cầu xác minh thông tin khác nhau, thông thường chính là thông tin bạn sử dụng để đăng ký tài khoản

# Tấn công bằng Backdoor



- **Backdoor (cửa hậu)**

- Backdoor trong phần mềm hay hệ thống máy tính thường là một cổng không được thông báo rộng rãi.
- Cho phép người quản trị xâm nhập hệ thống để tìm nguyên nhân gây lỗi hoặc bảo dưỡng (do nhà phát triển tạo ra).
- Hacker và gián điệp dùng backdoor để truy cập bất hợp pháp vào hệ thống (cài đặt thông qua một số mã độc).

# Tấn công bằng Backdoor



- **Cách phát hiện tấn công Backdoor**
  - Rất khó phát hiện, tùy thuộc vào hệ điều hành
  - Dùng phần mềm antimalware quét và kiểm tra backdoor
  - Một số trường hợp khác đòi hỏi phải sử dụng các công cụ chuyên dụng, hoặc các công cụ giám sát giao thức để kiểm tra gói mạng mới có thể phát hiện được backdoor

# Tấn công bằng Backdoor



- **Cách phòng chống**

- Tuân thủ đúng các phương pháp bảo mật
- Chỉ cài đặt các phần mềm tin cậy và đảm bảo đã bật tường lửa (firewall) trên thiết bị (firewall có thể ngăn chặn các cuộc tấn công backdoor, hạn chế lưu lượng truyền qua các cổng mở)
- Theo dõi lưu lượng mạng để phát hiện và kiểm tra xem có sự hiện diện của backdoor hay không

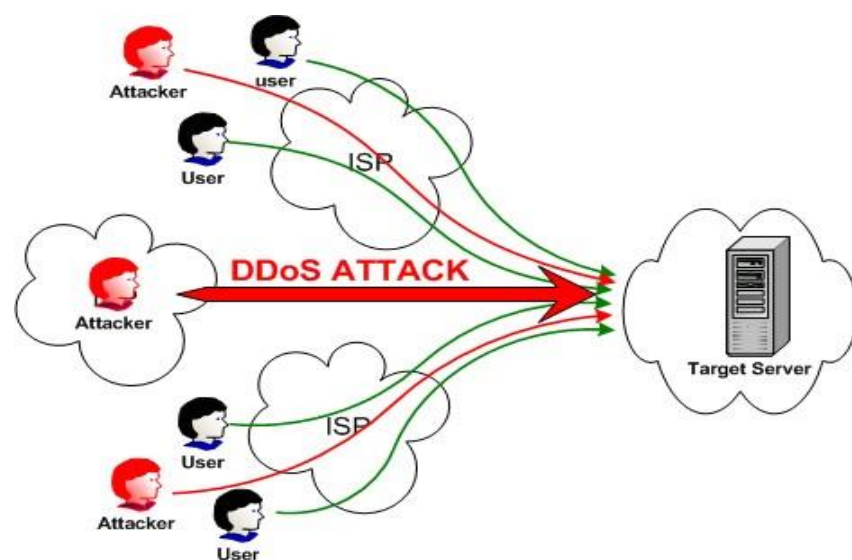
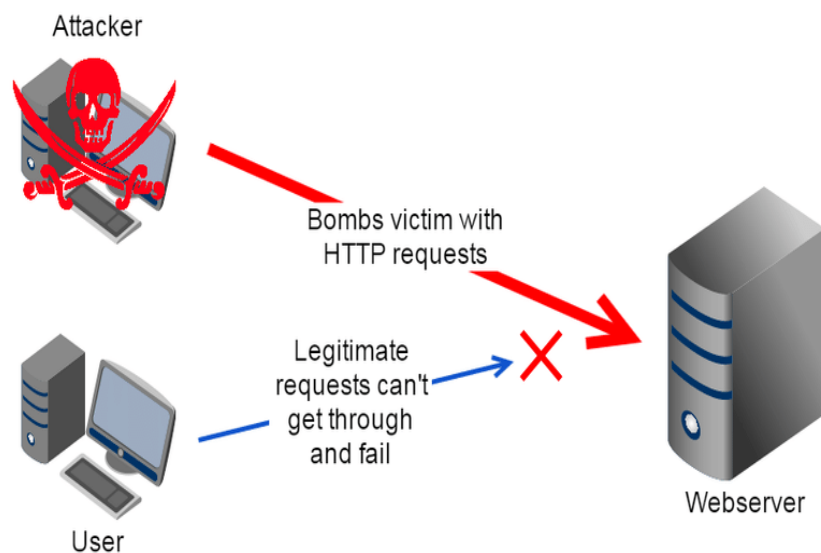
# *Tấn công từ chối dịch vụ (Denial of Service)*

---

- Là hình thức tấn công khá phổ biến hiện nay, nó khiến cho máy tính mục tiêu không thể xử lý kịp các tác vụ và dẫn đến quá tải.
- Các cuộc tấn công DOS này thường nhắm vào các máy chủ ảo (VPS) hay Web Server của các doanh nghiệp lớn như ngân hàng, chính phủ hay là các trang thương mại điện tử ... hoặc hacker cũng có thể tấn công để “bỏ ghét”.

# Tấn công từ chối dịch vụ (*Denial of Service*)

- Tấn công DOS thường chỉ được tấn công từ một địa điểm duy nhất, tức là nó sẽ xuất phát tại một điểm và chỉ có một dải IP thôi. Bạn có thể phát hiện và ngăn chặn được.



# Tấn công từ chối dịch vụ (*Denial of Service*)

## Distributed Denial Of Service (DDoS)

- Là một dạng tấn công nhằm gây cạn kiệt tài nguyên hệ thống máy chủ và làm ngập lưu lượng băng thông Internet, khiến truy cập từ người dùng tới máy chủ bị ngắt quãng, truy cập chập chờn, thậm chí không thể truy cập được internet, làm tê liệt hệ thống hoặc thậm chí là cả một hệ thống mạng nội bộ.
- Tấn công **DDOS** mạnh hơn **DOS** rất nhiều, điểm mạnh của hình thức này đó là nó được phân tán từ nhiều dải IP khác nhau, chính vì thế người bị tấn công sẽ rất khó phát hiện để ngăn chặn được.
- Hacker không chỉ sử dụng máy tính của họ để thực hiện một cuộc tấn công vào một trang web hay một hệ thống mạng nào đó, mà họ còn lợi dụng hàng triệu máy tính khác để thực hiện việc này.

# Tấn công Mail Bombs

- Là một dạng của DoS
- Một số lượng lớn email được gửi đến một tài khoản với mục đích chính là hạ gục tài khoản email mục tiêu (gián đoạn trong quá trình nhận/chuyển và xử lý các thư hợp pháp)



# Tấn công Mail Bombs

---

- Tấn công Mailbomb thường tấn công các máy chủ email.
- Trong kiểu tấn công này thay vì các gói, các email quá lớn hoặc email rác được lọc (ngăn chặn) thì lại liên tục được gửi đến một máy chủ email mục tiêu.
- Điều này thường làm sập máy chủ email do tải đột ngột và khiến chúng vô dụng cho đến khi được sửa chữa.

# Tấn công Man-in-the-middle

## Tấn công xen giữa (Man-in-the-middle)

- Là một kiểu tấn công mạng, trong đó kẻ tấn công chặn đường liên lạc giữa 2 bên
- Mục tiêu là bất kỳ loại giao tiếp trực tuyến nào, như trao đổi email, phương tiện truyền thông mạng xã hội hoặc thậm chí các trang web tài chính, các kết nối liên quan đến khóa công khai hoặc khóa riêng và các trang web yêu cầu đăng nhập.
- Tin tặc có thể xem dữ liệu riêng tư của bạn (các cuộc hội thoại, thông tin đăng nhập hoặc thông tin tài chính). Họ cũng có thể gửi và nhận dữ liệu mà bạn không biết.

# Tấn công Man-in-the-middle

---

## Các loại tấn công Man-in-the-middle

- Email Hijacking (Đánh cắp email)
  - Chiếm quyền điều khiển email của các tổ chức ngân hàng hoặc tài chính. Họ có quyền truy cập vào tài khoản cá nhân của nhân viên và khách hàng và theo dõi các giao dịch. Khi có cơ hội, họ sử dụng địa chỉ email của ngân hàng để gửi hướng dẫn riêng cho khách hàng. Bằng cách làm theo các hướng dẫn này, khách hàng vô tình gửi tiền của họ cho những kẻ tấn công thay vì ngân hàng của họ.

# Tấn công Man-in-the-middle

---

## Các loại tấn công Man-in-the-middle

- Wi-Fi Eavesdropping (Nghe lén Wifi )
  - Kẻ tấn công thiết lập một địa chỉ Wi-Fi có tên có vẻ hợp pháp. Sau đó, họ chờ người dùng (bạn) kết nối với mạng Wi-Fi. Khi bạn kết nối với Wi-Fi, tin tặc có thể truy cập thiết bị của bạn, theo dõi hoạt động của bạn và chặn dữ liệu cá nhân của bạn. Sau đó dùng các thông tin đó thực hiện một tấn công khác.

# Tấn công Man-in-the-middle

---

## Các loại tấn công Man-in-the-middle

- **Session Hijacking (chiếm phiên làm việc)**
  - Một phiên là khoảng thời gian bạn đã đăng nhập và làm việc trong hệ thống (các hệ thống ngân hàng, tài chính)
  - Mục tiêu lấy thông tin đăng nhập, thông tin cá nhân, theo dõi phiên làm việc thông qua các cookie của bạn thậm chí thay mặt bạn thực hiện một số giao dịch.

**IP Spoofing/DNS Spoofing/HTTPS Spoofing**

# Tấn công Man-in-the-middle

---

## **Bảo vệ khỏi tấn công MITM**

- Sử dụng kết nối HTTPS
- Sử dụng HSTS (HTTP Strict Transport Security)
- Luôn luôn cập nhật hệ thống và chương trình của bạn
- Cẩn thận với mạng Wi-Fi
- Sử dụng mạng riêng ảo (VPN)

# Tấn công Sniffing

---

- Sniffing là một chương trình lắng nghe trên hệ thống mạng để truyền dữ liệu. Sniffing cho phép các cá nhân nắm bắt dữ liệu khi nó truyền qua mạng.
- Kỹ thuật này được sử dụng bởi các chuyên gia mạng để chuẩn đoán các sự cố mạng và bởi những users có ý định xấu để thu thập dữ liệu không được mã hóa, như password và username. Nếu thông tin này được ghi lại trong quá trình người dùng có thể truy cập vào hệ thống hoặc mạng.
- Khởi đầu Sniffer là tên một sản phẩm của Network Associates có tên là Sniffier Analyzer.

# Tấn công Sniffing

---

- Đối tượng Sniffing là:
  - Password (từ Email, Web, SMB, FTP, SQL hoặc Telnet)
  - Các thông tin về thẻ tín dụng
  - Văn bản của Email
  - Các tập tin đang di động trên mạng (tập tin Email, FTP hoặc SMB)

# Tấn công Sniffing

- Sniffing thường được sử dụng vào 2 mục đích khác biệt nhau.
  - Tích cực:
    - Chuyển đổi dữ liệu trên đường truyền để quản trị viên có thể đọc và hiểu ý nghĩa của những dữ liệu đó.
    - Bằng cách nhìn vào lưu lượng của hệ thống cho phép quản trị viên có thể phân tích lỗi đang mắc phải trên hệ thống lưu lượng của mạng.
    - Một số Sniffing tân tiến có thêm tính năng tự động phát hiện và cảnh báo các cuộc tấn công đang được thực hiện vào hệ thống mạng mà nó đang hoạt động. (Intrusion Detecte Service)
    - Ghi lại thông tin về các gói dữ liệu, các phiên truyền...Giúp các quản trị viên có thể xem lại thông tin về các gói dữ liệu, các phiên truyền sau sự cố...Phục vụ cho công việc phân tích, khắc phục các sự cố trên hệ thống mạng.
  - Tiêu cực:
    - Nghe lén thông tin trên mạng để lấy các thông tin quan trọng.

# Tấn công sử dụng mã độc (*malicious code*)

---

- **Khái niệm:** Mã độc là những chương trình khi được khởi chạy có khả năng phá hủy hệ thống, bao gồm Virus, sâu (Worm) và Trojan, ...
- Tấn công bằng mã độc có thể làm cho hệ thống hoặc các thành phần của hệ thống hoạt động sai lệch hoặc có thể bị phá hủy.

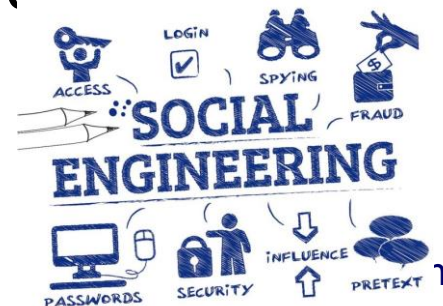
# *Tấn công xâm nhập (Intrusion attack)*

---

- Là hình thức tấn công, nhằm truy nhập bất hợp pháp vào các HTTT.
- Kiểu tấn công này được thực hiện với mục đích đánh cắp dữ liệu hoặc thực hiện phá hủy bên trong HTTT.

# Tấn công sử dụng kỹ nghệ xã hội (Social engineering)

- Là kỹ thuật tác động đến con người, nhằm mục đích lấy được thông tin hoặc đạt được một mục đích mong muốn.
- Dựa vào điểm yếu tâm lý, nhận thức sai lầm của con người về việc bảo mật thông tin, sử dụng sự ảnh hưởng và thuyết phục để đánh lừa người dùng nhằm khai thác các thông tin có lợi cho cuộc tấn công, hoặc thuyết phục nạn nhân thực hiện một hành động nào đó.



# *Tấn công sử dụng kỹ nghệ xã hội (Social engineering)*

---

Là kỹ thuật tác động đến con người, nhằm mục **Các hình thức tấn công Social Engineering phổ biến**

- **Phishing**
- **Watering Hole**
- **Pretexting**
- **Baiting và Quid Pro Quo**

# *Tấn công sử dụng kỹ nghệ xã hội (Social engineering)*

---

## **Phishing**

- Ghép từ “Fishing” và Phony” (“câu cá” và “lừa đảo”)
- Là một hình thức lừa đảo bằng cách giả mạo các tổ chức có uy tín như ngân hàng, trang web giao dịch trực tuyến, các công ty thẻ tín dụng để lừa người dùng chia sẻ thông tin tài chính bí mật như: tên đăng nhập, mật khẩu giao dịch và những thông tin nhạy cảm khác.

# Tấn công sử dụng kỹ nghệ xã hội (Social engineering)

## Các kiểu tấn công Phishing

- **Spear phishing**

- Tấn công cá nhân hoặc tổ chức cụ thể, với nội dung được thiết kế riêng cho nạn nhân. Hacker phải thu thập và đối chiếu các thông tin của nạn nhân (tên, chức danh, email, tên đồng nghiệp, mối quan hệ,...) để tạo ra một email lừa đảo đáng tin cậy, yêu cầu bạn cung cấp thông tin của mình. Bạn tưởng email đó là email từ một người hoặc bất kỳ tổ chức nào mà bạn biết.
- Ví dụ, **something.com** có thể có tên miền phụ tên là **paypal.something.com**. Kẻ tấn công tạo một ID email là **support@paypal.something.com**. Email có vẻ khá giống với ID email liên quan đến PayPal.
- Là mối đe dọa nghiêm trọng đối với doanh nghiệp, chính phủ và gây thiệt hại lớn

# Tấn công sử dụng kỹ nghệ xã hội (Social engineering)

## Các kiểu tấn công Phishing

- **Spear phishing:** Các biện pháp bảo vệ khỏi Spear Phishing
  - Nếu bạn nhận được bất kỳ email nào, dưới bất kỳ hình thức nào, yêu cầu bạn cung cấp thông tin chi tiết, thứ mà bạn không cảm thấy thoải mái khi chia sẻ, hãy coi đó là một hình thức spear phishing và trực tiếp loại bỏ nó. Bỏ qua các email, tin nhắn đó và kết thúc các cuộc gọi như vậy.
  - Chỉ chia sẻ những gì cần thiết trên các trang mạng xã hội
  - Nên có một phần mềm bảo mật tốt để lọc các email của mình. Bạn có thể thêm chứng chỉ email và mã hóa cho các ứng dụng email mà bạn sử dụng để bạn được bảo vệ tốt hơn. Nhiều cuộc tấn công spear phishing có thể bị phát hiện bằng các chương trình hoặc chứng chỉ bảo mật được tích hợp hay cài đặt cho ứng dụng email.

# *Tấn công sử dụng kỹ nghệ xã hội (Social engineering)*

---

## **Các kiểu tấn công Phishing**

- **Clone phishing**

- Hacker sao chép các email hợp pháp, nhưng thay thế đường dẫn hoặc trong email. Khi người dùng nhấp vào liên kết hoặc mở tệp đính kèm, tài khoản của họ sẽ bị hacker kiểm soát. Sau đó, hacker sẽ giả mạo danh tính của nạn nhân để thực hiện phishing trong chính tổ chức của nạn nhân

# *Tấn công sử dụng kỹ nghệ xã hội (Social engineering)*

---

## **Các kiểu tấn công Phishing**

- **Phone phishing**
  - “vice phishing” hoặc “vishing”
  - Các phisher sẽ tự xưng là đại diện của ngân hàng, sở cảnh sát, hoặc thậm chí sở thuế vụ tại địa phương bạn sống. Họ sẽ đe dọa và yêu cầu bạn cung cấp thông tin tài khoản hoặc nộp phạt qua chuyển khoản hoặc bằng thẻ trả trước để tránh bị theo dõi

# Tấn công sử dụng kỹ nghệ xã hội (Social engineering)

## Các kiểu tấn công Phishing

- **Lừa đảo qua mạng xã hội:**
  - Hacker thực hiện bằng cách gửi đường dẫn qua tin nhắn, trạng thái Facebook hoặc các mạng xã hội khác. Các tin nhắn này có thể là thông báo trúng thưởng các hiện vật có giá trị như xe SH, xe ô tô, điện thoại iPhone,... và hướng dẫn người dùng truy cập vào một đường dẫn để hoàn tất việc nhận thưởng.
  - Ngoài việc lừa nạn nhân nộp lệ phí nhận thưởng, tin tặc có thể chiếm quyền điều khiển tài khoản, khai thác thông tin danh sách bạn bè sử dụng cho các mục đích xấu như lừa mượn tiền, mua thẻ cào điện thoại,...

# *Tấn công sử dụng kỹ nghệ xã hội (Social engineering)*

---

## **Cách phòng tránh tấn công Phishing**

- Không mở email từ người lạ
- Không nhấp vào các liên kết đáng ngờ trong email
- Nếu nghi ngờ một trang web trong có vẻ hợp pháp, bạn hãy nhập địa chỉ trang web hợp pháp trên trình duyệt web theo cách thủ công
- Kiểm tra xem các website có cùng các giao thức hỗ trợ bảo mật không
- Nếu nhận một email không hợp pháp, hãy lấy các thông tin trong email đó để kiểm tra xem có cuộc tấn công lừa đảo nào thực hiện bằng phương pháp tương tự không
- Sử dụng phần mềm bảo mật chống phần mềm độc hại đáng tin cậy

# *Tấn công sử dụng kỹ nghệ xã hội (Social engineering)*

---

## **Watering Hole**

- Hacker tấn công có chủ đích vào các TC/DN thông qua việc lừa các thành viên truy cập vào các trang web chứa mã độc.
- Tin tặc thường nhắm đến các trang web có nhiều người truy cập, web “đen” hoặc tạo ra các trang web riêng để lừa người dùng, trong đó cố ý chèn vào website các mã khai thác liên quan đến các lỗ hổng trình duyệt.
- Nếu truy cập vào website, các mã độc này sẽ được thực thi và lây nhiễm vào máy tính của người dùng.

# Tấn công sử dụng kỹ nghệ xã hội (Social engineering)

## Kịch bản của tấn công Watering Hole

- **Bước 1:** Thu thập thông tin về TC/DN mục tiêu, gồm danh sách các website mà các nhân viên hay lãnh đạo của tổ chức thường xuyên truy cập. Sau đó, tin tặc bắt đầu tìm kiếm các trang web mà chúng để có thể xâm nhập, kết hợp với kỹ thuật tấn công local attack để nâng cao khả năng tấn công.
- **Bước 2:** Sau khi đã chiếm được quyền điều khiển của một website mà các nhân viên của tổ chức thường xuyên truy cập, tin tặc sẽ thực hiện chèn các mã khai thác các lỗ hổng thông qua trình duyệt, ứng dụng flash hay java
- **Bước 3:** Sau khi người dùng truy cập vào các trang web độc hại, ngay lập tức mã độc sẽ được thực thi. Khi đó, tin tặc sẽ chiếm quyền điều khiển và cài đặt các chương trình độc hại cho phép điều khiển từ xa lên máy tính nạn nhân. Từ đó, khai thác các thông tin từ người dùng hoặc sử dụng chính máy đó để tấn công các máy tính khác.

# *Tấn công sử dụng kỹ nghệ xã hội (Social engineering)*

---

## **Pretexting**

- Hacker tập trung vào việc tạo ra một lý do hợp lý, hoặc một kịch bản đã được tính toán từ trước để ăn cắp thông tin cá nhân của nạn nhân.
- Hacker có thể sẽ cố thao túng các mục tiêu để khai thác các điểm yếu về cấu trúc của một tổ chức hoặc công ty. Ví dụ, một tin tặc mạo danh một kiểm toán viên của dịch vụ CNTT bên ngoài công ty với những lý lẽ hợp lý, đủ sức thuyết phục nhân viên an ninh về mặt vật lý, cho phép tin tặc vào cơ sở làm việc của công ty đó.
- Không giống như các email lừa đảo vốn lợi dụng sự sợ hãi và khẩn cấp của nạn nhân, các cuộc tấn công Pretexting dựa vào việc xây dựng cảm giác tin cậy cho đối tượng cần khai thác.

# Tấn công sử dụng kỹ nghệ xã hội (Social engineering)

---

## Baiting và Quid Pro Quo

- Lợi dụng sự tò mò của con người hoặc hứa hẹn về một mặt hàng hay một sản phẩm hấp dẫn nào đó để đánh lừa nạn nhân. Ví dụ điển hình là một kịch bản tấn công mà tin tặc sử dụng một tệp độc hại được giả mạo thành bản cập nhật phần mềm hoặc phần mềm phổ biến nào đó.
- Hacker cũng có thể tấn công Baiting về mặt vật lý, ví dụ như phát miễn phí thẻ USB bị nhiễm độc trong khu vực lân cận của tổ chức mục tiêu và đợi nhân viên nội bộ lấy nhiễm phần mềm độc hại vào máy tính của công ty. Sau khi được thực thi trên các máy tính, các phần mềm độc hại được cài đặt trên các USB này sẽ giúp tin tặc chiếm được toàn quyền điều khiển, qua đó phục vụ cho mục đích tấn công tiếp theo.

# *Tấn công sử dụng kỹ nghệ xã hội (Social engineering)*

---

## **Baiting và Quid Pro Quo**

- Quid Pro Quo hay Something For Something là biến thể của Baiting.
- Thay vì dụ đưa ra lời hứa về một sản phẩm, hacker hứa hẹn một dịch vụ hoặc một lợi ích dựa trên việc thực hiện một hành động cụ thể nào đó qua một dịch vụ hoặc lợi ích được tin tặc xây dựng để trao đổi thông tin hoặc quyền truy cập.
- Hacker mạo danh nhân viên CNTT của một tổ chức lớn. Hacker đó cố gắng liên lạc qua điện thoại với nhân viên của tổ chức định tấn công, sau đó cung cấp và hướng dẫn cho họ một số thông tin liên quan đến việc nâng cấp hoặc cài đặt phần mềm. Để tạo điều kiện cho việc thực hiện các hành vi độc hại, các hacker sẽ yêu cầu nạn nhân tạm thời vô hiệu hóa phần mềm antivirus cài trong máy, nhờ đó ứng dụng độc hại được thực thi mà không gặp phải bất cứ trở ngại nào.

# Tấn công sử dụng kỹ nghệ xã hội (Social engineering)

## Biện pháp phòng chống Social Engineering- Đối với cá nhân

- Cẩn thận và không nên trả lời bất kỳ thư rác nào yêu cầu xác nhận, cập nhật bất kỳ thông tin nào về tài khoản của cá nhân, TC/DN.
- Không kích chuột vào bất kỳ liên kết đi kèm với thư rác nếu không chắc chắn về nó.
- Cảnh giác với các thông tin khuyến mại, trúng thưởng nhận được trên MXH; Không nhấp chuột vào các đường dẫn của các trang web lạ; Không cung cấp thông tin cá nhân, đặc biệt là tài khoản ngân hàng; Sử dụng mật khẩu phức tạp đối với các tài khoản MXH và thường xuyên thay đổi các mật khẩu này.
- Cảnh giác khi thực hiện truy cập vào các trang web, đặc biệt là các trang web không phổ biến vì chúng rất có thể tồn tại lỗ hổng mà tin tặc đang nhắm vào để khai thác.

# Tấn công sử dụng kỹ nghệ xã hội (Social engineering)

## **Biện pháp phòng chống Social Engineering- Đối với cá nhân**

- Phân chia tài khoản, quyền hạn và trách nhiệm rõ ràng đối với các tài khoản MXH, website, hệ thống.
- Tránh sử dụng một mật khẩu cho nhiều tài khoản khác nhau nhằm tránh nguy cơ lộ lọt thông tin.
- Hạn chế đăng những thông tin cá nhân, thông tin công ty, doanh nghiệp lên mạng xã hội để tránh kẻ xấu mạo danh.
- Nâng cao kiến thức về tấn công và cách phòng tránh Social Engineering, kỹ năng ATTT cho cán bộ, nhân viên; Thực hiện các buổi tập huấn với các tình huống giả mạo, qua đó nâng cao nhận thức, ý thức cảnh giác và kinh nghiệm đối phó với những tình huống tương tự.
- Thường xuyên cập nhật bản vá cho phần mềm, hệ điều hành.

# Xu hướng tấn công HTTT

---

## *1. Sử dụng các công cụ tấn công tự động*

- Những kẻ tấn công sẽ sử dụng các công cụ tấn công tự động có khả năng thu thập thông tin từ hàng nghìn địa chỉ trên Internet một cách nhanh chóng, dễ dàng và hoàn toàn tự động.
- Các HTTT có thể bị quét từ một địa điểm từ xa để phát hiện ra những địa chỉ có mức độ bảo mật thấp. Thông tin này có thể được lưu trữ, chia sẻ hoặc sử dụng với mục đích bất hợp pháp.

# Xu hướng tấn công HTTT (tiếp)

---

## *2. Sử dụng các công cụ tấn công khó phát hiện*

- Một số cuộc tấn công được dựa trên các mẫu tấn công mới, không bị phát hiện bởi các chương trình bảo mật, các công cụ này có thể có tính năng đa hình, siêu đa hình cho phép chúng thay đổi hình dạng sau mỗi lần sử dụng.

# Xu hướng tấn công HTTP (tiếp)

---

## *3. Phát hiện nhanh các lỗ hổng bảo mật*

- Thông qua các lỗ hổng bảo mật của hệ thống, phần mềm kẻ tấn công khai thác các lỗ hổng này để thực hiện các cuộc tấn công.
- Hàng năm, nhiều lỗ hổng bảo mật được phát hiện và công bố, tuy nhiên điều này cũng gây khó khăn cho các nhà quản trị hệ thống để luôn cập nhật kịp thời các bản vá. Đây cũng chính là điểm yếu mà kẻ tấn công tận dụng để thực hiện các hành vi tấn công, xâm nhập bất hợp pháp.

# Xu hướng tấn công HTTT (tiếp)

---

## *4. Tấn công bất đối xứng và tấn công diện rộng*

- Tấn công bất đối xứng xảy ra khi bên tấn công mạnh hơn nhiều so với đối tượng bị tấn công.
- Tấn công diện rộng thực hiện khi kẻ tấn công tạo ra một mạng lưới kết hợp các hoạt động tấn công.

# Xu hướng tấn công HTTT (tiếp)

---

## 5. *Thay đổi mục đích tấn công*

- Thời gian trước, các tấn công chỉ từ mục đích thử nghiệm, hoặc khám phá hệ thống an ninh.
- Hiện nay, mục đích tấn công với nhiều lý do khác nhau như về tài chính, giả mạo thông tin, phá hủy, và đặc biệt nguy hiểm đó là mục đích chính trị, chính vì vậy mà độ phức tạp của các cuộc tấn công đã tăng lên và tác hại lớn hơn rất nhiều so với trước đây.

# Mã độc và các phòng chống mã độc

---

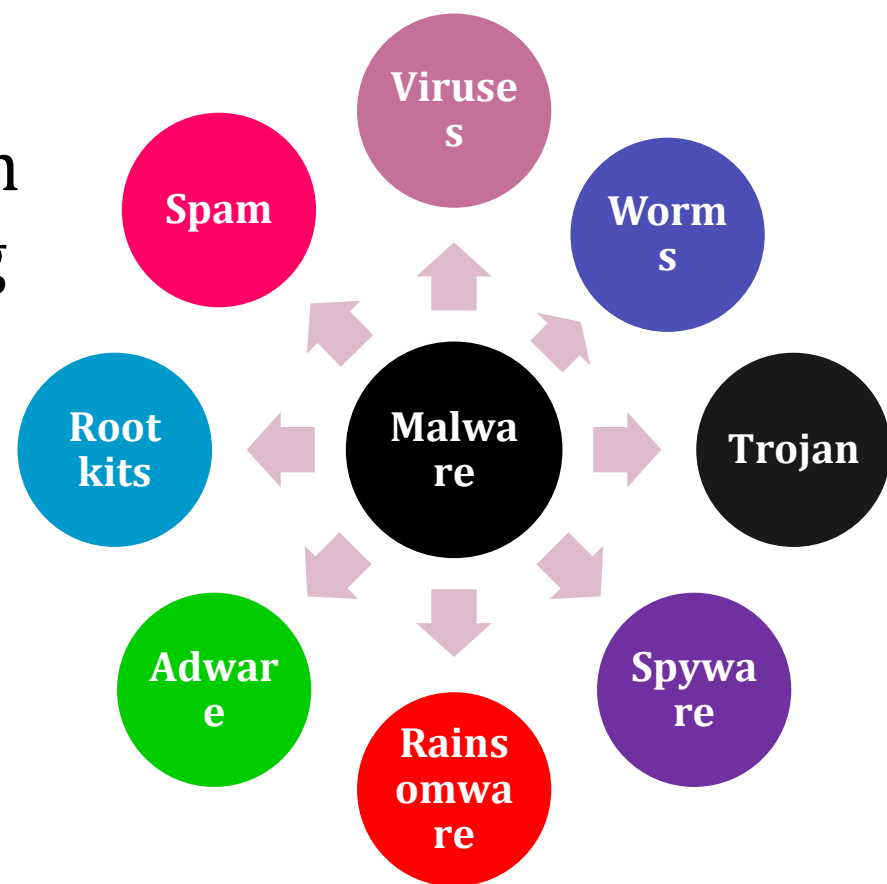
## Mã độc là gì?

- Mã độc là một khái niệm chung dùng để chỉ các phần mềm độc hại được viết với mục đích có thể lây lan phát tán (hoặc không lây lan, phát tán) trên hệ thống máy tính và internet, nhằm thực hiện các hành vi bất hợp pháp nhằm vào người dùng cá nhân, cơ quan, tổ chức để chuộc lợi cá nhân, kinh tế, chính trị hoặc đơn giản là để thỏa mãn ý tưởng và sở thích của người viết.

# Mã độc và các phòng chống mã độc

## Phân loại và đặc tính của mã độc

- Tuỳ thuộc vào cơ chế, hình thức lây nhiễm và phương pháp phá hoại mà người ta phân biệt mã độc thành nhiều loại khác nhau: virus, trojan, backdoor, adware, spyware...



# Mã độc và các phòng chống mã độc

## Một số loại mã độc

- **Trojan**: Trojan là loại mã độc ẩn trong các chương trình hợp pháp, khi ta kích hoạt nó hoặc tự động “nằm vùng” trong máy tính sau đó kích hoạt nhằm mục đích lấy thông tin của người dùng như tài khoản cá nhân (email, username, password, số tài khoản ...), xóa file, làm đổ vỡ các chương trình thông thường, ngăn chặn người dùng kết nối internet...
- **Worm**: Giống trojan về hành vi phá hoại, tuy nhiên nó có thể tự nhân bản để thực hiện lây nhiễm qua nhiều máy tính.
- **Spyware**: là phần mềm cài đặt trên máy tính người dùng nhằm thu thập các thông tin người dùng một cách bí mật, không được sự cho phép của người dùng.
- **Adware**: phần mềm quảng cáo, hỗ trợ quảng cáo, là các phần mềm tự động tải, pop up, hiển thị hình ảnh và các thông tin quảng cáo để ép người dùng đọc, xem các thông tin quảng cáo. Adware không có tính phá hoại nhưng nó làm ảnh hưởng tới hiệu năng của thiết bị và gây khó chịu cho người dùng.

# Mã độc và các phòng chống mã độc

## Một số loại mã độc

- **Ransomware**: đây là phần mềm khi lây nhiễm vào máy tính nó sẽ kiểm soát hệ thống hoặc kiểm soát máy tính và yêu cầu nạn nhân phải trả tiền để có thể khôi phục lại điều khiển với hệ thống.
- **Virus**: là phần mềm có khả năng lây nhiễm trong cùng một hệ thống máy tính hoặc từ máy tính này sang máy tính khác dưới nhiều hình thức khác nhau. Quá trình lây lan được thực hiện qua hành vi lây file. Ngoài ra, virus cũng có thể thực hiện các hành vi phá hoại, lấy cắp thông tin...
- **Rootkit**: là một kỹ thuật cho phép phần mềm có khả năng che giấu danh tính của bản thân nó trong hệ thống, các phần mềm antivirus từ đó nó có thể hỗ trợ các module khác tấn công, khai thác hệ thống.

# Mã độc và các phòng chống mã độc

## Kỹ thuật phá hoại

- **Định thời:** virus sẽ dựa vào một giá trị nào đó (ví dụ ngày, tháng, số lần lây, số lần khởi động máy tính ...). Khi giá trị này bằng hoặc lớn hơn một giá trị cho trước, virus sẽ bắt đầu phá hoại. Do chỉ phá hoại một lần nên virus này thường rất nguy hiểm.
- **Ngẫu nhiên và liên tục:** không giống như định thời, sau khi lây nhiễm, virus sẽ bắt đầu phá hoại. Do tính chất này, virus không mang tính phá hoại mà đơn giản là gây ra một số hiệu ứng ở loa, chuột, màn hình, hoặc lấy cắp thông tin, reset máy hoặc format đĩa, ....
  - Ví dụ là virus Pingpong, sau khi xâm nhập xong, vào phút sau sẽ thấy trên màn hình xuất hiện một trái banh chuyển động và tuân theo các định luật phản xạ khi gặp đường biên

# Mã độc và các phòng chống mã độc

---

## Kỹ thuật phát hiện Malware

- **Dynamic analysis (Phân tích động):** là quá trình này có nghĩa là quan sát hành vi của mã độc khi nó đang chạy. Cụ thể là những công việc như: Khởi chạy mã độc trên một môi trường ảo, quan sát xem khi mà mã độc chạy nó sẽ làm những gì,.... Debug mã độc sử dụng một công cụ Debugger nào đó:
- Ví dụ winDBG, OllyDBG để quan sát từng bước hành vi của mã độc khi nó đang được thực thi bởi bộ nhớ và load trong RAM.

# Mã độc và các phòng chống mã độc

---

## Kỹ thuật phát hiện Malware

- **Static analysis (Phân tích tĩnh):** Là quá trình dịch ngược mã độc (RCE - reverse engineering). Dịch ngược mã độc từ mã máy ra ngôn ngữ mà con người có thể đọc hiểu (asm, IL,...). Trong quá trình này các nhà phân tích sẽ sử dụng những công cụ dịch ngược như IDA, khi thực hiện dịch ngược IDA không load mã độc vào RAM như ollyDBG, IDA.

# Mã độc và các phòng chống mã độc

---

## Một số biện pháp phòng chống

- **Luôn luôn cài đặt và sử dụng một phần mềm diệt virus chính hãng.** Ví dụ: Kaspersky, CyStack, Bitdifender, Avast, Norton, Bkav, ...
- **Xây dựng chính sách với các thiết bị PnP:** Với các thiết bị loại này: USB, CD/DVD, ... virus có thể lợi dụng để thực thi mà không cần sự cho phép của người dùng. Do đó, cần thiết lập lại chế độ cho các thiết bị và chương trình này để hạn chế sự thực thi không kiểm soát của mã độc. Ngoài ra, trong quá trình sử dụng các thiết bị như USB, chúng ta không nên mở trực tiếp bằng cách chọn ổ đĩa rồi nhấn phím Enter, hoặc nhấp đôi chuột vào biểu tượng mà nên bấm chuột phải rồi click vào explore

# Mã độc và các phòng chống mã độc

## Một số biện pháp phòng chống

- **Thiết lập quy tắc đối xử với các file:** Không nên mở hoặc tải về các file không rõ nguồn gốc, đặc biệt là các file thực thi (các file có đuôi .exe, .dll, ...). Với các file không rõ nguồn gốc này, tốt nhất chúng ta nên tiến hành quét bằng phần mềm diệt virus hoặc thực hiện kiểm tra trực tiếp trên website: <https://www.virustotal.com> Khi có nghi ngờ được cảnh báo cần dừng việc thực thi file lại để đảm bảo an toàn.
- **Truy cập web an toàn:** Khi truy cập web cần chú ý: Không nên truy cập vào các trang web đen, các trang web độc hại, có nội dung không lành mạnh, không tùy tiện click vào các url từ các email hoặc từ nội dung chat, trên các website, ... Các website và url như trên thường xuyên ẩn chứa các mã độc và chỉ đợi người dùng click, nó sẽ tự động tải về, thiết lập cài đặt để thực thi hợp pháp trên máy tính người dùng. Một ví dụ tiêu biểu đó là khi chúng ta phân tích và theo dõi các máy của các nhân viên văn phòng, các máy tính này hầu hết đều bị cài đặt các addon hoặc các phần mềm quản cáo do quá trình duyệt web chính bản thân người sử dụng đã cho phép addon hoặc phần mềm đó thực thi.

# Mã độc và các phòng chống mã độc

## Một số biện pháp phòng chống

- **Cập nhật máy tính, phần mềm:** Thường xuyên cập nhật các bản vá được cung cấp từ hệ điều hành, các bản vá cho các ứng dụng đang sử dụng và đặc biệt là cập nhật chương trình diệt virus. Đây là yếu tố quan trọng để tránh được các loại mã độc lợi dụng các lỗ hổng để lây lan, đồng thời cũng cập nhật được các mẫu mã độc mới để giúp phần mềm diệt virus làm việc hiệu quả hơn.
- **Nhờ chuyên gia can thiệp:** Khi thấy máy tính có các dấu hiệu bị lây nhiễm cần tiến hành quét ngay bằng phần mềm diệt virus, nếu vẫn không có tiến triển tốt, cần nhờ sự giúp đỡ của các chuyên gia để kiểm tra máy tính, phát hiện và tiêu diệt mã độc ngay. Có thể việc này sẽ làm tốn thời gian và tiền bạc nhưng nó thật sự cần thiết vì rất có thể tác hại của việc để nguyên máy tính còn tồn kém và thiệt hại hơn rất nhiều lần.

# Các mối đe dọa an ninh mạng hàng đầu năm 2022

---

## *1. Social Engineering (Tấn công phi kỹ thuật)*

- Dựa vào lỗi của con người hơn là các lỗ hổng kỹ thuật, theo báo cáo Điều tra vi phạm dữ liệu của Verizon, 85% tất cả các vụ vi phạm dữ liệu liên quan đến sự tương tác của con người.

## *2. Third-Party Exposure*

- Tội phạm mạng có thể xâm nhập các hệ thống bảo mật bằng cách tấn công các mạng ít được bảo vệ hơn thuộc các bên thứ ba có đặc quyền truy cập vào mục tiêu chính của tin tặc.

# Các mối đe dọa an ninh mạng hàng đầu năm 2022

---

## 3. *Configuration Mistakes (Các lỗi cấu hình)*

- Viện Ponemon báo cáo rằng một nửa số chuyên gia CNTT thừa nhận họ không biết các công cụ an ninh mạng mà họ đã cài đặt thực sự hoạt động tốt như thế nào, có nghĩa là ít nhất một nửa số chuyên gia CNTT đã không thử nghiệm và bảo trì thường xuyên.

## 4. *Cyber Hygiene kém*

- “Cyber Hygiene” đề cập đến các thói quen và thực hành thường xuyên liên quan đến việc sử dụng công nghệ, như tránh các mạng WiFi không được bảo vệ và thực hiện các biện pháp bảo vệ như VPN hoặc xác thực đa yếu tố.

# Các mối đe dọa an ninh mạng hàng đầu năm 2022

---

## 5. *Lỗ hổng trên đám mây*

- IBM báo cáo rằng các lỗ hổng trên đám mây đã tăng 150% trong 5 năm qua. Verizon DBIR đã phát hiện ra rằng hơn 90% trong số 29.000 vi phạm được phân tích trong báo cáo là do vi phạm web app.

## 6. *Lỗ hổng thiết bị di động*

- Theo Báo cáo Bảo mật Di động của Check Point Software, trong suốt năm 2021, 46% công ty đã gặp sự cố bảo mật liên quan đến một ứng dụng di động độc hại do một nhân viên tải xuống.

# Các mối đe dọa an ninh mạng hàng đầu năm 2022

---

## *7. Internet of Things*

- Các nhà doanh nghiệp tập trung vào hiệu suất và khả năng sử dụng thiết bị. Các biện pháp bảo mật, mã hóa dữ liệu đều không được chú trọng và dễ dàng bỏ qua những lỗ hổng cơ bản. Đó là lý do tại sao các thiết bị IoT thường bị tấn công.

## *8. Ransomware*

- Khảo sát năm 2021 với 1.263 chuyên gia an ninh mạng, 66% cho biết các công ty của họ bị mất doanh thu đáng kể do một cuộc tấn công bằng ransomware.

# Các mối đe dọa an ninh mạng hàng đầu năm 2022

---

## *9. Quản lý dữ liệu kém*

- Quản lý dữ liệu không chỉ đơn thuần là giữ cho hệ thống lưu trữ và tổ chức của bạn gọn gàng. Nói một cách dễ hiểu, lượng dữ liệu do người tiêu dùng tạo ra tăng gấp đôi sau mỗi bốn năm, nhưng hơn một nửa số dữ liệu mới đó không bao giờ được sử dụng hoặc phân tích. Các đồng dữ liệu dư thừa dẫn đến nhầm lẫn, khiến dữ liệu dễ bị tấn công mạng.

## *10. Các thủ tục sau tấn công không đầy đủ*

- Các lỗ hổng bảo mật phải được vá ngay sau một cuộc tấn công an ninh mạng. Trong một cuộc khảo sát năm 2021 đối với 1.263 công ty đã bị nhắm mục tiêu trong một vụ vi phạm an ninh mạng, 80% nạn nhân đã nộp tiền chuộc cho biết họ đã trải qua một cuộc tấn công khác ngay sau đó.

# Các giải pháp an ninh mạng năm 2022

---

1. Ưu tiên bảo mật không gian mạng
2. Không thờ ơ với quyền riêng tư và bảo vệ dữ liệu
3. Thiết lập và duy trì các chính sách làm sạch an ninh mạng và CNTT
4. Mật khẩu là chưa đủ
5. Sử dụng Zero-trust
6. Hãy thận trọng với những lừa đảo có công nghệ hỗ trợ
7. Ưu tiên bảo mật 5G
8. Tăng cường bảo mật làm việc từ xa
9. Không nên đơn độc trong đảm bảo an ninh mạng
10. Có thể sử dụng dịch vụ bảo mật CNTT thuê ngoài

# Các mối đe dọa phổ biến khi mua sắm trực tuyến

- 1) WiFi công cộng
- 2) Các website TMĐT giả mạo
- 3) Phần mềm đánh cắp thông tin thẻ tín dụng
- 4) Mã độc web
- 5) Các cuộc tấn công bộ định tuyến (router) và thiết bị IoT
- 6) Các dịch vụ trực tuyến bị chiếm quyền



# Các mối đe dọa phổ biến khi mua sắm trực tuyến



# Các mối đe dọa phổ biến khi mua sắm trực tuyến

## BIỆN PHÁP phòng ngừa

- ✗ Không **cung cấp thông tin, hình ảnh cá nhân** hoặc đưa lên mạng xã hội
- ✗ Không cung cấp **mật khẩu, mã OTP** của ngân hàng, ví điện tử cho người khác
- ✗ Không **click vào những đường link lạ**, có chứa mã độc trên các website
- ✓ Luôn **nâng cao cảnh giác** và không làm theo để tránh bị lừa đảo chiếm đoạt tài sản
- ✓ Cảnh giác khi cài các **app “vay tiền”** để tránh chịu lãi suất cao, bị đòi nợ theo kiểu “tín dụng đen”...
- ✓ **Trình báo cơ quan công an** gần nhất để được hỗ trợ

# CÂU HỎI VÀ BÀI TẬP (tiếp)

---

1. Phân biệt và trình bày mối tương quan mỗi đe dọa – lỗ hổng – rủi ro. Cho ví dụ
2. Trình bày các loại mã độc (malware). Sự khác biệt giữa worm và virus là gì? Trojan horse có chứa đựng virus hoặc worm không?
3. Tại sao tính đa hình của các mã độc lại gây ra mối quan tâm lớn hơn mã độc hại truyền thống? Nó ảnh hưởng đến việc phát hiện/nhận dạng mã độc như thế nào?
4. Trình bày các loại mã độc hiện nay mà bạn biết

# Câu hỏi & bài tập

---

1. Tấn công mật khẩu (password) là gì? Trình bày các kiểu tấn công mật khẩu. Một người quản trị viên một hệ thống thông tin có thể làm gì để chống lại tấn công mật khẩu?
2. Tấn công từ chối dịch vụ (denial of service) là gì? Cho ví dụ minh họa thực tế một hệ thống thông tin bị tấn công từ chối dịch vụ.
3. Phân biệt giữa tấn công từ chối dịch vụ (DoS) và tấn công từ chối dịch vụ phân tán (DDoS). Loại nào nguy hiểm hơn? Tại sao?

# Câu hỏi & bài tập

---

4. Tại sao tính đa hình của các mã độc lại gây ra mối quan tâm lớn hơn mã độc hại truyền thống? Nó ảnh hưởng đến việc phát hiện/nhận dạng mã độc như thế nào?
5. Để một cuộc tấn công sniffer thành công, kẻ tấn công phải làm gì? Làm thế nào kẻ tấn công có thể truy cập được vào một hệ thống thông tin để thám thính?
6. Phương pháp nào để kẻ tấn công social engineering thực hiện thu tập thông tin tài khoản đăng nhập và mật khẩu của người dùng? Phương pháp này sẽ khác biệt như thế nào nếu như mục tiêu nhắm đến là một quản trị viên và một nhân viên nhập dữ liệu?

# CÂU HỎI VÀ BÀI TẬP (tiếp)

- Website BẢO HIỂM MANULIFE của Manulife Financial cung cấp các dịch vụ xem danh mục các sản phẩm đa dạng từ sản phẩm bảo hiểm truyền thống đến sản phẩm bảo hiểm sức khỏe, giáo dục, liên kết đầu tư, hưu trí... cho hơn 700.000 khách hàng thông qua đội ngũ đại lý hùng hậu và chuyên nghiệp tại 55 văn phòng trên 40 tỉnh thành cả nước. Khách hàng có thể chọn lựa, đặt câu hỏi, cần tư vấn hay mua gói bảo hiểm trực tuyến trên Website. Xem thông tin và quyền lợi bảo hiểm, xem hợp đồng bảo hiểm đã mua. Ngoài ra Website còn giúp cho công ty có thể quản lý toàn bộ các hoạt động của công ty như quản lý khách hàng, nhân viên, hợp đồng bảo hiểm,...
- Hãy nhận dạng và giải thích được ít nhất 3 mối đe dọa ảnh hưởng đến an toàn đến các dịch vụ mà Website cung cấp.

# Câu hỏi và Bài tập

---

- 1) Trình bày ít nhất 5 phương thức tấn công mà website của nhóm có thể gặp phải.
- 2) Trình bày giải pháp cụ thể cho mỗi cách tấn công trên và giải thích lý do anh/chị lựa chọn giải pháp đó.
- 3) Trình bày các mối đe dọa thường gặp đến một hệ thống thông tin. Các rủi ro có thể xảy ra và biện pháp phòng ngừa.

# CÂU HỎI VÀ BÀI TẬP (tiếp)

## Tình huống 1:

Bạn là một nhân viên thu ngân phí bảo hiểm của công ty bảo hiểm ANZ. Bạn được cấp một máy tính có kết nối internet và phần mềm để thực hiện công việc hàng ngày của mình. Do ít khách hàng nên bạn cũng khá nhàn rỗi. Những lúc nhàn rỗi, bạn hay dùng máy tính làm việc lên internet để tải game, nhạc, phim về để giải trí. Các website bạn vào hầu như là các website không an toàn. Bạn hãy:

- Chỉ ra 2 mối đe dọa mà bạn có thể gặp phải trong tình huống trên
- Nêu ra được lý do tại sao có những mối đe dọa đó
- Phân tích hậu quả nếu các mối đe dọa đó thật sự xảy ra

# CÂU HỎI VÀ BÀI TẬP (tiếp)

## Tình huống 2:

Bạn là trưởng phòng kinh doanh của một doanh nghiệp lớn. Bạn thường xuyên phân công công việc, theo dõi công việc các nhân viên thuộc cấp dưới của mình qua hệ thống website của doanh nghiệp. Đồng thời thường xuyên giao dịch hợp đồng với khách hàng qua email, cũng như báo cáo kết quả công việc cho sếp. Đợt vừa rồi bạn có một chuyến công tác 1 tuần ở các một số tỉnh. Thật là không may mắn, máy laptop làm việc của bạn bị hư đột xuất và không có nơi nào sửa chữa liền được. Để giải quyết các công việc hàng ngày, bạn phải dùng máy tính công cộng tại các khách sạn mà bạn lưu trú tại nơi công tác. Bạn hãy:

- Chỉ ra 2 mối đe dọa mà bạn có thể gặp phải trong tình huống trên
- Nêu ra được lý do tại sao có những mối đe dọa đó.
- Phân tích hậu quả nếu các mối đe dọa đó thật sự xảy ra.

**THANKS YOU**

---