



# TRƯỜNG CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG KHOA KHOA HỌC MÁY TÍNH

## **AN TOÀN VÀ BẢO MẬT THÔNG TIN** (Information security)

**Chương 1-2: Tổng quan về an  
toàn thông tin**



# Nội dung

## 1. Tình hình An toàn thông tin (ATTT)

- Tình hình ATTT
- Hệ thống thông tin an toàn
- An ninh và chính sách an ninh

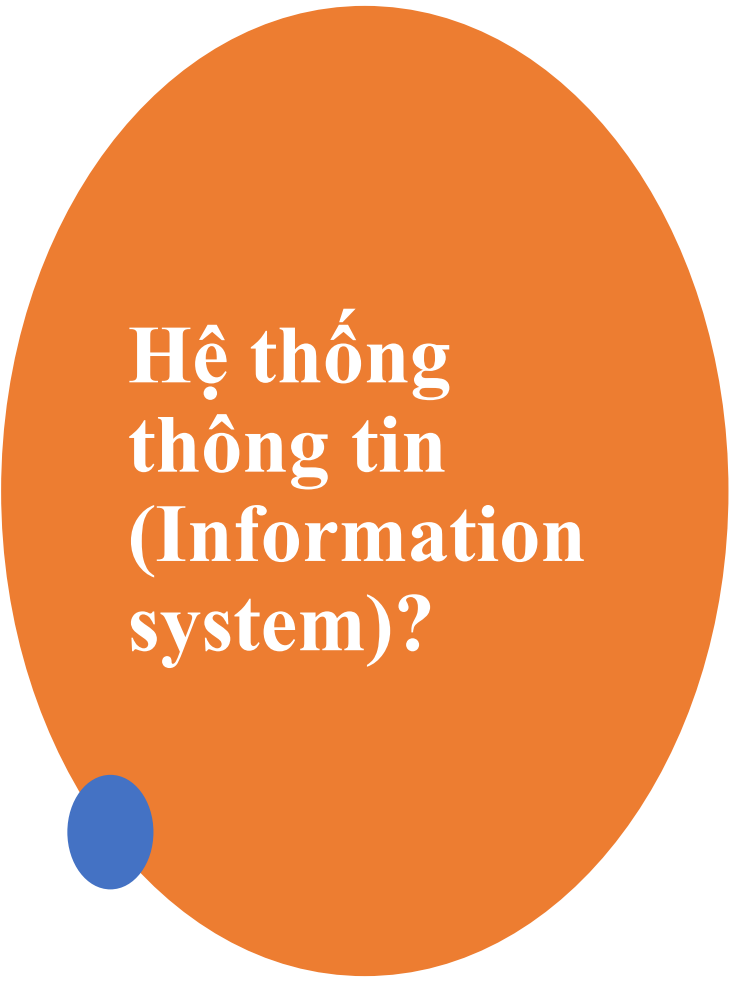
## 2. Tổng quan về tấn công mạng

- Tổng quan TCM
- Các hình thức tấn công mạng
- Một số kỹ thuật ngăn chặn

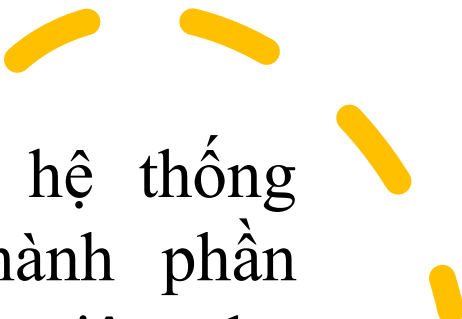


# 1.1. An toàn hệ thống thông tin



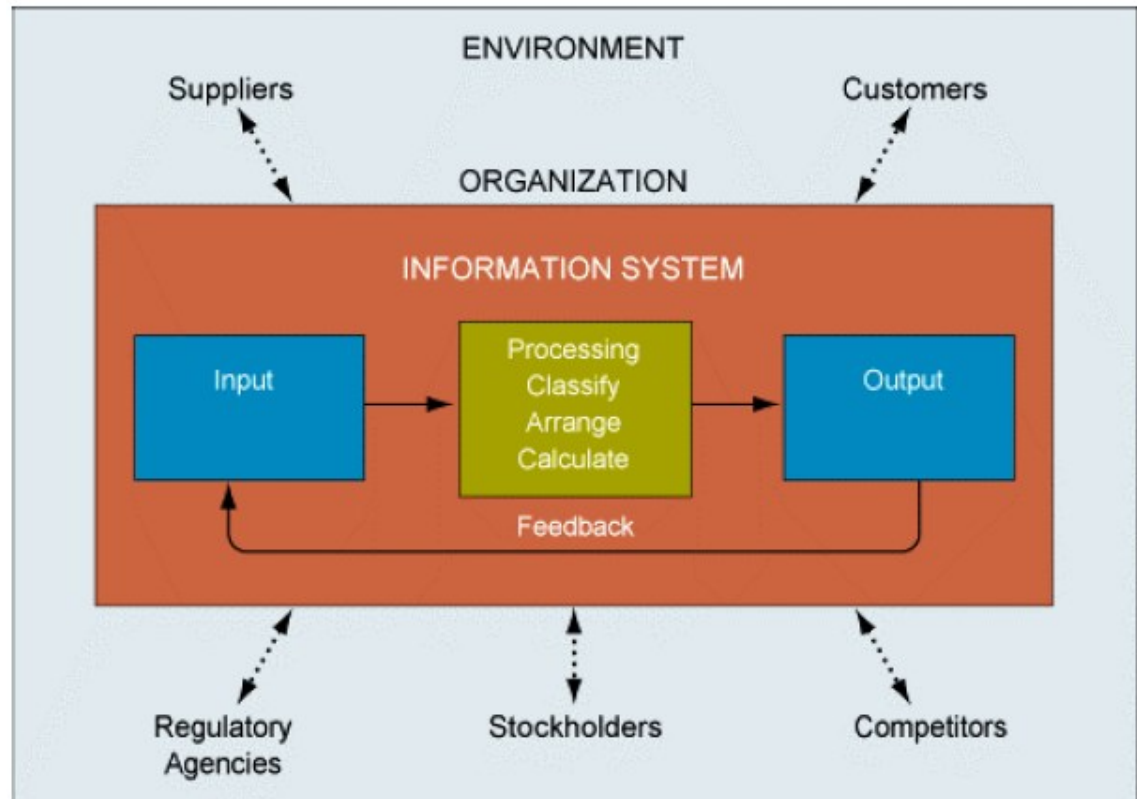


## Hệ thống thông tin (Information system)?

- 
- HTTT Là một hệ thống tích hợp các thành phần nhằm phục vụ việc thu thập, lưu trữ, xử lý thông tin và chuyển giao thông tin, tri thức và các sản phẩm số..

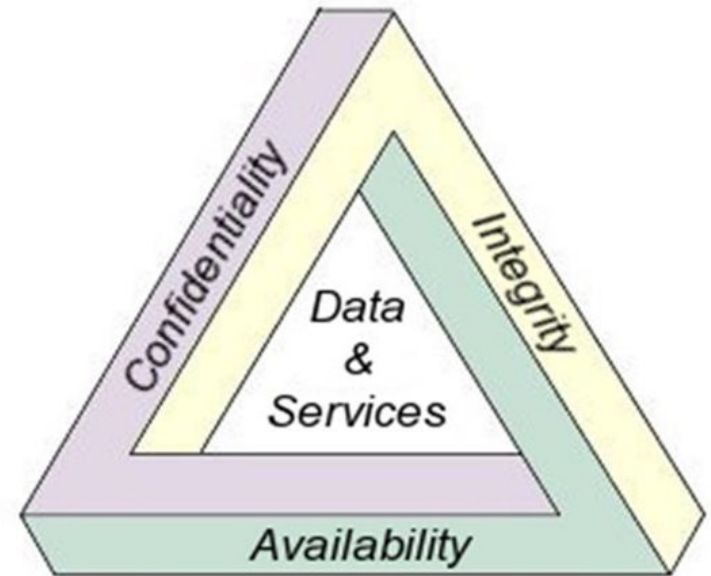
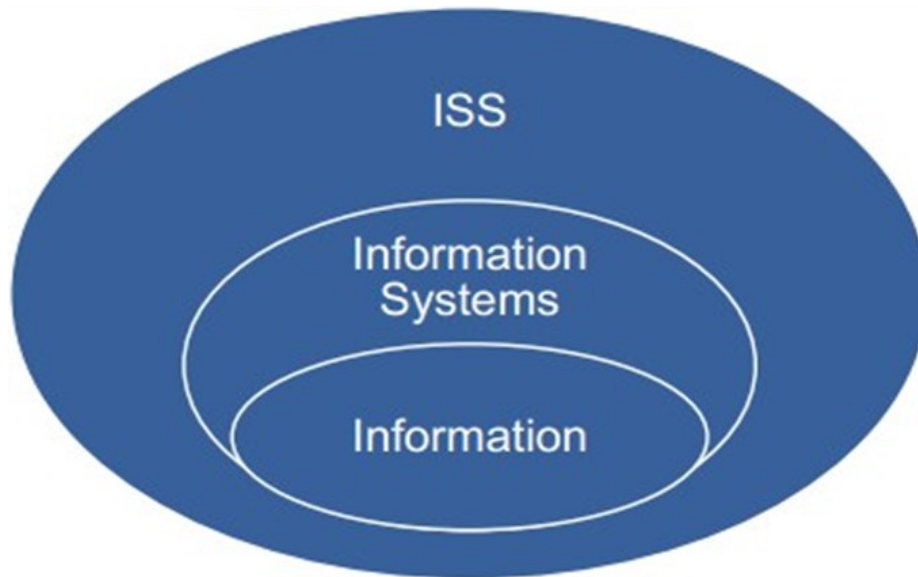
# Mô hình hệ thống thông tin

---

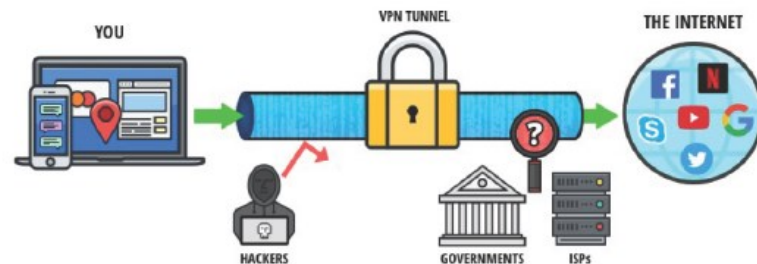


# An toàn hệ thống thông tin

- Là việc đảm bảo các thuộc tính an ninh an toàn của hệ thống thông tin.
- 3 mục tiêu bảo mật:
  - Bí mật (Confidentiality)
  - Toàn vẹn (Integrity)
  - Sẵn dùng (Availability)



# An toàn hệ thống thông tin

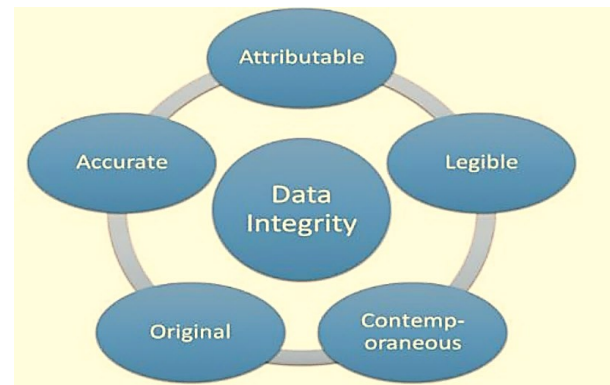


## ▪ Tính bí mật (*Confidentiality*)

- **Thông tin bí mật** là TT mà chỉ có các **đối tượng** được cấp quyền mới truy cập được.
- **Tính bí mật** đề cập đến việc *giới hạn đối tượng được quyền truy cập đến thông tin*.
- **Mức độ BM**: Tùy theo tính chất quan trọng của TT
- Yếu tố thường xem xét: *Tồn tại thông tin và nội dung thông tin*
- **Cơ chế BM**: dựa trên phương tiện vật lý, mật mã (cryptography), hoặc kiểm soát truy cập, ...

Ví dụ: Sử dụng đường hầm VPN để bảo mật tin

# An toàn hệ thống thông tin



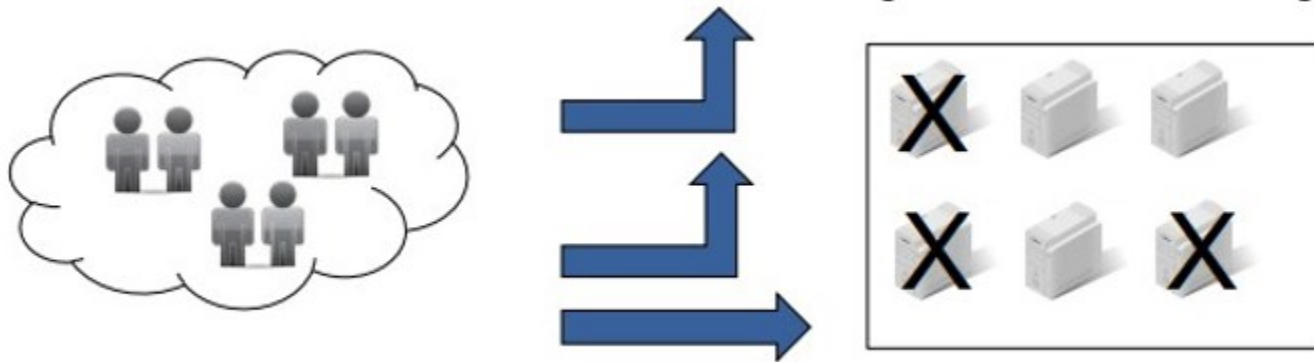
## ▪ Tính toàn vẹn (*Integrity*)

- Thông tin về cơ bản không bị thay đổi, không bị làm hư hỏng và mất mát
- Đề cập đến việc **ngăn chặn** mọi HV thay đổi, làm hư hỏng và mất mát TT
- Thường đánh giá: *toàn vẹn về nội dung* và *toàn vẹn về nguồn gốc TT*
- Cơ chế:
  - + *Ngăn chặn (prevention mechanisms)*
  - + *Phát hiện (Detection mechanisms)*

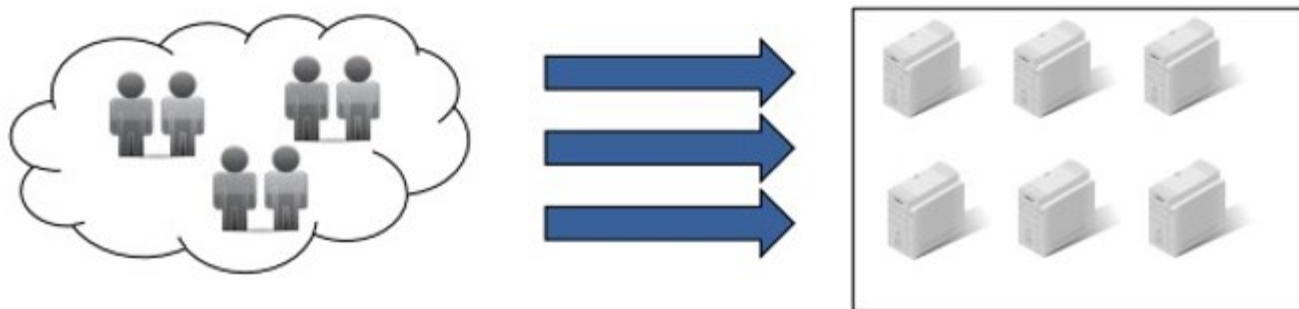


# An toàn hệ thống thông tin

- Không đảm bảo tính sẵn dùng



- Đảm bảo tính sẵn dùng



# An toàn hệ thống thông tin

## ▪ Tính sẵn dùng (*Availability*)

- Thông tin có thể truy nhập bởi người dùng hợp pháp bất cứ khi nào họ có yêu cầu.
- Tính sẵn dùng có thể được đo bằng các yếu tố:
  - + Thời gian cung cấp dịch vụ (Uptime);
  - + Thời gian ngừng cung cấp dịch vụ (Downtime);
  - + Tỷ lệ phục vụ:  $A = (\text{Uptime}) / (\text{Uptime} + \text{Downtime})$ ;
  - + Thời gian trung bình giữa các sự cố;
  - + Thời gian trung bình ngừng để sửa chữa;
  - + Thời gian khôi phục sau sự cố.



# Các thành phần của ATTT

- An toàn máy tính và dữ liệu (Computer and data security)
- An ninh mạng (Network security)
- Quản lý ATTT (Management of information security)
- Chính sách ATTT (Policy)



## 1.2. Nguy cơ và rủi ro hệ thống thông tin



# Nguy cơ và rủi ro hệ thống thông tin

- ❖ Mối đe dọa (threat): Mối đe dọa là bất kỳ một hành động nào có thể gây hư hại đến các tài nguyên hệ thống (gồm phần cứng, phần mềm, CSDL, các file, dữ liệu, hoặc hạ tầng mạng vật lý,...).
- ❖ Điểm yếu (weakness): là những khiếm khuyết hoặc lỗi tồn tại trong hệ thống:
  - Điểm yếu phần cứng
  - Điểm yếu phần mềm (Hệ điều hành và ứng dụng)
- ❖ Lỗ hổng (vulnerability): là bất kỳ điểm yếu nào trong hệ thống cho phép mối đe dọa có thể gây tác hại.

## Nguy cơ (danger)

📖 là mối nguy, gây ra thiệt hại lớn, đe dọa đến các hoạt động bình thường của HTTT. Nguy cơ liên quan đến những sự kiện, hành vi có khả năng xảy ra và *Nếu nó xảy ra thì có khả năng ảnh hưởng đến sự AT HTTT.*

Ví dụ:

- Tấn công DoS và DDoS - là nguy cơ
- Tấn công của sâu Nimda (2001) – không là nguy cơ

## Rủi ro (risk)

📖 là mối nguy, gây ra thiệt hại lớn, đe dọa đến các hoạt động bình thường của HTTT. *Nếu nó xảy ra thì có khả năng ảnh hưởng đến sự AT HTTT.*

Ví dụ:

- Tấn công DoS và DDoS - là nguy cơ
- Tấn công của sâu Nimda (2001) – không là nguy cơ

# Lỗi hỏng bảo mật và điểm yếu hệ thống

## ❖ Các dạng lỗi hỏng bảo mật thường gặp:

- Lỗi tràn bộ đệm (*buffer overflows*)
- Không kiểm tra đầu vào (*invalidated input*)
- Các vấn đề với điều khiển truy cập (*access-control problems*)
- Các điểm yếu (*weaknesses*) trong xác thực, trao quyền (*authorization*), các hệ mật mã
- Các lỗi hỏng bảo mật khác

🔊 *SV tìm hiểu và trình bày các dạng lỗi hỏng BM trên?*





# Lỗi hỏng bảo mật: Phân loại

- Lỗi Bảo vệ hệ thống bằng mật khẩu.
- Lỗi Kết nối và Quyền hạn truy cập CSDL.
- Lỗi Quản trị:
  - Phần mềm/Hệ điều hành,
  - Người Quản lý,
  - Các sản phẩm thông dụng.

# Lỗ hổng bảo mật: Mật khẩu

- Mật khẩu yếu: sử dụng các ký tự thông thường.
- Mật khẩu đặt thông dụng: dễ nhớ.
- Mật khẩu quá ngắn: ít ký tự.
- Phiên sử dụng (Transaction) không được cấu hình hoặc quá lâu.
- Mật khẩu được xác thực chỉ 1 lớp: chỉ xác thực mật khẩu (bỏ qua các lớp: Capcha, OTP, ...).
- Mật khẩu cấp quyền truy cập không hợp lý: Không kiểm tra kỹ quyền truy cập.

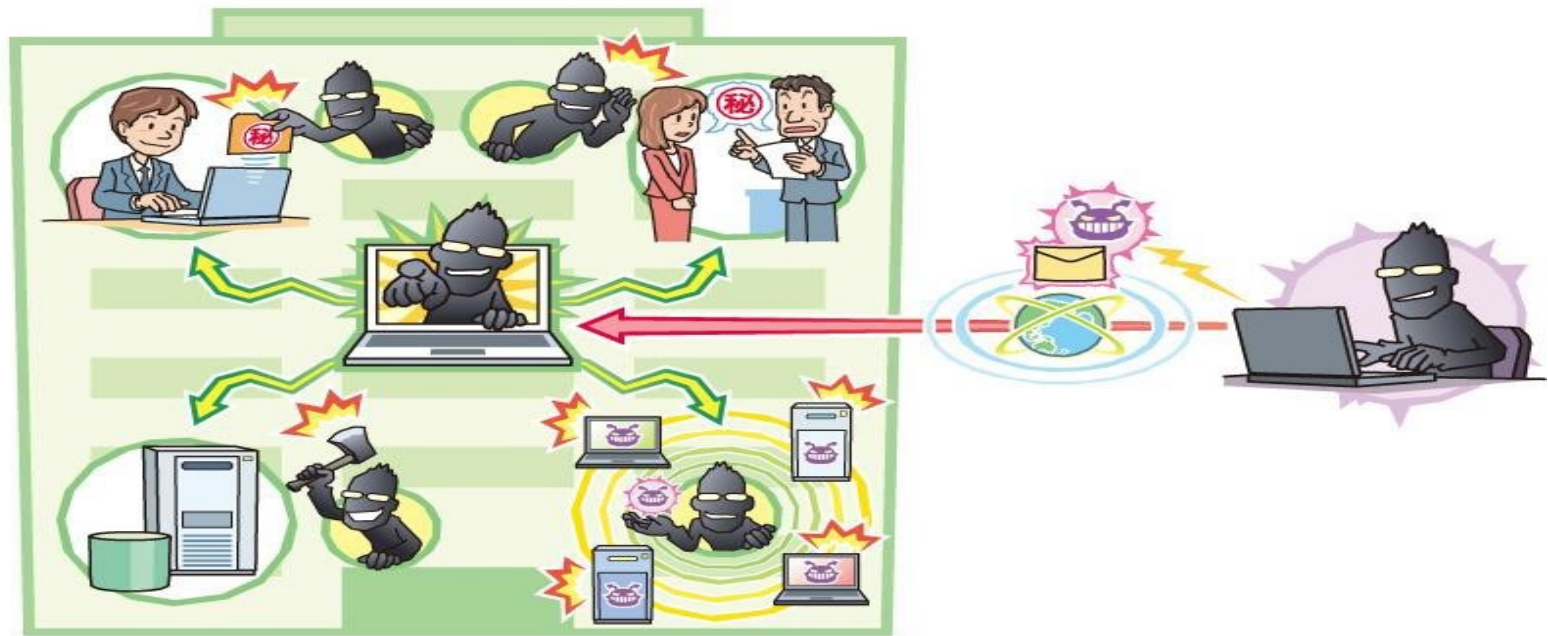
# Lỗ hổng bảo mật: Kết nối và Truy cập CSDL

- Lỗi thường biết đến: SQL Injection.
- Nguyên nhân:
  - Sử dụng câu lệnh SQL thuần trong lập trình. Trong quá trình này sẽ khó tránh khỏi sai sót.
  - Không phân quyền rõ ràng trong Database.
  - Hiển thị mã lỗi trong thông báo.

# Lỗ hổng bảo mật: Quản trị

- Hệ điều hành và Phần mềm: lỗi bị phát hiện sau một thời gian sử dụng.
- Người Quản lý: tồn tại ai đó có thể đi vào hệ thống (nhắm giữ khóa chủ chốt).
- Các sản phẩm thông dụng có thể có lỗi/bị cài mã độc:
  - Hệ điều hành, Phần mềm.
  - Website, Dịch vụ Web và App.
  - Source Code và API.
  - IoT và Thiết bị mạng.
  - Cơ chế xác thực, các giao thức truyền tải, mã hóa: lạc hậu theo thời gian.

# Các đe dọa/nguy cơ với vùng người dùng





## 1.3. An ninh và chính sách an ninh





# Khái niệm

- An toàn thông tin: thông tin tin cậy được trao đổi giữa những đối tác tin cậy.
- An ninh thông tin: các giải pháp đảm bảo an toàn thông tin.

# Nguyên nhân mất ATTT: Cá nhân

- Người tấn công mạng: chưa ý thức rõ về Vi phạm pháp luật từ hành vi Tấn công mạng (khoản 8, điều 2, Luật ANM 2018).
- Người sử dụng mạng: chưa ý thức tốt về ATTT (để lộ lọt thông tin cho những kẻ xấu).
- Đa số người dùng: sử dụng phần mềm không có bản quyền.



# Nguyên nhân mất ATTT: Quản lý

- Người quản lý TT trên mạng: Chưa thực hiện đầy đủ các biện pháp được hướng dẫn của Cục ATTT.
  - Theo định kỳ hàng tháng.
  - Cảnh báo các lỗ hổng bảo mật, đặc biệt là lỗ hổng Zero-Day.
- Người triển khai HTTT bỏ qua quy trình về ATTT:
  - (1) HTTT thiếu giải pháp bảo mật,
  - (2) HTTT chưa được kiểm tra và đánh giá về ATTT,
  - (3) HTTT chưa được phân loại cấp độ thông tin nên chưa có giải pháp bảo mật phù hợp.

# Chính sách ATTT

- Chính sách ATTT: An ninh để An toàn.
- Giải pháp An ninh:
  - Tạo môi trường ATTT: xây dựng **Luật** và tạo Ý thức ATTT cho người tham gia trao đổi thông tin.
  - Phân loại cấp độ ATTT: **5 cấp độ**
    - + Từ Tồn hại quyền và lợi ích hợp pháp của tổ chức và cá nhân
    - + Tới Tồn hại đặc biệt nghiêm trọng tới Quốc phòng và An ninh quốc gia.
  - **Xây dựng mô hình 4 lớp ATTT.**

# Năm cấp độ

- **Cấp độ 1:** Khi bị phá hoại làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức cá nhân nhưng không làm tổn hại tới lợi ích chung (công cộng, trật tự an toàn xã hội, Quốc phòng, An ninh quốc gia).
- **Cấp độ 2:** Tổn hại nghiêm trọng tới lợi ích hợp pháp của tổ chức cá nhân hoặc tổn hại tới lợi ích công cộng, nhưng không làm tổn hại Quốc phòng và An ninh quốc gia.
- **Cấp độ 3:** Tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng, trật tự và an toàn xã hội hoặc làm tổn hại tới Quốc phòng, An ninh quốc gia.
- **Cấp độ 4:** Tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng hoặc nghiêm trọng tới Quốc phòng và An ninh quốc gia.
- **Cấp độ 5:** Tổn hại đặc biệt nghiêm trọng tới Quốc phòng và An ninh quốc gia.

# Khái niệm và tổ chức

- Khái niệm: Mô hình 4 lớp là mô hình về mặt tổ chức, quản lý phục vụ công tác bảo đảm an toàn cho các HTTT nói chung và an toàn cho Chính phủ điện tử, Chính quyền điện tử.
- Mô hình tổ chức:
  - Lớp 1: Lực lượng tại chỗ.
  - Lớp 2: Lực lượng giám sát bảo vệ chuyên nghiệp.
  - Lớp 3: Lực lượng kiểm tra đánh giá độc lập (kiểm tra đánh giá định kỳ).
  - Lớp 4: Lực lượng quốc gia (kết nối chia sẻ thông tin với hệ thống giám sát quốc gia).



# ATTT cá nhân



# Thông tin cá nhân

- Luật quy định:

- (1) Thông tin cá nhân (TTCN):

- Thông tin đủ để xác định chính xác danh tính một cá nhân,
    - Ví dụ: họ tên, ngày sinh, nghề nghiệp, chức danh, địa chỉ liên hệ, thư điện tử, số điện thoại, số CCCD, ...

- (2) Bí mật cá nhân: Hồ sơ y tế, hồ sơ nộp thuế, số thẻ BHXH, số thẻ tin dụng, ...



# Dữ liệu cá nhân

- TTCN dưới dạng số gắn liền hoặc xác định một con người cụ thể.
- Phân loại:
  - (1) Dữ liệu cơ bản: gắn liền với định danh cá nhân, xác định danh tính.
  - (2) Dữ liệu nhạy cảm: gắn liền với quyền riêng tư, bí mật cá nhân.

# Bảo vệ TTCN: Nguyên tắc

1. Cá nhân: Tự bảo vệ và tuân thủ các quy định pháp luật về cung cấp thông tin cá nhân trên mạng.
2. Trách nhiệm: Cơ quan, tổ chức, cá nhân xử lý TTCN có trách nhiệm bảo đảm an toàn cho TTCN.
3. Công khai: Tổ chức, cá nhân xử lý TTCN phải công bố công khai biện pháp bảo vệ TTCN.
4. Luật: Bảo vệ TTCN được thực hiện theo quy định của Luật pháp.
5. Ngoại lệ: Việc xử lý TTCN phục vụ mục đích Quốc phòng, An ninh Quốc gia , Trật tự An toàn xã hội không nhằm mục đích thương mại.



# Bảo vệ TTCN: Thu thập và sử dụng

1. Tổ chức, cá nhân xử lý TTCN có trách nhiệm:
  - Thu thập: phải có sự đồng ý của chủ thể về mục đích sử dụng.
  - Sử dụng khác với mục đích ban đầu: cũng phải có sự đồng ý của chủ thể.
  - Chỉ chia sẻ: khi có sự đồng ý của chủ thể hoặc của cơ quan Nhà nước có thẩm quyền.
2. Cơ quan NN chịu trách nhiệm lưu trữ và bảo vệ TTCN do mình thu thập.
3. Chủ thể có quyền yêu cầu cung cấp TTCN của mình đã được tổ chức, cá nhân thu thập và lưu trữ.

# Bảo vệ TTCN: Cập nhật, sửa đổi và hủy bỏ

1. Chủ thể TTCN có quyền yêu cầu Bên Thu thập và Lưu trữ TTCN của mình: cập nhật, sửa đổi hoặc hủy bỏ, hoặc ngưng cung cấp cho bên thứ 3.
2. Bên Thu thập và Lưu trữ TTCN được yêu cầu phải có trách nhiệm:
  - Thông báo cho chủ thể hoặc cung cấp cho chủ thể quyền tiếp cận dữ liệu để thực hiện yêu cầu của mình.
  - Bảo vệ TTCN với biện pháp phù hợp và trong trường hợp chưa thực hiện được yêu cầu phải thông báo cho chủ thể lý do.
3. Tổ chức, cá nhân phải hủy bỏ TTCN và thông báo cho chủ thể khi đã hoàn thành mục đích hoặc hết thời hạn lưu trữ, trừ trường hợp có quy định khác.

# Nguy cơ lộ lọt TTCN, DLCN

- Mục tiêu sử dụng TTCN, DLCN của kẻ xấu:
  - Vay tiền hoặc vay vốn dưới tên người bị lộ TTCN
  - Đe dọa, Tổng tiền nạn nhân
  - Quảng cáo
- Nguyên nhân:
  - TTCN bị lộ đều xuất phát từ vô tình đến cố tình.
  - Trong đó:
    - + 80% bị lộ do chủ thẻ bất cẩn,
    - + 20% do nhà cung cấp dịch vụ đã chia sẻ hoặc làm lộ.

## 2. Tổng quan tấn công mạng

# Lừa đảo

---

## ■ Loại Lừa đảo:

- Giả mạo thương hiệu
- Chiếm đoạt tài khoản
- Kết hợp khác

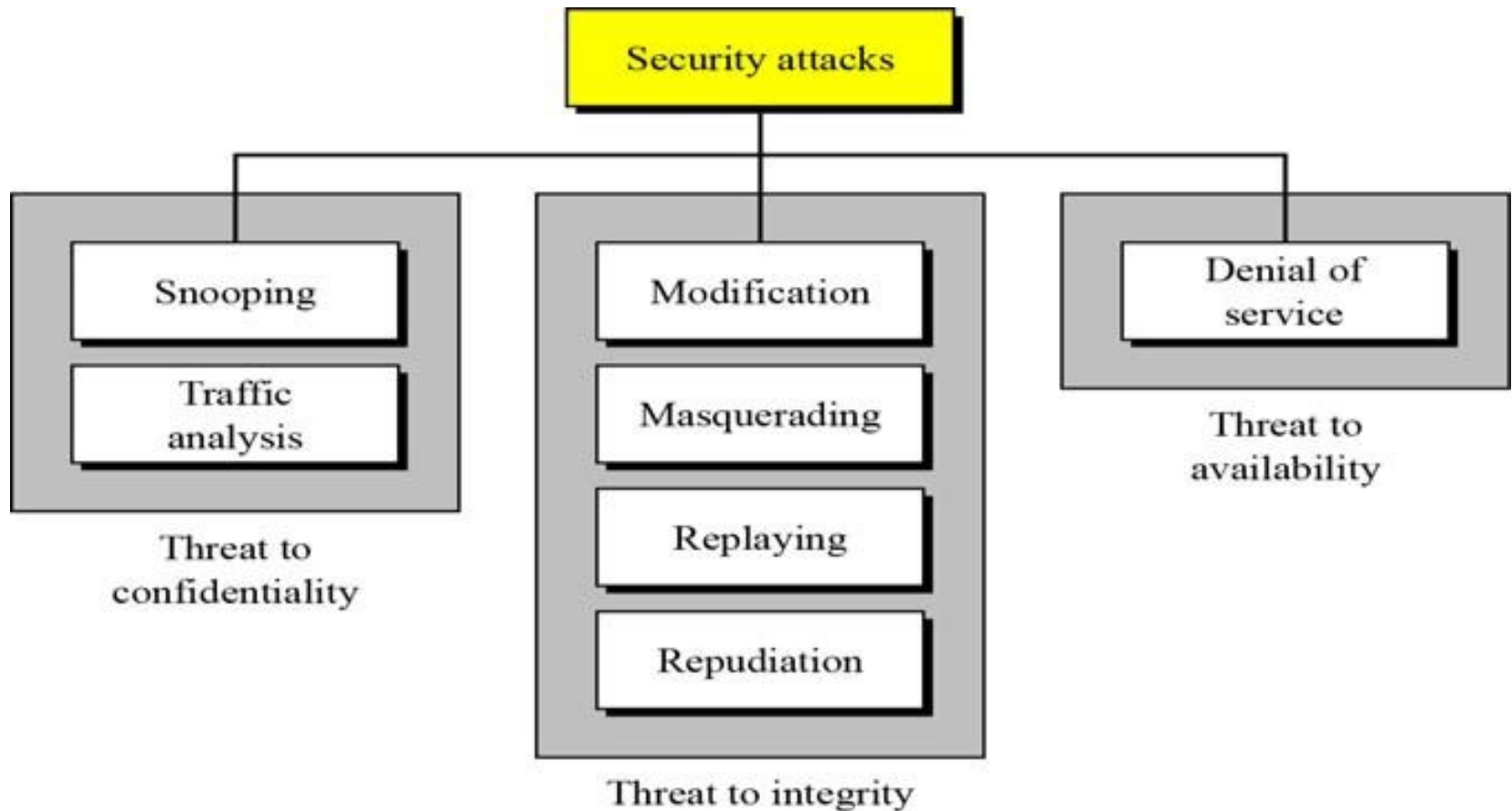
## ■ Hình thức Lừa đảo:

- Lừa đảo người lớn tuổi (rất thường xuyên): du lịch giá rẻ, cuộc gọi video giả hình( Deepfake), giả giọng (Deep Voice), ...
- Dẫn dụ trẻ em: Tuyển người mẫu nhí, Rao bán hàng giả, ...
- Lừa đảo sinh viên, thanh niên: Lừa đảo đầu tư chứng khoán, tiền ảo, đa cấp, ...
- Dẫn dụ công nhân, nhân viên văn phòng, người lập động: giả danh Cty tài chính cung cấp khoản vay lãi suất thấp, Việc nhẹ lương cao, ...

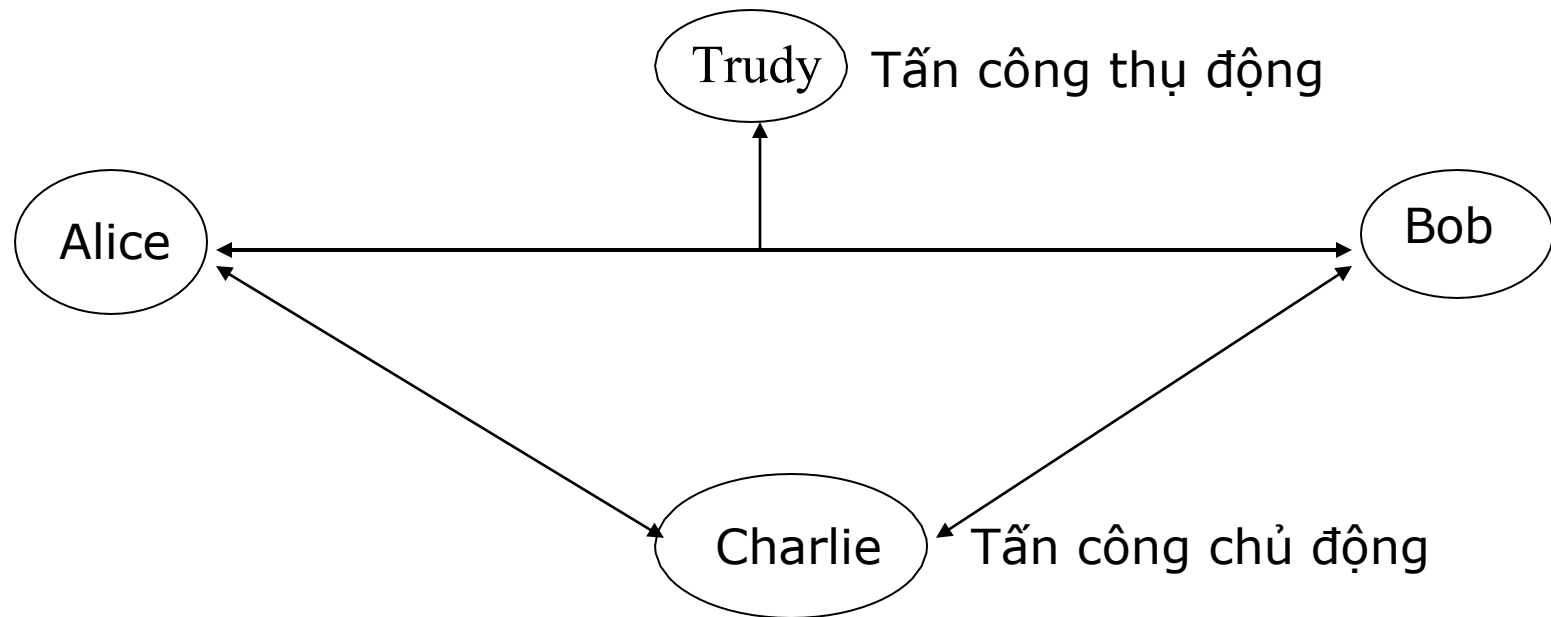
# Tấn công mạng

1. 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.

# Phân loại theo mục tiêu ATTT



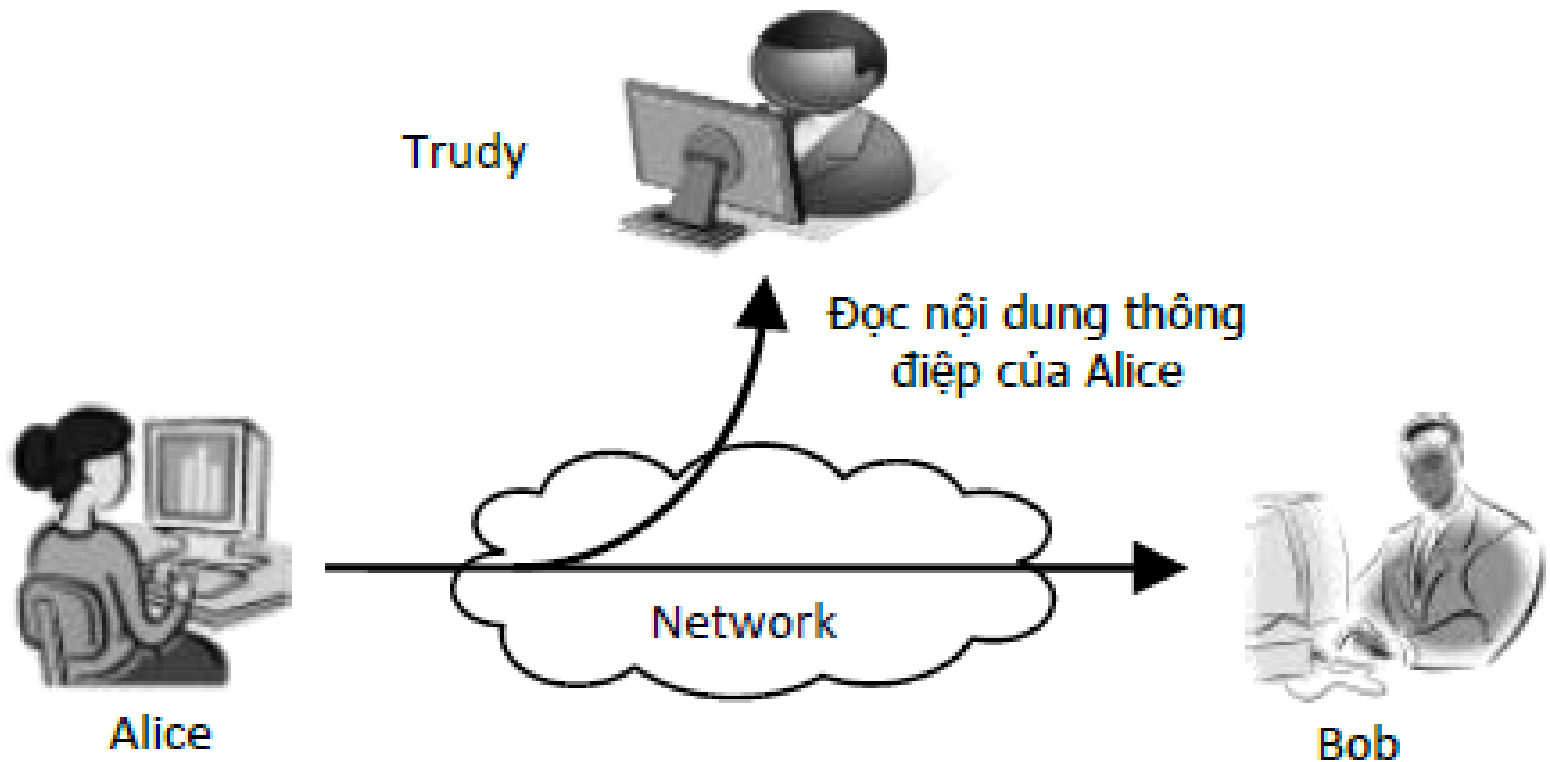
# Các kiểu tấn công an ninh





# Tấn công thụ động - Passive attacks

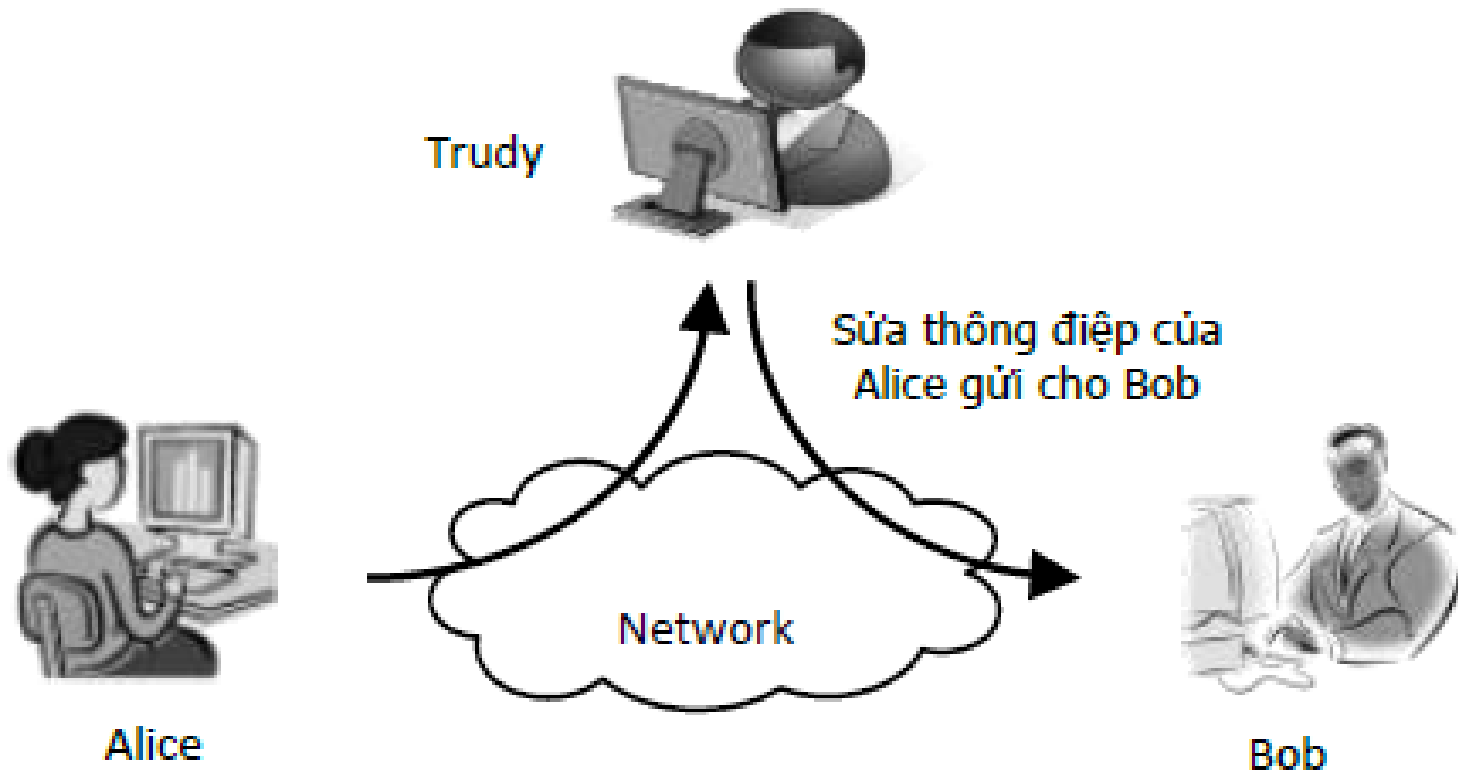
- 1) Release of Message Content
  - Xem trộm thông tin



## Tấn công thụ động - Passive attacks

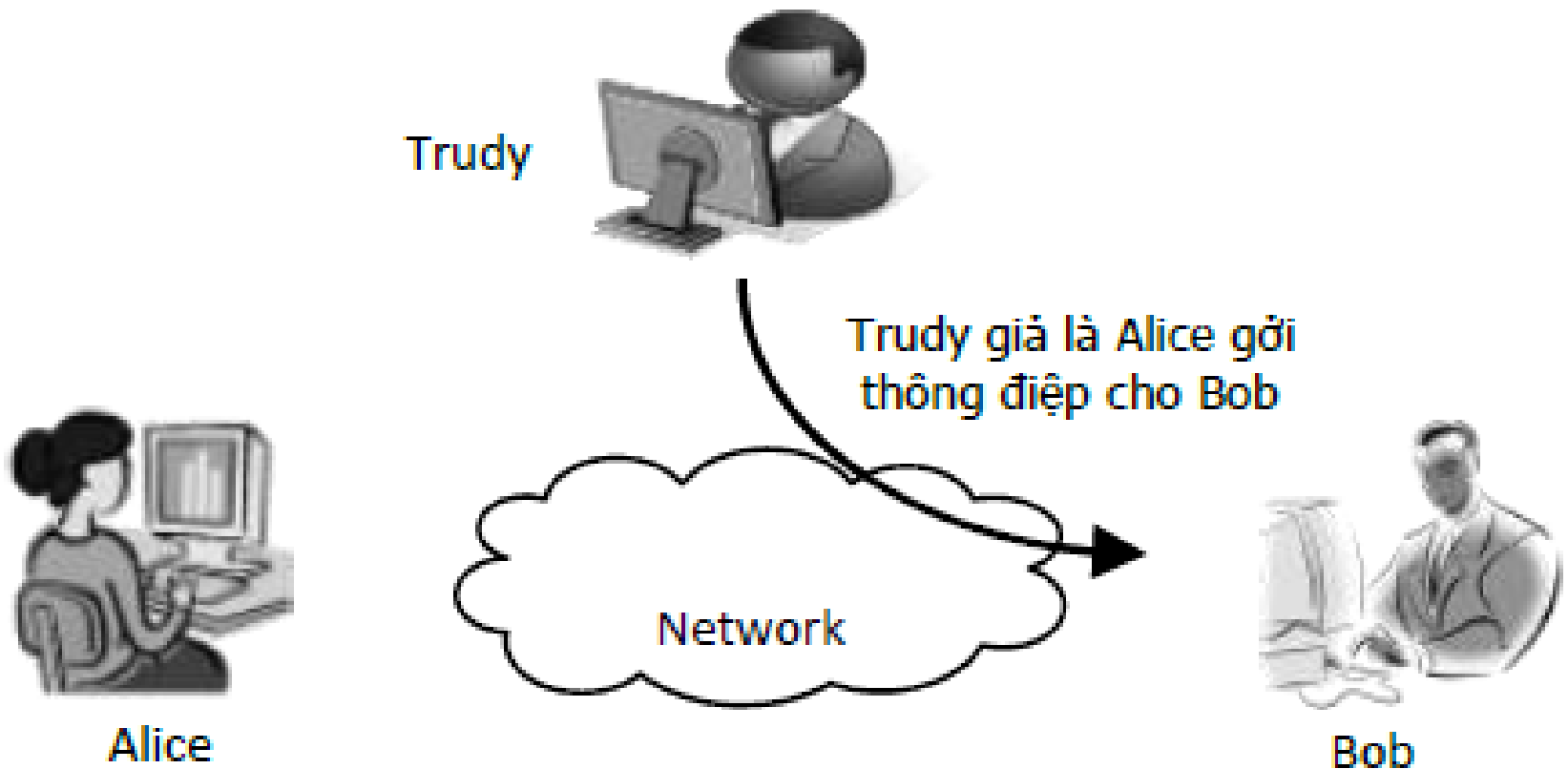
### 2) Modification of Message

- Thay đổi thông điệp



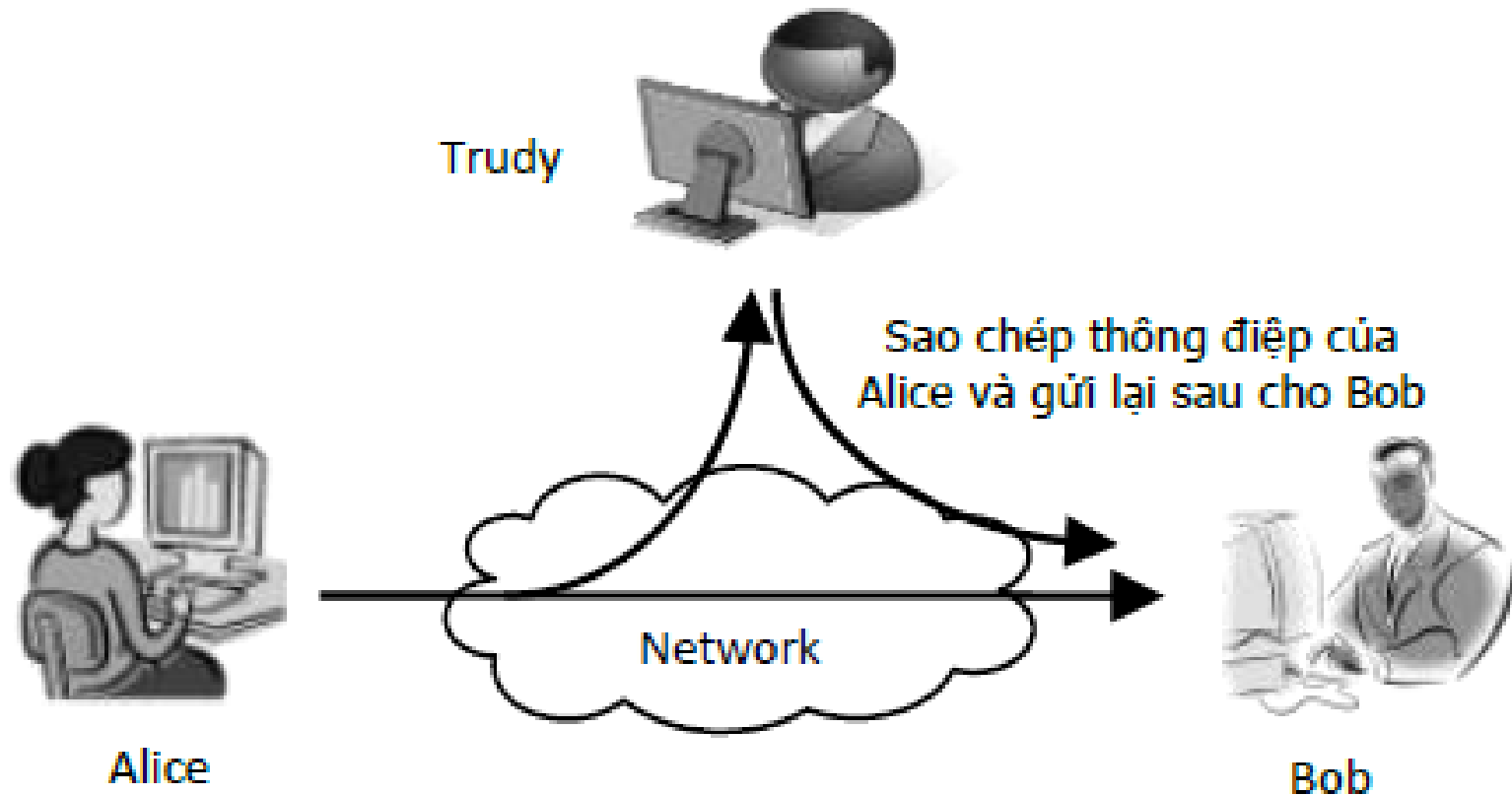
# Tấn công chủ động - **Active** attacks

## 3) Masquerade - Mạo danh



## Tấn công chủ động - Active attacks

### 4) Replay - Phát lại thông điệp





# Truy cập trái phép

- Truy cập trái phép là hình thức truy cập vào mạng máy tính, mạng viễn thông, máy tính cá nhân hoặc tài khoản cá nhân mà không được cấp quyền.
- Người truy cập trái phép sử dụng nhiều chiêu trò khác nhau:
  - Lỗ hổng bảo mật hoặc
  - Sử dụng phần mềm độc hại hoặc
  - Lừa đảo.



# Tấn công mã độc

- Tấn công mã độc (Malware = Malicious + Software) là phần mềm do các tin tặc hay các kẻ phá hoại tạo ra nhằm phá hoại hệ thống máy tính.
- Mã độc gồm: Virus và Sâu máy tính.
  - Virus: đoạn code hoặc chương trình máy tính có thể lây lan trên máy tính để phá hoại.
  - Sâu máy tính: chương trình máy tính chứa phần mềm độc hại có thể tự sao chép và tự lây lan trên mạng.




# Hệ thống lọc phần mềm độc hại

- Hệ thống phần cứng: Kiến trúc kết nối chuẩn các máy tính, thiết bị mạng kết hợp thiết bị phát hiện vi phạm kết nối.
  - Hệ thống phần mềm: phần mềm chạy trên mạng để phát hiện, ngăn chặn và thống kê các phần mềm độc hại.
  - Ví dụ: IDS, Firewall, Honeynet.
-

# Xâm nhập hệ thống

- Tương tác với người dùng:
  - Tải tệp đính kèm email và mở tệp,
  - Truy cập đường link lạ và nhấn nút Like,
  - Cắm USB và sao chép dữ liệu,...
- Không cần tương tác với người dùng:
  - Khai thác lỗ hổng hệ điều hành, lỗi phần mềm, chẳng hạn: Buffer Overflow trong phần mềm Họp trực tuyến.
  - Cài cấy chip gián điệp trên thiết bị phần cứng, ...





# Phòng chống Tấn công mạng



# Dấu hiệu bị nhiễm mã độc

- Khởi động chậm có nhiều cửa sổ hiện lên rồi tắt ngay.
  - Máy tính chạy chậm luôn trong tình trạng cạn kiệt tài nguyên.
  - Kết nối Internet chậm hoặc tự động kết nối tới Domain/IP lạ.
  - Có tập tin lạ hoặc các tập tin có dấu hiệu bị sao chép.
  - Xuất hiện thông báo: Tường lửa hoặc phần mềm Antivirus bị vô hiệu hóa.
-



# Xử lý khi bị nhiễm mã độc

- Ngắt kết nối mạng, cô lập thiết bị bị nhiễm.
  - Lưu trữ bằng chứng.
  - Phòng ngừa tấn công tái phát.
  - Cài đặt lại hệ điều hành.
-



# Phòng chống lây nhiễm mã độc

- Luôn cập nhật Hệ điều hành hoặc phần mềm lên phiên bản mới
  - Cân nhắc sử dụng phần mềm Antivirus miễn phí hay có trả phí.
  - Không mở tập tin khi chưa cân nhắc kỹ.
-