TRƯỜNG ĐẠI HỌC NGUYỄN TẤT THÀNH
KHOA CÔNG NGHỆ THÔNG TIN

AN TOÀN THÔNG TIN

information security

Giảng Viên: ThS. Nguyễn Thị Phong Dung
ntpdung@ntt.edu.vn

Chương II. Mối đe dọa & Các kiểu tấn công

I. Chức năng của ATTT

II. Các mối đe dọa

III. Các kiểu tấn công

I. Chức năng của ATTT

Chức năng:

- **Bảo vệ các tính năng hoạt động của tổ chức**

Chức năng của doanh nghiệp

- **Bảo vệ sự thu thập và sử dụng dữ liệu**

An toàn dữ liệu

- **Tạo điều kiện cho hoạt động an toàn của các ứng dụng**

Phần mềm, ứng dụng, website

- **Bảo vệ tài sản công nghệ của tổ chức**

PC, Server, router, ...

I. Chức năng của ATTT

Khái niệm

Nguy cơ (Threat)	• Thất lạc – Đánh cắp – Phá hủy
Lỗ hổng (Vulnerability)	• Off firewall, không cài CT virus
Rủi ro (Risk)	• Khả năng nguy cơ xảy ra
Tấn công (Attack)	• Biến nguy cơ thành hiện thực
Đối tượng nguy cơ (Threat Agent)	• Người tấn công

I. Chức năng của ATTT

Ví dụ:

- Công ty phần mềm Trí Tuệ Trẻ triển khai phần mềm quản lý nhà hàng – café cho quán café Cát Đằng trên đường Trần Hưng Đạo.

Hãy xác định các **Threat, Threat Agent, Vulnerability, Risk** và **Attack** có thể xảy ra đối với hệ thống.

II. Các mối đe dọa

1. Xâm phạm tài sản trí tuệ

- *Hành vi cạnh tranh không lành mạnh*
- *Hành vi xâm phạm quyền sở hữu trí tuệ*

II. Các mối đe dọa

2. Software attacks

- Virus
- Worms
- Trojan Horses
- Back Door or Trap Door
- Polymorphic Threats
- Virus and Worm Hoaxes

II. Các mối đe dọa

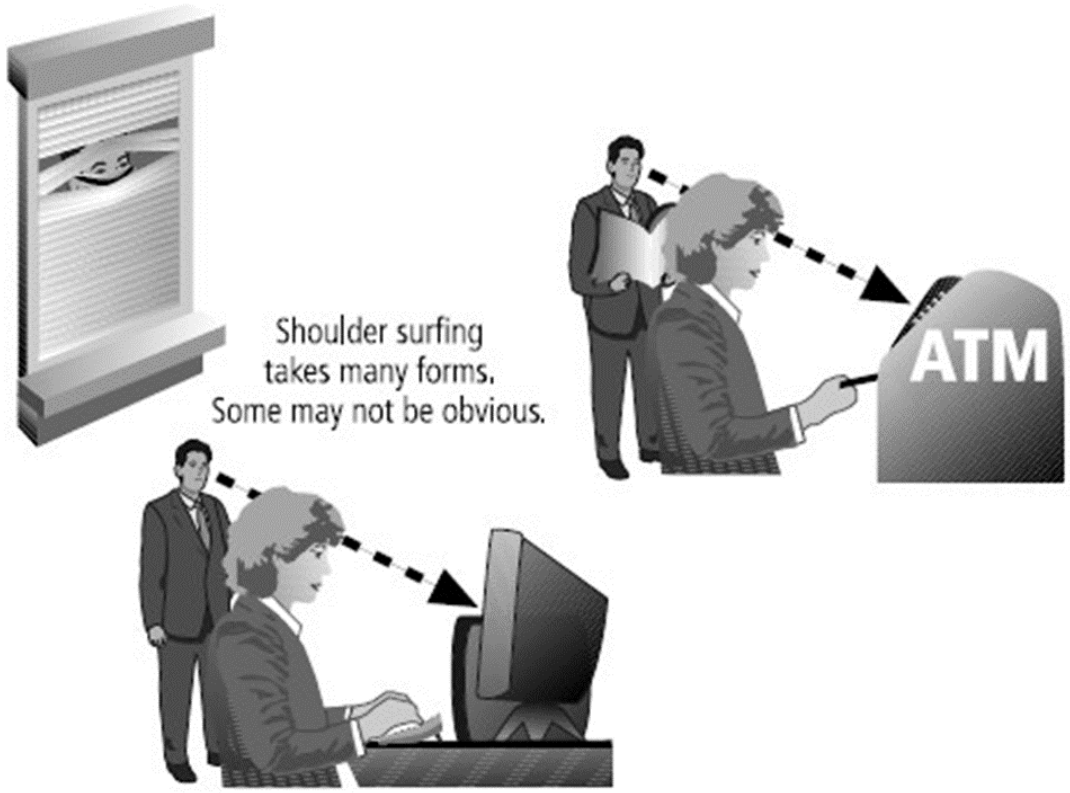
3. Sai lệnh về QoS (quality of service)

- Các vấn đề về Internet dịch vụ
- Liên lạc thông tin và các vấn đề khác của nhà cung cấp dịch vụ
- Vấn đề bất thường

II. Các mối đe dọa

4. Gián điệp hoặc xâm phạm

- Espionage
- Trespass



II. Các mối đe dọa

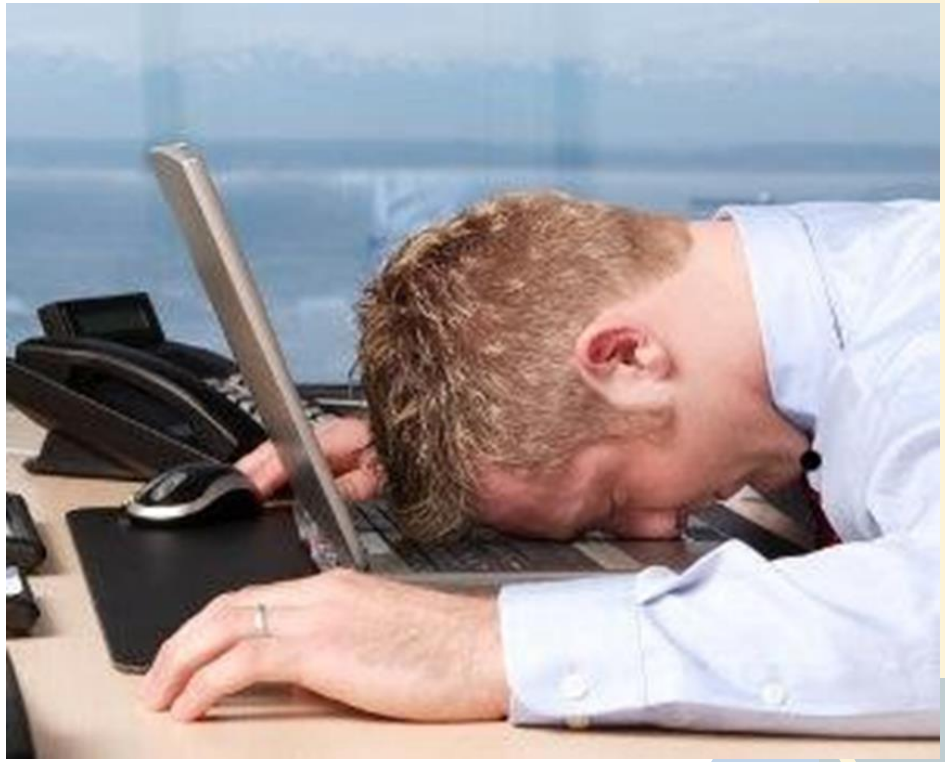
5. Ảnh hưởng của tự nhiên

Forces of nature

II. Các mối đe dọa

6. Lỗi do con người hay thất bại

Human error or failure



II. Các mối đe dọa

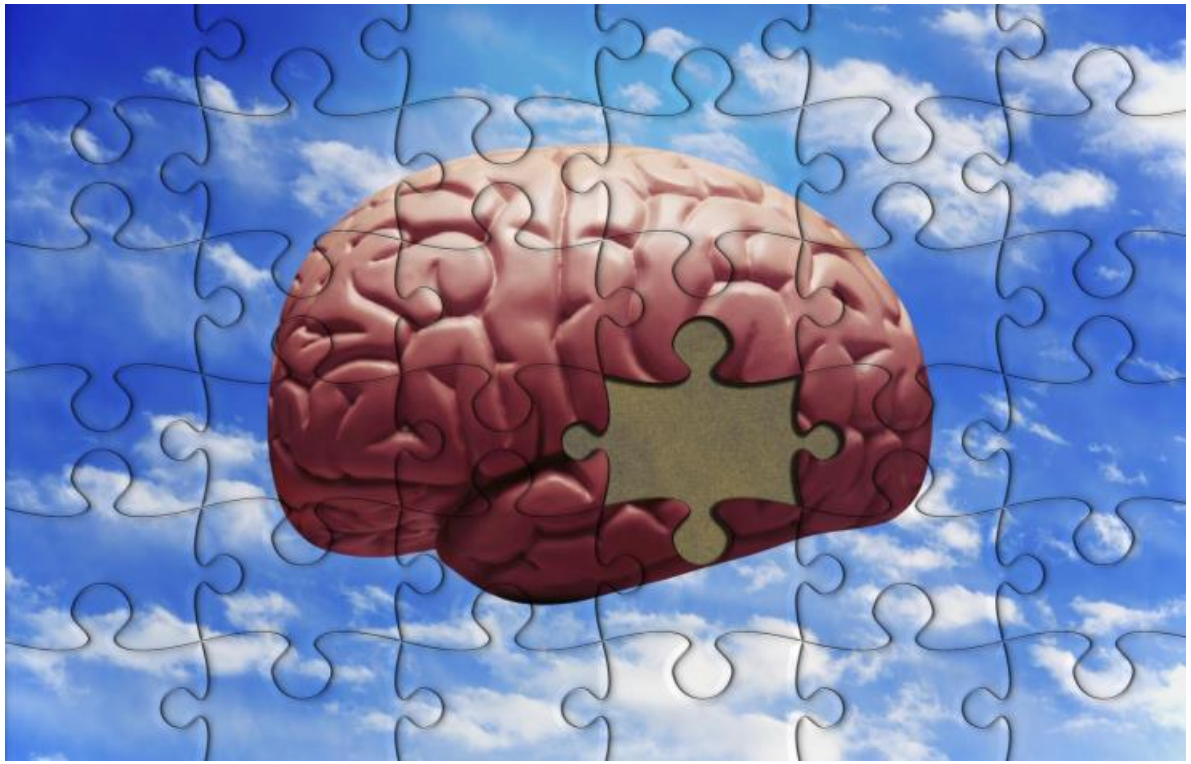
7. Thông tin tống tiền

Information extortion

II. Các mối đe dọa

8. Thiếu, không đủ hoặc không đầy đủ

Missing, inadequate, or incomplete



II. Các mối đe dọa

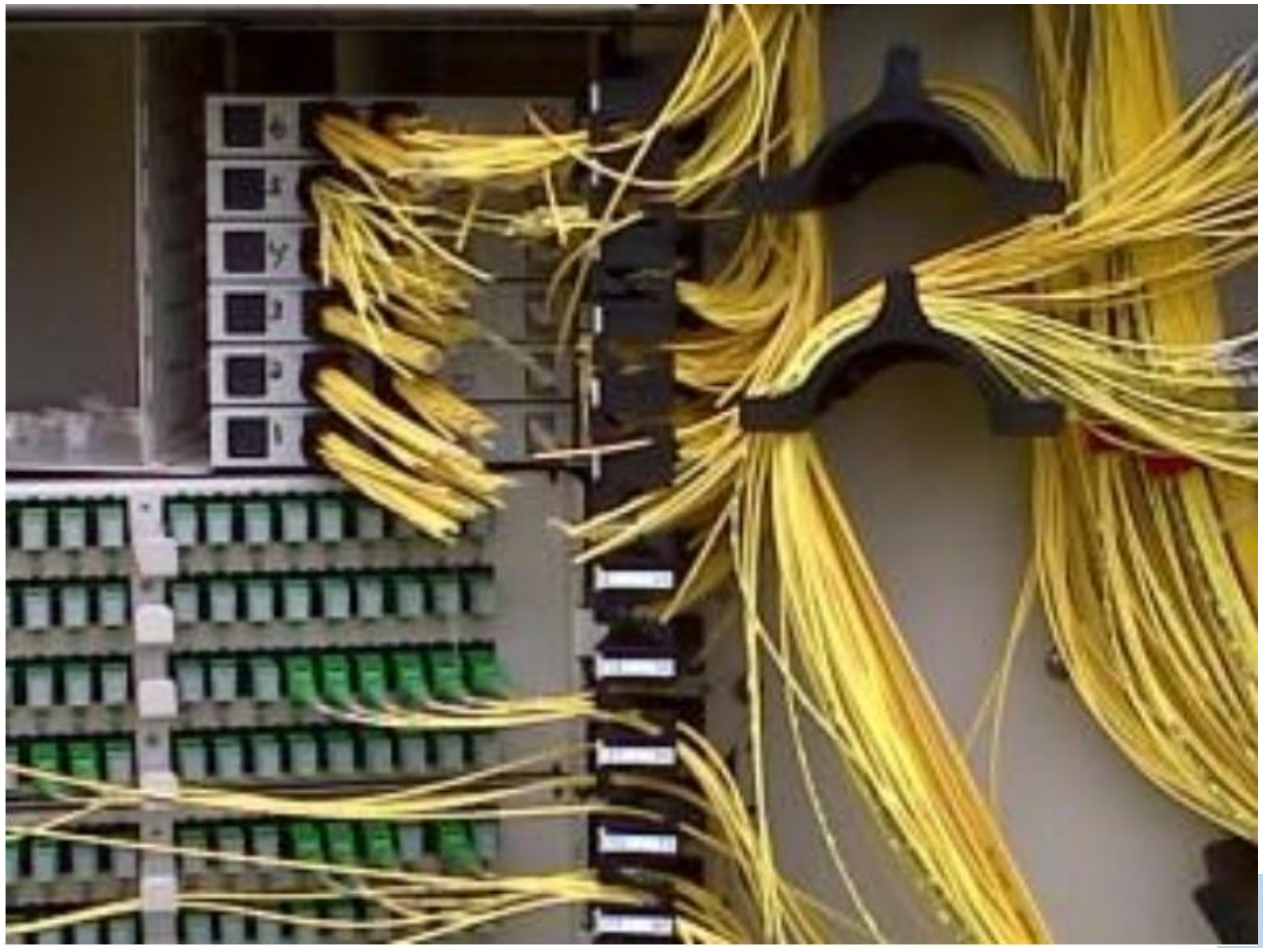
9. Thiếu kiểm soát chặt chẽ

Missing, inadequate, incomplete controls

II. Các mối đe dọa

10. Sự sụp đổ hoặc phá hoại hệ thống

Sabotage or vandalism



II. Các mối đe dọa

11. Trộm, cắp

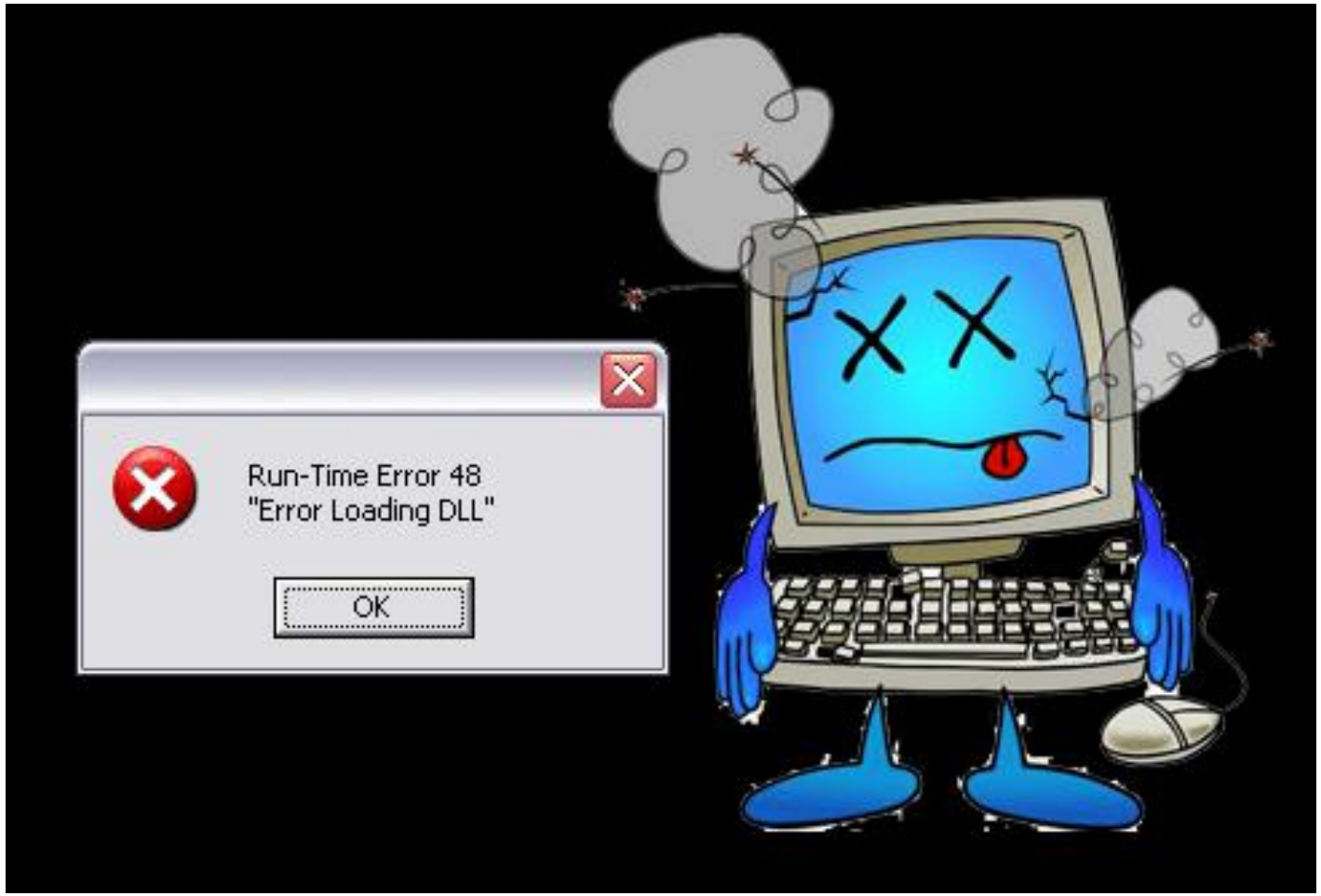
Theft

12. Lỗi hoặc lỗi kỹ thuật phần cứng

Technical hardware failures or errors

13. Lỗi hoặc lỗi kỹ thuật phần mềm

Technical software failures or errors



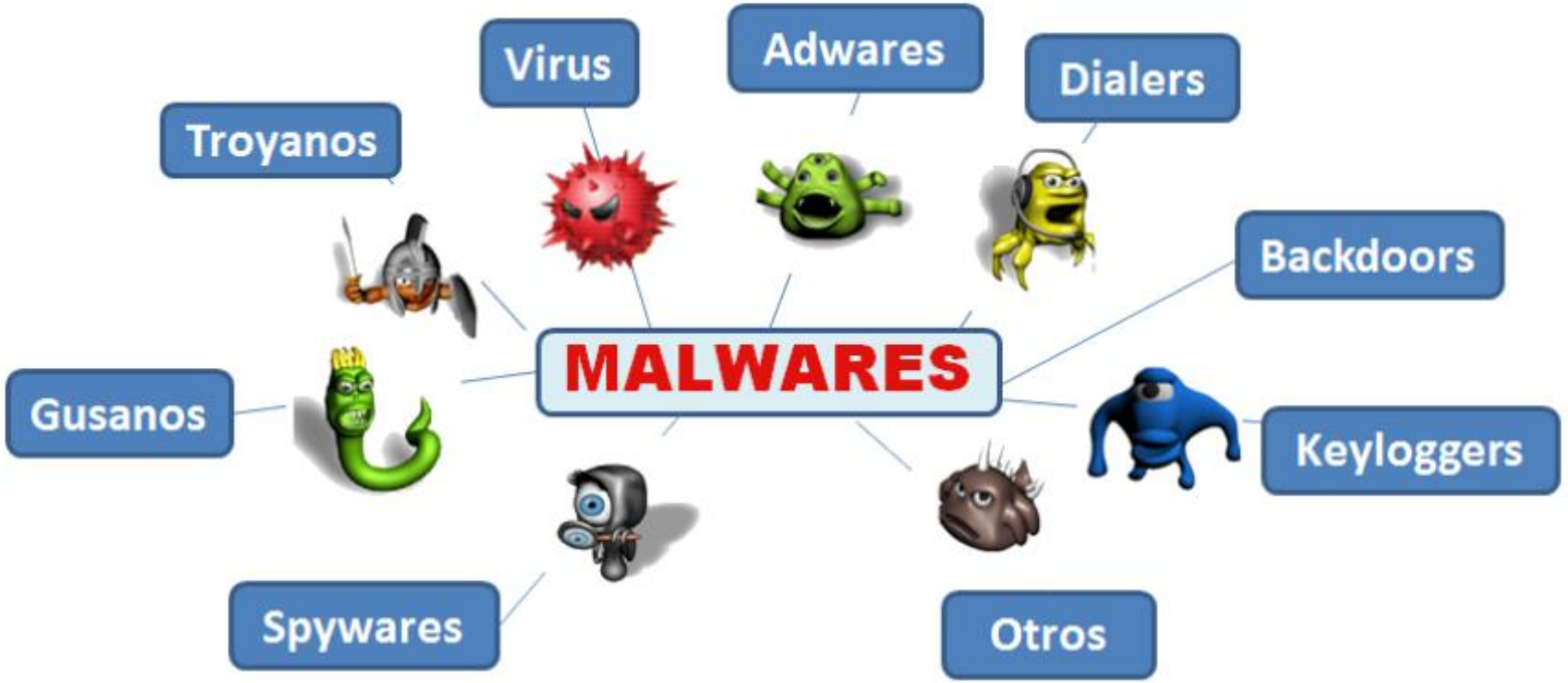
II. Các mối đe dọa

14. Lạc hậu về công nghệ

Technological obsolescence

III. Các kiểu tấn công (Thuyết trình Nhóm)

Destroy or steal information (Phá huỷ hoặc đánh cắp thông tin).



1. Malicious Code – Mã độc

❖ Spyware

- **Phần mềm gián điệp**
- **Thu thập thông tin**
  - Không thông qua chủ máy
  - Cài theo phần mềm miễn phí (Freeware) hoặc phần mềm chia sẻ (shareware)
  - Lấy thông tin – chuyển thông tin đi
  - Biến thể của phần mềm quảng cáo (adware)
- **Spyware điển hình**
  - WildTangent, Xupite, DoubleClick, WinWhatWhere, Gator và Wallet

1. Malicious Code – Mã độc

❖ Spyware

Phòng chống

- Thường gặp trong windows
- Không crack
- Update win
- Phân quyền người dùng
- Safe mode -> restore
- Đọc kỹ licence mỗi khi cài phần mềm
- Tránh xa các trang web quảng cáo
- Sử dụng phần mềm quét spyware

1. Malicious Code – Mã độc

❖ Virus

- Tự nhân bản
- Sao chép chính nó vào đối tượng lây nhiễm

1. Malicious Code – Mã độc

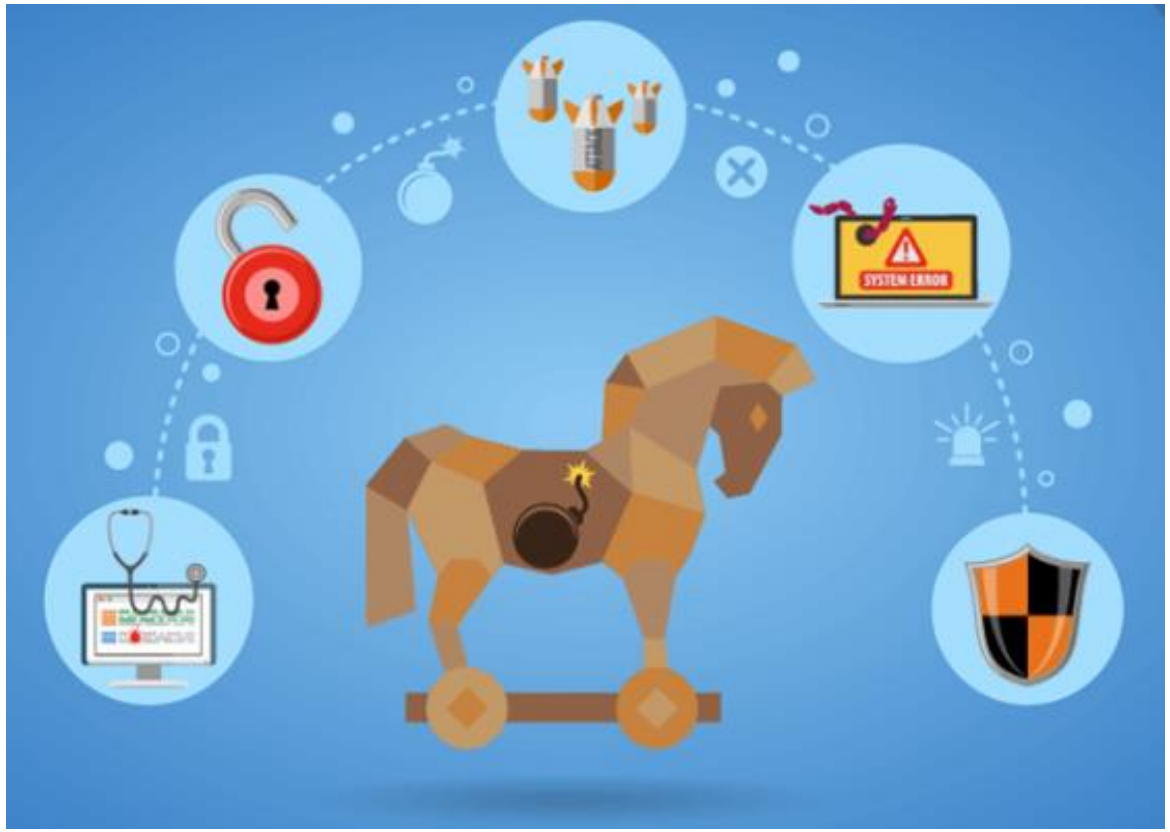
❖ Worm

- Sâu máy tính
- Là một spyware
- Tự nhân bản
- Chương trình độc lập # Virus
- Lây lan cùng hệ điều hành, cùng mạng -> phá hoại
- Mang theo phần mềm gián điệp – mở cửa hậu
- Định dạng khác của sâu:

  Sâu thư, bạch tuộc (octopus), Thỏ (rabbit)

1. Malicious Code – Mã độc

❖ trojan horse



- Là một malware
- Không tự nhân bản # virus
- Phần mềm độc lập
- khả năng phá hoại như virus
- Ẩn mình dưới một chương trình hữu ích

1. Malicious Code – Mã độc

❖ Adware

- Phần mềm quảng cáo
- Thường không độc hại
- Gây khó chịu
- Đôi khi làm tràn màn hình điều khiển

1. Malicious Code – Mã độc

❖ Keylogger

- Theo dõi bàn phím
- Trộm thông tin

1. Malicious Code – Mã độc

❖ Ransomware

- Phần mềm tống tiền
- Mã hóa dữ liệu cá nhân -> đòi tiền chuộc

1. Malicious Code – Mã độc

❖ Rootkit

- Cài đặt trong nhân hệ điều hành
- Che giấu các tiến trình đang chạy
- Ẩn danh như một driver

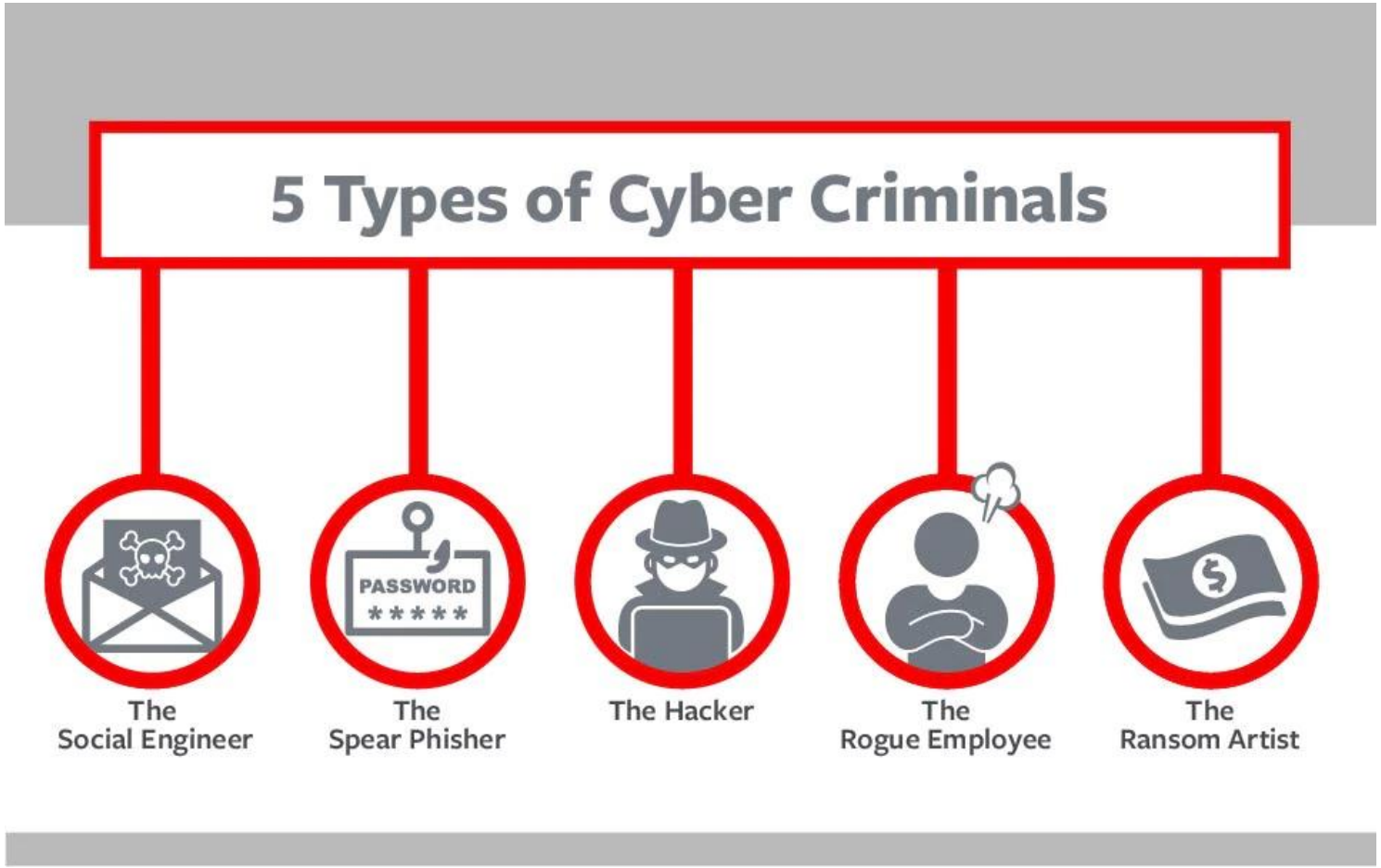
1. Malicious Code – Mã độc

❖ Phishing

- Lừa đảo
- Giả mạo một doanh nghiệp đáng tin cậy

List of computer criminals

https://en.wikipedia.org/wiki/List_of_computer_criminals



2. Hoaxes – Lừa đảo

- Image
- Message
- Tương tự phishing
- **Ví dụ:** googledrump

3. Back Doors - Cửa Sau

- Lỗ hổng thiết kế hệ thống
- Lỗ hổng người quản trị
- Bỏ qua chứng thực người dùng

→ trap door (Mở 1 cổng và truy cập từ xa)

4. Password Crack

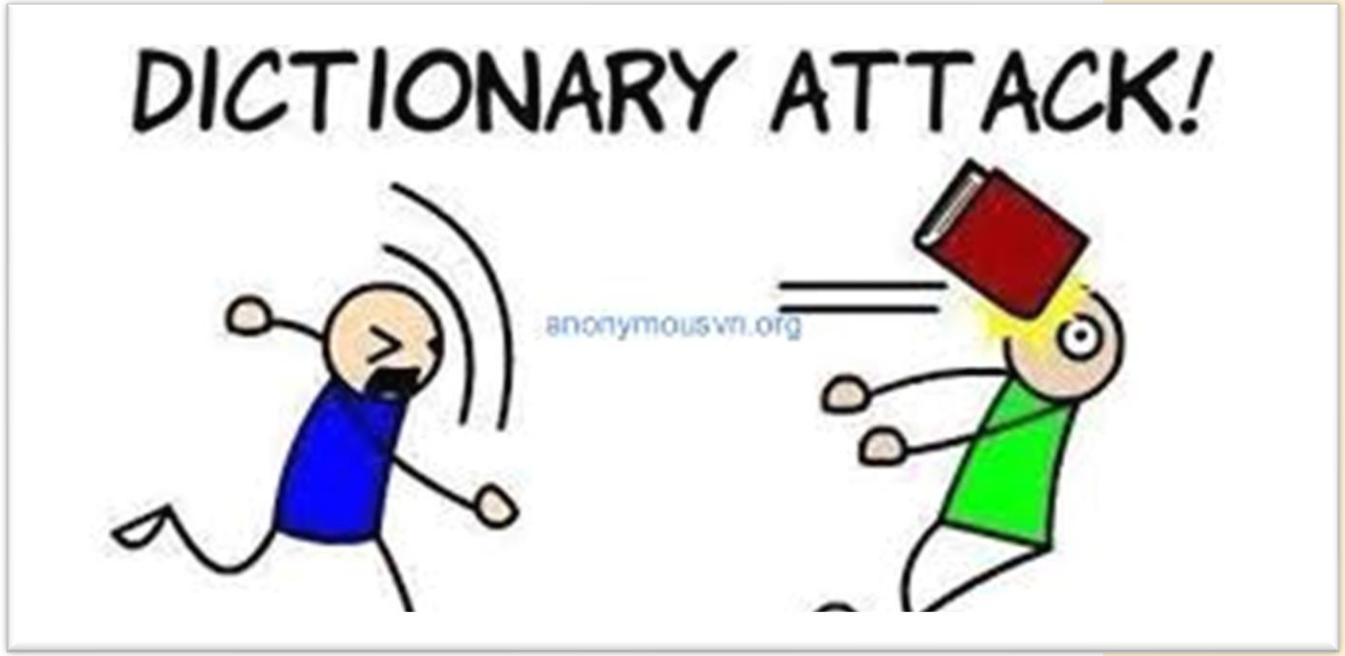
- Dictionary (Sử dụng từ điển làm wordlist)
- Hash mật khẩu sử dụng cùng một thuật toán
- Show Password
- Cookie
- Relogin/ URL

5. Brute Force

- Thử mọi tình huống có thể
- Brute Force Attack (hay còn gọi là Brute Force) là hình thức tấn công (hack) cổ điển phổ biến nhất.
- Đây chính là hình thức dò mật khẩu và tài khoản của người quản trị cao nhất.

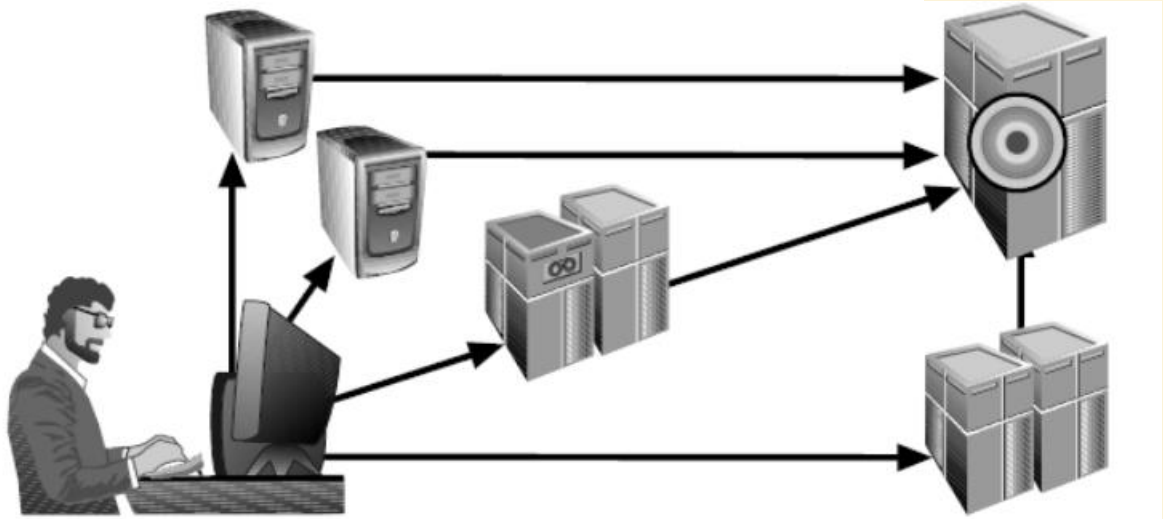
6. Dictionary

- Danh sách mật khẩu thường được sử dụng
- Dictionary attack là một kĩ thuật giúp máy tính có thể bẻ khóa được các cơ chế mã hóa hoặc cơ chế xác thực hoặc mật khẩu (password).

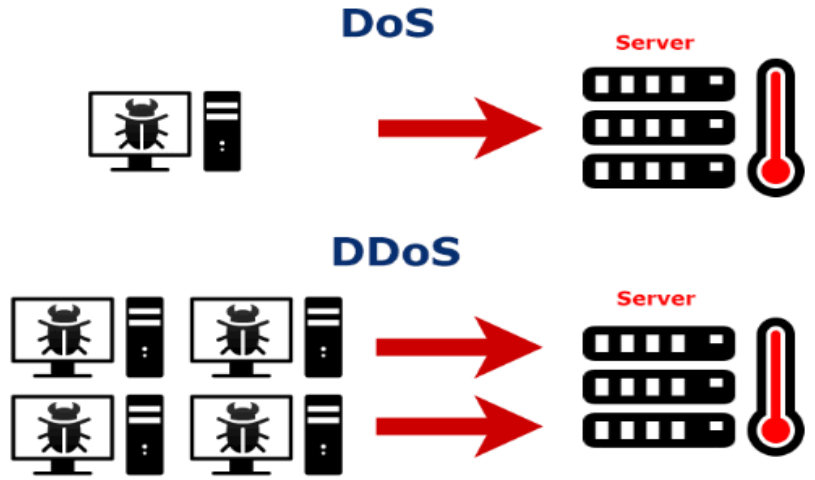


7. DoS, DDos

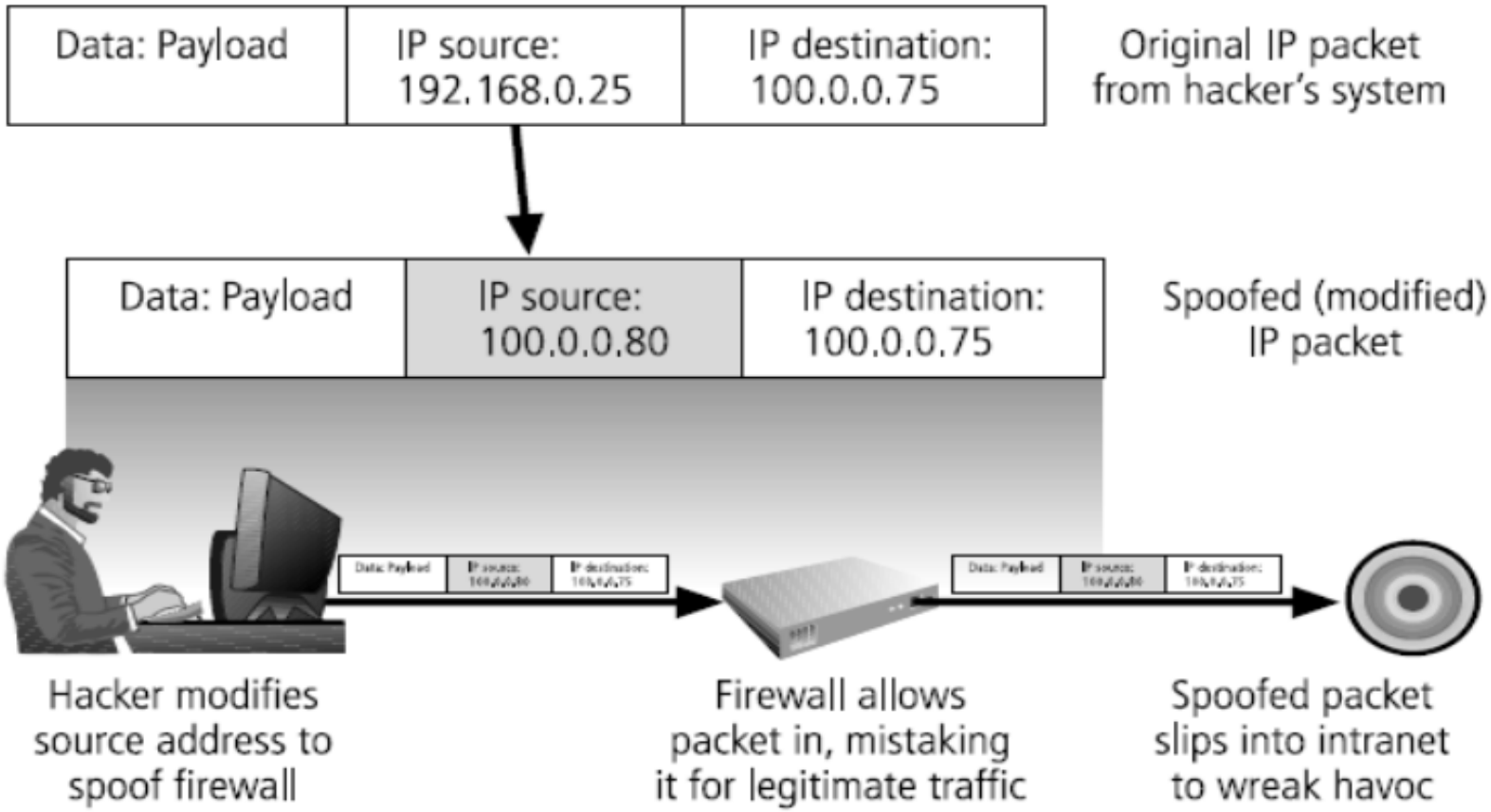
- **DoS** (Denial of Service):từ chối dịch vụ.
- Tấn công từ chối dịch vụ DoS là cuộc tấn công nhằm làm sập một máy chủ hoặc mạng, khiến người dùng khác không thể truy cập vào máy chủ/mạng đó.



- **DDoS** (Distributed Denial of Service): từ chối dịch vụ phân tán.
- Tấn công DDoS là nỗ lực làm sập một dịch vụ trực tuyến bằng cách làm tràn ngập nó với traffic từ nhiều nguồn.



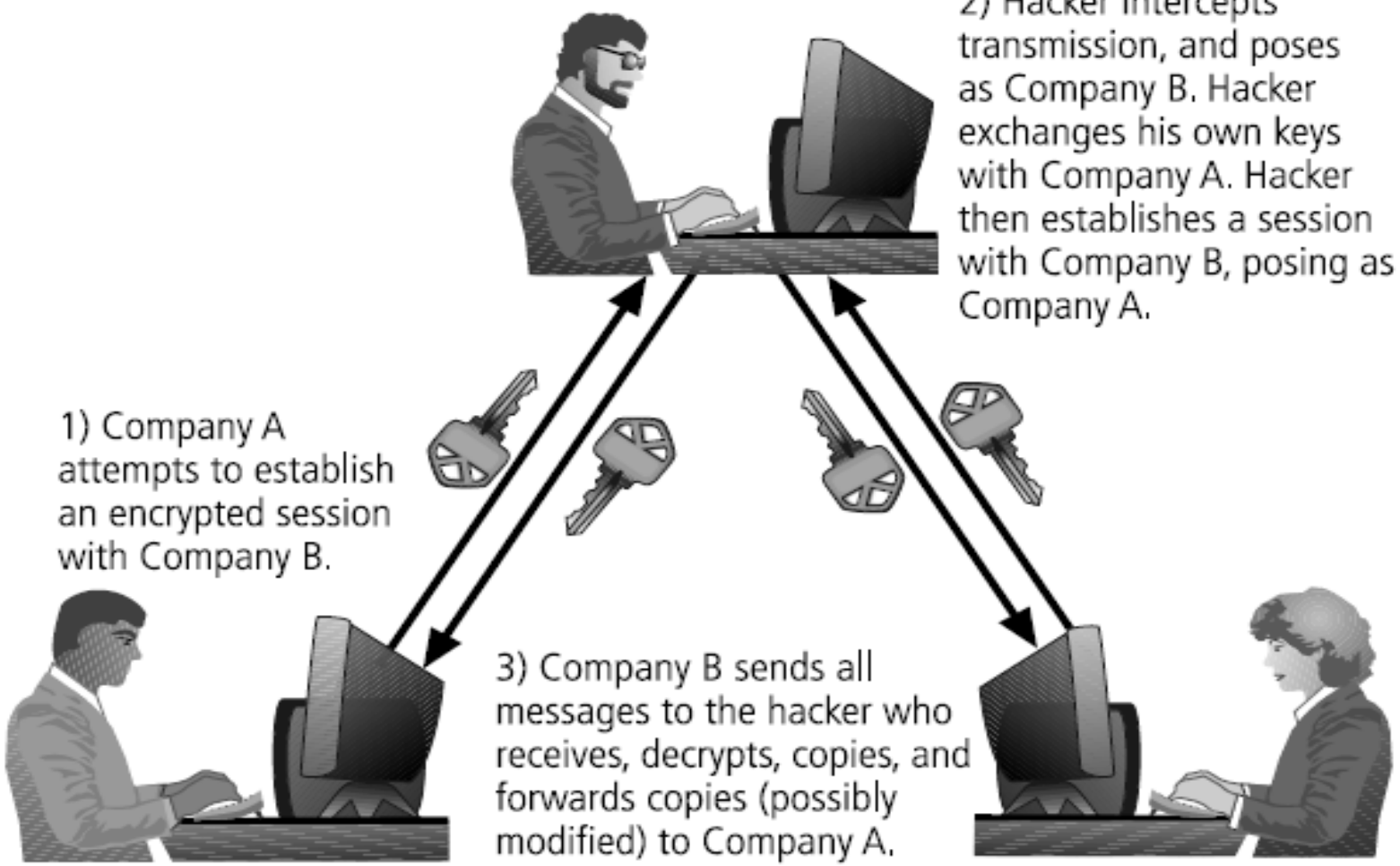
8. Spoofing



- Thay đổi địa chỉ IP
- Route, firewall thế hệ mới có thể ngăn chặn

9. Man-in-the-Middle

- Kẻ tấn công giám sát (hoặc đánh hơi) các gói từ mạng, sửa đổi chúng và chèn họ trở lại mạng



10. Spam

Stupid - Pointless - Annoying – Messages

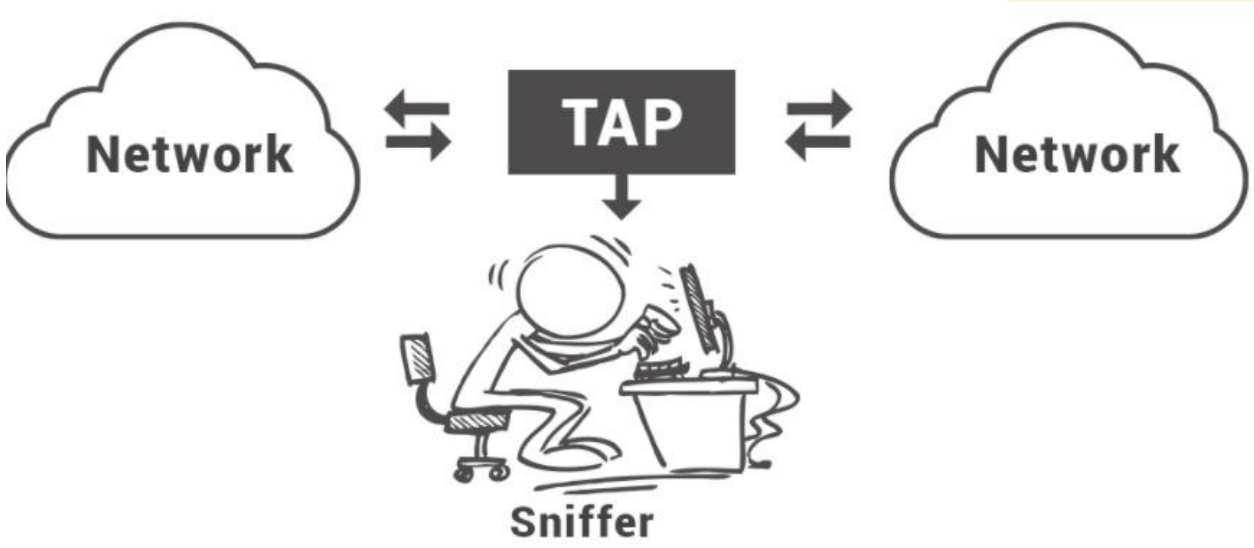
- Spam xuất hiện trên nhiều phương tiện như Spam chat, Spam tin tức, Spam tin nhắn, Spam trong các forum, Spam trên những mạng xã hội.
- **Spam** : những thông tin vô bổ, thiếu tính xác thực được phát tán rộng rãi khiến nhiều người cảm thấy khó chịu và không muốn nhận nó.

11. Mail Bombing – Bom Thư Điện Tử

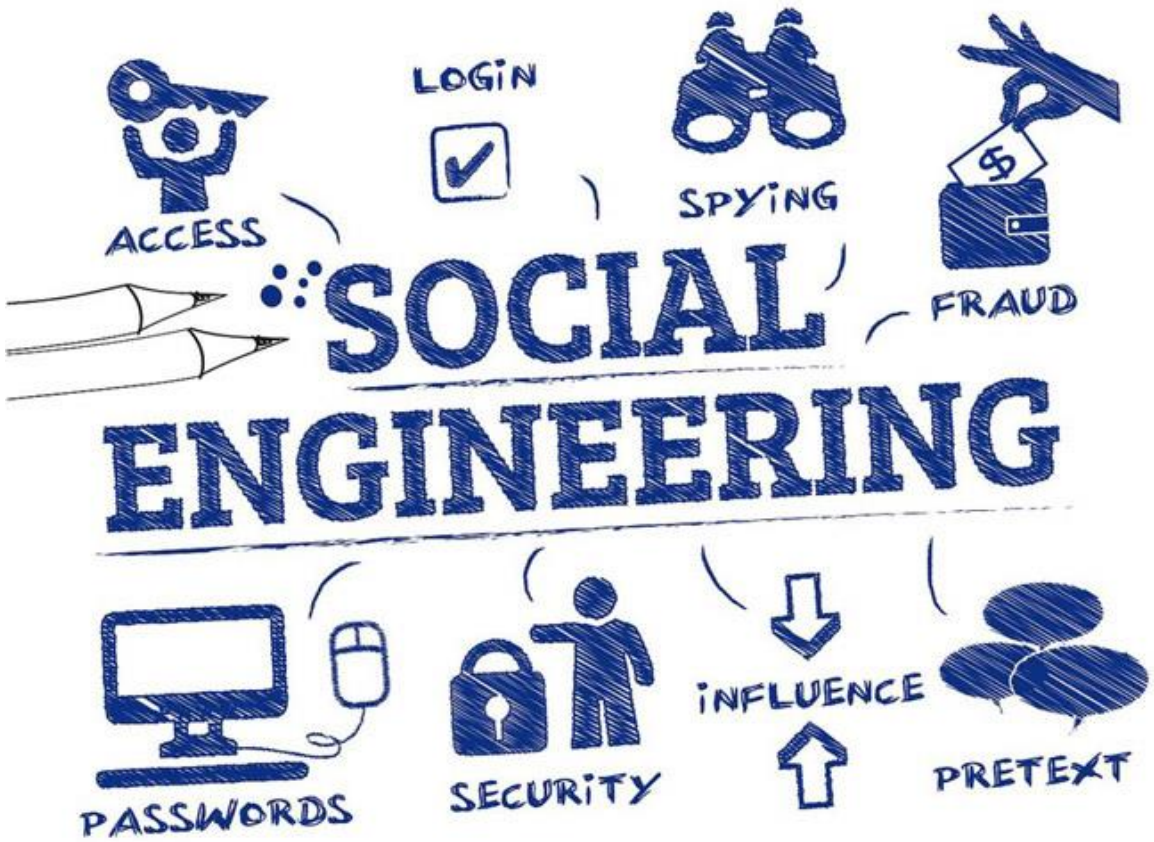
- DoS of email attack
- **Email boming** là các cuộc tấn công vào hộp thư (mail) của bạn bằng việc liên tục gửi một lượng lớn thư đến email
- Tin nhắn này thường có nội dung hoàn toàn vô nghĩa, nhưng thường sẽ là email xác nhận đăng ký và các email thông báo bảo mật

12. Sniffers

- Monitor data traveling over a network
- **Sniffer** là một công cụ phần mềm dùng để giám sát hoặc xem xét dữ liệu di chuyển qua lại giữa các liên kết trong mạng máy tính theo thời gian thực.
- Sniffer có thể là một chương trình phần mềm độc lập hoặc một thiết bị phần cứng tích hợp các phần mềm tương thích.



13. Social Engineering



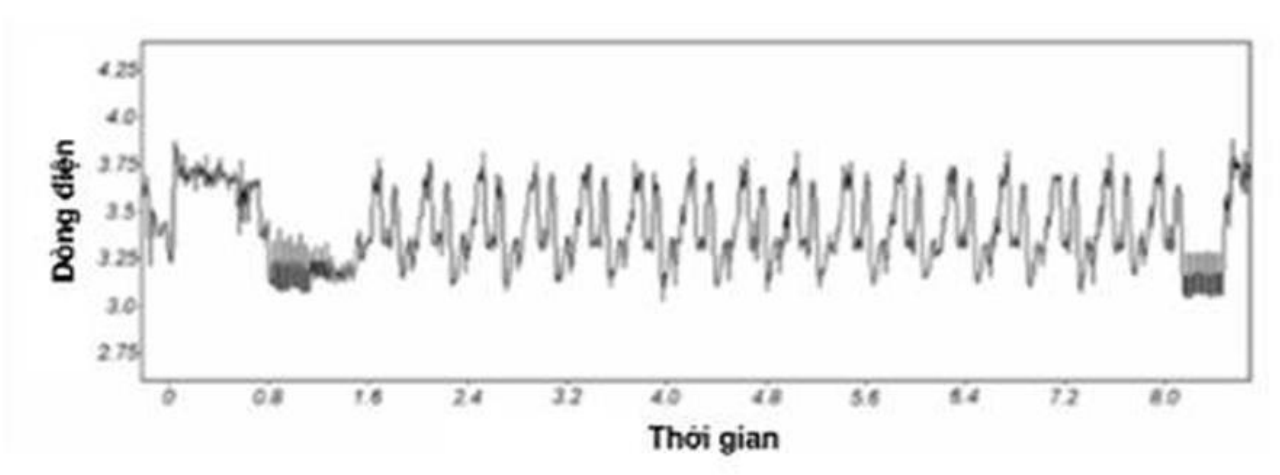
- **Social engineering** là nghệ thuật điều khiển mọi người để họ tiết lộ những thông tin bí mật.
- Sử dụng chiến thuật Social engineering vì tấn công điểm yếu của người dùng sẽ dễ hơn là hack phần mềm

14. Pharming

- **Pharming** là một loại tấn công mạng liên quan đến việc chuyển hướng lưu lượng truy cập web từ trang hợp pháp sang một trang giả mạo.
- Thường sử dụng Trojans, worms, or other virus
- Khai thác Domain Name System

15. Timing Attack

- Kẻ tấn công có thể biết chi tiết các hoạt động trong hệ thống mật mã và các tấn công là dựa vào các chi tiết hoạt động đặc biệt của hệ thống.
- Tìm hiểu nội dung bộ nhớ cache
- Lưu trữ cookie độc hại trên máy client



TÓM TẮT CHƯƠNG

1.Chức năng của ATTT

2.Các mối đe dọa

3.Các kiểu tấn công

Thanks.