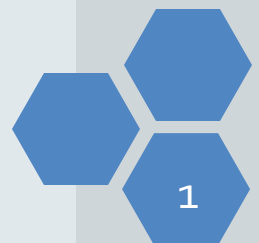




# CH9: Bảo mật và An toàn trong TMĐT

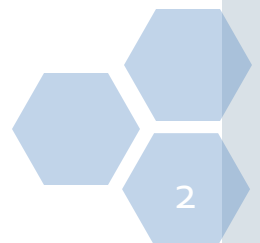
**Lương Trần Hy Hiến (HIENLTH)**





# Nội dung

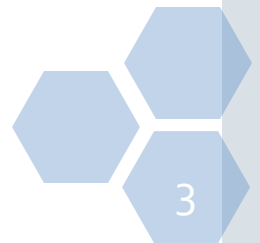
1. Các vấn đề cơ bản
2. Các loại đe dọa và tấn công TMĐT
3. Một số giải pháp đảm bảo an toàn TMĐT





# 1 - Các vấn đề cơ bản

- ❖ Virus máy tính
- ❖ Sâu máy tính (worms)
- ❖ Trojan
- ❖ Lừa đảo qua mạng (Phishing)
- ❖ Spam mail





# 1 - Các vấn đề cơ bản

## Hacking:

- Bị tấn công từ chối phục vụ (**Denial of Service**): hacker tự động gửi hàng loạt yêu cầu về server làm server này quá tải
- **Bị cướp tên miền:**
  - Tìm email quản lý tên miền
  - Lừa chủ tài khoản email để lấy được password
  - Yêu cầu nhà cung cấp dịch vụ quản lý tên miền cung cấp password để quản lý tên miền
  - Thay đổi thông số tên miền, chuyển tên miền sang website quản lý khác, thay đổi password quản lý,...



# 1 - Các vấn đề cơ bản

## Hacking:

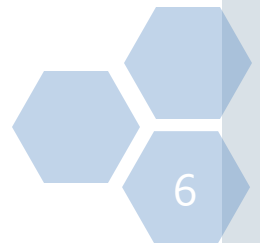
- **Bị xâm nhập dữ liệu trái phép:**
  - Tấn công nội bộ (local attack) tức hacker mua một host trên cùng một server với host “nạn nhân”
  - Tìm kẽ hở để đột nhập thông qua việc tìm kiếm trên các search engine
  - Tìm cách có được password của host
  - Nghiên cứu kẽ hở trong lập trình để thâm nhập vào host
  - Tham nhập vào cơ sở dữ liệu của website





# Giới thiệu

- ❖ Bảo mật, an ninh mạng là vấn đề **nóng hổi** trong hoạt động TMĐT
- ❖ Làm thế nào để khách hàng **tin tưởng** khi thực hiện các giao dịch trên mạng?
- ❖ Nhà cung cấp dịch vụ giao dịch trực tuyến + ISP có **đảm bảo** các giao dịch trên mạng được **an toàn**?





# Giới thiệu

- ❖ An toàn và bảo mật trên mạng có nhiều tiến triển
  - **Tường lửa** (firewall)
  - **Mã hóa** (encryption)
  - **Chữ ký điện tử** (digital signature)  
→ vẫn còn nhiều nguy cơ đe dọa
- ❖ **Điểm yếu** là ý thức và hành vi của người dùng
  - Đánh lừa người khác để lấy thông tin
  - Tấn công hay phá hoại thông qua lỗ hổng của HĐH
  - Mở thư đã bị nhiễm virus
  - Xem những trang web chứa 1 số đoạn mã có ý xấu





# Các vấn đề bảo mật

## ❖ Bảo mật trong EC

- **Authentication** – Chứng thực người dùng
  - Sự ủy quyền thông qua mật mã, thẻ thông minh, chữ ký
- **Authorization** – Chứng thực quyền sử dụng
- **Auditing** – Theo dõi hoạt động
- **Confidentiality (Privacy)** – Giữ bí mật nội dung thông tin
  - Mã hóa
- **Integrity** – Toàn vẹn thông tin
- **Availability** – Khả năng sẵn sàng đáp ứng
- **Nonrepudiation** – Không thể từ chối trách nhiệm
  - Chữ ký







## 2 – Các loại tấn công

### ❖ Không sử dụng chuyên môn

- Lợi dụng sức ép, tâm lý để đánh lừa người
- dùng và làm tổn hại đến mạng máy tính
- Hình thức
  - Gọi điện thoại, gửi mail, phát tán links

### ❖ Sử dụng chuyên môn

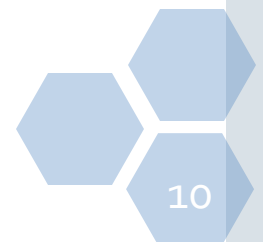
- Các phần mềm, kiến thức hệ thống, sự thành thạo
- Hình thức
  - DoS, DDoS
  - Virus, worm, trojan horse





## 2 – Một số mối đe dọa

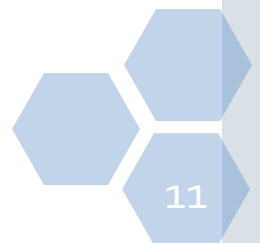
- ❖ Client
  - Hiện thị **nội dung**
  - Cung cấp các liên kết (**link**)
  - Plugin
- ❖ Internet
  - Sniffer
  - Backdoor
- ❖ Server
  - Quyền
  - Cookies
  - Database





## 3 – Giải pháp

- ❖ Chứng chỉ số
- ❖ Nghị thức SSL (Secure Sockets Layer)
- ❖ Mã hóa (Encryption)
- ❖ Chữ ký điện tử





# Thảo luận