**Bài 1:  
  
1. Keylogger là gì?**

Keylogger (viết tắt của *Keystroke Logger*) là một loại phần mềm hoặc thiết bị phần cứng được thiết kế để ghi lại mọi thao tác bàn phím của người dùng mà không có sự cho phép. Keylogger thường được tin tặc hoặc tổ chức giám sát sử dụng để thu thập thông tin nhạy cảm như mật khẩu, thông tin đăng nhập, số thẻ tín dụng và dữ liệu cá nhân khác.

#### ****2. Ứng dụng của Keylogger****

Keylogger có thể được sử dụng vào nhiều mục đích, cả hợp pháp và bất hợp pháp:

**Ứng dụng hợp pháp:**

* **Giám sát nhân viên:** Một số công ty sử dụng keylogger để theo dõi hoạt động làm việc của nhân viên nhằm nâng cao năng suất.
* **Giám sát con cái:** Phụ huynh có thể dùng keylogger để theo dõi hoạt động trực tuyến của con cái nhằm bảo vệ chúng khỏi nội dung xấu trên mạng.
* **Phân tích hành vi người dùng:** Một số nghiên cứu UX/UI có thể sử dụng keylogger để thu thập dữ liệu về hành vi nhập liệu nhằm tối ưu hóa trải nghiệm người dùng.

**Ứng dụng bất hợp pháp:**

* **Đánh cắp dữ liệu cá nhân:** Tin tặc sử dụng keylogger để lấy cắp thông tin đăng nhập ngân hàng, tài khoản mạng xã hội.
* **Theo dõi bất hợp pháp:** Keylogger có thể bị cài lén để giám sát người khác mà họ không hề hay biết.
* **Tấn công mạng quy mô lớn:** Một số phần mềm độc hại tích hợp keylogger để đánh cắp dữ liệu hàng loạt từ các tổ chức hoặc cá nhân.

### ****3. Phân biệt các loại Keylogger****

Keylogger có thể được chia thành hai loại chính: **Hardware Keylogger (Keylogger phần cứng)** và **Software Keylogger (Keylogger phần mềm).**

#### ****3.1. Hardware Keylogger (Keylogger phần cứng)****

**Định nghĩa:**  
Là các thiết bị vật lý được gắn vào bàn phím hoặc cổng USB để ghi lại dữ liệu đầu vào từ bàn phím.

**Đặc điểm:**

* Hoạt động độc lập, không cần cài đặt phần mềm.
* Không bị phát hiện bởi phần mềm diệt virus.
* Dữ liệu được lưu trữ trên bộ nhớ của thiết bị và có thể trích xuất sau đó.

**Ví dụ về Hardware Keylogger:**

* **USB Keylogger:** Một thiết bị cắm vào cổng USB giữa bàn phím và máy tính.
* **BIOS Keylogger:** Được tích hợp trực tiếp vào phần cứng của máy tính.
* **Wi-Fi Keylogger:** Gửi dữ liệu qua kết nối không dây đến hacker mà không cần phải trực tiếp lấy thiết bị.

**Cách nhận diện và phòng tránh:**

* Kiểm tra kỹ các thiết bị ngoại vi như cổng USB, bàn phím để phát hiện thiết bị lạ.
* Sử dụng bàn phím ảo khi nhập thông tin quan trọng.
* Kiểm tra BIOS nếu nghi ngờ bị theo dõi từ phần cứng.

#### ****3.2. Software Keylogger (Keylogger phần mềm)****

**Định nghĩa:**  
Là phần mềm độc hại hoặc tiện ích chạy ẩn trong hệ thống, ghi lại thao tác bàn phím và gửi dữ liệu về máy chủ của kẻ tấn công.

**Đặc điểm:**

* Hoạt động lén lút, có thể ẩn dưới dạng ứng dụng hợp pháp.
* Dễ dàng phát tán qua email, link độc hại, phần mềm bẻ khóa.
* Có thể ghi lại tổ hợp phím, chụp màn hình, quay video hoạt động trên máy tính.

**Ví dụ về Software Keylogger:**

* **Trojan Keylogger:** Lây nhiễm qua file đính kèm hoặc website giả mạo.
* **Hook-Based Keylogger:** Móc vào hệ thống Windows để ghi lại phím bấm.
* **Form-Grabbing Keylogger:** Đánh cắp dữ liệu từ các biểu mẫu nhập liệu trên trình duyệt.

**Cách nhận diện và phòng tránh:**

* Cài đặt phần mềm diệt virus và thường xuyên cập nhật hệ thống.
* Kiểm tra các tiến trình lạ trong Task Manager.
* Sử dụng bàn phím ảo hoặc phương thức xác thực hai yếu tố (2FA).
* Tránh tải phần mềm từ nguồn không rõ ràng.

### ****4. Cách phòng tránh Keylogger****

**Sử dụng phần mềm bảo mật:**

* Cài đặt **Windows Defender**, **Malwarebytes**, **Kaspersky**, hoặc các phần mềm diệt virus uy tín khác.
* Bật tính năng **chống keylogger** trên trình duyệt hoặc phần mềm bảo mật.

**Kiểm tra và bảo vệ phần cứng:**

* Kiểm tra bàn phím và cổng USB để phát hiện thiết bị đáng ngờ.
* Tránh sử dụng bàn phím công cộng hoặc máy tính lạ khi nhập thông tin quan trọng.

**Cẩn trọng khi tải phần mềm:**

* Chỉ tải phần mềm từ trang chính thức.
* Không mở file đính kèm email đáng ngờ.
* Tránh sử dụng phần mềm bẻ khóa (crack) vì có thể chứa keylogger.

**Sử dụng xác thực hai yếu tố (2FA):**

* Dùng ứng dụng xác thực như **Google Authenticator**, **Authy** thay vì nhập mật khẩu.

**Sử dụng bàn phím ảo:**

* Khi nhập thông tin quan trọng, sử dụng bàn phím ảo trên Windows (Win + R → "osk").

**Cập nhật hệ thống và phần mềm thường xuyên:**

* Cập nhật Windows, trình duyệt và phần mềm bảo mật để ngăn chặn các lỗ hổng bảo mật.

**Bài 2:**