**Bài lab 2**

**Họ và tên : Lê Hoàng Phúc**

**MSSV : 1050080153**

**Lớp : 10 CNPM2**

1. Nêu biện pháp phòng tránh; các cách phát hiện Keylogger trên máy tính - điện

thoại và minh họa nếu có thể.

- Keylogger thường rất hay xảy ra trên các thiết bị thông qua 2 đường chính là được cài đặt và bị cài đặt.

**Trong trường hợp được cài đặt Keylogger**

Phương pháp phòng chống này chỉ có tác dụng với hệ thống máy chủ (nắm quyền quản trị, nắm root), đó là bạn không để cho ai khác sử dụng chung thiết bị máy tính đó với bạn.

Tiến hành khóa lại các chương trình bảo vệ, đưa máy về trạng thái yêu cầu mật khẩu ngay tại lock screen mỗi khi bạn rời máy đi đâu đó. Trong trường hợp bắt buộc phải sử dụng chung thì bạn cần cấu hình cho user đó mức truy cập tối thiểu (ví dụ chỉ là tài khoản guest với WindowXP, chế độ user với [hệ điều hành Linux](https://bkhost.vn/blog/he-dieu-hanh-linux/)), kiểm soát tất cả phát sinh cài đặt của những tài khoản đó.

**Khi bị cài đặt Keylogger**

Trường hợp này xảy ra khi các kyelogger vào máy không do người nào đó trực tiếp đưa vào mà chúng được đưa thông qua các [mã độc](https://bkhost.vn/blog/malware-la-gi/), virus, [spyware](https://bkhost.vn/blog/spyware/), [trojan](https://bkhost.vn/blog/trojan-la-gi/),… một cách bạn không hề phát hiện ra. Hãy thực hiện các biện pháp phòng như sau:

* Không nên tùy ý mở các tập tin lạ, không rõ nguồn gốc (đặc biệt chú ý các tập tin có đuôi \*.exe, \*.com, \*.bat, \*.scr, \*.swf, \*.zip, \*.rar, \*.js, \*.gif…). Không biết thì tốt nhất là bạn nên xóa đi, hoặc quét qua các chương trình như Antivirus, Antispyware rồi mở sau nếu không thấy vấn đề gì.
* Không truy cập vào các trang web lạ, đặc biệt là web đen vì ở những web này luôn chứa các nguy cơ ẩn như worm, virus hay mã độc chỉ chờ bạn click vào.
* Không click vào các đường link lạ được ngẫu nhiên gửi.
* Không cài đặt các ứng dụng, chương trình lạ.
* Tránh tải các ứng dụng từ các trang web lạ, không đáng tin cây. Hãy kiểm tra chữ ký điện tử trước để kiểm tra xem chương trình có bị sửa đổi hay không.
* Không sử dụng các bản crack và cũng không nên dowload.
* Luôn active các chương trình bảo vệ thiết bị như chống virus, spyware và cả hệ thống [tường lửa](https://bkhost.vn/blog/firewall/).
* Thực hiện cập nhất [hệ điều hành](https://bkhost.vn/blog/he-dieu-hanh-os-operating-system/), ứng dụng thường xuyên để vá các lỗ hổng.
* Bạn cũng có thể dowload thêm các bản phần mềm chống keylog uy tín để nâng cao tính năng bảo vệ

**Tránh keylogger**

Khi nghi ngờ nó có keylogger mà không có điều kiện kiểm tra thì biện pháp tốt nhất bạn nên tránh những keylogger như thế này, vừa đỡ một mối nguy cơ có thể đe dọa giúp bạn yên tâm hơn nhiều

2. Tìm thêm và giới thiệu một số loại Keylogger trên máy tính và điện thoại khác.

**Hardware Keylogger (Keylogger phần cứng)**

* Là thiết bị vật lý gắn vào cổng USB hoặc bàn phím để ghi lại thao tác bàn phím.
* Ví dụ: **Keyllama USB Keylogger, AirDrive Keylogger**.

**Software Keylogger (Keylogger phần mềm)**

* Cài đặt trực tiếp trên hệ điều hành, có thể chạy ẩn và gửi dữ liệu từ xa.
* Ví dụ:
  + **Spyrix Free Keylogger** – Ghi lại bàn phím, clipboard, ảnh chụp màn hình.
  + **Elite Keylogger** – Chạy ẩn và gửi dữ liệu qua email.
  + **Revealer Keylogger** – Miễn phí, ghi lại phím bấm và lưu trữ cục bộ.

**Android Keylogger**

* Ứng dụng chạy nền, ghi lại thao tác bàn phím và gửi dữ liệu từ xa.
* Ví dụ:
  + iKeyMonitor – Theo dõi tin nhắn, bàn phím, chụp ảnh màn hình.
  + FlexiSPY – Ghi lại thao tác bàn phím, cuộc gọi, vị trí GPS.

**2️⃣ iOS Keylogger**

* Cần **Jailbreak** thiết bị để cài đặt phần mềm gián điệp.
* Ví dụ:
  + mSpy – Theo dõi tin nhắn, bàn phím, ứng dụng mạng xã hội.
  + Spyera – Ghi lại hoạt động bàn phím, chụp ảnh màn hình.