**Họ Tên : Phạm Ngọc Hà Minh**

**MSSV:1050080061**

**Bài tập 2 lý thuyết**

**Bài 1:**

**1.** **Nêu biện pháp phòng tránh; các cách phát hiện Keylogger trên máy tính - điện  thoại và minh họa nếu có thể:**

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

**Câu 1:**

Để phòng tránh việc bị đánh cắp dữ liệu từ Keylogger khi chúng được đưa vào máy tính của bạn thông qua các mã độc, virus, trojan, spyware,… mà bạn không hề hay biết, hãy thực hiện các biện pháp sau:

·        Bạn có thể lưu mật khẩu với trình quản lý mật khẩu Locker để tự tự động điền khi đăng nhập, từ đó tránh bị Keylogger ghi lại các thông tin đăng nhập. Đồng thời, kích hoạt tính năng 2FA trong Locker để kẻ xâm nhập không thể đăng nhập ngay cả khi có được mật khẩu.

·        Đổi trật tự gõ phím khi đăng nhập vào tài khoản mạng xã hội, tài khoản ngân hàng trên mạng bằng cách gõ sai tên đăng nhập và mật khẩu rồi xóa đi những ký tự sai đó để Keylogger không nhận diện được tên đăng nhập và mật khẩu đúng.

·        Sử dụng bàn phím ảo cũng là một cách đơn giản để Keylogger không thể ghi nhận được các thao tác phím.

·        Cẩn trọng trước những tập tin lạ, không nên tùy ý mở các tập tin không rõ nguồn gốc, đặc biệt là những tập tin có đuôi \*.com, \*.exe, \*.scr, \*.zip, \*.rar, \*.swf, \*.gif,…

·        Không truy cập vào các website lạ, đặc biệt là những web đen vì những trang web này luôn tiềm ẩn các nguy cơ về mã độc, virus hay worm và chỉ chờ bạn click vào.

·        Không click vào những đường link lạ được ngẫu nhiên gửi.

·        Không cài đặt các chương trình, ứng dụng lạ.

·        Không sử dụng bản crack các chương trình, phần mềm.

·        Tránh tải các ứng dụng từ những website lạ, không đáng tin cậy. Hãy kiểm tra chữ ký điện tử trước để xem chương trình có bị sửa đổi hay không.

·        Thực hiện cập nhật hệ điều hành, ứng dụng định kỳ để kịp thời vá các lỗ hổng.

·        Luôn active các chương trình bảo vệ thiết bị như chống virus, cài đặt thêm hệ thống tường lửa trong trình duyệt, hệ điều hành.

**1. Biện pháp phòng tránh Keylogger**

Để ngăn chặn Keylogger (phần mềm gián điệp ghi lại thao tác bàn phím), bạn có thể áp dụng các biện pháp sau:

**Trên máy tính**

Cài đặt phần mềm bảo mật & diệt virus: Sử dụng các phần mềm uy tín như Windows Defender, Malwarebytes, Kaspersky, Bitdefender...

Cập nhật hệ điều hành và phần mềm thường xuyên: Các bản vá lỗi bảo mật giúp ngăn chặn phần mềm độc hại.

Không tải phần mềm từ nguồn không rõ ràng: Keylogger có thể ẩn trong file crack, phần mềm lậu.

Dùng bàn phím ảo hoặc copy-paste mật khẩu: Một số Keylogger không thể ghi lại thao tác này.

Sử dụng trình quản lý mật khẩu: Giúp hạn chế nhập mật khẩu bằng bàn phím.

Kiểm tra Task Manager và các tiến trình chạy ngầm: Keylogger thường hoạt động ẩn, có thể xuất hiện với tên lạ.

Dùng phần mềm phát hiện Keylogger: SpyShelter, Zemana AntiLogger, GhostPress...

**Trên điện thoại**

Cài ứng dụng từ cửa hàng chính thức (Google Play, App Store).

Không cấp quyền truy cập bàn phím, ghi âm hoặc quản trị viên cho ứng dụng không rõ nguồn gốc.

Kiểm tra ứng dụng chạy ngầm trong cài đặt.

Dùng phần mềm bảo vệ như Malwarebytes Mobile, Kaspersky Mobile Security...

**Cách phát hiện Keylogger**

**Trên máy tính:**

Kiểm tra Task Manager (Ctrl + Shift + Esc) → Tab Processes: Tìm tiến trình đáng ngờ.

Kiểm tra thư mục khởi động: Mở Run (Windows + R) → nhập "msconfig" → Startup.

Dùng phần mềm quét Keylogger: SpyShelter, Malwarebytes, Zemana AntiLogger...

Kiểm tra kết nối mạng bất thường: Nếu có chương trình gửi dữ liệu ra ngoài, có thể là Keylogger.

**Trên điện thoại:**

Xem ứng dụng chạy ngầm: Kiểm tra trong Cài đặt → Ứng dụng → Quyền hạn.

Kiểm tra bàn phím mặc định: Một số Keylogger hoạt động như bàn phím ảo.

Xóa các ứng dụng không rõ nguồn gốc & dùng phần mềm bảo vệ.

**Câu 2. Một số loại Keylogger phổ biến**

**Trên máy tính**

Elite Keylogger: Ghi lại phím bấm, clipboard, ảnh chụp màn hình, gửi dữ liệu từ xa.

Refog Keylogger: Hoạt động ẩn, ghi nhật ký chat, trang web, email.

Ardamax Keylogger: Nhẹ, khó phát hiện, thường bị hacker lợi dụng.

Spyrix Free Keylogger: Miễn phí, có thể bị lạm dụng để theo dõi người khác.

**Trên điện thoại**

 iKeyMonitor: Dùng cho giám sát trẻ em nhưng có thể bị hacker lợi dụng.

mSpy: Theo dõi tin nhắn, lịch sử cuộc gọi, có thể hoạt động như Keylogger.

Spyzie: Ẩn danh, ghi lại hoạt động bàn phím trên Android/iOS.

Hoverwatch: Theo dõi vị trí, bàn phím, cuộc gọi, tin nhắn..

Tải keylogger







