Câu 1

**Phòng chống**

**Máy tính**

* Cài đặt phần mềm diệt virus và tường lửa: Sử dụng các phần mềm bảo mật mạnh như Windows Defender, Kaspersky, Bitdefender, Malwarebytes để quét và phát hiện keylogger.
* Không tải phần mềm không rõ nguồn gốc: Chỉ tải ứng dụng từ trang web chính thức hoặc Microsoft Store.
* Cập nhật hệ điều hành và phần mềm: Luôn cập nhật Windows, trình duyệt và ứng dụng để vá lỗ hổng bảo mật.
* Sử dụng xác thực hai yếu tố (2FA): Để bảo vệ tài khoản, ngay cả khi mật khẩu bị đánh cắp.
* Không mở email và tệp đính kèm đáng ngờ: Tránh nhấp vào đường link hoặc tải file lạ từ email lừa đảo.
* Giám sát tiến trình đang chạy: Kiểm tra Task Manager (Ctrl + Shift + Esc) để phát hiện ứng dụng lạ.

**Điện thoại**

* Chỉ tải ứng dụng từ Google Play Store hoặc App Store: Tránh cài đặt từ file APK hoặc nguồn không rõ ràng.
* Kiểm tra quyền ứng dụng: Nếu một ứng dụng không liên quan nhưng yêu cầu quyền truy cập bàn phím hoặc ghi lại thao tác, hãy gỡ bỏ ngay.
* Bật Google Play Protect hoặc iOS Security: Để quét và phát hiện ứng dụng nguy hiểm.
* Không root/jailbreak thiết bị: Việc này làm tăng nguy cơ bị cài đặt phần mềm độc hại.
* Thường xuyên kiểm tra danh sách ứng dụng cài đặt: Nếu thấy ứng dụng lạ, hãy gỡ bỏ ngay.

**Phát hiện keylogger**

**Máy tính**

* Kiểm tra Task Manager: (Ctrl + Shift + Esc) → Tab *Processes* → Tìm các tiến trình lạ hoặc chiếm nhiều CPU, RAM mà bạn không biết.
* Kiểm tra chương trình khởi động cùng Windows: Nhấn Win + R → gõ msconfig → tab *Startup* → Vô hiệu hóa ứng dụng đáng ngờ.
* Kiểm tra thư mục ẩn: Một số Keylogger lưu dữ liệu trong thư mục bí mật. Nhấn Win + R → nhập %AppData%, %Temp%, %LocalAppData% → Tìm file lạ.
* Dùng phần mềm quét Keylogger: Malwarebytes, Spybot Search & Destroy, Zemana AntiLogger.
* Kiểm tra thiết bị phần cứng lạ: Một số Keylogger là thiết bị cắm vào cổng USB.

**Điện thoại**

* Kiểm tra quyền ứng dụng: Vào *Cài đặt* → *Ứng dụng* → Xem ứng dụng nào có quyền truy cập bàn phím, ghi âm, điều khiển màn hình.
* Xem ứng dụng chạy ngầm: Vào *Cài đặt* → *Pin* hoặc *Hiệu suất* để kiểm tra ứng dụng tiêu tốn tài nguyên bất thường.
* Dùng phần mềm bảo mật: Kaspersky Mobile, Malwarebytes Mobile Security, Avast Mobile Security để quét phần mềm độc hại.

Câu 2

**Máy tính**

**Keylogger phần cứng**

Đây là các thiết bị vật lý được gắn trực tiếp vào máy tính để ghi lại thao tác bàn phím. Một số dạng phổ biến:

* Thiết bị cắm giữa bàn phím và máy tính: Thiết bị nhỏ gọn được cắm giữa cổng kết nối bàn phím và máy tính, ghi lại mọi phím bấm mà không cần phần mềm hỗ trợ.
* Bàn phím tích hợp keylogger: Bàn phím được chế tạo sẵn với mạch keylogger bên trong, khó phát hiện hơn do không có thiết bị ngoại vi nào khác.

**Keylogger phần mềm**

Đây là các chương trình được cài đặt trên hệ điều hành để theo dõi và ghi lại thao tác của người dùng. Một số loại phổ biến:

* Keylogger dựa trên API: Sử dụng các hàm API của hệ điều hành để ghi lại thao tác bàn phím.
* Keylogger dựa trên form grabbing: Ghi lại dữ liệu khi người dùng nhập thông tin vào các biểu mẫu trực tuyến trước khi chúng được mã hóa và gửi đi.
* Keylogger chụp màn hình: Định kỳ chụp ảnh màn hình để theo dõi hoạt động của người dùng.

**Điện thoại**

Trên thiết bị di động, keylogger thường là các ứng dụng gián điệp được cài đặt để theo dõi hoạt động của người dùng. Một số ứng dụng phổ biến:

* Xnspy: Ứng dụng giám sát cho phép theo dõi các tổ hợp phím trên các ứng dụng nhắn tin như Facebook Messenger, Viber, Skype và WhatsApp. Tuy nhiên, Xnspy không cho phép theo dõi mật khẩu hoặc địa chỉ email do vi phạm pháp luật.
* Spyzie: Ứng dụng giám sát mạnh mẽ, ghi lại thao tác bàn phím, tin nhắn, cuộc gọi và vị trí GPS của thiết bị.
* mSpy: Ứng dụng theo dõi phổ biến, cho phép giám sát tin nhắn, cuộc gọi, email và hoạt động internet trên thiết bị di động.