**C. CÂU HỎI**

Sau quá trình thực hành, sinh viên trả lời các câu hỏi sau:

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

thoại và minh họa nếu có thể.

**Biện pháp phòng tránh:**

* Cập nhật phần mềm thường xuyên: Windows, macOS, Android, iOS, trình duyệt, phần mềm diệt virus... phải luôn update để vá lỗi bảo mật.
* Không tải phần mềm lạ: Tránh tải phần mềm từ trang web không uy tín.
* Không bấm vào link lạ, nhất là từ email, Facebook, Zalo...Sử dụng phần mềm diệt virus có tiếng
* Ví dụ: Kaspersky, Bitdefender, Windows Defender, Malwarebytes, v.v.
* Bật xác thực 2 yếu tố (2FA): Dù bị lộ mật khẩu, vẫn an toàn nếu người khác không có mã xác thực.
* Dùng bàn phím ảo khi nhập thông tin quan trọng
* Đặc biệt ở máy công cộng hoặc nghi ngờ có keylogger.

**Cách phát hiện:**

* *Windown*

|  |  |
| --- | --- |
| **Cách** | **Mô tả** |
| **Task Manager** (Ctrl+Shift+Esc) | Kiểm tra ứng dụng chạy ngầm. Nếu có cái lạ như keylog.exe hay winlogsvc... thì nghi ngờ. |
| **Windows Defender/Diệt virus** | Quét toàn bộ máy. |
| **Autoruns** (từ Microsoft Sysinternals) | Kiểm tra các ứng dụng khởi động cùng Windows (cực hiệu quả). |
| **Quét bằng phần mềm chống Keylogger** | **SpyShelter, Zemana AntiLogger, Malwarebytes** |

* *Điện thoại Android*

|  |  |
| --- | --- |
| **Cách** | **Mô tả** |
| **Kiểm tra ứng dụng không rõ nguồn gốc** | Vào Cài đặt > Ứng dụng, kiểm tra cái nào khả nghi. |
| **Dùng ứng dụng quét malware** | Như Bitdefender Mobile Security, Norton Mobile Security. |
| **Xem quyền ứng dụng** | App nào yêu cầu quyền bàn phím, đọc bàn phím, gõ phím thì nên nghi ngờ. |

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

Trên máy tính:

* Spyrix Keylogger
* Refog Keylogger
* Actual Keylogger

Trên điện thoại:

* iKeyMonitor
* KidLogger
* FlexiSPY
* mSpy