**BÀI THỰC HÀNH**

**BẢO VỆ MÁY TÍNH AN TOÀN**

* **Bài tập:**

**Câu 1:** Hãy mô tả 3 nguy cơ (mối đe dọa) về an toàn và bảo mật thông tin có thể xảy ra đối với máy tính người dùng? Khi mô tả cần nêu rõ tên nguy cơ, cách thức xảy ra, mối nguy hại của nó.

- Một số nguy cơ về an toàn và bảo mật thông tin có thể xảy ra đối với máy tính người dùng:

+ Lối và thiếu sót của người dùng: do nhận thức và trình độ chuyên môn của người dùng còn hạn chế dẫn đến họ trở thành nạn nhân của nhiều vụ lừa đảo gây tổn thất lớn cho hệ thống thông tin của cá nhân hay tổ chức.

+ Gian lận và đánh cắp thông tin: do những kẻ tấn công từ bên trong hệ thống, gồm những người dùng giả mạo hoặc người dùng có ý đồ xấu. dẫn đến thông tin người dùng sẽ bị lợi dụng với nhiều mục đích bất chính gây nên nhiều tổn thất.

+ Kẻ tấn công nguy hiểm: xâm nhập vào hệ thống để tìm kiếm thông tin, phá hủy thông dữ liệu, phá hủy hệ thống. gây thiệt hại lớn về kinh tế, an ninh quốc gia

**Câu 2:** Firewall (tường lửa) là một trong các giải pháp được sử dụng bảo vệ máy tính và mạng máy tính, hãy mô tả chức năng, điểm mạnh và điểm yếu của firewall. Hãy liệt kê một số firewall phổ biến trên hệ điều hành windows.

* Chức năng của Firewall (tường lửa): có thể lọc lưu lượng từ các nguồn truy cập nguy hiểm như hacker, một số loại virus tấn công để chúng không thể phá hoại hay làm tê liệt hệ thống của bạn. Ngoài ra vì các nguồn truy cập ra vào giữa mạng nội bộ và mạng khác đều phải thông qua tường lửa nên tường lửa còn có tác dụng theo dõi, phân tích các luồng lưu lượng truy cập và quyết định sẽ làm gì với những luồng lưu lượng đáng ngờ như khoá lại một số nguồn dữ liệu không cho phép truy cập hoặc theo dõi một giao dịch đáng ngờ nào đó.
* Điểm mạnh: Giám sát được lượng truy cập; Bảo vệ chống lại Trojan; ngăn chặn tin tặc; Kiểm soát truy cập; Bảo mật tốt hơn
* Điểm yếu: Chi phí; Hạn chế người dùng; Hiệu suất; Các cuộc tấn công bằng phần mềm độc hại; Hoạt động phức tạp.
* Một số firewall phổ biến trên hệ điều hành windows như: Windows firewall, comodo firewall, Tinywall, ZoneAlarm…

**Câu 3:** Virus máy tính và phần mềm gián điệp là những mối nguy hại đối với an toàn bảo mật thông tin người dùng, hãy cho biết cách thức phòng tránh, cách thức phát hiện khi máy tính bị nhiễm, cách thức loại bỏ chúng khi bị nhiễm, cũng như liệt kê một số phần mềm diệt virus phổ biến nhất hiện nay.

* Môt số cách thức phòng tránh Virus máy tính và phần mềm gián điệp: Cài đặt một phần mềm chống virus bản quyền, chất lượng và có hiệu quả; Phần mềm chống gián điệp phải có khả năng bào vệ thời gian thực; Thực hiện quét virus hằng ngày, hằng tuần theo định kỳ; Cài đặt một trình duyệt web an toàn.; Vô hiệu hóa tính năng Autorun; Vô hiệu hóa tính năng xem trước hình ảnh của Outlook; Không bấm vào liên kết e-mail hoặc file đính kềm; Kết hợp sử dụng tường lửa dựa trên phần cứng và phần mềm; Triển khai bảo vệ DNS.
* Cách thức phát hiện khi máy tính bị nhiễm: Truy xuất tập tin, mở các chương trình ứng dụng chậm; Duyệt web chậm; Nội dung các trang web hiển thị trên trình duyệt web chậm; Các file lạ tự động sinh ra khi bạn mở ổ đĩa USB; Xuất hiện các file có phần mở rộng .exe có tên trùng với tên các thư mục; Trang chủ trình duyệt web bị thay đổi; Thanh công cụ lạ xuất hiện trên trình duyệt; Hoạt động của CPU tang cao không rõ nguyên nhân..
* Cách thức loại bỏ chúng khi nhiễm: Bật Safe Mode; Sử dụng windows Defender quét ngọa tuyến; Xóa các phần mềm đáng ngờ, Reset cài đặt gốc cho Windows; Sử dụng phần mềm diệt virus hoặc diệt virus theo cách thủ công; Phát hiện và gỡ bỏ spyware; Giành quyền truy cập ổ đĩa; Dọn dẹp trình duyệt..
* Một số phần mềm diệt virus phổ biến nhất hiện nay: BKAV, CMC, AVG, Kaspersky AntiVirus..

**Câu 4:** Mật khẩu là một trong các phương pháp chứng thức sử dụng phổ biến nhất hiện nay. Hãy cho biết những nguy cơ có thể xảy ra khi sử dụng mật khẩu cũng như cách thức tăng cường tính bảo mật của mật khẩu.

- Mật khẩu là một chuỗi các kí tự dùng xác minh danh tính của một tên người dùng trong quá trình đăng nhập vào một tài khoảng hay một dịch vụ nào đó.

- Một số nguy cơ có thể xảy ra khi sử dụng mật khẩu: Khi sử dụng mật khẩu có thể kèm theo một số nguy cơ như bị mất, hoặc bị các đối tượng xấu đánh cắp mật khẩu, dẫn đến dữ liệu cá nhân bị khai thác vào những mục đích xấu gây nên nhiều thiệt hại về vật chất lẫn tinh thần đối với cá nhân.

- Một số các cách thức tăng cường tính bảo mật của mật khẩu:

+ Không dùng chung mật khẩu cùng lúc với nhiều tài khoảng.

+ Không đặt mật khẩu quá dễ đoán như sinh nhật, 123456…

+ Không đặt mật khẩu quá ngắn có thể đặt từ 8 dến 16 kí tự hoặc dài hơn.

+ Mật khẩu nên chứa kí tự đặt biệt như #,\*….

+ Mật khẩu nên có chữ số, chữ in hoa…

+ Nên thay mật khẩu định kì.

+ Không nên ghi nhớ mật khẩu trên những thiết bị không tin cậy.

+ Không nhập mật khẩu vào web lạ.

**Câu 5:** Phishing là một trong các mối đe dọa an ninh thông tin trên mạng Internet. Hãy nêu cách thức hoạt động và cách thức phòng tránh.

* Cách thức hoạt động của Phishing: Là một dạng lừa đảo trong đó một thủ phạm gửi một e-mail trông giống với e-mail chính thống để cố gắng lấy được thông tin cá nhân, thông tin tài chính người dùng. Một số thông điệp e-mail lừa đảo yêu cầu chúng ta trả lời với thông tin cá nhân của chúng ta; Trong những trường hợp khác, nội dung e-mail có thể dẫn đến một trang web giả mạo, hoặc một cửa sổ bật lên trông giống như một trang web chính thống để thu thập thông tin. Nếu bạn nhận được một e-mail có vẻ chính thống và yêu cầu bạn cập nhật số thẻ tín dụng, số chứng minh nhân dân, số hộ chiếu, số tài khoảng ngân hàng, mật khẩu, hoặc những thông tin khác, thường thì những e-mail này là những e-mail Phishing.
* Cách thức phòng tránh: Không bao giờ bấm vào một liên kết trong một e-mail gửi đến cho chúng ta, Thay vào đó, chúng ta đánh trực tiếp địa chỉ vào trình duyệt web.