

## 8 NGUYÊN TẮC CƠ BẢN KHI SỬ DỤNG PC CÔNG CỘNG

Sử dụng máy tính công cộng trong thư viện, quán cà phê Internet, điểm truy cập Internet... đều rất nhanh chóng, rẻ và tiện lợi. Nhưng sử dụng những máy tính này có thực sự an toàn? An toàn với máy tính công cộng phụ thuộc rất lớn vào cách sử dụng của người dùng.

Sử dụng máy tính công cộng trong thư viện, quán cà phê Internet, điểm truy cập Internet... đều rất nhanh chóng, rẻ và tiện lợi. Nhưng sử dụng những máy tính này có thực sự an toàn? An toàn với máy tính công cộng phụ thuộc rất lớn vào cách sử dụng của người dùng. Dưới đây là 8 nguyên tắc cơ bản khi sử dụng máy tính công cộng, giúp bạn an toàn hơn:

1. Sử dụng phần mềm chống Spyware Tải phần mềm chống phần mềm gián điệp (spyware) như X-Cleaner của Xblock.com. Phần mềm này có dung lượng rất nhỏ gọn, có thể sử dụng ngay trên đĩa mềm hoặc trên USB mà không cần phải cài đặt. Hãy sử dụng các phần mềm chống gián điệp để quét máy tính công cộng trước khi sử dụng. Đó là một ý kiến hay.
2. Không lưu lại những thông tin đăng nhập Thay vì đóng cửa sổ trình duyệt hay gõ vào địa chỉ trang Web khác, bạn hãy thoát khỏi (logout) trang Web bằng nhấn vào nút hoặc liên kết logout trên trang Web. Điều này hạn chế khả năng người sử dụng khác có thể truy cập vào các thông tin trong trang Web mà bạn vừa ghé thăm. Rất nhiều chương trình, đặc biệt là các trình nhắn tin như Yahoo Messenger, MSN, AOL...đều có tính năng tự động đăng nhập (login) để lưu lại tên người sử dụng và mật khẩu, giúp người sử dụng không phải gõ lại tên người dùng và mật khẩu. Tính năng này chỉ hữu ích khi sử dụng trên máy tính của riêng bạn, chúng sẽ rất nguy hiểm khi sử dụng ở những máy tính công cộng. Hãy vô hiệu chức năng này mỗi khi sử dụng máy tính công cộng.
3. Bảo vệ mật khẩu Các trình duyệt cũng có khả năng ghi nhớ mật khẩu. Trước khi lướt Web, nếu đang sử dụng Internet Explorer, hãy chọn Tools -> Internet Options, trong thẻ Content, vào AutoComplete và bỏ chọn toàn bộ các mục đánh dấu. Sau khi đã hoàn thành, hãy chọn Tools->Internet Options. Tới thẻ Content, nhấn vào AutoComplete, và chọn Clear Forms và Clear Passwords để xóa toàn bộ mật khẩu và các dữ liệu. Những chương trình theo dõi thao tác bàn phím (keylogger) có thể ghi lại mật khẩu của bạn một cách đơn giản. Nhưng chúng không thể ghi lại được nếu bạn sử dụng các thao tác sao chép và dán từng chữ cái vào trong mật khẩu. Ví dụ: nếu mật khẩu là "gh68@" hãy sao chép từng một trang nào đó từng kí tự 'g' , 'h' , '6' , '8' , '@' và dán vào trường mật khẩu. Tuy có hơi phiền phức nhưng lại an toàn hơn.
4. Không hiển thị những thông tin nhạy cảm trên màn hình Đừng để máy tính hiển thị những thông tin quan trọng, nhạy cảm như: thông tin cá nhân, mã số tài khoản ngân hàng, mã số thẻ tín dụng... Khi có việc cần phải đi ra ngoài một chút, bạn hãy đóng toàn bộ các cửa sổ chương trình, thoát khỏi các cửa sổ có chứa những thông tin nhạy cảm.
5. Xóa mọi dấu vết Sau khi sử dụng máy tính công cộng, hãy xóa bỏ mọi tập tin đệm và danh sách History của Internet Explorer. Để xóa các tập tin tạm và History trong IE bạn hãy thực hiện như sau: - Trong Internet Explorer, chọn Tools -> Internet Options - Trong thẻ General, chọn Temporary Internet files -> Delete Files, nhấn vào Delete Cookies. - Dưới mục History, chọn Clear History.
6. Đừng quá tin tưởng vào khả năng mã hoá (encryption) Hiện nay, có rất nhiều phần mềm mã hoá trên thị trường. Chúng có thể được sử dụng để mã hoá các email. Tuy nhiên, các phần mềm này chỉ mã hoá các thư sau khi đã sẵn sàng để gửi thư. Điều này quả thực là khá muộn màng nếu như một phần mềm ghi chép mọi thao tác bàn phím đã được cài đặt vào trong máy (keylogger). Chúng sẽ ghi lại toàn bộ mật khẩu và nội dung thư được viết ra và gửi về dưới dạng email cho những kẻ cài đặt keylogger mà người sử dụng máy tính không hề hay biết.
7. Hãy chú ý xung quanh Bởi vì có rất nhiều thông tin nói rằng những hacker có thể sử dụng những phương tiện kĩ thuật số nào đó để

theo dõi người sử dụng nhằm ăn cắp mật khẩu, do đó chúng ta cũng không nên sao lãng những kiểu tấn công cổ điển này. Hãy quan sát kỹ xung quanh và chú ý tới những người ngồi bên cạnh mỗi khi nhập mật khẩu. 8. Đừng nhập những dữ liệu "nhạy cảm" vào máy tính công cộng Những phương pháp trên có thể cung cấp cho bạn một phương thức chống lại những hành vi quen thuộc của hacker sẽ dùng lại những chiếc máy tính công cộng này sau khi bạn sử dụng. Tuy nhiên, hacker hay những tên ăn trộm chuyên nghiệp có thể sử dụng các phần mềm keylogger để ăn cắp thông tin, email ... Những công cụ mà chúng sử dụng sẽ vô hiệu hoá, và lấy cắp được thông tin của bạn dễ dàng ngay khi bạn đã xoá mọi dữ liệu liên quan. Vì vậy, để thực sự an toàn, hãy tránh gõ vào số thẻ tín dụng, bất cứ những thông tin tài chính hoặc các thông tin nhạy cảm vào trong máy tính công cộng. Đó là cách sử dụng an toàn nhất cho bạn. Minh Phúc