5 kiểu đánh cắp dữ liệu bạn nên biết để phòng tránh

Bạn đã thực hiện bảo mật dữ liệu của mình để không ai có thể ăn cắp dữ liệu từ máy tính hoặc thiết bị mạng của bạn chưa? Nếu có thì thật tuyệt bởi vì bạn vừa giải quyết được vấn đề bảo mật tồi tệ nhất gây rắc cho các tập đoàn trên khắp thế giới.

Sự thật là bảo mật dữ liệu là vấn đề phức tạp và khó khăn. Nếu bạn nghĩ dữ liệu của mình hoàn toàn an toàn thì có thể có những lỗ hổng mà bạn chưa biết. Đó là lý do tại sao cần biết cách dữ liệu bị ăn cắp từ máy tính hoặc thiết bị mạng để có những cách đối phó thích hợp.

1. Thanh USB

Những chiếc USB nhỏ gọn phù hợp để trong túi hoặc treo lên móc chìa khóa. Nó nhỏ, dễ giấu và thậm chí có thể ngụy trang, nhưng những thanh USB flash này lại đầy rẫy nhưng nguy cơ bảo mật cao.

Ví dụ, chúng có thể bị mất hoặc bị đánh cắp, mặc dù những chiếc USB này có vẻ không có dữ liệu nhưng với phần mềm khôi phục, những thông tin bí

mật bạn lưu giữ trên đó có thể bị khám phá. Ngoài ra còn có những phần mềm độc hại dành cho USB chuyên cung cấp worm và Trojans để lây nhiễm trên máy tính, chờ đợi để ăn cắp thông tin đăng nhập và dữ liệu nhạy cảm.

Các thanh USB có ngoại hình giống nhau nên dễ bị nhầm lẫn đặc biệt trong môi trường làm việc. Một đồng nghiệp có thể dễ dàng cầm nhầm USB của bạn mang về nhà.

Nếu có thể mở khóa được máy tính thì chỉ cần một thanh USB, bất cứ ai cũng có thể ăn cắp dữ liệu từ máy tính bằng cách cắm vào đó, chuyển dữ liệu sang USB, tháo và rời đi. Quá trình này rất dễ, thậm chí còn dễ hơn ăn cắp tài liệu bằng giấy.

Gã khổng lồ công nghệ IBM đã áp dụng một chính sách bảo mật mới năm 2018: một lệnh cấm không được sử dụng các thiết bị lưu trữ có thể tháo rời như thanh USB, thẻ SD và ổ flash nhưng có vẻ đã quá muộn.

2. Điện thoại thông minh hoặc máy tính bảng

Mặc dù đã cấm sử dụng các thiết bị lưu trữ USB, nhưng IBM vẫn chưa giới hạn sử dụng các phương tiện lưu trữ di động phổ biến khác như điện thoại di động. Khi được thiết lập ở chế độ lưu trữ với dung lượng lớn, một chiếc điện thoại có thể trở thành một ổ cứng di động hoặc ổ USB.

Máy tính bảng và máy nghe nhạc MP3 cũng có thể sử dụng theo cách tương tự. Đối với người dùng IBM, đây có thể là giải pháp cho việc không thể sử dụng ổ USB. Có lẽ công ty nhận ra rằng họ có thể phát hiện dữ liệu nào đã được chuyển từ thiết bị nào và biết danh tính người sử dụng điện thoại mà những chiếc USB thì không thể.

Dù bằng cách nào đi nữa, bất cứ ai cũng có thể sao chép dữ liệu từ một chiếc máy tính đã được mở khóa, không được giám sát bằng một chiếc điện thoại và cáp USB.

3. Thẻ nhớ flash

Thẻ nhớ flash nhỏ hơn một thanh USB nên có thể được sử dụng để lén lút ăn cắp dữ liệu. Nhiều thiết bị ngày nay có tính năng đọc thẻ, thường kích hoạt phương tiện được chèn vào cạnh của đầu đọc, khiến chúng khó bị phát hiện.

Với một thiết bị flash USB, những thẻ nhớ nhỏ này có thể dễ dàng bị bỏ túi, nhưng máy tính phải mở và không bị giám sát thì mới có thể ăn cắp được dữ liệu. Ví dụ, một người bạn sử dụng máy tính của bạn để xem ảnh từ thẻ nhớ máy ảnh. Mặc dù có thể họ không có ý định ăn cắp dữ liệu nhưng phần mềm độc hại có thể từ thẻ xâm nhập vào máy tính. Và tất cả những rủi ro từ thanh USB đều có thể xảy ra với thẻ nhớ flash.

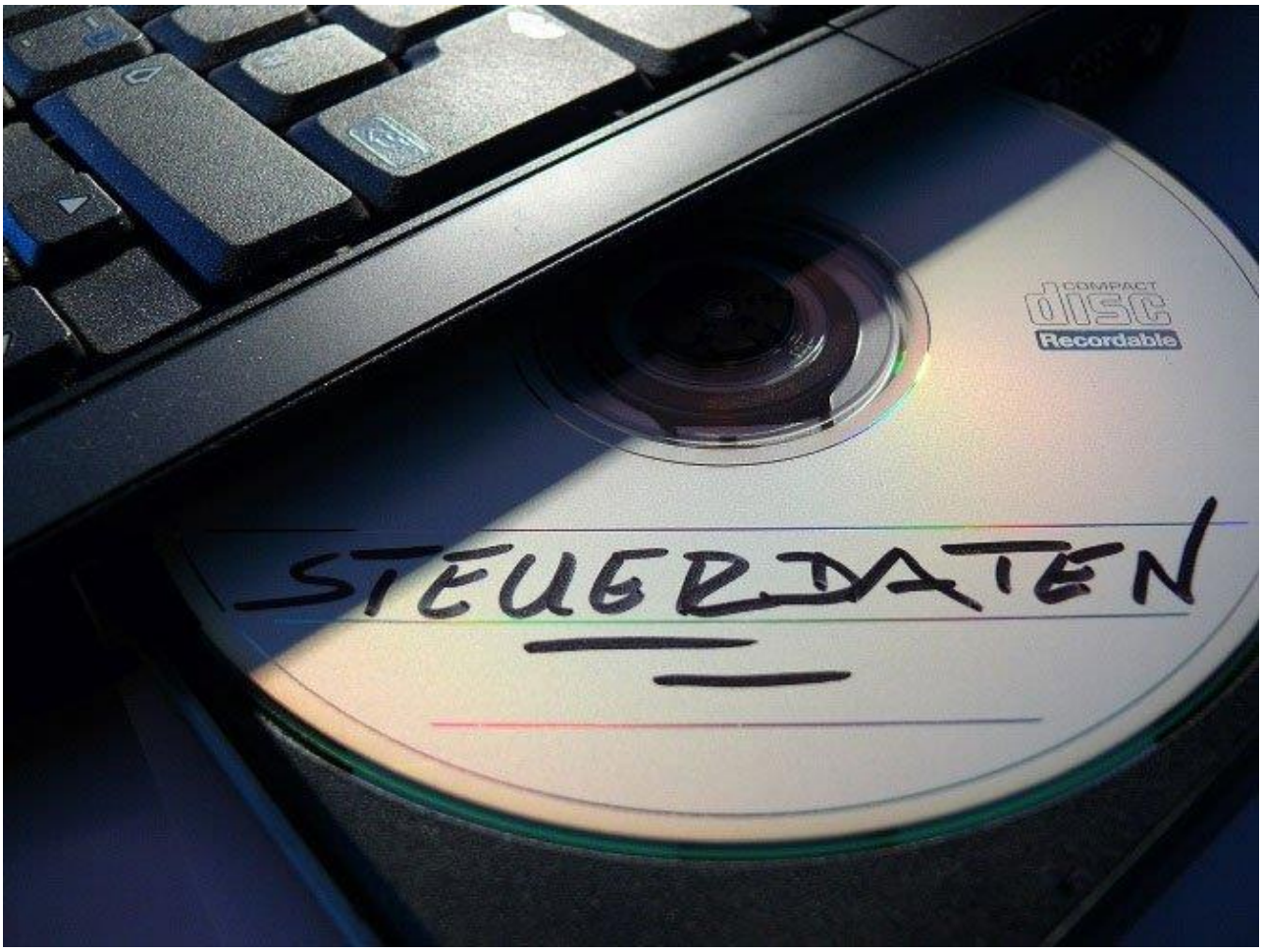
4. Thiết bị NAS hoặc ổ cứng HDD di động

Một số rủi ro đánh cắp dữ liệu máy tính khác đến từ các ổ cứng di động (HDD). Chúng có thể dễ dàng được kết nối qua USB. Tuy nhiên có một loại ổ khác còn mang đến nguy cơ rủi ro cao hơn cho dữ liệu của bạn.

Network Attached Storage ngày càng phổ biến như một phương tiện lưu trữ dữ liệu trên một mạng cục bộ, thường là ở nhà. Các hộp NAS có giá cả phải chăng và có thể cung cấp khả năng khôi phục dữ liệu, thậm chí bạn có thể tự xây dựng bằng cách sử dụng Raspberry Pi.

Vấn đề là, nếu đang lưu trữ tất cả các dữ liệu quan trọng của bạn trên một hộp NAS, có nguy cơ dữ liệu này sẽ bị ăn cắp. Nó nhỏ hơn một máy tính cá nhân, có thể kết nối dễ dàng từ mạng gia đình và thực hiện ăn cắp dữ liệu. May mắn thay bạn có một giải pháp ở đây là để hộp NAS ở những nơi ngoài tầm với, tốt nhất nên khóa nó lại.

5. Các phương tiện lưu trữ di động khác



Ở trên chúng ta đã xem xét các phương tiện lưu trữ nhỏ gọn phổ biến nhất hiện nay, nhưng còn một số phương tiện khác như đĩa CD, DVD, ZIP và REV. Những loại đĩa này nhỏ hơn ổ cứng di động và dễ dàng che giấu.

Mặc dù không được sử dụng rộng rãi, nhưng các phương tiện lưu trữ bằng băng từ (tape media) được sử dụng để lưu trữ khối lượng lớn, sao lưu và khôi phục dữ liệu trong các doanh nghiệp và một số máy chủ gia đình. Những phương tiện này cần được để ở một nơi an toàn bởi vì chúng thường giữ một bản sao toàn bộ nội dung của máy chủ.

Cách bảo mật và bảo vệ dữ liệu

Bạn thường lưu trữ dữ liệu nào trên máy tính: trò chơi điện tử, tác phẩm nghệ thuật, một cuốn tiểu thuyết đang viết dở hay thông tin giá trị hơn như dữ liệu

khách hàng, thông tin nhạy cảm thương mại hoặc thông tin nếu lộ ra bạn có thể bị mất việc.

Nếu lo lắng những thông tin này bị đánh cắp từ máy tính ở nhà hoặc máy tính xách tay nơi làm việc, thì điều quan trọng bạn nên biết cách dữ liệu bị ăn cắp để có biện pháp phòng tránh thích hợp. Như trên đã đề cập, dữ liệu của bạn sẽ có nguy cơ bị ăn cắp từ:

- Thanh USB.
- Điện thoại thông minh, máy tính bảng và máy nghe nhạc MP3 (được kết nối qua USB).
- Thẻ nhớ flash.
- Thiết bị NAS và ổ HDD di động.
- Phương tiện di động: đĩa quang, ổ đĩa cứng di động, thiết bị lưu trữ bằng băng từ.

Nếu muốn bảo mật dữ liệu, bạn có thể xem xét sử dụng mã hóa ổ đĩa. Nếu sếp của bạn yêu cầu làm việc từ xa trên dữ liệu lưu trữ tập trung, bạn nên thiết lập VPN, điều này sẽ cải thiện đáng kể bảo mật dữ liệu.

Một điều cuối cùng: mặc dù các thiết bị này có thể được sử dụng để lấy cắp dữ liệu từ máy tính của bạn, chúng cũng có thể được sử dụng để đưa Trojans và phần mềm độc hại vào máy tính. Đảm bảo cập nhật các phần mềm diệt virus và bảo mật Internet.