XÓA DỮ LIỆU TRIỆT ĐỂ BẰNG CÁCH NÀO?

Cảnh báo khi xóa dữ liệu Hầu hết người dùng hiện nay đều dùng lệnh "Delete" trong Windows để xóa dữ liệu. "Chắc ăn" hơn, họ còn vào Recycle Bin để "Empty" nó đi một lần nữa và tin tưởng rằng dữ liệu đã xóa coi như không còn

Cảnh báo khi xóa dữ liệu Hầu hết người dùng hiện nay đều dùng lệnh "Delete" trong Windows để xóa dữ liệu. "Chắc ăn" hơn, họ còn vào Recycle Bin để "Empty" nó đi một lần nữa và tin tưởng rằng dữ liệu đã xóa coi như không còn tồn tại trên đời. Một số người dùng "am hiểu" hơn còn biết xóa dữ liệu "triệt để" bằng cách vào DOS để format lại ổ đĩa, hoặc xóa trực tiếp trong DOS bằng một công cụ nào đó…Tiếc rằng chỉ với vài thao tác là những dữ liệu đó có thể hoàn toàn được phục hồi nguyên xi. Dữ liệu riêng tư của người dùng, dữ liệu mật của công ty… đều có thể bị lộ vì sự thiếu hiểu biết thấu đáo , nhất là trong các trường hợp trả lại máy tính đã thuê, vứt đi hay tặng lại máy tính cũ, chuyển máy tính cho người mới sử dụng, đem đĩa cứng đi bảo hành, cho mượn thẻ nhớ Flash v.v Có rất nhiều trường hợp bạn rất cần xóa "sạch sành sanh" dữ liệu, chẳng hạn như xóa dữ liệu đã chép tạm từ đĩa cứng này sang đĩa cứng khác, xóa dữ liệu đã bị nhiễm virus, xóa hoặc format đĩa cứng để cài đặt lại hệ điều hành mới, xóa đi mọi thư từ, hình ảnh riêng tư v.v Nhưng tiếc rằng nếu những đĩa cứng hoặc thẻ nhớ flash này lọt được vào tay những "cao thủ" thì những dữ liệu đã xóa của bạn hều hết đều ở tình trạng "mời cụ xơi". Delete hay format không hoàn toàn xóa sạch được dữ liệu! Đa số người dùng đều không biết rằng Windows và mọi ứng dụng chạy trên nó đều có "thói quen" tạo ra nhiều tập tin dữ liệu có nội dung hệt như dữ liệu mà người dùng đang thao tác và lưu trữ vào Swap Files và Page Files để hỗ trợ bộ nhớ ảo, hoặc sao lại thành một phiên bản khác để lưu vào Temp hay Temporary Files…Tất cả mọi động tác này của Windows đều nhằm mục đích bảo tồn dữ liệu của người dùng trong trường hợp mất điện đột ngột, hoặc người dùng lơ đãng quên lưu dữ liệu… nhưng thật ra đây là hành động có tính "bất cẩn" của Windows khi tự động sao chép dữ liệu ra làm nhiều bản mà lại không biết tự động xóa đi khi đã dùng xong. Đây được xem là một lỗ hở cực lớn, tạo điều kiện "tối ưu" cho những kẻ ăn cắp dữ liệu hoạt động. Và như vậy, dù người dùng có xóa đi dữ liệu và "Emply Recycle Bin", hoặc format lại một phân vùng đĩa cứng nào đó thì những dữ liệu đã từng lưu trên đó vẫn có thể còn nằm nguyên vẹn đâu đó trong Windows, chưa kể hiện nay có rất nhiều công cụ phục hồi dữ liệu cực mạnh có khả năng phục hồi lại mọi dữ liệu bất chấp phân vùng đĩa cứng đó đã được format tới vài lần. Thực chất rằng với lệnh Delete, người dùng chỉ xóa đường dẫn đến dữ liệu chứ chưa xóa sạch thông tin ra khỏi đĩa cứng, điều này giống như bạn chỉ bỏ trang mục lục của một cuốn sách mà chưa hủy những trang hay chương sách tương ứng. Lệnh Delete này chỉ được xem là lệnh "làm gọn" lại đĩa cứng bằng mắt thường chứ không có tác dụng "delete" thực sự, nên đổi lệnh Delete lại thành "Tidy" (gọn gàng) có lẽ phù hợp hơn. Một số phương pháp hoặc tiện ích giúp xóa sạch dữ liệu! Để bảo mật thông tin các dự án, thông báo nội bộ, số liệu tài chính-kế toán, dữ liệu khách hàng, dữ liệu cá nhân v.v... bạn cần biết đến những phương pháp hoặc phần mềm xóa sạch dữ liệu đáng tin cậy. Hiện trên thế giới đang sử dụng phổ biến một số phương pháp xóa dữ liệu an toàn như sau: 1. Single Pass (xóa 1 lần): toàn bộ khu vực DL trên ổ cứng được ghi đè (overwrite) bằng kí tự 0 hoặc 1 hoặc dữ liệu ngẫu nhiên.. 2. DoD: Phương pháp xóa dữ liệu triệt để này là của Bộ Quốc Phòng Mỹ. Đây là biến thể của phương pháp Single Pass với số lần ghi đè là 7, trong đó luân phiên ghi đè bằng ký tự 0 hoặc 1 hay dữ liệu ngẫu nhiên. Tiếp đó, theo tài liệu hướng dẫn 5220.22 M, có tên là Chương trình bảo mật công nghiệp quốc gia (NISPOM) của Bộ quốc phòng Mỹ. Theo tài liệu này, để tẩy sạch dữ liệu trên đĩa phải kết hợp với các biện pháp sau:

- Khử từ: dùng từ trường để tái lập lại các thanh từ trong thiết bị bằng thiết bị khử từ loại I hay II - Ghi đè mọi địa chỉ trên ổ cứng bằng 1 ký tự, kể cả các thành phần liên quan, rồi tiếp tục ghi đè bằng ký tự ngẫu nhiên và kiểm tra xác nhận. Tuy nhiên, BQP Mỹ cũng lưu ý rằng phương pháp này không dùng để xóa dữ liệu lưu trữ thông tin tuyệt mật - Hủy thiết bị lưu trữ thông tin, bao gồm tháo rã mọi thành phần của thiết bị lưu trữ, đốt hủy, nghiền thành bột, cắt vụn, hoặc làm tan chảy bằng nhiệt độ cao. 3. Tẩy sạch dữ liệu bằng phương pháp Guttman: dữ liệu được xóa bằng phương pháp này được ghi đè đến những 35 lần. Phương pháp này dùng ký tự ngẫu nhiên để ghi đè và áp dụng các thuật toán mã hóa của nhiều hãng sản xuất đĩa cứng khác nhau… 4. Phương pháp hủy dữ liệu bằng cách ghi đè tùy chọn từ 1 đến 99 lần. Ngoài ra còn khá nhiều phương pháp tẩy sạch dữ liệu do các tổ chức và quốc gia khác nhau đưa ra. Qua việc tham khảo các phương pháp tẩy sạch dữ liệu như trên ta cảm giác rằng dường như chỉ có hai cách duy nhất để xóa sạch dữ liệu là ghi đè và phá hủy theo kiểu "tận diệt", nhưng rõ ràng "tận diệt" là phương pháp mà ít ai dám làm vì quá tốn kém. Người dùng cần lưu ý rằng ngay cả chuyên gia Peter Guttman, cha đẻ của phương pháp Guttman cũng đã nhận định rằng:"Không thể xóa sạch 100 % dữ liệu dù có ghi đè lên bao nhiêu lần đi nữa…" Như vậy chúng ta chỉ có thể giảm thiểu nguy cơ phục hồi được dữ liệu bằng cách ghi đè lên thật nhiều lần mà thôi… Người dùng có thể tham khảo về "Recover My Files", một công cụ phục hồi dữ liệu cực kỳ hiệu quả, bất chấp dữ liệu đã được Delete hoặc Format. Hiện nay, hầu hết các phần mềm hỗ trợ tẩy sạch dữ liệu chạy trên nền DOS tỏ ra hiệu quả hơn những phần mềm chạy trên Windows, nhưng nó lại tỏ ra kém thân thiện với người dùng. Nhưng có lẽ việc hỗ trợ xóa dữ liệu mật nên dành cho bộ phận CNTT trong doanh nghiệp hoặc cơ quan. Dưới đây là một vài Website cung cấp các giải pháp xóa sạch dữ liệu tương đối hiệu quả. Người dùng có thể vào các website này để tham khảo và tải bản dùng thử về dùng trước khi chọn cho mình một công cụ đắc địa nhất. BCWipe: http://www.jetico.com/index.htm#/bcwipe.htm Data Eraser: http://www.ontrack.co.uk Directory Snoop: http://www.briggsoft.com/dsnoop.htm Disk CleanUp: http://www.gregorybraun.com/CleanUp.html Eraser: http://www.tolvanen.com/eraser M-Sweep: http://www.securedata.com/ms.html PGP Wipe: http://web.mit.edu/network/pgp.html RMD: http://www.dmares.com/maresware/ps.htm#RM WipePro+: http://www.marcompress.com Wipe Info: http://www.symantec.com With Out a Trace: http://www.karmadromesoft.com Nova Drive Erase Pro: http://www.novadevelopment.com. HOÀNG KIM ANH