PHÁ PASSWORD CMOS BẰNG CÁCH NÀO?

Cài password CMOS được xem là một trong những biện pháp khá hữu hiệu để bảo mật máy tính. Phá password CMOS là một điều hết sức khó khăn nhưng không phải là không thể làm được. Tuy nhiên để thực hiện thành công cũng đòi hỏi bạn phải c&

Cài password CMOS được xem là một trong những biện pháp khá hữu hiệu để bảo mật máy tính. Phá password CMOS là một điều hết sức khó khăn nhưng không phải là không thể làm được. Tuy nhiên để thực hiện thành công cũng đòi hỏi bạn phải có một "tay nghề" nhất định. Có một vài cách để phá password CMOS như: thay chip BIOS, ngắt mạch chip BIOS, sử dụng jumper, tháo pin trên mainboard, phá password CMOS bằng một số lệnh, nhập vào các password mặc định của nhà sản xuất... nhưng đối với giới tin học "bình dân học vụ" như chúng ta thì may ra có 2 phương pháp sau là tạm có thể áp dụng được. 1. Nhập vào các password chuẩn của BIOS do nhà sản xuất đã mặc định sẵn. - Đối với loại Award BIOS thì ta có thể nhập vào các password mặc định sau để thử bẻ khóa password đã đặt trước đó: AWARD SW, AWARD_SW, Award SW, AWARD PW, _award, awkward, J64, j256, j262, j332, j322, 01322222, 589589, 589721, 595595, 598598, HLT, SER, SKY_FOX, aLLy, aLLY, Condo, CONCAT, TTPTHA, aPAf, HLT, KDD, ZBAAACA, ZAAADA, ZJAAADC, djonet. - Đối với loại Ami BIOS thì dùng: AMI, A.M.I., AMI SW, AMI_SW, BIOS, PASSWORD, HEWITT RAND, Oder. - Một số password dùng chung cho Ami, Award và một số BIOS khác có thể thử như: LKWPETER, lkwpeter, BIOSTAR, biostar, BIOSSTAR, biosstar, ALFAROME, Syxz, Wodj. Nhưng thực ra phương pháp này cũng không hiệu quả lắm vì ngoài những nhãn hiệu Award, Ami... thì còn hàng chục nhãn hiệu BIOS khác mà hầu như ta không thể biết được các password mặc định là gì. 2. Phá password CMOS bằng phần mềm chuyên dùng hoặc câu lệnh ở môi trường DOS: Nếu bạn được phép sử dụng một máy tính đang được cài password CMOS thì bạn có thể dùng một số lệnh DEBUG chạy trong môi trường DOS để phá password. Đây là những lệnh có thể làm mất hiệu lực bộ nhớ BIOS, giúp cho nó trở về trạng thái nguyên thuỷ, tức trước khi bị cài password. Nhưng thực chất việc này cũng hết sức khó khăn vì không phải lúc nào cũng có thể vào được môi trường DEBUG. Một cách hiệu quả hơn là bạn vào địa chỉ http://www.cgsecurity.org/cmospwd-4.8.zip để tải về công cụ mang tên "Cmos Password Recovery Tools 4.8" -> Giải nén file này -> Tìm đến thư mục Windows -> Kích hoạt file cmospwd_win.exe để file này tự động xóa đi bộ nhớ BIOS hiện tại. Nếu may mắn thì lần khởi động sau sẽ không password BIOS nữa. Để "chắc ăn", bạn nên vào thư mục "DOS" và kích hoạt file cmospwd.exe để thử lại một lần nữa. 3. Tháo hẳn cục pin mainboard để xóa hoàn toàn bộ nhớ BIOS. Đây là thao tác tác động vào phần cứng để xóa hoàn toàn bộ nhớ BIOS được xem là hiệu quả nhất, nếu "gan" một chút thì ai cũng có thể làm được. Ban đầu bạn phải tháo thùng máy ra -> Quan sát thật kỹ trên bản mạch máy tính để tìm ra một viên pin có đường kính cỡ như một đồng xu 200 đồng được gắn trong một ô hình tròn vừa khít với viên pin. Tìm được viên pin này thực ra cũng không khó lắm -> Quan sát kỹ và tháo viên pin ra bằng cách bấm vào cái "jumper" như hình minh họa -> Lấy pin ra và chờ khoảng 30 phút cho "chắc ăn", tức đảm bảo cho mọi dữ liệu lưu trong BIOS sẽ "bay hơi" hết -> sau đó gắn vào đúng như hình minh họa. Khi khởi động lại máy tính thì BIOS sẽ tự động trả về mọi thứ đúng như mặc định ban đầu và dĩ nhiên password cũng sẽ biến mất. Đảm bảo rằng đa số trường hợp tháo pin ra đều thành công còn nếu khi gắn pin vào mà password vẫn còn nguyên thì bạn lại phải tháo ra và chờ đợi thời gian "bay hơi" lâu hơn nữa, có thể là cả ngày. THỤY KHANH (Tổng hợp)