

NHỮNG NIỀM TIN NHẦM LẤN VỀ CÔNG NGHỆ

Người

Người ta cứ tưởng rằng việc phân vùng và chống phân mảnh cho đĩa cứng là có thể làm cho máy tính hoạt động ở mức tốt nhất. Thực tế, "phong độ" đó tùy thuộc vào lượng file mà người dùng thay đổi/xóa đi mỗi ngày.

Theo báo PC World (Mỹ), đây là một trong những niềm tin tưởng như "bất biến" đối với nhiều chuyên gia công nghệ. "Hệ điều hành có thói quen gốc ghếch là tận dụng mọi ô lưu trữ (cluster) trống, ngay cả khi nó nằm giữa vùng sử dụng lớn, trong khi có rất nhiều vùng trống ở sau", Mario Apicella, chuyên gia của tạp chí InfoWorld, nhận xét. "Do đó, có những file nằm rải rác khắp ổ cứng, khiến thiết bị phải mất thời gian đi tìm để gộp chúng lại với nhau".

Nhưng khi tiến hành thử nghiệm, PC World không thấy sự tăng tốc đáng kể nào sau khi dùng một loạt các chương trình chống phân mảnh. Ví dụ: sản phẩm của Diskeeper Corporation được quảng cáo là có thể tăng cường khả năng xử lý của máy tính nhưng phải có ít nhất 20% dung lượng đĩa trống. Do đó, mỗi thiết bị có sự thay đổi khác nhau.

Về bản chất, việc phân vùng một đĩa cứng lớn thành nhiều ổ logic nhỏ hơn không tăng tốc cho máy tính mà chỉ mang đến cho người dùng một số lợi ích. Ví dụ: dễ quản lý các chương trình hệ thống (ổ C) và kho dữ liệu (ổ D, E...). Khi phải cài lại hệ điều hành chẳng hạn, các thông tin trên ổ C sẽ mất hết, do đó, người dùng có thể sao lưu dữ liệu trên ổ lưu trữ còn lại. Dưới đây là một số "nhầm lẫn" khác đã được ghi nhận.

Thẻ nhớ tốc độ cao trong camera giúp chụp nhanh hơn

"Sản phẩm này chỉ cho phép máy ảnh số lưu file nhanh hơn chứ không đồng nghĩa với việc chụp nhanh hơn", Mike Wong, Giám đốc PR của SanDisk, cho biết.

Nếu dùng một máy ảnh tốc độ cao với thẻ nhớ tốc độ chậm, người chụp sẽ thấy máy lưu ảnh rất lâu. Còn việc dùng thẻ nhanh với máy ảnh chậm giống như đặt động cơ xe đua cho một con rùa. Tuy nhiên, sự khác biệt này chỉ thể hiện rõ ở máy SLR (ống kính đơn), còn loại ngắm và chụp đơn giản thì không.

Thẻ tốc độ cao cũng giảm thời gian chuyển file sang máy tính, miễn là có đầu đọc thẻ nhanh tương ứng. Điều này trở nên quan trọng khi độ phân giải của ảnh và dung lượng thẻ lớn.

Khi PC bị hack và biến thành "zombie", người dùng sẽ biết

Lawrence Baldwin, thuộc trang tin MyNetWatchman, cho rằng điều này là không có. Nếu hacker biến máy tính của bạn thành nơi phát tán spam, hệ thống chỉ có thể báo khi có phần mềm bảo mật chuyên kiểm tra lượng e-mail gửi đi. Nhưng thường thì mã độc đã tắt các phần mềm diệt virus, tường lửa, dịch vụ Windows Update để tự do hoành hành.

Người dùng chỉ rõ về vấn đề này khi nhà cung cấp dịch vụ thông báo có một "ổ" phát hiện ra địa chỉ IP của họ để lợi dụng và những e-mail chúng gửi đã bị chặn vì một ban bảo mật ở địa phương tìm ra. Theo chuyên gia này, người sử dụng PC không nên ngây thơ đặt niềm tin hoàn toàn vào các phần mềm chặn mã độc.

Máy soi X-quang ở sân bay có thể xóa hết ảnh trong camera

"Thiết bị của chúng tôi sẽ không gây ảnh hưởng đến các máy ảnh số và thẻ nhớ", Ủy ban an ninh giao thông Mỹ, khẳng định.

Thực tế, thẻ CompactFlash, Secure Digital hay Sony Memory Stick bền hơn người ta tưởng. Trong các kiểm tra của tạp chí Digital Camera Shopper, những sản phẩm này có thể hoạt động được sau khi bị ngâm trong bồn tắm, quay trong máy giặt, bị ván trượt đè lên...

Còn trong trường hợp mất ảnh trên thẻ, bạn có thể dùng phần mềm CardRecovery, EasyRecovery Lite... để khôi phục.

Pin sạc có hiệu quả kinh tế hơn loại dùng một lần

Hiệu quả chi phí của pin sạc còn phụ thuộc vào loại pin và tần suất sử dụng. Ví dụ: pin sạc nickel cadmium và nickel metal hydride hết năng lượng nhanh chóng khi được giữ trong thiết bị lâu mà không dùng đến. Trong khi đó, pin sạc lithium-ion giữ năng lượng lâu hơn.

"Pin sạc là giải pháp tiết kiệm với người dùng thường xuyên", Blayne Murphy, chuyên gia của hãng pin Duracell, tư vấn. "Nhưng với người ít dùng, loại sử dụng một lần tỏ ra ưu thế hơn".

Ngoài ra, họ còn phải dành tiền để mua sạc pin và xem thiết bị lưu trữ năng lượng này có thể hoạt động qua bao nhiêu lần sạc.

Google có thể tìm thấy mọi thứ trên mạng và thông tin đó không thể xóa khỏi cơ sở dữ liệu của họ

Nếu theo chỉ dẫn trên Google Webmaster Central, bạn có thể bỏ đi các trang mà họ tìm thấy, trong đó có trang của bạn. Nếu trang web đã có liên kết với những site khác, quá trình này sẽ tốn nhiều thời gian hơn.

Nếu tự gõ địa chỉ URL, người dùng sẽ không vào nhầm trang phishing

Theo Dave Jevans, Chủ tịch hãng Anti-Phishing Working Group, có 2 mối nguy hiểm rình rập người sử dụng.

Một là trong các vụ tấn công pharming (đầu độc tên miền), dù tay gõ đúng tên miền, người dùng vẫn có thể bị dẫn vào trang mạo danh. Jevans cho biết cách duy nhất để phòng tránh là lưu các trang này vào khu vực bảo mật riêng (bắt đầu là https:). Ngoài ra, họ cũng cần chú ý đến những cảnh báo từ trình duyệt.

Hai là mã độc có thể viết lại các tập tin host trong máy tính hoặc tấn công trình duyệt. Do đó, cần cập nhật thường xuyên các bản vá lỗi của hãng.