Bảo mật - Mã hóa mọi dữ liệu của bạn

Bạch Đình Vinh

Mã hóa là một cách tuyệt vời để giữ cho dữ liệu an toàn, cho dù bạn truyền nó qua Internet, sao lưu lên máy chủ hoặc mang qua an ninh sân bay trên máy tính xách tay của mình. Việc mã hóa không cho phép bất cứ ai (trừ bạn và người sẽ nhận nó) đọc được dữ liệu của bạn.

Nhiều phần mềm được sử dụng trong văn phòng, trên máy tính cá nhân đã có chức năng mã hóa tích hợp. Bạn chỉ cần biết nơi để tìm thấy chúng và phải làm như thế nào mà thôi. Đó chính là mục đích của bài viết này.

Trước tiên, hãy nói về mật khẩu

Những điều nên làm khi tạo mật khẩu	Những điều không nên làm khi tạo mật khẩu
Tạo các mật khẩu dài (ít nhất là 7 ký tự).	Không sử dụng tất cả hoặc một phần của tên đăng nhập.
Bao gồm các chữ cái viết thường và viết hoa, các chữ số, và các ký hiệu.	Không sử dụng một từ có nghĩa trong bất kỳ ngôn ngữ nào.
Sử dụng ít nhất một ký hiệu trong vị trí thứ 2 đến thứ 6.	Không sử dụng các chữ số thay thế các chữ cái tương tự để tạo ra một từ.
Sử dụng ít nhất 4 ký tự khác nhau (không nhắc lại cùng các ký tự).	Không sử dụng các chữ cái hoặc chữ số liên tiếp (ví dụ, "abcdefg" hoặc "234567").
Sử dụng các chữ cái và chữ số ngẫu nhiên.	Không sử dụng các phím cạnh nhau trên bàn phím của bạn (ví dụ, "qwerty").

Hầu hết các hình thức mã hóa đều yêu cầu bạn thiết lập mật khẩu, cho phép bạn mã hóa tập tin và sau đó giải mã nó khi bạn muốn xem lại. Nếu bạn sử dụng mật khẩu yếu, tin tặc có thể phá mã hóa và truy cập tập tin, làm thất bại mục đích của mã hóa. Một mật khẩu mạnh nên có từ 10-12 ký tự. Nó nên là sự kết hợp của chữ hoa và chữ thường, số và ký hiệu. Nếu bạn thấy mật khẩu chỉ chứa chữ cái sẽ dễ nhớ hơn, thì một mật khẩu vẫn có thể an toàn nếu nó dài hơn đáng kể, ví dụ như gồm 20 ký tự hoặc nhiều hơn.

Nếu bạn không chắc chắn về việc liệu mật khẩu của mình đã đủ tốt hay chưa, hãy kiểm tra nó thông qua dịch vụ kiểm tra mật khẩu miễn phí của Microsoft (https://www.microsoft.com/en-gb/security/pc-security/password-checker.aspx). Đừng bao giờ sử dụng một mật khẩu bị đánh giá dưới mức "Strong".

Tham khảo bài "Tạo và nhớ mật khẩu" trên Số Hóa:http://sohoa.vnexpress.net/tin-tuc/kinh-nghiem/Tao-va-nho-mat-khau-1544098.html.

1. Mã hóa toàn bộ ổ cứng

Có thể bạn đã có mật khẩu đăng nhập Windows trên máy tính của mình, nhưng

Những điều nên làm khi quản lý mật khẩu	Những điều không nên làm khi quản lý mật khẩu
Giữ bí mật mật khẩu của bạn.	Không viết nó ra.
Sử dụng các mật khẩu khác nhau cho các trang web khác nhau.	Không sử dụng tính năng "remember my password" (nhớ mật khẩu của tôi) trên web.
Thay đổi các mật khẩu của bạn ít nhất 6 tháng một lần.	

mật khẩu đó sẽ không thực sự bảo vệ dữ liệu nếu ai đó đánh cắp máy tính hoặc ổ cứng của bạn. Tên trộm chỉ cần cắm ổ đĩa của bạn vào máy tính khác và truy cập dữ liệu trực tiếp. Nếu có thông tin nhạy cảm, bạn sẽ muốn thực hiện mã hóa đĩa cứng để bảo vệ dữ liệu ngay cả khi máy tính rơi vào tay kẻ xấu.

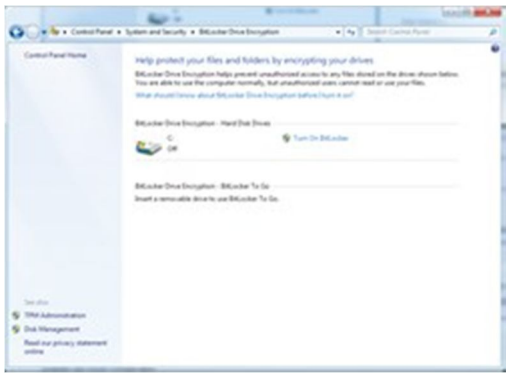
Phần mềm BitLocker của Microsoft làm cho việc thiết lập mã hóa đĩa đầy đủ trong

Windows vô cùng dễ dàng, miễn là máy tính của bạn đáp ứng 2 tiêu chí sau đây:

1. Bạn có phiên bản Ultimate/Enterprise của Windows 7/Windows Vista, hoặc phiên bản Pro/Enterprise của Windows 8.

2. Máy tính của bạn có chip TPM (Trusted Platform Module).

Cách dễ nhất để xem liệu máy tính của bạn có chip TPM hay không là cố gắng kích hoạt BitLocker. Windows sẽ cho bạn biết nếu bạn không có chip này.



Sử dụng BitLocker của Microsoft để mã hóa đĩa đầy đủ.

Để kích hoạt BitLocker, vào Control Panel > System and Security > BitLocker Drive Encryption, hoặc thực hiện tìm kiếm đối với từ "BitLocker" trong Windows 8. Trong menu BitLocker, nhấp Turn on BitLocker bên cạnh ổ đĩa bạn muốn mã hóa. Nếu máy tính của bạn không đáp ứng các yêu cầu cho BitLocker, bạn vẫn có thể sử dụng TrueCrypt hoặc DiskCryptor để mã hóa đĩa đầy đủ, miễn phí.

2. Mã hóa ổ cứng lắp ngoài, ổ USB của bạn

Để mã hóa đĩa đầy đủ cho ổ USB, ổ cứng lắp ngoài (qua cổng USB), bạn có thể sử dụng BitLocker To Go - được thiết kế cho các đĩa tháo lắp được. Bạn vẫn cần phiên bản Professional hoặc Enterprise của Windows, nhưng bạn không cần chip TPM để sử dụng BitLocker To Go.

Tất cả những gì bạn phải làm là cắm thiết bị mà bạn muốn mã hóa vào máy tính, sau đó vào menu BitLocker một lần nữa. Ở dưới cùng của menu, bạn sẽ thấy phần BitLocker To Go, nơi bạn có thể nhấp vào Turn on BitLocker ở bên cạnh thiết bị.

3. Mã hóa lưu lượng truy cập Internet

BitLocker cũng bảo vệ các ổ đĩa bỏ túi.

Đôi khi bạn muốn mã hóa lưu lượng Internet đi/đến của mình. Nếu bạn đang ở trên một mạng Wi-Fi không an toàn (ví dụ, tại sân bay), tin tặc có thể chặn dữ liệu chứa thông tin nhạy cảm được truyền đến/đi từ máy tính xách tay của bạn. Để làm những dữ liệu đó trở nên vô dụng đối với tin tặc, bạn có thể mã hóa dữ liệu bằng cách sử dụng mạng riêng ảo (VPN).

Mạng riêng ảo tạo ra "đường hầm" an toàn đến máy chủ của bên thứ ba đáng tin cậy. Dữ liệu được gửi thông qua đường hầm này (hoặc đến hoặc từ máy tính của bạn) được mã hóa, vì vậy nó an toàn ngay cả khi bị chặn. Bạn có thể tìm thấy nhiều VPN dựa trên web có mức thu phí hàng tháng thấp, nhưng cung cấp truy cập rất dễ dàng. Bạn còn có thể thiết lập VPN của riêng cá nhân hoặc VPN của doanh nghiệp.

Quá trình lựa chọn, thiết lập VPN được mô tả trong bài "Triển khai hệ thống IPSec/VPN trên Windows Server 2003" trên website PC World VN (http://www.pcworld.com.vn/) và bài "An toàn khi truy cập Wi-Fi công cộng" trên Số Hóa (http://sohoa.vnexpress.net): http://sohoa.vnexpress.net/tin-tuc/kinh-nghiem/An-toan-khi-truy-cap-Wi-Fi-cong-cong-1719084.html.

TrueCrypt giúp thêm mức độ bảo vệ khác cho dữ liệu Dropbox.

4. Mã hóa Dropbox (hoặc dịch vụ lưu trữ đám mây khác) của bạn

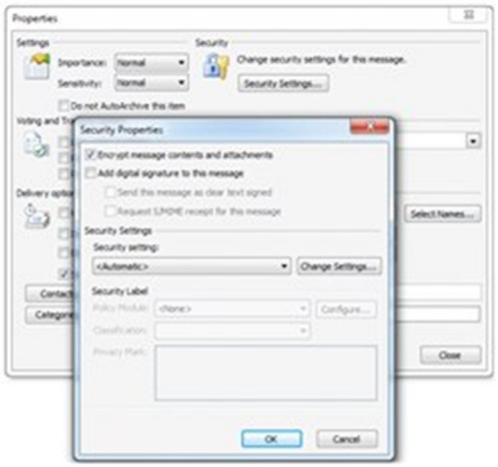
Nếu bạn hoặc những người khác trong tổ chức của mình sử dụng Dropbox hoặc SugarSync, bạn sẽ biết rằng các dịch vụ lưu trữ đám mây phổ biến này đã mã hóa dữ liệu của bạn, bảo vệ dữ liệu khi truyền và trong khi được lưu trên các máy chủ của họ. Thật không may, cũng chính những dịch vụ đó nắm giữ chìa khóa giải mã, có nghĩa là họ có thể giải mã các tập tin của bạn nếu như các lực lượng thực thi pháp luật bắt họ phải làm như vậy.

Nếu bạn có bất kỳ tập tin thực sự nhạy cảm nào trong dịch vụ lưu trữ đám mây của mình, hãy sử dụng lớp mã hóa thứ hai để giữ cho chúng an toàn khỏi những con mắt tò mò. Cách đơn giản nhất để làm điều này là sử dụng TrueCrypt (hãy xem phần cuối bài viết này).

Nếu bạn muốn có thể truy cập dữ liệu từ các máy tính khác, hãy đặt phiên bản di động (portable) của TrueCrypt trong Dropbox của mình. Để làm như vậy, hãy chạy trình cài đặt TrueCrypt. Trong khi cài đặt, chọn tùy chọn Extract, và chọn để đặt các tập tin đã được bung (extracted file) trong Dropbox hoặc dịch vụ lưu trữ đám mây khác của bạn.

5. Mã hóa email

Email của bạn có thể chứa thông tin nhạy cảm, do đó chúng cần được mã hóa ngay. Nếu



Bạn phải tích vào hộp kiểm để mã hóa email Outlook.

sử dụng Outlook, việc giữ cho thư của bạn được an toàn là tương đối dễ dàng.

Mã hóa của Outlook không dựa trên mật khẩu. Thay vào đó, tất cả những người muốn sử dụng tính năng bảo mật bằng mật mã trong Outlook nhận được một chứng chỉ số để tự động mã hóa/giải mã các email. Trước khi 2 người dùng có thể gửi cho nhau thư đã mã hóa, họ phải chia sẻ chứng chỉ của mình bằng cách gửi cho nhau email có chữ ký số. Tuy nghe có vẻ phức tạp, nhưng quá trình này thực sự đơn giản, và chỉ mất vài phút. Để thiết lập Outlook nhằm gửi email đã mã hóa, hãy làm theo các bước trong hướng dẫn chính thức của Microsoft (http://office.microsoft.com/en-us/outlook-help/get-a-digital-id-HP010355070.aspx).

Một khi đã nhận được và trao đổi ID số, nhấp vào *Options* > *More Options* > *Security Settings* và tích vào hộp kiểm Encrypt message contents and attachments, bạn có thể gửi email đã được mã hóa bằng cách mở cửa sổ New Message (thư mới)

6. Mã hóa thư Gmail

Khi bạn sử dụng Gmail, bảo mật email hơi khác một chút do thư được lưu trữ trên máy chủ của Google chứ không phải trên máy tính của bạn. Khi bạn soạn hoặc xem các email, chúng truyền qua kết nối HTTPS đã mã hóa, vì vậy bạn không phải lo lắng về việc bị chặn. Nguy cơ bảo mật chính với Gmail là người khác sẽ truy cập được vào tài khoản của bạn. Bạn có thể giảm thiểu nguy cơ này thông qua việc đặt mật khẩu và xác thực 2 bước.

Bảo vệ thư Gmail bằng một cách tiếp cận khác.

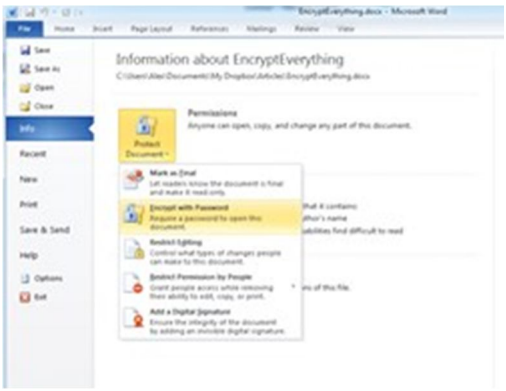
Nếu bạn muốn gửi email văn bản mà chỉ người nhận có thể đọc được, hãy sửdụng ứng dụng mã hóa dựa trên trình duyệt để mã hóa email của mình một cách thủ công rồi gửi email đã mã hóa văn bản đến người nhận. Sau đó, sử dụng một số kênh khác để gửi cho người nhận mật khẩu để họ có thể sử dụng cùng ứng dụng web đó nhằm giải mã email.

Tham khảo bài "Bảo mật: Gmail, bất khả xâm phạm!" trên Số Hóa (http://sohoa.vnexpress.net): http://sohoa.vnexpress.net/tin-tuc/kinh-nghiem/Bao-mat:-Gmail,-bat-kha-xam-pham-1718993.html.

7. Mã hóa tài liệu Word, Excel và PowerPoint

Trong Office 2010 và 2013, bạn có thể mã hóa bất kỳ tài liệu Word, Excel hoặc PowerPoint nào theo cùng một cách: Nhấp File, chọn tab Info và sau đó nhấp vào nút Protect Document. Cuối cùng, bấm vào Encrypt with Password và chọn một mật khẩu mạnh cho tập tin của bạn. Bất cứ ai muốn truy cập tập tin này sẽ cần mật khẩu. Hãy lưu ý, sẽ không an toàn nếu gửi mật khẩu thông qua cùng kênh mà bạn sử dụng để gửi tập tin.

8. Mã hóa tập tin PDF



Các tài liệu Office được bảo vệ bằng mật khẩu.

Cũng giống như các sản phẩm Office của Microsoft, Adobe Acrobat X Pro làm choviệc mã hóa tập tin khá dễ dàng. Tùy chọn này trong tab Tools ở phía trên bên phải, trong phần Protection. Nhấp vào nút Encrypt, sau đó nhấp vào tùy chọn Encrypt With Password.

Mã hóa ghi chú Evernote

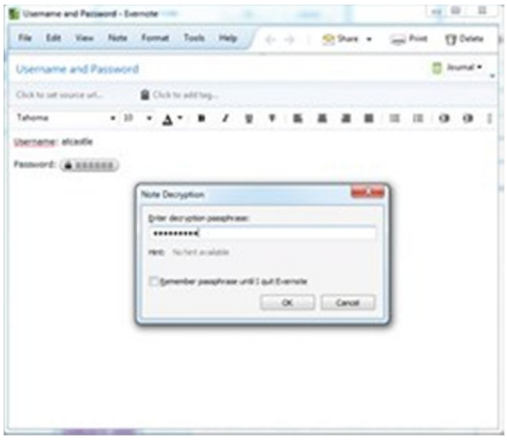
Ứng dụng điện toán đám mây Evernote (ghi chú) là một cách tuyệt vời để nhớ, tổ chức những thông tin quan trọng như các chi tiết tài khoản, hồ sơ y tế/tài chính và các dữ liệu nhạy cảm khác. Nếu

cảm thấy không thoải mái để tất cả những thông tin cá nhân đó mở, bạn nên biết rằng Evernote đã có tính năng mã hóa tích hợp.

Đơn giản chỉ cần mở ghi chú ra, đánh dấu đoạn văn bản bạn muốn ẩn và nhấp chuột phải vào nó. Trong menu hiện ra, chọn Encrypt Selected Text và sau đó tạo ra mật khẩu. Evernote giấu đoạn văn bản đã được lựa chọn, thay thế nó bằng biểu tượng khóa nhỏ. Bất cứ khi nào bạn muốn xem lại đoạn văn bản bị ẩn đó, chỉ cần nhấp đúp chuột vào biểu tượng và nhập mật khẩu của bạn.

9. Mã hóa những thứ khác

Một cách để mã hóa bất cứ thứ gì trên máy tính của bạn là dùng ứng dụng nguồn mở miễn phí TrueCrypt. TrueCrypt cho phép bạn mã hóa bất kỳ tập tin/nhóm tậptin nào trên máy tính của mình. Nếu máy tính riêng hoặc tại nơi làm việc của bạn có nhiều tài liệu nhạy cảm, TrueCrypt có lẽ là lựa chọn tốt nhất cho bạn.



Mở một ghi chú Evernote đã mã hóa.

Adobe cung cấp nhiều thiết lập bảo mật phong phú cho các tập tin PDF.

Để sử dụng TrueCrypt, đầu tiên hãy tải chương trình về từhttp://www.truecrypt.org/ và sau đó chạy trình cài đặt. Hãy giữ nguyên các tùy chọn cài đặt mặc định và chỉ cần nhấp

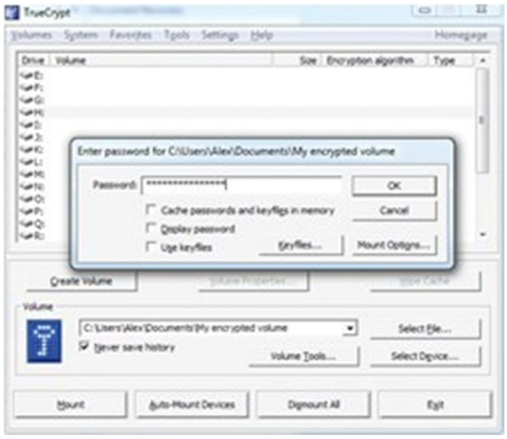
vào nút Next cho đến cuối.

Tiếp theo, chạy TrueCrypt và nhấp vào nút Create Volume. Một cửa sổ sẽ bật lên hướng dẫn bạn. Trên 2 màn hình đầu tiên, hãy giữ nguyên các tùy chọn mặc định và nhấp vào nút Next. Trên màn hình thứ 3, bạn sẽ được yêu cầu chỉ ra vị trí của volume. Đây là nơi mà các dữ liệu đã mã hóa sẽ được lưu trữ trên đĩa cứng, do đó hãy chọn vị trí và tên giúp bạn dễ nhớ. Để xác định vị trí, nhấp Select File sẽ mở ra cửa sổ duyệt tậptin. Tuy nhiên, không giống như hầu hết các cửa sổ duyệt tập tin, đây là nơi bạn nhập tên vào trường Name, sau đó một tập tin với tên đó sẽ được tạo racho TrueCrypt sử dụng.

TrueCrypt có thể bảo vệ bất kỳ loại tập tin nào.

Màn hình tiếp theo yêu cầu các thiết lập mã hóa. Hãy giữ nguyên những giá trị mặc định và nhấp vào nút Next. Sau đó, bạn sẽ được yêu cầu chỉ ra kích thước của volume. Tất cả các tập tin mà bạn muốn mã hóa sẽ phải vừa với volume, do đó hãy chắc chắn để cấp phát cho đủ. Nếu bạn chỉ đang lưu trữ các tài liệu văn bản thì 500MB có thể là đủ, nhưng nếu bạn sẽ lưu trữ rất nhiều tập tin đa phương tiện thì ít nhất bạn phải có vàigigabyte.

Đến đây bạn sẽ được yêu cầu cung cấp mật khẩu, hãy chọn một mật khẩu! Sau đó, bạn có thể kết thúc quá trình. Hãy thựchiện theo các hướng dẫn trên màn hình cuối cùng, và nhấp vào Format.



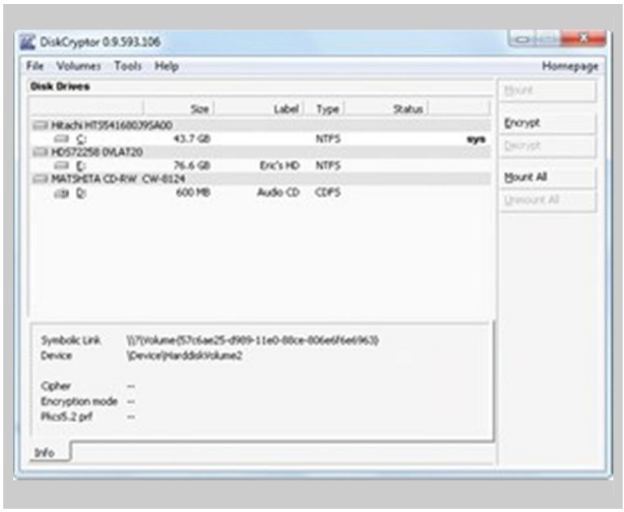
Trong TrueCrypt, hãy thiết lập mật khẩu để bảo vệ dữ liệu của bạn.

Bây giờ volume của bạn đã được tạo ra, bạn có thể sử dụng nó để lưu trữ các tập tin. Trong TrueCrypt, nhấp vào Select File và chọn tập tin volume mà bạn vừa tạo ra. Tiếp

theo, nhấn vào một ký tự ổ đĩa và nhấp vào Mount. Sau khi bạn nhập mật khẩu của mình, TrueCrypt tạo ra một ổ ảo và phần còn lại trên máy tính của bạn xử lý nó như thể bạn vừa lắp thêm một ổ cứng thực sự. Bạn có thể truy cập nó bạn làm với bất cứ ổ đĩa nào khác bằng cách, mở File Explorer ra và nhấp vào ký tự ổ đĩa của nó ở bên trái.
Kéo bất cứ tập tin nào bạn muốn mã hóa vào ổ cứng ảo. Khi thực hiện xong, nhấn Dismount trong TrueCrypt. Các tập tin mà bạn lưu trữ trong ổ cứng ảo được mã hóa và lưu trữ bên trong tập tin volume của bạn. Khi bạn muốn truy cập chúng một lần nữa, chỉ cần chạy TrueCrypt và gắn kết (mount) tập tin volume cũng giống như bạn đã làm trước đó.

Sử dụng DiskCryptor để mã hóa ổ cứng

Một khi bạn đã áp dụng mã hóa với DiskCryptor, mỗi lần bật máy tính của mình, bạn sẽ phải nhập mật khẩu mã hóa để cho phép nó khởi động. Sau khi nhập mật khẩu, Windows khởi động như bình thường. Nếu bạn có mật khẩu Windows riêng, bạn cũng sẽ phải nhập mật khẩu đó.



Màn hình chính của DiskCryptor.

Nếu bạn muốn sử dụng DiskCryptor, hãy tải xuống từ website của công ty (http://diskcryptor.net/wiki/Downloads/en). Bạn có thể sẽ muốn chọn phiên bản Stable Installer (cài đặt ổn định) mới nhất.
Như nhà sản xuất của DiskCryptor khuyến nghị, bạn nên theo hướng dẫn của công ty (http://diskcryptor.net/wiki/LiveCD/en) để tạo ra đĩa Windows có khả năng khởi động (LiveCD) có chứa DiskCryptor trước khi mã hóa ổ đĩa Windows của mình. Bằng cách đó, nếu gặp vấn đề khi khởi động,

bạn có thể đút đĩa LiveCD vào và sử dụng tiện ích trong DiskCryptor để giải mã ổ đĩa với mật khẩu của mình.

Khi bạn đã sẵn sàng để mã hóa, chỉ cần mở DiskCryptor, chọn ổ đĩa hệ thống (thường là C:\) và nhấn Encrypt. Sau đó, làm theo các hướng dẫn để cấu hình nhiều thiết lập khác nhau. DiskCryptor có thể mất một vài giờ để mã hóa ổ đĩa, tùy thuộc vào kích thước của ổ đĩa. Bạn có thể tiếp tục sử dụng máy tính của mình, nhưng nếu cần phải khởi động lại hoặc tắt máy, hãy nhớ nhấp vào Pause đầu tiên. Để tiếp tục quá trình, bạn chỉ cần chọn ổ đĩa và nhấn Encrypt một lần nữa. Nếu đang mã hóa máy tính xách tay, hãy cắm bộ sạc vào ổ điện trên tường, bạn sẽ không bị mất điện trong quá trình này.

Sau khi bạn đã hoàn tất mã hóa ổ đĩa của mình, hãy sao lưu thông tin tiêu đề (header) volume ổ đĩa của bạn. Nhờ đó, nếu header bị mất hoặc bị hỏng, bạn có thể khôi phục lại nó và không bị mất dữ liệu đã được mã hóa. Để sao lưu, mở DiskCryptor ra, nhấp vào Tools > Backup Header và sau đó lưu sao lưu vào ổ USB hoặc máy tính khác.

Hãy nhớ rằng, các tiện ích bên ngoài Windows (như LiveCD hoặc ổ USB có khả năng khởi động) không thể truy cập ổ đĩa đã mã hóa của bạn. Kết quả là, bạn sẽ không thể sửa chữa, cài đặt lại hoặc nâng cấp Windows mà không giải mã ổ đĩa hệ thống trước - hoặc bằng cách chạy DiskCryptor trong Windows hoặc bằng cách sử dụng đĩa Windows có khả năng khởi động mà bạn tạo ra có chứa DiskCryptor.

Tham khảo bài "Mã hóa ổ cứng để bảo vệ dữ liệu của bạn" trên Số Hóa : http://sohoa.vnexpress.net/tin-tuc/doi-song-so/bao-mat/Ma-hoa-o-cung-de-bao-ve-du-lieu-cua-ban-1544279.html.