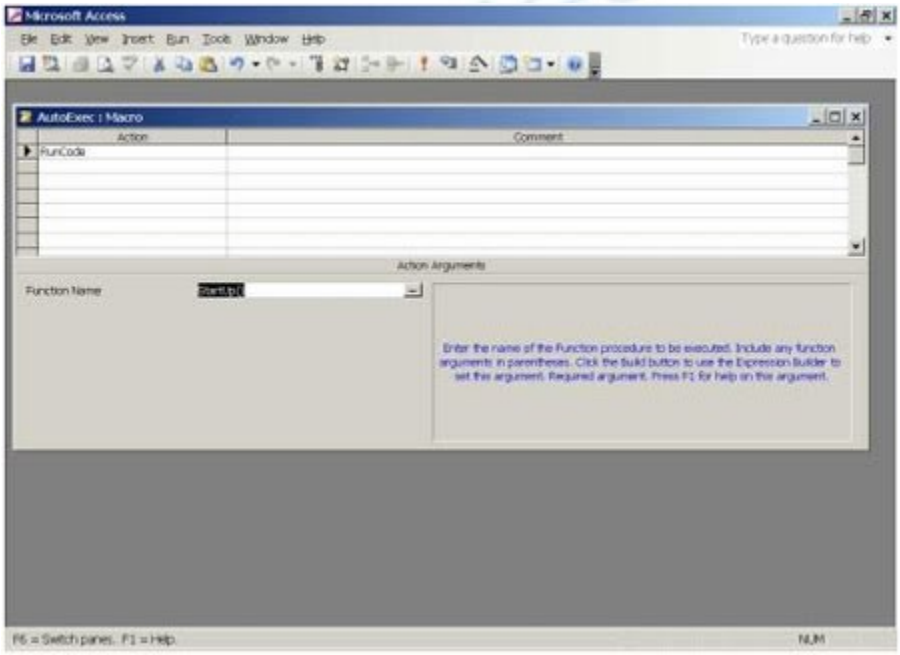
Bảo mật cơ sở dữ liệu trong Access

Sau đây là 10 thủ thuật bảo mật cơ sở dữ liệu Access

Cơ sở dữ liệu là kho chứa dữ liệu quan trọng cần được bảo vệ. Bạn có thể sử dụng những phần mềm bảo mật chuyên nghiệp để cơ sở dữ liệu, nhưng để có phần mềm đó chắc hẳn bạn sẽ phải trả một khoản phí không nhỏ. Ngược lại, bạn có thể sử dụng một số tính năng bảo mật của Access để bảo mật cơ sở dữ liệu ở một mức độ nhất định.

Những thủ thuật dưới đây sẽ giúp bạn khai thác được một số tính năng bảo mật sẵn có của Microsoft Access.

1. Sử dụng macro AutoExec để kiểm tra và thiết lập lại cài đặt



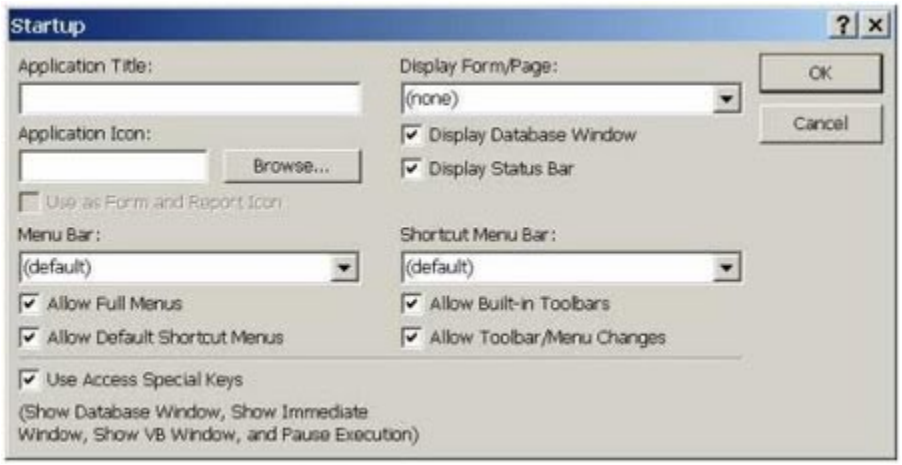
Sử dụng macro AutoExec để kiểm tra và thiết lập lại các tùy chọn bảo mật có thể bị thay đổi trong các phiên làm việc trước đó. AutoExec là một macro đặc biệt có thể thực hiện mở cơ sở dữ liệu. Để tạo một macro AutoExec, chỉ cần đặt tên cho một macro AutoExec mới. Ví dụ, macro Startup() (trong hình) có chức năng xác định người dùng, thực hiện kiểm tra và cài đặt các thuộc tính bảo mật trước khi người dùng truy cập.

2. Ẩn cửa sổ Database

Những tùy chọn khởi động trong hình B cho phép bạn xác định các thuộc tính của cơ sỡ dữ liệu khi mở. Hai trong số những thuộc tính này giúp cơ sở bảo dữ liệu bảo mật hơn:

*** Display Database Window:** Hủy chọn tùy chọn này để ẩn cửa sổ Database khi ai đó mở cơ sở dữ liệu. Do đó người dùng sẽ không thể truy cập trực tiếp vào bất cứ đối tượng nào.

*** Use Access Special Keys:** Bỏ tùy chọn này để người dùng không thể sử dụng phím F11 làm hiện cửa sổ Database.



Hai cài đặt này hỗ trợ cho nhau, vì nếu không bỏ chọn tùy chọn **Use Access Special Keys** người dùng có thể ấn phím **F11** để làm hiện cửa sổ Database.

Để truy cập vào những tùy chọn **Startup**, vào menu **Tools\ Startup**. Trong Access 2007, click vào nút **Office\ Access Options\ Current Database** trong cửa sổ trái và bạn sẽ thấy những tùy chọn này trong **Application Options**. **Access 2007** không có cửa sổ Database, nhưng bạn có thể làm ẩn **Navigation Pane** theo cách tương tự. Tùy chọn đó nằm trong **Navigation**, ngay bên dưới **Application Options**.

Việc bỏ chọn tùy chọn **Display Database** sẽ hủy lệnh **Startup**. Người dùng có thể loại những tùy chọn này bằng cách giữ phím **Shift** trong khi mở sơ sở dữ liệu. Đây là thủ thuật nhắc nhở cho bạn nhưng sẽ rất nguy hiểm nếu người khác biết được. Ngoài ra người dùng có thể đưa nhiều đối tượng vào một cơ sở dữ liệu trống để tránh những cài đặt khởi động.

3. Chặn phím Shift

Bạn có thể sử dụng chính giao diện để ẩn cửa sổ **Database**. Nhưng việc sử dụng phím Shift lại gây nguy hiểm cho cơ sở dữ liệu. Bạn có thể hủy bỏ việc sử dụng phím Shift bằng cách đổi giá trị của thuộc tính **AllowBypassKey** thành **False** khi đóng cơ sở dữ liệu. Tuy nhiên, bạn cũng có thể gọi đoạn mã sau từ một tác vụ đóng bất kì:

```
Public Sub SetStartupOptions(propname As String, _
propdb As Variant, prop As Variant)
'Set passed startup property.
```

```
Dim dbs As Object
Dim prp As Object
Set dbs = CurrentDb
On Error Resume Next
dbs.Properties(propname) = prop
If Err.Number = 3270 Then
Set prp = dbs.CreateProperty(propname, _
propdb, prop)
dbs.Properties.Append prp
End If
Set dbs = Nothing
Set prp = Nothing
End Sub
```

Khi gọi thủ tục, cần đảm bảo phải lựa chọn đúng tùy chọn khởi động. Ví dụ:

```
Call SetStartupOptions("AllowBypassKey", dbBoolean, False)
```

Sau khi cài đặt thuộc tính này cho tiến trình đóng, cơ sở dữ liệu sẽ vô hiệu hóa phím Shift.
Ngoài ra bạn có thể cài đặt bất kì thuộc tính khởi động nào. Ví dụ làm ẩn cửa sổ Database:

```
Call SetStartupOptions("StartupShowDBWindow", dbBoolean, False)
```

Bạn có thể cài đặt những tùy chọn đóng và mở cơ sở dữ liệu với một ngoại lệ. Đó là thuộc tính **AllowBypassKey** phải được cài đặt khi đóng cơ sở dữ liệu, và bạn cần đặt tham chiếu tới thư viện **Data Access Objects (DAO)**. Nếu không thủ tục này sẽ gây ra lỗi tham chiếu.

Tuy nhiên, nếu ai đó biết sử dụng phím Shift cũng có thể biết cách khôi phục lại nó bằng cách thay đổi giá trị của **AllowBypassKey** thành **True**. Trong trường hợp này bạn sẽ phải áp dụng phương pháp bảo mật nhóm làm việc để chỉ cho phép admin truy cập vào thuộc tính này.

4. Chia cơ sở dữ liệu

Việc bảo vệ một cơ sở dữ liệu nhỏ sẽ dễ dàng hơn rất nhiều so với cơ sở dữ liệu lớn với nhiều đối tượng dữ liệu và giao diện. Bạn có thể chia một cơ sở dữ liệu lớn thành hai cơ sở dữ liệu nhỏ, trong đó cơ sở dữ liệu thứ nhất chứa bảng và quan hệ (được gọi là backend), và cơ sở dữ liệu còn lại chứa các đối tượng giao diện (còn gọi là frontend). Hai cơ sở dữ liệu này giao tiếp thông qua các bảng đã được liên kết. Một điểm quan trọng là người dùng trong frontend không thể thay đổi thiết kế bảng trong backend. (có nhiều cách để phân chia cở sở dữ liệu nhưng bài viết này chỉ hướng vào mục đích bảo mật).

Để chia cơ sở dữ liệu, vào menu **Tools\ Database Utilities\ Database Spliter** sau đó làm theo hướng dẫn. Trong **Access 2007**, click **Access Database** trong nhóm **Move Data** của **tab Database Tools**.

5. Tránh sử dụng Compact On Close

Những ai đã từng sử dụng Access có lẽ đều biết đến tác dụng của việc nén cơ sở dữ liệu tường xuyên. Quá trình nén sẽ tạo ra một bản sao của cơ sở dữ liệu, kiểm tra các đối tượng, xóa bỏ dữ liệu tạm thời và sắp xếp lại những phần vỡ trên ổ đĩa. Tóm lại, nén giúp cơ sở dữ liệu luôn ổn định.

Tùy chọn **Compact On Close,** được tích hợp đầu tiên trong Access 2000, giúp nén cơ sở dữ liệu tự động khi kết thúc phiên làm việc. Không may, tiến trình này lại giữ lại cả những file không cần thiết. Nếu thấy những file tạm thời như *db1.mdb, db2.mdb,* … trong folder chứa cơ sở dữ liệu của bạn, chúng có thể là một sản phẩm phụ của tính năng nén.

Những file thừa này có thể gây ra rắc rối cho bạn nếu ai đó vào folder cũng có thể truy cập cả vào những file tạm thời. Đó là một lỗ hổng bảo mật. Có 2 cách để bảo vệ cơ sở dữ liệu của bạn:

* Thường xuyên kiểm tra và xóa những file tạm. (Tuy nhiên đây không phải là biện pháp thiết thực và thậm chí không có hiệu quả).

* Không sử dụng tính năng Compact On Close. Thay vào đó nên nén cơ sở dữ liệu theo cách thủ công. Đây là cách tốt nhất để bảo vệ cơ sở dữ liệu khỏi lỗ hổng trên.

6. Ẩn các đối tượng

Việc ẩn đi những đối tượng như bảng, truy vấn, form, … không phải là phương pháp bảo vệ hữu hiệu, vì nếu người dùng tìm thấy thì họ có thể thay đổi chúng. Tuy nhiên những đối tượng này sẽ được bảo mật hơn nếu người dùng không biết tới sự tồn tại của chúng. Việc ẩn các đối tượng chỉ đơn thuần giúp hạn chế lỗi gây mất dữ liệu mà không có tác dụng bảo mật. Để ẩn một đối tượng trong cửa sổ Database (hay Navigation), bạn chỉ cần phải chuột lên đối tượng, chọn **Properties** sau đó chọn tùy chọn **Hidden Attribute.**

Tuy nhiên, những người dùng Access có thể làm hiện những đối tượng này bằng cách vào menu **Tools\ Options**, chọn tab **View** sau đó hủy chọn tùy chọn **Hidden Objects** trong mục **Show**. Trong **Access 2007**, phải chuột vào thanh menu **Navigation**, chọn **Navigation Options\ Show Hidden Objects\ OK.**

Như đã nói, việc ẩn các đối tượng không có tác dụng bảo mật. Nếu bạn sử dụng phương pháp này, cần nhớ rằng những module ẩn vẫn hiển thị trên **Visual Basic Editor (VBE)**. Hơn nữa, chỉ nên ẩn những đối tượng quan trọng vì khi người dùng truy cập vào mà không thấy cửa sổ Database họ sẽ tìm kiếm nó. Bạn không thể nhập

những đối tượng ẩn vào một cơ sở dữ liệu nếu quá trình nhập không phù hợp.

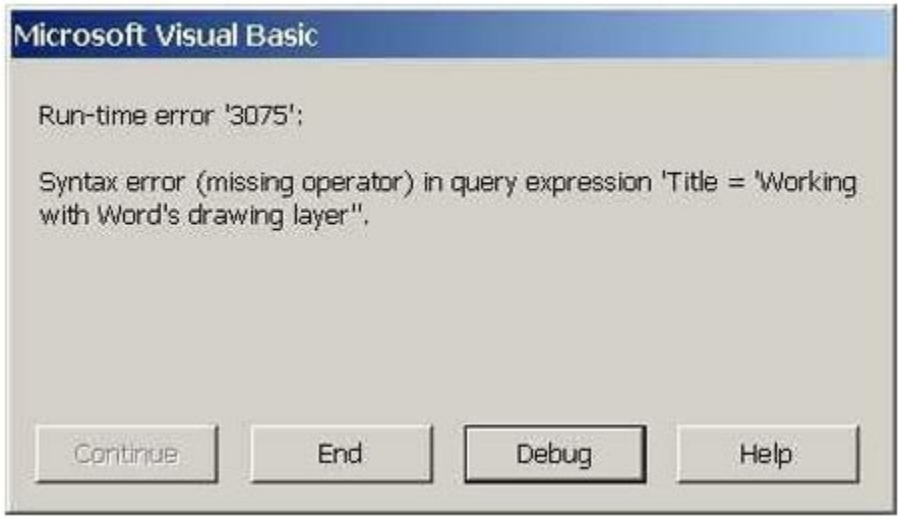
Bạn có thể lập trình để ẩn đi một đối tượng bằng mã VBA sau:

CurrentDb.TableDefs(tablename).Attributes = dbHiddenObject

Từ phiên bản Office 2000 trở về trước, việc sử dụng mã để gán thuộc tính ẩn vào một bảng rất rắc rối vì Access coi bảng đó là bảng tạm thời. Và trong lần nén tiếp theo Access sẽ xóa bỏ nó cùng với dữ liệu. Vì vây tránh sử dụng phương pháp này khi làm việc với các phiên bản đó.

7. Chặn thông báo lỗi

Khi xuất hiện lỗi trong mã, VBA hiển thị thông báo lỗi. Nếu người dùng nhận được thông báo đó và click vào nút Debug họ sẽ tiếp cận được với module chứa lỗi đó trong VBE. Trong trường hợp này người dùng có toàn quyền đối với đoạn mã. Thông thường, người dùng sẽ không biết xử lý và yêu cầu người lập trình giúp đỡ. Trái lại, cũng có tình huống người dùng xóa bỏ tất cả đoạn mã đó.



Trong giai đoạn phát triển, khả năng truy cập nhanh vào mã giúp tiết kiệm thời gian. Nhưng khi quản lý cơ sở dữ liệu thì đó là một thảm họa. Tốt nhất, trong mỗi thủ tục nên bổ sung một số tính năng xử lý lỗi để chặn thông báo và loại bỏ nút **Debug**.

8. Đặt mật khẩu bảo vệ cơ sở dữ liệu

Việc thiết lập mật khẩu cho cơ sở dữ liệu sẽ giới hạn quyền truy cập cho từng người dùng cụ thể cũng rất quan trọng mặc dù hiện nay có nhiều chương trình nhóm ba có thể phá bỏ mật khẩu của cơ sở dữ liệu.

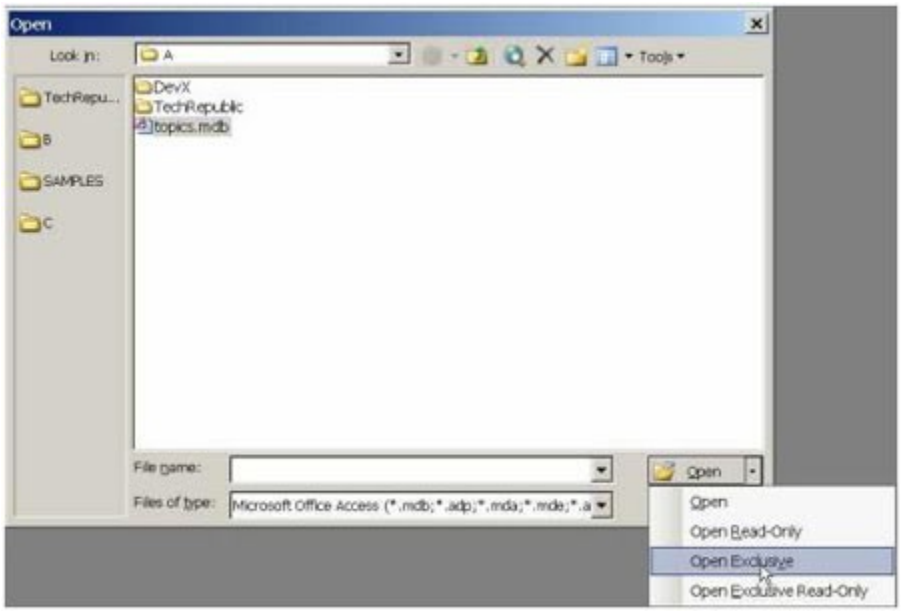
Để cài đặt mật khẩu bạn chỉ cần thực hiện các thao tác sau:

* Mở cơ sở dữ liệu theo chế độ **Exclusive** bằng cách chọn **Open Exclusive** trong hộp thoại **Open.**

* Vào menu **Tools\ Security\ Set Database Password.**

* Nhập mật khẩu vào hộp **Password** và **Retype Password**.

* Thực hiện xong click **OK**.



Để gỡ bỏ mật khẩu thực hiện các bước sau:

* Mở cơ sở dữ liệu trong chế độ **Exclusive.**

* Vào menu **Tools\ Security\ Unset Database Password.**

* Nhập mậu khẩu.

* Click **OK**.

Bạn cũng có thể đặt mật khẩu bảo vệ cho các module VBA:

* Từ menu **Tools** của **VBE**, chọn **Project Properties.**

* Chọn tiếp tab **Protection.**

* Chọn tùy chọn **Lock Project For Viewing**.

* Nhập mật khẩu (hai lần).

* Click **OK.**

9. Chuyển đổi định dạng sang “mde” hay “accde”

Access bổ sung tính năng bảo mật dưới một định dạng file mde hoặc accde (trong Access 2007). Định dạng này là một phiên bản “chỉ thực hiện” của cơ sở dữ liệu, có nghĩa là người dùng không có quyền truy cập vào mã qua VBE và họ không thể thay đổi các đối tượng. Định dạng này chỉ bảo vệ được thiết kế mà không bảo vệ được dữ liệu của bạn. Vì vậy bạn cần copy file mdb/accdb gốc trước khi nâng cấp hay thay đổi.

Tuy nhiên khi sử dụng bạn cần lưu ý:

* Chỉ sử dụng định dạng này với frontend. Không sử dụng để bảo mật cho backend hay một cơ sở dữ liệu độc lập. Còn nếu muốn thực hiện, bạn cần phải chuyển mọi dữ liệu sang một cơ sở dữ liệu mới mỗi khi nâng cấp frontend.

* Định dạng này cũng không bảo vệ bảng biểu, truy vấn, macro, quan hệ, thuộc tính cở dữ liệu và những tùy chọn khởi động.

Để chuyển đổi một cơ sở dữ liệu frontend sang định dạng mde hay accde bạn thực hiện các thao tác sau:

* Trong Access XP (hay các phiên bản Access trước đó), vào menu **Tools\ Database Utilities\ Make MDE** File. Trong Access 2007, click vào **Make ACCDE** của **Database Tools** trong tab **Database Tools.**

* Trong hộp thoại kết quả, đặt tên cơ sở dữ liệu mới và chọn đường dẫn thư mục lưu sau đó click **Save.**

10. Đặt mật khẩu bảo vệ hệ thống

Không phải lúc nào người dùng cũng làm việc trên máy tính, đôi khi họ phải đảm trách nhiều công việc khác. Những lúc đó máy tính của họ sẽ không được chú ý và rất có thể sẽ bị xâm nhập. Cách tốt nhất để tránh tình huống trên là đặt mật khẩu bảo vệ màn hình. Tiện ích bảo vệ màn hình sẽ tự động được kích hoạt khi máy tính nhàn rỗi. Người dùng sẽ phải nhập mật khẩu trước khi truy cập vào hệ thống.

Trong Windows XP, bạn có thể đặt mật khẩu cho tiện ích bảo vệ màn hình theo cách sau:

* Vào menu **Start\ Control Panel\ Display.**

* Chọn tab **ScreenSaver.**

* Chọn kiểu **ScreenSaver.**