10 security tips for Access database

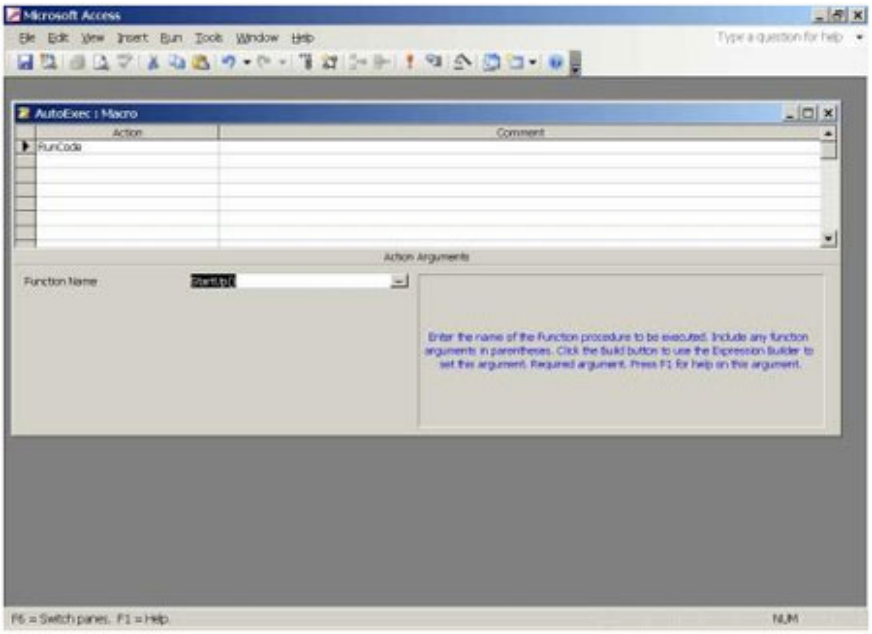
The following tips will help you explore some of the Microsoft Access security features available.

***Network administration* - Database is an important data repository that needs to be protected. You can use professional security software to database, but to have that software you will have to pay a small fee. Conversely, you can use some of Access's security features to secure the database to a certain extent.**

The following tips will help you explore some of the Microsoft Access security features available.

1. Use AutoExec macro to check and reset settings

Use the AutoExec macro to check and reset security options that may be changed during previous sessions. AutoExec is a special macro that can perform database opening. To create an AutoExec macro, simply name a new AutoExec macro. For example, the Startup () macro (pictured) has a function to identify users, perform checks and install security attributes before users access.

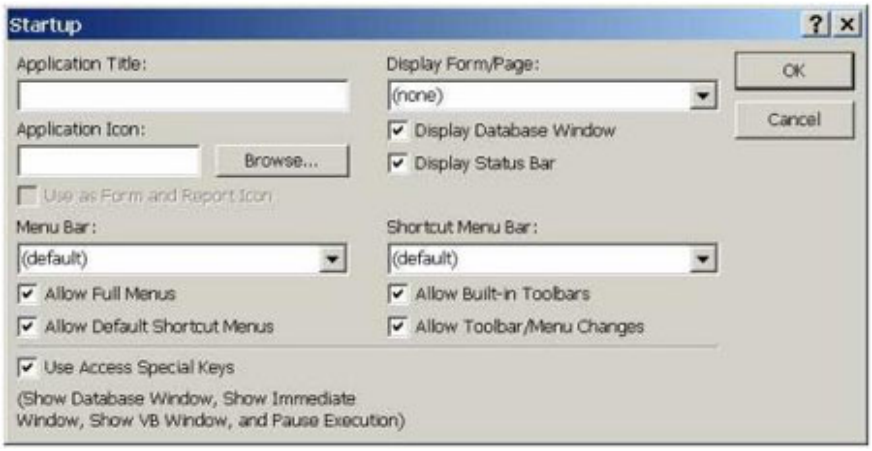


2. Hide the Database window

The boot options in Figure B allow you to specify the properties of the database when opened. Two of these attributes make the database more secure:

1. **Display Database Window** : Uncheck this option to hide the Database window when someone opens the database. Therefore users will not be able to directly access any object.

1. **Use Access Special Keys** : Remove this option so that users cannot use the F11 key to display the Database window.



These two settings support each other, because if you do not uncheck the **Use Access Special Keys option,** you can press F11 to bring up the Database window.

To access Startup options, go to **Tools Startup** menu. In Access 2007, click the **Office Access Options Current Database button** in the left window and you will see these options in **Application Options** . Access 2007 does not have a Database window, but you can hide the Navigation Pane in the same way. That option is in **Navigation** , just below **Application Options** .

Unchecking the **Display Database** option will cancel the **Startup** command. Users can remove these options by holding down the **Shift** key while opening the database. This is a trick to remind you, but it will be dangerous if other people know it. In addition, users can put multiple objects into an empty database to avoid boot settings.

3. Block the Shift key

You can use the same interface to hide the Database window. But using the Shift key is dangerous for the database. You can cancel the use of the Shift key by changing the value of **AllowBypassKey** to **False** when closing the database. However, you can also call the following code from any closed action:

```
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
```

When calling the procedure, be sure to select the right boot option. For example:

Call SetStartupOptions ("AllowBypassKey", dbBoolean, False)

After setting this property for the closing process, the database will disable the Shift key.
In addition, you can install any boot attribute. Example of hiding Database window:

Call SetStartupOptions ("StartupShowDBWindow", dbBoolean, False)

You can install closed and open options with an exception. That is the **AllowBypassKey** attribute must be set when the database is closed, and you need to set a reference to the **Data Access Objects** library (DAO). Otherwise this procedure will cause a reference error.

However, if someone knows that using the Shift key can know how to restore it by changing the value of **AllowBypassKey** to **True** . In this case you will have to apply the workgroup security method to only allow the admin to access this attribute.

4. Divide the database

Protecting a small database is much easier than a large database with multiple data objects and interfaces. You can split a large database into two small databases, in which the first database contains tables and relations (called *backend*), and the other database contains allotment objects. (also called *frontend*). These two databases communicate through linked tables. An important point is that users in the *frontend* cannot change the table design in the *backend* . (There are many ways to split the database but this article is only for security purposes.)

To split the database, go to **Tools Database Utilities Database Spliter** menu then follow the instructions. In Access 2007, click **Access Database** in the **Move Data** group of the **Database Tools** tab.

5. Avoid using Compact On Close

Anyone who has ever used Access probably knows about the effect of compressing the wall database. The compression process will create a copy of the database, examine the objects, delete temporary data and rearrange the broken parts on the drive. In short, compression makes the database stable.

The **Compact On Close option** , first integrated in Access 2000, helps compress the database automatically at the end of the session. Unfortunately, this process retains unnecessary files. If you see temporary files like *db1.mdb, db2.mdb, .* in the folder containing your database, they can be a by-product of the compression feature.

These redundant files can cause problems for you if anyone enters the folder and can access the temporary files. That is a security hole. There are 2 ways to protect your database:

1. Regularly check and delete temporary files. (However, this is not a practical and even ineffective measure.)

1. Do not use the Compact On Close feature. Instead, compress the database manually. This is the best way to protect the database from the vulnerability.

6. Hide objects

Hiding objects such as tables, queries, forms, etc. is not an effective method of protection, because if users find them, they can change them. However, these objects will be more secure if users do not know their existence. Hiding objects simply helps to limit errors that cause data loss without security effects. To hide an object in the Database window (or Navigation), right-click the object, select **Properties,** and then select the **Hidden Attribute** option.

However, Access users can display these objects by going to the **Tools Options** menu, selecting the **View** tab and then **unchecking the Hidden Objects** option in the **Show** section. In Access 2007, right-click the **Navigation** menu bar, select **Show Hidden Objects Navigation Options OK** .

As mentioned, hiding objects does not have a security effect. If you use this method, remember that hidden modules are still displayed on the **Visual Basic Editor** (VBE). Moreover, only important objects should be hidden because when users access without seeing the Database window they will search for it. You cannot import hidden objects into a database if the import process does not match.

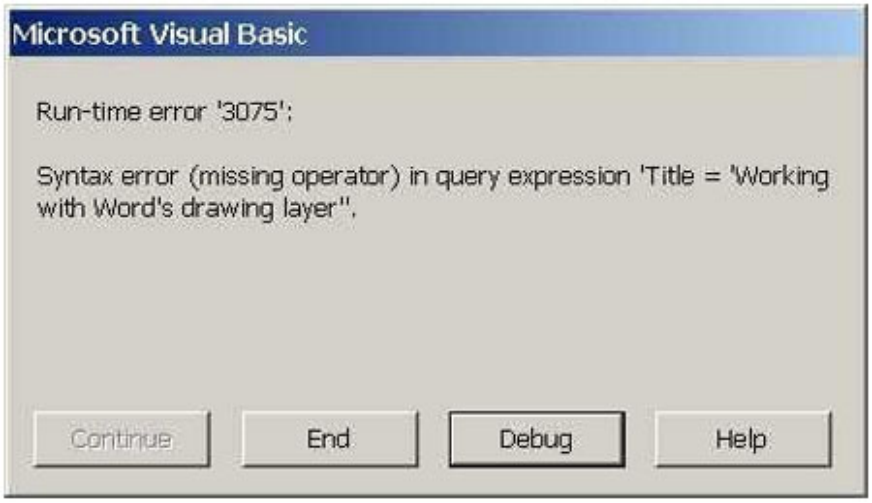
You can program to hide an object using the following VBA code:

CurrentDb.TableDefs (tablename) .Attributes = dbHiddenObject

From Office 2000 and earlier, the use of code to assign hidden properties to a table is very troublesome because Access considers that table to be a temporary table. And in the next compression, Access will delete it with the data. So avoid using this method when working with those versions.

7. Block error messages

When an error occurs in the code, VBA displays an error message. If the user receives that message and clicks on the **Debug** button, they will have access to the module containing the error in VBE. In this case the user has full control over the code. Typically, users will not know how to handle and ask programmers to help. In contrast, there is also a situation where users delete all the code.



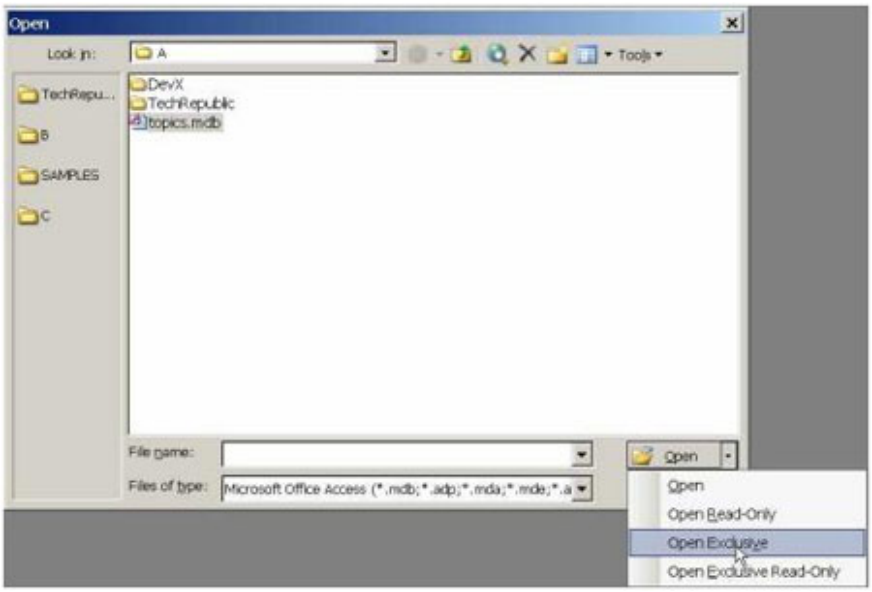
In the development phase, quick access to code saves time. But when managing databases, it is a disaster. Ideally, in each procedure should add some error handling features to block the message and remove the **Debug** button.

8. Set password to protect the database

It is also important to set a password for the database that limits access for each specific user, although many third-party programs can now break the database password.

To set up a password, you only need to do the following:

1. Open the **Exclusive** database by selecting **Open Exclusive** in the **Open** dialog box.
1. Go to **Tools Security Set Database Password** menu.
1. Enter the password in the **Password** and **Retype Password** box.
1. Done click **OK** .



To remove the password, perform the following steps:

1. Open the database in **Exclusive** mode.
1. Go to **Tools Security Unset** menu **Password Database** .
1. Import and export.
1. Click **OK** .

You can also set password protection for VBA modules:

1. From the **Tools** menu of VBE, select **Project Properties** .
1. Select the **Protection** tab.
1. Select the **Lock Project For Viewing option** .
1. Enter the password (twice).
1. Click **OK** .

9. Convert the format to 'mde' or 'accde'

Access adds security in a file format *mde* or *accde* (in Access 2007). This format is an 'only executable' version of the database, meaning that users do not have access to the code via VBE and they cannot change the object. This format only protects the design without protecting your data. So you need to copy the original *mdb / accdb* file before changing it or changing it.

However, when using, you should note:

1. Only use this format with the *frontend.* Not used for security for the *backend* or a standalone database. If you want to do this, you need to transfer all data to a new database every time you upgrade the *frontend* .

1. This format also does not protect tables, queries, macros, relations, data attributes, and boot options.

To convert a *frontend* database to the mde or *accde format,* do the following:

1. In Access XP (or earlier Access versions), go to the **Tools Database Utilities Make MDE File** menu. In Access 2007, click **Make ACCDE** of **Database Tools** in the **Database Tools** tab.

1. In the resulting dialog box, name the new database and select the directory path to save then click **Save** .

10. Set password to protect the system

Users don't always work on computers, sometimes they have to take on many other jobs. At that time their computers will not be noticed and will most likely be compromised. The best way to avoid the above situation is to set a screen saver password. The screensaver utility will automatically be activated when the computer is idle. Users will have to enter the password before accessing the system.

In Windows XP, you can set a password for the screen saver utility in the following way:

1. **Go to Start Control Panel Display** menu.

1. Select the **ScreenSaver** tab.

1. Select **ScreenSaver** type.

1. Set when **ScreenSaver** starts.

1. Select the option **On Resume, Password Protection** .

1. Click **OK** .