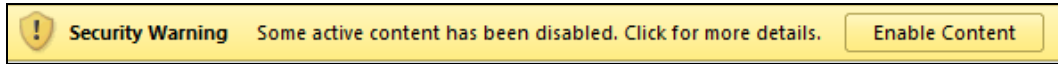


Setting a Trusted Folder in MS Access

We will use **macros** and **Visual Basic code** to automate tasks. Since macros and VB code are executable programs, they could be programmed do something malicious. By default, Access protects you by disabling them. It also displays a Security Warning that provides the option to allow them to run.

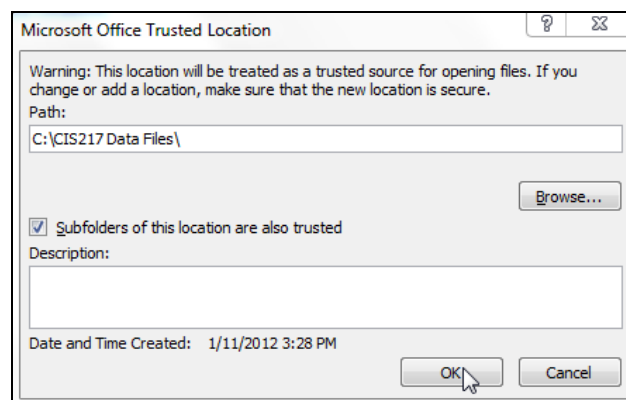


Imagine how it becomes tedious to have to click the **Enable Content** button each time you open a database file. Fortunately, you can designate a folder as a **Trusted Location**, which tells Access to permit macros and VB code to execute whenever one of the folder's files is opened.

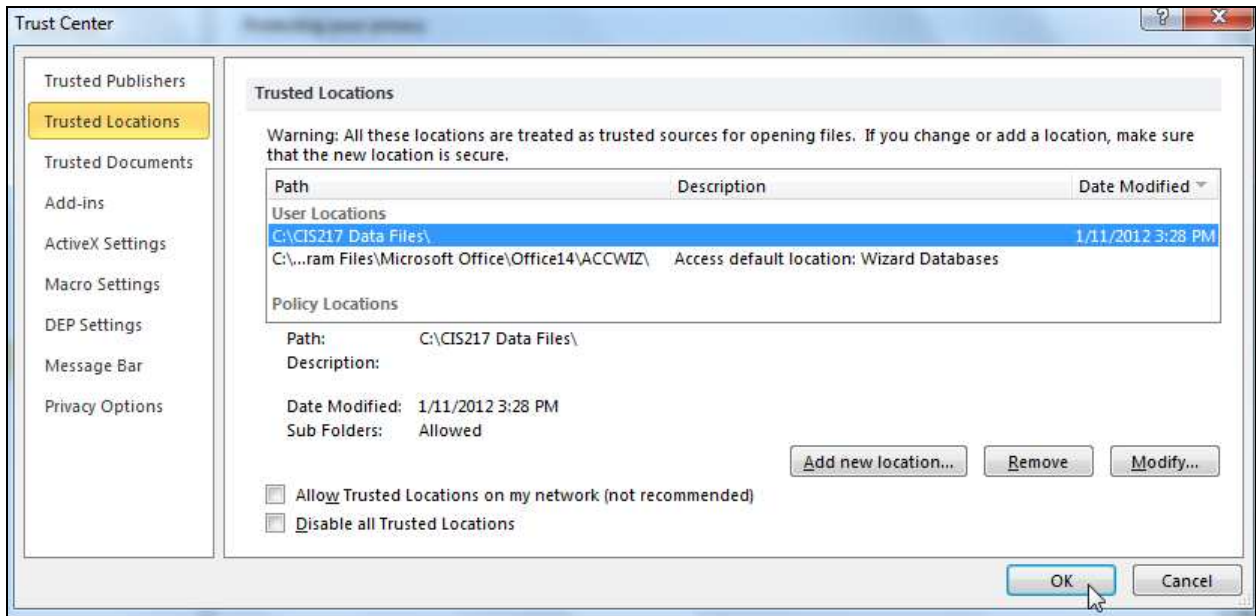
Perform the steps below to designate **C:\CIS217 Data Files** (and its subfolders) as a Trusted Folder.

Note: *This assignment can be completed only by those students who have a Windows PC with Access installed. Other students (who will be launching Access from within mySCC) will not be able to designate their H:\CIS217 Data Files folder a Trusted Folder. They do need to understand the concepts discussed above... so they'll know why they have to click Enable Content each time!*

1. Launch Access.
2. Click **File > Options > Trust Center > Trust Center Settings... > Trusted Locations > Add new location... > Browse....**
3. Navigate to the folder containing your class data files (eg: C:\CIS217 Data Files).
4. Click the checkbox for *Subfolders of this location are also trusted*.



5. Click **OK**. You should now see C:\CIS217 Data Files listed as a Trusted Location.



6. Click **Add new location...** and navigate to any additional folder that contains class data files, such as your USB flash drive's \CIS217 Data Files folder. Be sure to click the *Subfolders of this location are also trusted* option.
7. Click **OK** to close the *Trust Center* dialog box.
8. Click **OK** to close the *Access Options* dialog box and return to Access.