



PHISHING, RED TEAM AUTORUN, PENETRATION TESTING, PENTEST, PENTESTING, PHISHING,  
SOCIAL ENGINEERING

# Phishing with PowerPoint

[Carrie Roberts](#) & [Chevy Swanson](#) //

FOLLOW US

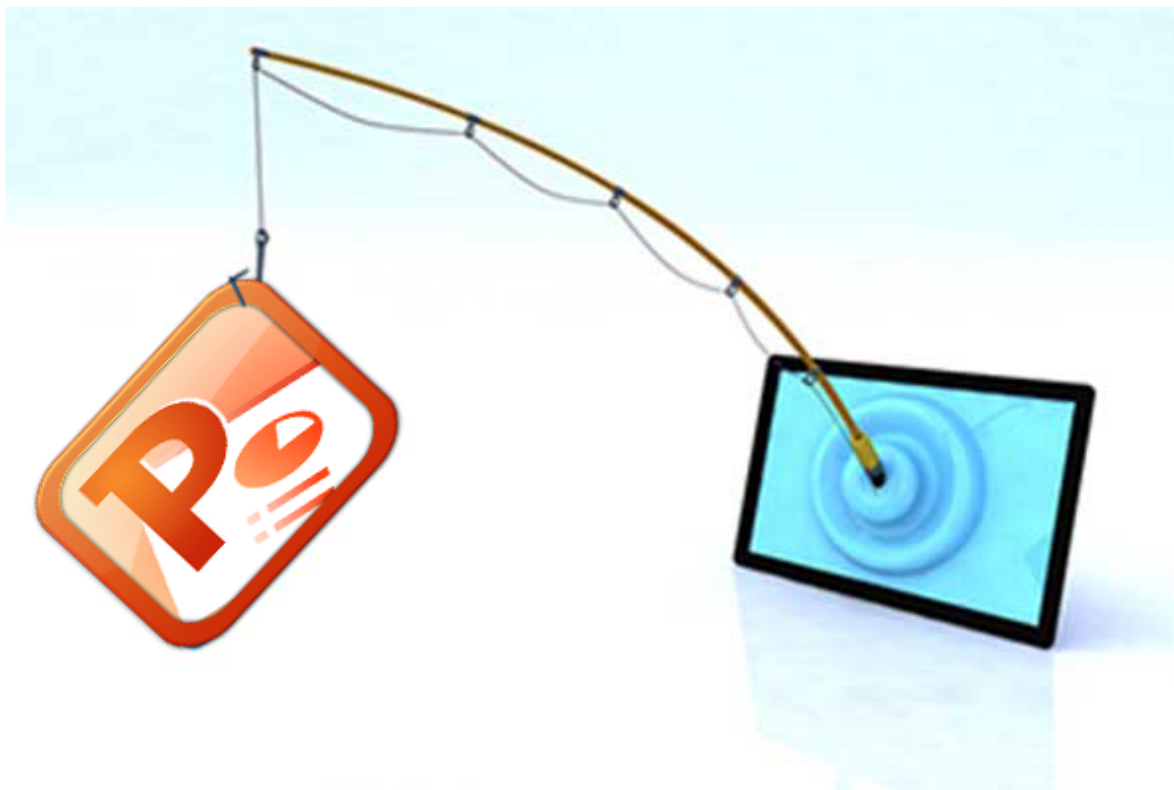


LOOKING FOR  
SOMETHING?



SUBSCRIBE TO THE  
BTHISBLOG

Don't get left in the dark! Enter  
your email address and every  
time a post goes live you'll get



How do we make sure people open up our malicious files and execute them? We simply let Microsoft work for years and years to gain people's trust, then we throw some dangerous macros into a powerpoint and people will actually have a smile on their face as they open it.

This other [great blog post](#) goes into more detail on the macros themselves and how to evade antivirus. This blog post adds a trick to get the macro to run as soon as the file is open without requiring additional user action, such as clicking or generating a mouseover event. This is a hack needed specifically for

instant notification! We'll also add you to our webcast list, so you won't miss our occasional emails about upcoming events! (We promise, we're not spammy!)

Subscribe

## BROWSE BY CATEGORY

Select Category ▼

## RECENT POSTS

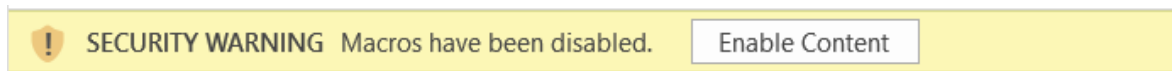


[Got Privs? Crack Those Hashes!](#)

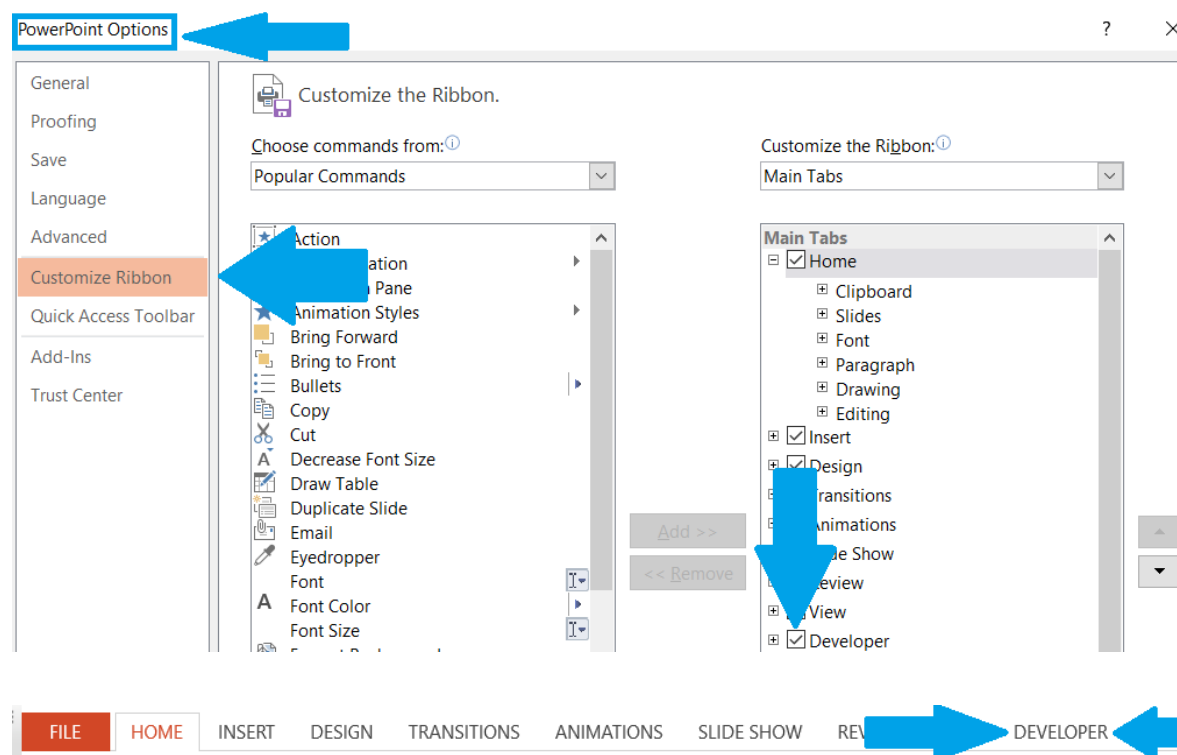
Joff Thyer// Black Hills  
Information Security  
loves

Powerpoint because it does not provide an Auto\_Open or Workbook\_Open option like Microsoft Word and Excel provide.

This blog post will cover how to get your macro to run as as soon as they enable macros via a nice little warning banner at the top of their screen.

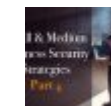


First things first, we need to open our powerpoint presentation and add the “DEVELOPER” Tab if it isn’t already there.



[WEBCAST: GDPR – Spring Storm Warning](#)

CJ Cox// Spring storms are often more dangerous and



[Small and Medium Business Security Strategies Part 4: CSC 3 – Vulnerability Management](#)

Jordan Drysdale// tl;dr

Vulnerability management is a

## BROWSE BY TOPIC

[ADHD](#) [anti-virus](#) [AV](#) [AV bypass](#)

[Blue Team](#) [Burp](#) [bypassing AV](#) [C2](#)

[Cylance](#) [Digital Ocean](#) [encryption](#)

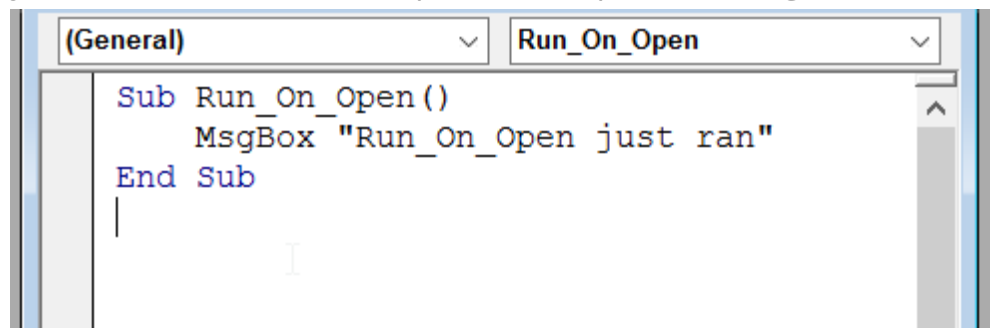
[hacking hardware](#) [hacking](#) [infosec](#) [it](#)

[security](#) [Linux](#) [Microsoft](#) [MS Word](#)

[Nessus](#) [Nmap](#) [Outlook](#) [OWA](#) [password](#)

[passwords](#) [password spraying](#)  
[pen-testing](#)  
[penetration testing](#)

In the developer tab click the “Visual Basic” button on the far left and that will open up a new window. Next, go to Insert>Module and here you can add in your macros. For this example we will open a message box.



Or, if you just want to copy the text for yourself:

```
Sub Run_On_Open()
```

```
    MsgBox "Run_On_Open just ran"
```

```
End Sub
```

Of course, if this had been an actual malicious attempt, you would have put your antivirus evading payload here instead, as shown in [Sally's blog post](#).

Save the powerpoint as a .pptm file and close it for now. Now there is the fast way and the barely slower way to do these next few steps. The fast way being the use of a program called CustomUI Editor which you can find a tutorial on how to use it for this purpose [here](#). We can't recommend the use of any

pentest **Pentesting**  
phishing **PowerShell**

PowerShell Empire privacy Red Team

red teaming RITA social engineering

steganography tool tools VPN

Vulnerabilities **webcast**

webcasts Windows

## ARCHIVES

Select Month ▼

random .msi file, so instead we are going to go through the more manual option.

First, you will want to unzip the powerpoint file into its own directory, then you will need to edit the \_rels/.rels file to add this line right before the last </Relationships>:

```
<Relationship
```


```
Type="http://schemas.microsoft.com/office/2006/relationships/ui/extensibility"
```

```
Target="/customUI/customUI.xml" Id="Rd6e72c29d34a427e" />
```

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId3"
Type="http://schemas.openxmlformats.org/package/2006/relationships/metadata/core-properties" Target="docProps/core.xml"/>
<Relationship Id="rId2" Type="http://schemas.openxmlformats.org/package/2006/relationships/metadata/thumbnail"
Target="docProps/thumbnail.jpeg"/><Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/o
Target="ppt/presentation.xml"/><Relationship Id="rId4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/exte
Target="docProps/app.xml"/><Relationship Type="http://schemas.microsoft.com/office/2006/relationships/ui/extensibility"
Target="/customUI/customUI.xml" Id="Rd6e72c29d34a427e" /></Relationships>
```

Next, you will need to create a new directory on the same level as the \_rels directory.

```
3201 Jan 1 1980 [Content_Types].xml
102 Mar 29 01:17 _rels
102 Mar 29 00:38 customUI
170 Mar 29 01:16 docProps
408 Mar 29 01:16 ppt
```



Create a file named customUI.xml in this new directory and add the following text:

```
1 <customUI xmlns="http://schemas.microsoft.com/office/2006/01/customui"
2   onLoad="Run_On_Open" > ← Name of Macro
3 </customUI>
```

```
<customUI xmlns="http://schemas.microsoft.com/office/2006/01/customui"
```

```
onLoad="Run_On_Open" >
```

```
</customUI>
```

Zip your files back up. If you are on a mac, make sure you exclude the .DS\_store files.

```
zip -r newRunOnOpen.pptm . -x "*.DS_Store"
```

Make sure you name it with a .pptm extension since the powerpoint must be able to load the custom ribbon we created. Your macros should now run upon opening of the powerpoint (once you enable macros).

---

**Share this:**



◀ What's trust among  
schoolchildren:  
Kerberos Authentication  
Explained

Nessus & Nmap ▶



## BLACK HILLS INFORMATION SECURITY

115 W. Hudson St. Spearfish, SD 57783 | 701-484-BHIS

© 2018

### LINKS



SEARCH THE SITE