Facebook To Safebook

Facebook Hacking And Security

Madhulika Singh
Department of Information Technology
Pacific Institute of Management, Pacific University
Udaipur, India
madhulika.singhr@gmail.com

Arun Kumar Singh
Department of Electronics and Communication
Graphic Era University
Dehradun, India
aruns444@gmail.com

Abstract— Social networking has become most popular activity in today's Internet world, with billions of people across the world are using this media to meet old friends, making new friends, to collect and share information, social networking while being a popular media has several disadvantages associated with it. These sites can be trapped by scammers or hackers leading to loss of confidentiality and identity theft, of the users. In addition there are many more risks like fake profiles with false information, malicious application, spam, and fake links which leads to phishing attacks etc., So in this paper we will discuss about various hacking methods and concentrate on securing our Facebook accounts from hackers and malicious users.

Keywords*- Phishing, Malicious user, Keyloggers, Hacker.*

*****

I. INTRODUCTION

Facebook is the most widely used Social Networking Site, having more than 1 Billion users and more than half of the users using it in mobile devices. Since it is a social networking site, many people make a lot of friends and many don't realize that there are more than 83 million fake Facebook profiles.

It is the second top website being accessed every day in the world according to Alexa.com which maintains the statistics of website rankings. And around 7,993,110 sites link to Facebook, which means that many sites provide link to Facebook page.

As Facebook has more than a billion users, Hackers and malicious users use Facebook as a medium of hacking, Several attacks and malicious links are posted in Facebook posing threat to several users. These can be easily prevented by using security features of Facebook and some simple softwares. But many people don't understand the risks behind these attacks.

We will discuss about various hacking methods and concentrate on securing our Facebook accounts from hackers and malicious users.

II. HACKING

A person who secretly gets access to a computer system in order to get information, cause damage, etc. is known as hacker. Hackers can be divided into three groups: white hats, black hats, and grey hats.

According to author Kimberley Graves (2007) [10], "Ethical hackers usually fall into the white-hat category, but sometimes they're former gray hats who have become security professionals and who use their skills in an ethical manner." Graves offers the following description for the three groups of hackers:

- *White Hats* are the good guys, the ethical hackers who use their hacking skills form protective purposes. White-hat hackers are usually security professionals with knowledge of hacking and the hacker toolset and who use this knowledge tolocate weaknesses and implement countermeasures .
- *Black Hats* are considered the bad guys: the malicious hackers or *crackers* use their skills for illegal or malicious purposes. They break into or otherwise violate the system integrity of remote machines, with malicious intent. Having gained unauthorized access, black-hat hackers destroy vital data, deny legitimate users service, and basically cause problems for their targets.
- *Grey Hats* are hackers who may work offensively or defensively, depending on the situation. This is the dividing line between hacker and cracker. Both are powerful forces on the Internet, and both will remain permanently. And some individuals qualify for both categories. The existence of such individuals further clouds the division between these two groups of people .

III. HOW HACKERS HACK FACEBOOK

Hackers hack the Facebook by the following hacking attacks:

A. *Facebook Phishing Attacks*

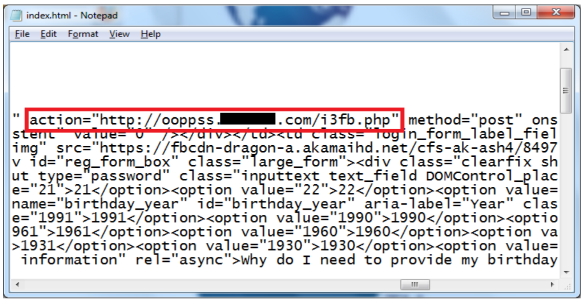
Creating a Facebook phishing page is similar to creating any other phishing page. The things we need to create a Facebook phishing page are,

1. Any free webhosting service or a paid hosting (For creating your fake page online) Ex: 000webhost.com, byethost.com, phpzilla.net etc.,

2. Fake Facebook page (index.html)

3. Phishing Script (i3fb.php)

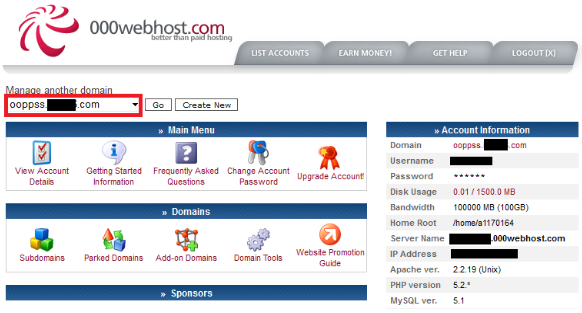
- First create an account with any free hosting services like 000webhost or byethost.
- Open the Facebook page at www.facebook.com
- Right Click on the page and select option "View page Source"
- Then we will get the source code of the Facebook page , select all content by right click and option select all (or) press 'ctrl+a' to select all.
- Then right click again and select option 'copy' to copy all the code. The shortcut for copying is 'ctrl+c'
- Now paste the contents in a notepad. Notepad can be opened from start menu or typing 'notepad' in the run command. (Shortcut for run command is 'windows key+r')
- Now find the word "action" in the notepad and here we have to replace the URL.
- Replace the URL to your newly created website and your "i3fb.php" which we are going to create and upload like the one below.



```
" action="http://ooppss.[redacted].com/i3fb.php" method="post" ons
stent" value="0" /></div></td><td class="login_form_label_fiel
img" src="https://fbcdn-dragon-a.akamaihd.net/cfs-ak-ash4/8497
v id="reg_form_box" class="large_form"><div class="clearfix sh
ut type="password" class="inputtext text_field DOMControl_plac
e="21">21</option><option value="22">22</option><option value=
name="birthday_year" id="birthday_year" aria-label="Year" clas
e="1991">1991</option><option value="1990">1990</option><optio
961">1961</option><option value="1960">1960</option><option va
>1931</option><option value="1930">1930</option><option value=
 information" rel="async">Why do I need to provide my birthday
```

Figure 1: php code

- Now save the file as "index.html" in your desktop or anywhere.
- Now our main page of our Facebook phishing page is ready. Now create a php script which will process and save our email and password details entered in that page.
- The header is used to denote the redirection page once our job is done, here we just redirect to the main facebook page.
- And the passwords are stored in a file named "madhu.txt" here. We can rename it to any name .
- Now save this file as "i3fb.php". Now our two files "index.html" and "i3fb.php" are ready.
- Now we have to upload these two files into our newly created website.
- The login page details and your account info are usually sent to your mail address used to register your webhosting service.
- Use the details to login to your webhosting panel and open the file manager of your website to upload your files.
- We open our control panel of our website.



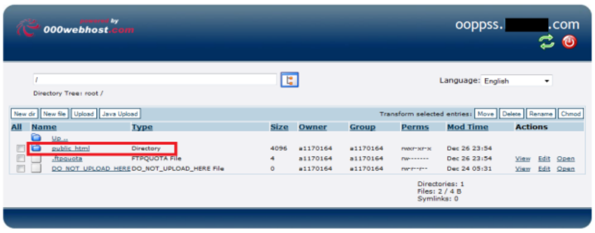
ooppss.[redacted].com

» Account Information

Domain	ooppss.[redacted].com
Username	[redacted]
Password	******
Disk Usage	0.01 / 1500.0 MB
Bandwidth	100000 MB (100GB)
Home Root	/home/a1170164
Server Name	[redacted].000webhost.com
IP Address	[redacted]
Apache ver.	2.2.19 (Unix)
PHP version	5.2.*
MySQL ver.	5.1

Figure 2:000webhost.com

- Then open the file manager to upload our files.



ooppss.[redacted].com

/

Directory Tree: root /

All	Name	Type	Size	Owner	Group	Perms	Mod Time	Actions
	Up ..							
□	public_html	Directory	4096	a1170164	a1170164	rwxr-xr-x	Dec 26 23:54	
□	.ftpquota	FTPQUOTA File	4	a1170164	a1170164	rw-------	Dec 26 23:54	View Edit Open
□	DO_NOT_UPLOAD_HERE	DO_NOT_UPLOAD_HERE File	0	a1170164	a1170164	rw-r--r--	Dec 24 05:31	View Edit Open

Directories: 1
Files: 2 / 4 B
Symlinks: 0

Figure 3: Upload file

- Then open the file manager to upload our files.

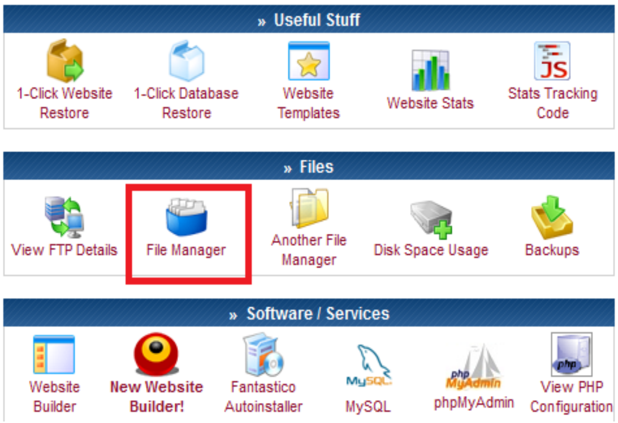
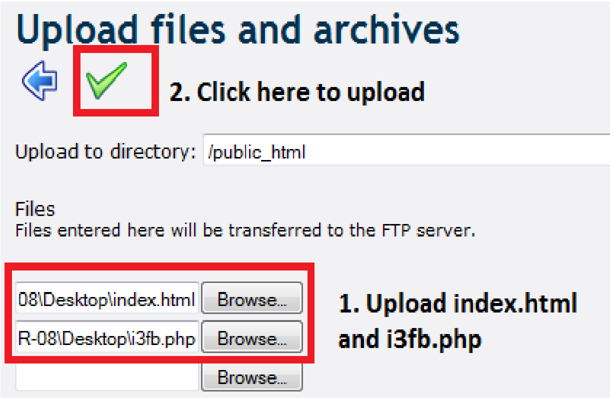


Figure 4: File Manager

- Click on "upload" button to upload our files into the "public_html" folder.

- Browse for the “index.html” and “i3fb.php” files and click on the tick mark to upload.
- 

Upload files and archives

Upload to directory: /public_html

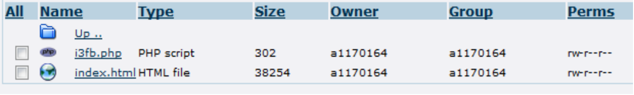
Files
Files entered here will be transferred to the FTP server.

08\Desktop\index.html

R-08\Desktop\i3fb.php

Figure 5: Upload Files

- Once the files are uploaded , we can see the files in the folder as shown below.



All	Name	Type	Size	Owner	Group	Perms
	Up ..					
□	i3fb.php	PHP script	302	a1170164	a1170164	rw-r--r--
□	index.html	HTML file	38254	a1170164	a1170164	rw-r--r--

Figure 6: Folder List

- Now our Phishing page is ready, to test it let us try some fake details in our phishing page.
- Open the website you have created. Here it is www.madhulika.com.
- Here we can see that it looks like a Facebook page, but it is a fake page.
- So our home page of our phishing page is working.
- Let us put some credentials and check the outcome.
- We try some fake credentials to test our Phishing page.
- Once we click on “Login” button the details are sent to our “i3fb.php” file from this page and it is processed and the credentials are stored.
- Here a new file called “madhu.txt” is created . This is done by “i3fb.php”. The credentials are stored in that file.
- We can open or download that file from our website file manager and view it.
- So the phishing page is working and the credentials are being stored successfully. This is how we create a phishing page.

B. Facebook Hacking By Keyloggers

Keyloggers are softwares which can capture all the keystrokes from your keyboard including special characters and sometimes even when using virtual keyboard. These keyloggers are easy to install and easy to use. Once a Malicious user installs a keylogger, even the anti-virus cannot find it easily. We will see how a hacker uses Keylogger Addon for firefox to perform Facebook Hacking.

Things Required are,

1. Firefox Browser

2. Keylogger Addon (Xenotix Keyloger)

3. FTP Account (Available with Web hosting Sites like 000Webhost)

- First we create an free webhosting account in any site like 000Webhost, Byethost etc.,
- We get the FTP details in our registered Email ID.
- Now we use the Xenotix Keylogger Addon (Has the extension *.xpi)
- In Firefox we go to menu bar -> Tools -> Addons
- We get the FTP details in our registered Email ID.
- Now after installation, Firefox requires restart and then the Configuration menu Pop-ups, asking for the FTP information. Enter the FTP host name.
- Then it ask for Username and Password of the FTP account to send the key logs to it.
- Now our key logger is installed and whatever is typed on that browser is sent to our FTP site as key logs.
- We test a login page of Facebook to verify that our Key logger works properly.
- Now we open our file manager of our Website and we can find a file named “log.html” in our main directory or the mentioned directory. We can find our Key logs there.

  This is how hackers or malicious users install keyloggers in a browser easily and hack our accounts. In many public internet centres or Cyber Café some malicious users use this technique to steal information of many people and hack their accounts. So verify the settings before you use any public computers or others PC

C. Facebook Social Engineering Attack

Social Engineering is the technique used by several people to collect information and use that information against the concerned people. It may be used to guess a password or to collect personal details such as Mobile number, Address, and pictures to use it for Fake identity .Social Engineering Attack doesn’t need any tool or software, it is just the art of human hacking, exploiting the weakness of Humans is known as Social Engineering. .

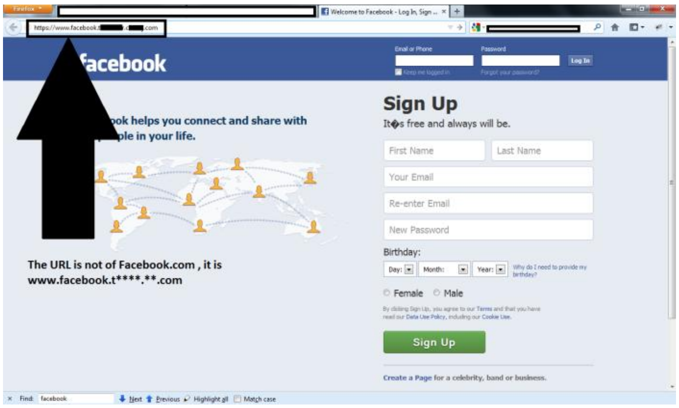
Next we will see how we protect ourselves from these kind of attacks.

IV. Protection from Various Attacks

A. *Facebook Phishing Attacks*

Facebook phishing attack is an attack when a malicious user or a Hacker creates a fake page similar to Facebook and makes the user to enter the credentials in his page.

This is a sample phishing page created for testing purpose, It looks like Facebook website but it is a phishing page.



https://www.facebook.t[redacted].c[redacted].com

Welcome to Facebook - Log In, Sign ...

The URL is not of Facebook.com , it is www.facebook.t****.**.com

Sign Up
It�s free and always will be.

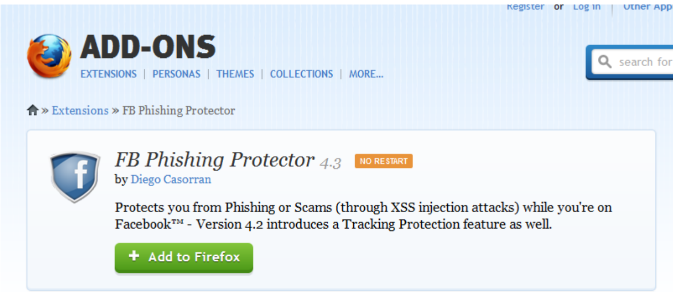
By clicking Sign Up, you agree to our Terms and that you have read our Data Use Policy, including our Cookie Use.

Create a Page for a celebrity, band or business.

Find: facebook

Figure 7: Phishing Page

So if we are presented with such a page , many users do not verify the URL before entering their credentials, So the attacker takes advantage of this weakness and succeeds in getting the user credentials. So to protect ourselves from such kind of attacks, we use an Add-on on Firefox named “FB Phishing Protector”.



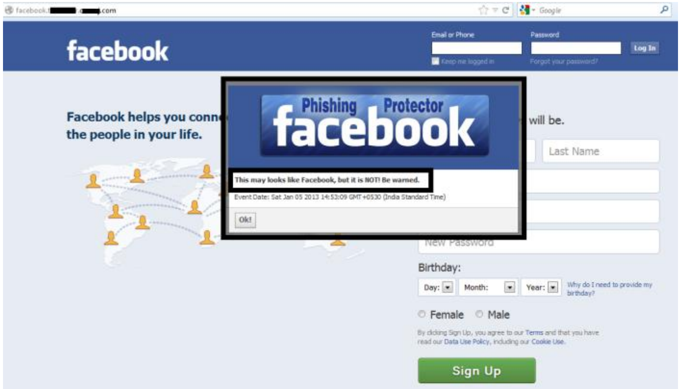
FB Phishing Protector 4.3
by Diego Casorran

Protects you from Phishing or Scams (through XSS injection attacks) while you're on Facebook™ - Version 4.2 introduces a Tracking Protection feature as well.

Register or Log in | Other App
ADD-ONS
EXTENSIONS | PERSONAS | THEMES | COLLECTIONS | MORE...
search for
Extensions » FB Phishing Protector
NO RESTART
+ Add to Firefox

Figure 8: Add-Ons

Use this Add-on to prevent phishing attacks on your browser. This Add-on checks for fake Facebook pages and phishing pages and reports to you if you visit that particular phishing page.



facebook.t[redacted].[redacted].com

This may looks like Facebook, but it is NOT! Be warned.

Event Date: Sat Jan 05 2013 14:53:09 GMT+0530 (India Standard Time)

Ok!

Figure 9: Fake Facebook Page

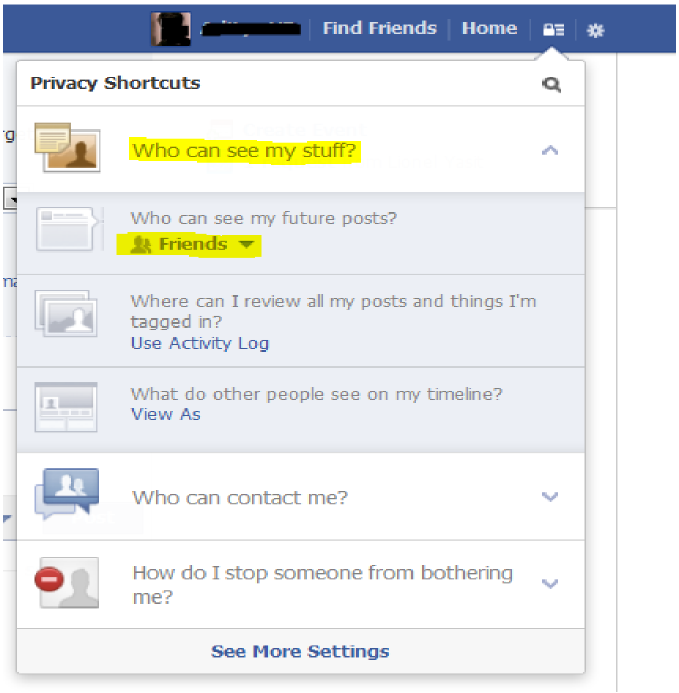
By using this , We can prevent phishing attacks and be secure from hackers using this method.

B. *Facebook Social Engineering Attack*

In Facebook there are several possibilities for social engineering, because it is a social networking site and all our details are left open to the public. So We will see some security measures to hide our data from public view.

1) *Hide your Wall posts*

Facebook has implemented new features for privacy settings in the home page of Facebook directly making it easier for users to utilize it.



[redacted]

Privacy Shortcuts

Who can see my stuff?

Who can see my future posts?
Friends

Where can I review all my posts and things I'm tagged in?
Use Activity Log

What do other people see on my timeline?
View As

Who can contact me?

How do I stop someone from bothering me?

See More Settings

Figure 10: Privacy Settings

In the home page of Facebook, at the top right corner we can see a lock symbol as shown previously, It is the privacy control settings.

We can set the viewers of our future posts from “Public” to “Friends”. So that any person who is not our friend cannot see your posts. It is a security measure to get details about us from our posts.

2) *Block Friend Requests from Unknown Person*

To block friend requests from unknown person, use the option “Who can contact me ? ”, Under that settings select “Who can send me friend Requests ? ” and set “Friends of Friends” . This option blocks anyone from sending us a friend request other than our friend’s friend[4].

3) *Blocking a Person*

If someone has been disturbing us or harassing us, we can simply block them directly by entering their email id or their Facebook name in the privacy setting menu.

These are some common privacy settings to prevent social engineering attacks, Do not provide an of our personal information to the public, It may be dangerous if someone else uses our information for any malicious activities.

V. Facebook Security Settings

Some of the common security setting of Facebook are disabled by default. We have to enable them in order to secure our account and online activity. The security settings of an account can be accessed from the settings menu button in top right of the Facebook page[7].

Once we are in the account settings , select the security settings tab in the left column. This has all the security related settings of our account.

In the security settings page we can see a list of settings such as

1) *Secure Browsing* – To enable HTTPS Browsing.

2) *Login Notifications* – To notify you whenever you login.

3) *App Passwords* - Set separate passwords for Facebook Apps .

4) *Recognized Devices* - To view recognized devices of that account .

5) *Active Sessions* - All active logins at current time.

VI. Conclusion

One of the most significant findings to emerge from this research is that most of the sites and services provide options for privacy settings to prevent attackers to view your information. We can make use of these options to choose/deny whom you want to allow to see your information. Limit the information you put in the social networking sites. Don’t put personal information like your family details, addresses, personal photographs, video, etc. In case if you put your personal photographs try to change settings and make visible only for friends. Be careful if you want to meet social networking friends in person, some times it may not be their true identity which is posted on the social networking sites. Use Virtual Keyboard, wherever possible to enter your password for better security as these cannot be captured by key-loggers[9].

References

[1] RD. Hartley, “Ethical Hacking: Teaching Students to Hack”, EastCarolina University, http://www.techspot.com/news/21942-universityoffers-ethical-hacking-course.html, , 2002.

[2] T. Wulf, “Teaching ethics in undergraduate network”Consortium forComputing Sciences in College, Vol 19 Issue 1, 2003.

[3] I. See http://www.cs.ruu.nl/cert-uu/satan.html.

[4] N.B. Sukhai, “Hacking And Cybercrime”, AT&T, 2005.

[5] www.facebook.com/i3indyatechnologies.

[6] http://www.cyberlawsindia.net/

[7] http://security.tipcentral.net/

[8] C.C. Palmer, Ethical hacking , IBM systems journal, http://www.research.ibm.com/journal/sj/403/palmer.html , 2001.

[9] www.facebook.com/mrooppss.

[10] Graves, K. (2007). *CEH Official Certified Ethical Hacker Review Guide* (1st ed.). Indianapolis,In: Wiley Publishing, Inc..