2012

Shield Against Hacking

Praneet Menezes

1/11/2012

Copyright notice

ISBN -> 978-1-300-34435-3

Liability disclaimer

The words “hack” and “hacking” as used in this book imply “ethical hack” and “ethical hacking”.

The author of this book does not dispense advice on hacking or prescribe the use of any technique for hacking. The intent of the author is only to offer educational information to help the reader develop a hacker defense attitude to prevent the hacking attacks discussed.

In the event a reader uses any of the information in this book for the purpose of unlawful hacking and causing damage, directly or indirectly, to anyone, the author disclaims all liability and assumes no responsibility for their action.

Foreword

Hi there, folks!

I am Praneet Menezes, 17, studying in FY, and the book you are reading is the first book I have ever written. Noticing how ignorant most people are about cyber security, I decided to write *Shield Against Hacking* to educate them about the hazards of hacking and what they could do to safeguard themselves from the attacks of hackers.

I have gathered the anti-hacking information you are about to read from various authentic sources and presented here in simple language and easy format. I am sure you will enjoy the book and use it to your benefit.

Dedication

To my mom and dad

Special Thanks

To Mr. Crizan Menezes, Mr. Prakash Deshmukh & Mr. Sebastian Gonsalves

CONTENTS

Vote of thanks
Reference
Contact info

Introduction

In the modern world of today, where everything from shopping to banking is available on the web, even the cyber frauds and hacking accounts have become increasingly sophisticated. A hacker can use a computer program of a very small size to find your password, steal your data, and rob you of every penny in your bank account. And, oops! Who do you think is caught up in the legal hassles following a cyber crime? Although you could go to the cyber crime cell of the police, it is always the victim who 'faces' the law, rarely the hacker himself.

As prevention is always better than cure, read this book and prevent your accounts from being hacked.

How to use this book ?

In this book, you will find out how hackers hack a computer system or an online account. You will also find out how one may safeguard oneself from hacking. THIS BOOK TEACHES WAYS OF PROTECTING FROM HACKERS, NOT WAYS OF HACKING.

This book is a must read for IT and other professionals, cyber security officers, businesspeople, bureaucrats, organizations handling sensitive information, government bodies, in fact, anyone who wants to secure themselves against cyber crimes.

Who is a hacker?

A hacker is a computer pro who is very well acquainted with computers. They like to explore and learn how computer systems work, finding ways to make them do what they do better, or do things they weren't intended to do.

There are two kinds of hackers: white hat and black hat.

White Hat: They are the good guys. They don't use their skills for unlawful purposes. They usually become Computer Security experts and help protect people from Black Hats.

Black Hat: They are the bad guys. They usually use their skills maliciously for personal gain. They are the ones who hack banks, steal credit cards, and deface websites.

Types of hackers

Beginners: They are the wannabe hackers. They are looked down upon in the hacker community because they make hackers look bad. They often do not have hacking skills and use tools developed by other hackers without knowing what is happening behind the scenes.

Intermediate hackers: They know about computers and networks, and have enough programming knowledge to understand what a script might do. However, like the beginners, they use pre-developed well-known hack tools to carry out attacks

Elite Hackers: They are skilled hackers. They are the ones who write many hacker tools and exploits out there. They can break into systems and hide their tracks or make it look like someone else did it.

Online Accounts

Online accounts mean email websites, social networking websites such as Gmail, facebook etc and any other account that you might be operating from the internet. In this chapter I will discuss various ways in which online accounts can be hacked as well as their countermeasures. There is no such thing as facebook hacking software or Gmail hacking software. People think that entering user name in hacking software would automatically hack the password for you. It is a myth. And if you find any such software on the web then they are Trojans or viruses. I will discuss viruses later in the book.

Here are the ways for hacking online account:

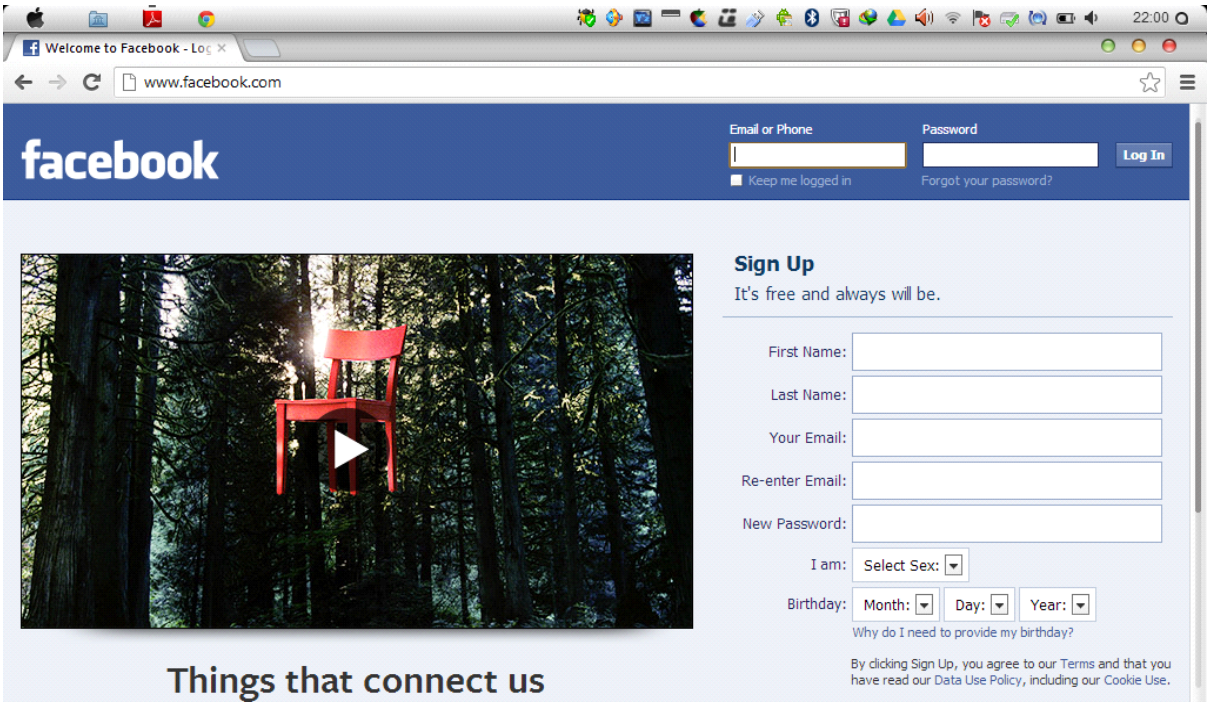
1. Phishing

Phishing refers to a process in which a hacker pretends to be someone he is not. In phishing, a victim receives a fake page which is the exact replica of an original page. This fake page is stored on a file hosting a website and a link to this page is sent to the victim via email. As soon as the victim opens the link, the fake phishing page opens. Then as soon as the victim enters his details, his sensitive information such as user name and password gets stolen.

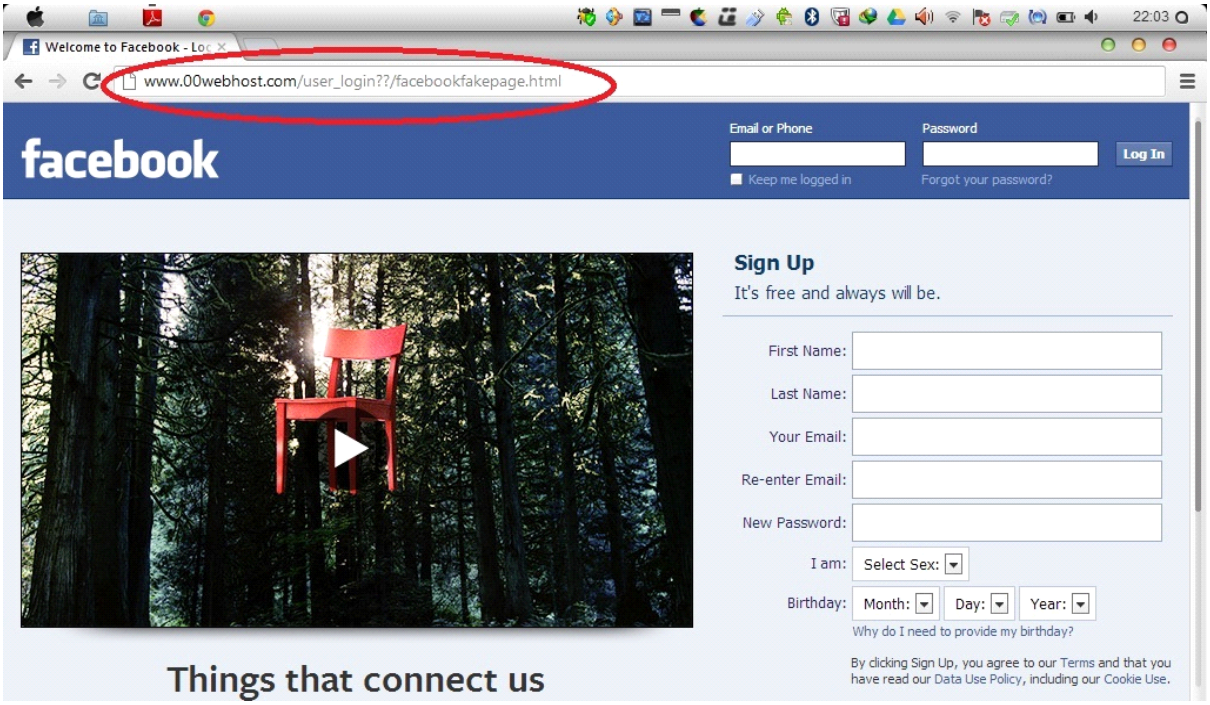
The hacker then redirects the victim automatically to the real facebook page. The victim thinks that they must have entered a wrong password and so they enter it again on the real facebook page. This time they get logged on to facebook, and so do not know they were a target of phishing. Now knowing the user name

and password, the hacker can login into the victim's account and cause trouble for him.

Here is an original facebook page :



And here is a replica of the facebook page used in phishing :



Countermeasure:

As you can see, the only difference between the original and fake pages is their URL. The URL for original facebook page is www.facebook.com whereas it is different for the fake page. Hence the difference in URL is the tool for identifying if the website is real or a phishing attack !

Website developers and software engineers are well aware of phishing. Hence modern web browsers come with anti-phishing technique. Example of such a browser is Chrome browser by Google Inc

To activate anti-phishing measures, you must go to settings in the Chrome browser, then click ‘show advanced options’ and then check the anti-phishing box in ‘privacy tab’.

2. Primary email address

Social networking websites use email for recovery of passwords. When recovery of password is selected in facebook, an email is sent to your email address which consists of your username and password. If a hacker gets access to your email id, it will be very easy for them to hack your account and various other accounts that are linked to email address.

Countermeasure:

Never let anyone have information about your primary email address. Remember that your email id is more important than your facebook. If your facebook is hacked, only your facebook account is hacked but if your email id is hacked then there is a threat that all other online accounts linked to the email address will be hacked too. So protection of your email id is of utmost importance.

3. Social Engineering

It is an old-fashioned way of obtaining a password from someone by pretending to be their well-wisher. For example, a hacker may call posing as a bank employee and tell a victim that there are upgrades to their credit card. He may ask the victim to reveal their credit card number as they have received some bonus points for the credit card. Likewise he might also ask them for passwords and other sensitive information with which he could hack the victim's bank account. And in their greed for some extra bonus points, the victim would readily reveal their bank information and – BAM! – All the sensitive information is lost in less time than it takes to blink. Often people tell their online account passwords to their trusted friends and then their accounts get hacked.

Countermeasure:

Never reveal your personal information to anyone. Moreover never trust anyone who claims to be your well-wisher. In most of the hacking cases, the hacker is a trusted friend of the victim, knows the victim's personal data and uses this information to hack the victims account. When it comes to bank account details or online account passwords, the only person you can trust is none other than yourself.

4. Guessing Passwords

Guessing passwords is a common way of hacking. Usually people form their passwords from their names, names of friends, lovers, girlfriends and boyfriends or their phone numbers, dates of birth and such things. Guessing passwords is surely the easiest way of hacking.

Countermeasure:

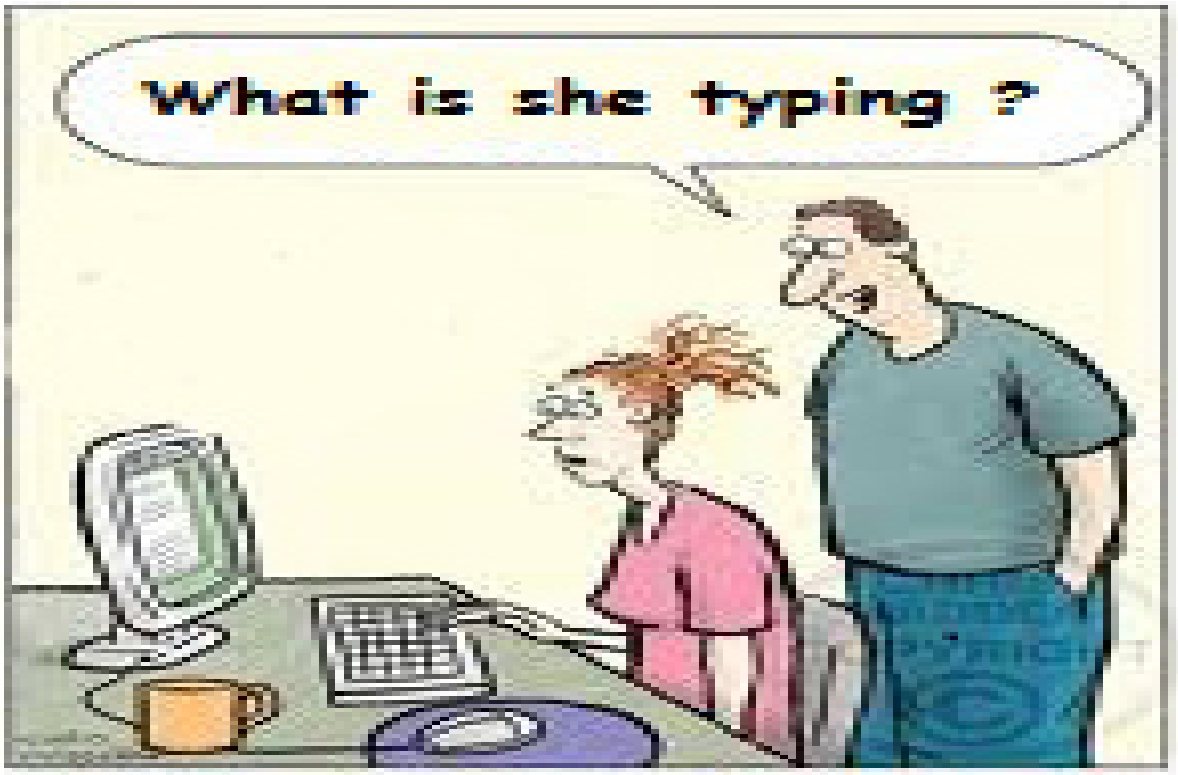
The only countermeasure is to never use a password that is easy to guess. Keeping difficult to crack yet easily remembered password is certainly a good thing. For example, a password like "hello2U" is easy to remember yet difficult to crack. Similarly, we can use a combination of numbers and symbols with lowercase and uppercase alphabet.

5. Shoulder Sniffing

Shoulder sniffing is exactly what it says – a hacker simply attempts to look over your shoulder as you type in your password. The hacker may also watch whether you look around your desk for a written down reminder or the password itself.

Countermeasure:

When you type in your password make sure there is no one behind you attempting to peak. Make sure you don't keep any sticky notes lying.

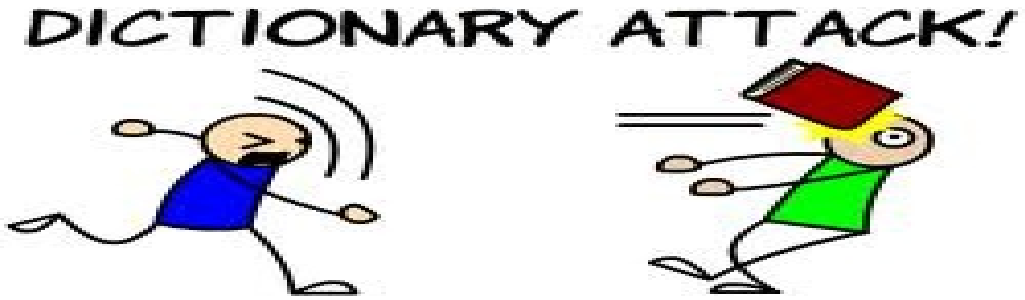


6. Dictionary Attack

In dictionary attack, a hacker tries all common passwords and all words in a dictionary as a password. There are high tech software's which automatically try all worlds in the dictionary to crack a password. But this is not a very effective way of cracking passwords.

Countermeasure:

The only countermeasure is not to use passwords that are listed in a dictionary. Also make it a point to change the default passwords such as 12345 or 0000 which are preset in mobile phones and internet provider's dial-up connections.



7. Security Questions

Several websites offer password recovery options such as answering security questions to change passwords. If a hacker is someone you trust then he could answer your security questions and hack your account. Moreover, security questions which are answered by your mother's name, your first grade teacher's

name, street address, favorite movie title or pet name are easily guessed by the hacker.

Countermeasure:

Never reveal personal data to anyone. Besides choose security questions that are difficult to guess.

Security questions could be changed too. Here is how to do it on yahoo. Once you have logged on to yahoo, click on your name at the top left corner, then click on 'account info', and then on 'update password-reset info'. Next select the 'change security questions' button. I advise you to create your own security questions. Give alternate email id and phone number at the websites. Hence even when your account gets hacked, you could recover it.

8. Brute-Force Attack

This is a way of password cracking in which permutation and combination are used. The software tries all possible password combinations. The software takes minimum and maximum number of digits a password could have. It also asks for the type of password such as alphabetical, numerical, alphanumerical or symbolical. From these inputs the software generates all possible combinations which at times could run into to millions and billions. The software tries out password combinations at a rate of 3500/sec. Thus, given enough time, the password is cracked. Brutus AET2 is one such software.

Countermeasure:

Brute-force attacks may be prevented by creating a very long password using many numbers and characters. The longer the