ଓଡ଼ିଶା ରାଜ୍ୟ ମୁକ୍ତ ବିଶ୍ୱବିଦ୍ୟାଳୟ, ସମ୍ବଲପୁର, ଓଡ଼ିଶା
Odisha State Open University, Sambalpur, Odisha
Established by an Act of Government of Odisha.

DIPLOMA IN CYBER SECURITY

DCS-04 – APPLICATION CYBER SECURITY

BLOCK

4 LABORATORY MANUAL

ଓଡ଼ିଶା ରାଜ୍ୟ ମୁକ୍ତ ବିଶ୍ୱବିଦ୍ୟାଳୟ, ସମ୍ବଲପୁର, ଓଡ଼ିଶା
Odisha State Open University, Sambalpur, Odisha
Established by an Act of Government of Odisha.

DIPLOMA IN CYBER SECURITY

Course Writer

Bijay Kumar Paikaray
Centurion University of Technology and Management, Odisha

DCS-04 – APPLICATION CYBER SECURITY LABORATORY

LIST OF EXPERIMENTS

SL. No.	Experiment
1	Study of steps to protect your personal computer system by creating User Accounts with Passwords and types of User Accounts for safety and security.
2	Study the steps to protect a Microsoft Word Document of different version with different operating system.
3	Study the steps to remove Passwords from Microsoft Word
4	Study various methods of protecting and securing databases.
5	Study "How to make strong passwords" and "passwords cracking techniques".
6	Study the steps to hack a strong password.

EXPERIMENT-1

Aim: To study the steps to protect your personal computer system by creating User Accounts with Passwords and types of User Accounts for safety and security.

1.0 Learning Objective

At the end of the session you will be able to

- Become familiar with how to operate the user account.
- Different types of user accounts and their options.
- How to protect your system with password.

1.1 Introduction to user accounts

An important part of managing the BIG-IP system is creating and managing user accounts for BIG-IP system administrators. By creating user accounts for system administrators, you provide additional layers of security. User accounts ensure that the system:

- Verifies the identity of users logging into the system.
- Controls user access to system resources.

1.2 Types of user accounts

The types of user accounts on the BIG-IP system are:

The root account

Every BIG-IP system has an account named root. A user who logs in to the system using the root account has full access to all BIG-IP system resources, including all administrative partitions and command line interfaces.

The admin account

Every BIG-IP system has an account named admin. A user who logs in to the system using the admin account has the Administrator role, which grants the user full access to all BIG-IP system resources, including all administrative partitions on the system. By default, the admin user account has access to the BIG-IP Configuration utility only. However, users logged in with this account can grant themselves access to

both tmsh and the advanced shell. Although the BIG-IP system creates this account automatically, you must still assign a password to the account before you can use it. To initially set the password for the admin account, you must run the Setup utility. To change its password later, you use the BIG-IP Configuration utility's Users screens.

Local accounts

A BIG-IP user with the correct user role can create other local user accounts for BIG-IP system administration. Each local user account on the BIG-IP system has one or more user roles assigned to the account (one per partition), as well as permissions related to tmsh and Bash shell access.

Remote accounts

If your organization stores user accounts on a remote authentication server (such as an Active Directory server), you can configure the BIG-IP system to control access to BIG-IP configuration objects for all BIG-IP user accounts stored on the remote server. In this case, the remote server authenticates each BIG-IP user at login time, while the BIG-IP system itself grants the specified access control permissions.

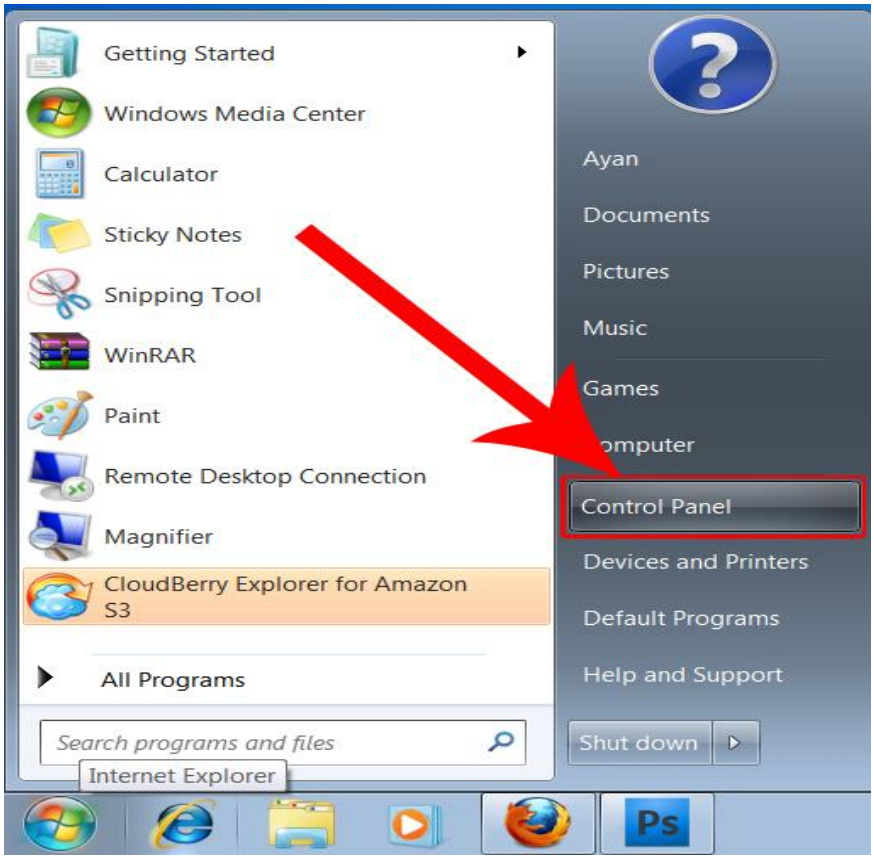
Note: You are not required to have any user accounts on the BIG-IP system other than the root and admin accounts. However, F5 Networks recommends that you create other user accounts, as a way to intelligently control administrator access to system resources.

1.3 Changing the root and admin account passwords

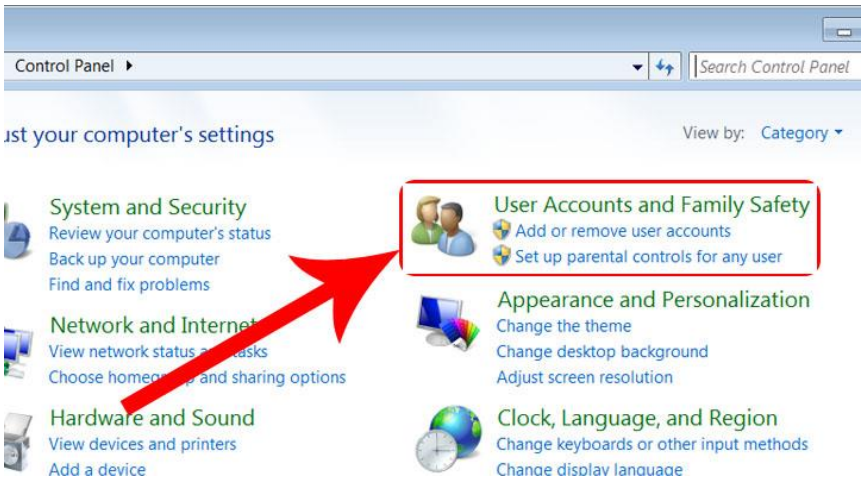
If you have an Administrator user role, you can use the BIG-IP Configuration utility to change the passwords of the root and admin accounts.

1. On the Main tab, expand System, and click Platform.
2. For the Root Account setting, type a new password in the Password box, and re-type the new password in the Confirm box.
3. For the Admin Account setting, type a new password in the Password box, and re-type the new password in the Confirm box.
4. Click the Update button.

You want to protect your computer from your roommate, parents, or brothers? Learn how to add a password to protect your computer!



1. Open Control Panel.



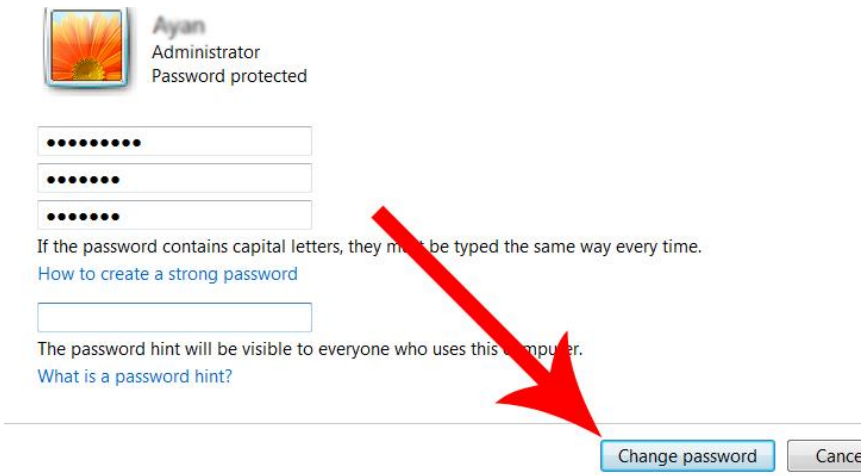
2. **Open "User Accounts".**

3. **Make a new user account or if the existing one is yours then skip this step.**

4. **Click on your account.**

5. **Click on "Change Password".**

6. **Choose a strong password which cannot be guessed.**



7. **Confirm Password**

8. **Click on OK.**

EXPERIMENT-2

Aim: To study the steps to protect a Microsoft Word Document of different version with different operating system.

2.0 Learning Objective

At the end of the session you will be able to

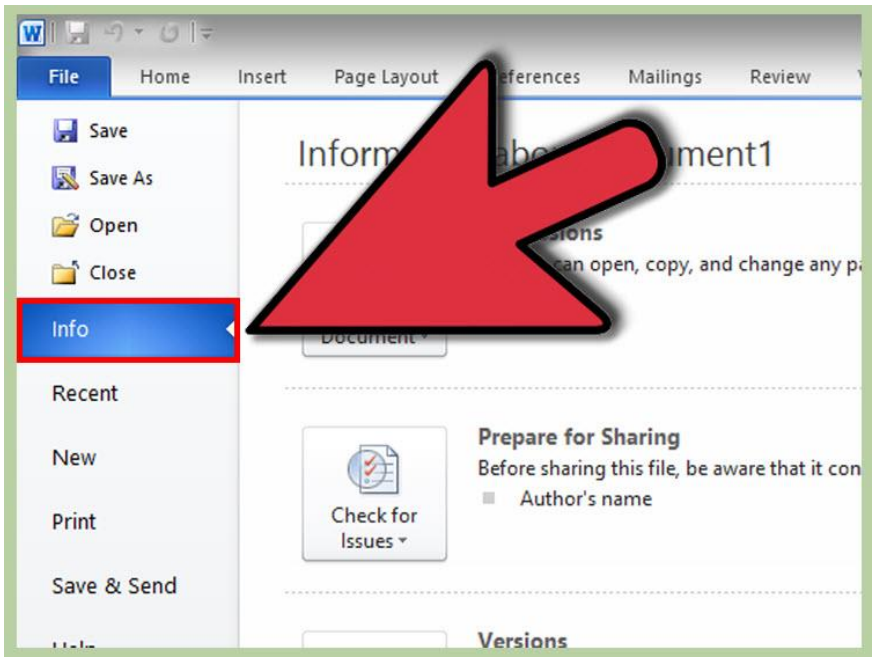
- Understand how to protect a Microsoft word document.
- Be familiar with how to password protect Microsoft word document in different type of operating system.

2.1 Introduction to password protect a Microsoft word document.

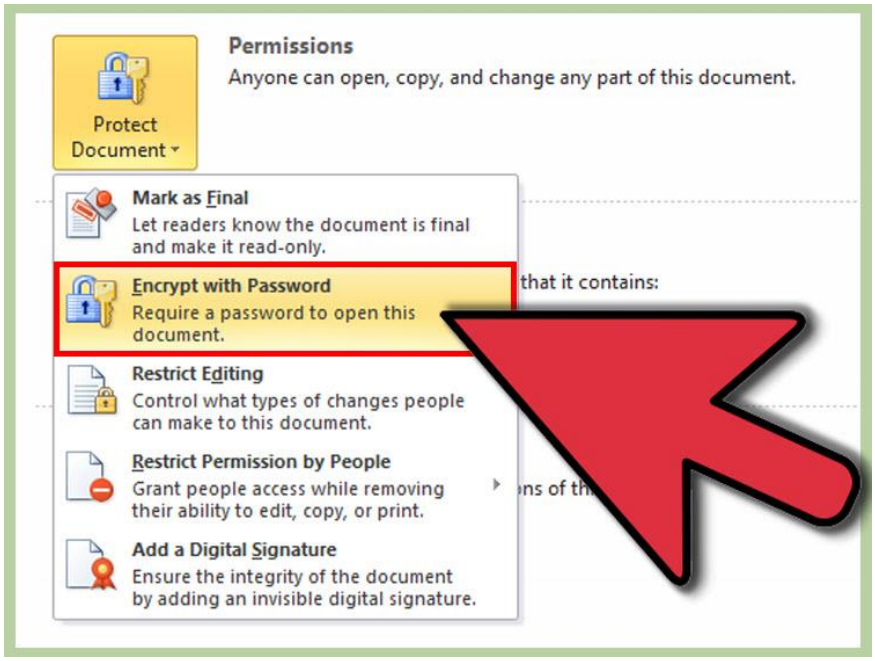
Password Protector is a system utility that allows you to password-protect any Windows file. Whenever you try to open protected file you will see the prompt that asks you to enter the valid password so only person who knows the correct password can launch this file. Once the file is protected, you may copy this file to another computer and it stays protected no matter what operating system this computer runs. Such behavior is achieved by adding a special code to your file (approximately 100 kb), implementing a true, and system-independent protection mechanism.

If you've got a Word document that you don't want prying eyes to see or modify, you'll want to lock down your file with a strong password. Word comes with password protection capabilities built-in to every version. Follow this guide to protect any document in any version of Word, for both Windows and Mac OS X.

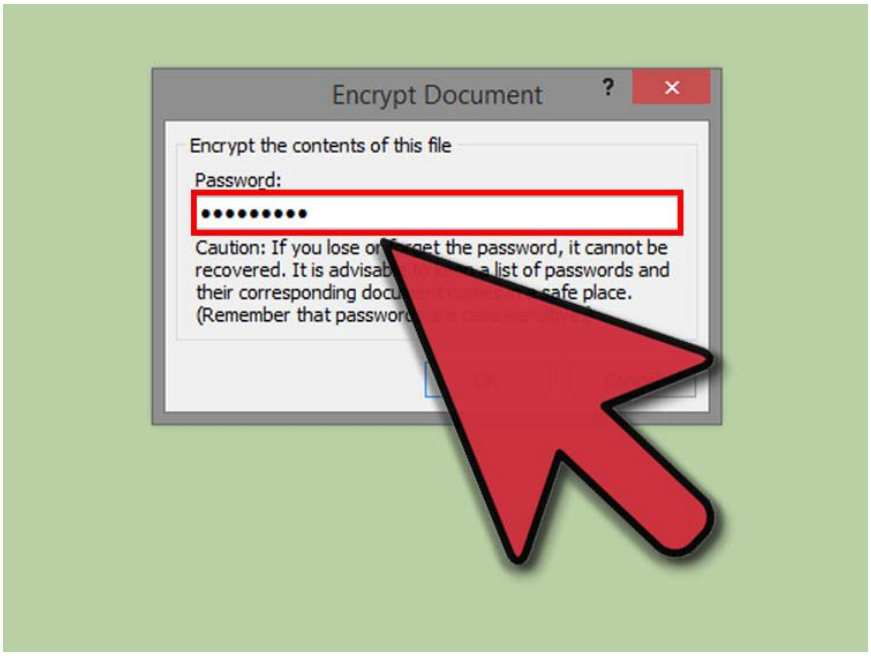
Method-1 Word 2010/2013



1. **Click the "File" in the upper-left corner.** If the Info tab doesn't automatically open, click the Info tab.

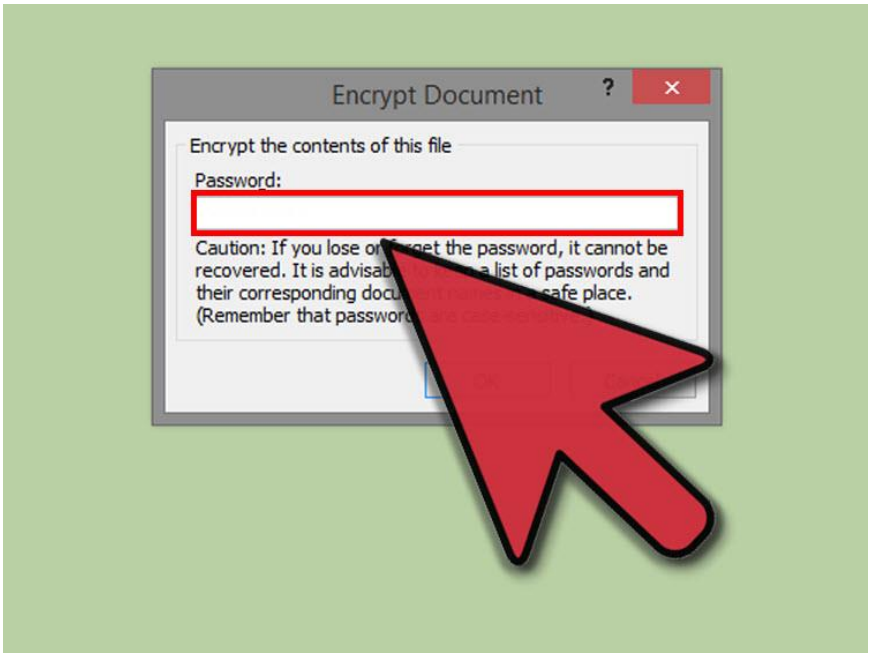


2. **Click Protect Document.** This square button is located under the "Information about <document>" section. Click "Encrypt with Password" in the menu that appears.

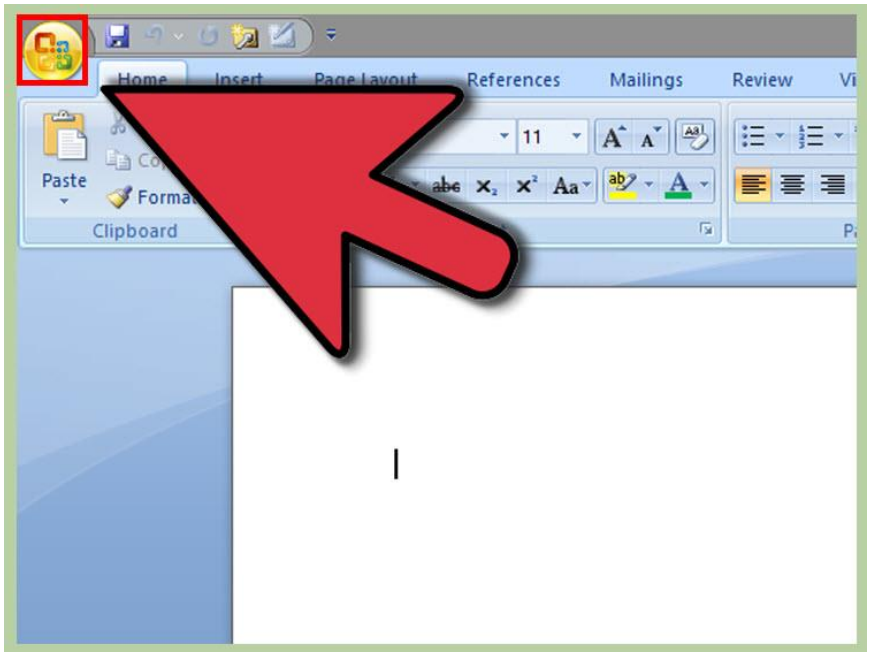


3. **Enter a password.** You will be asked to enter the password again to confirm it. You will not be able to retrieve this password if you forget it, so write it down in a safe location.

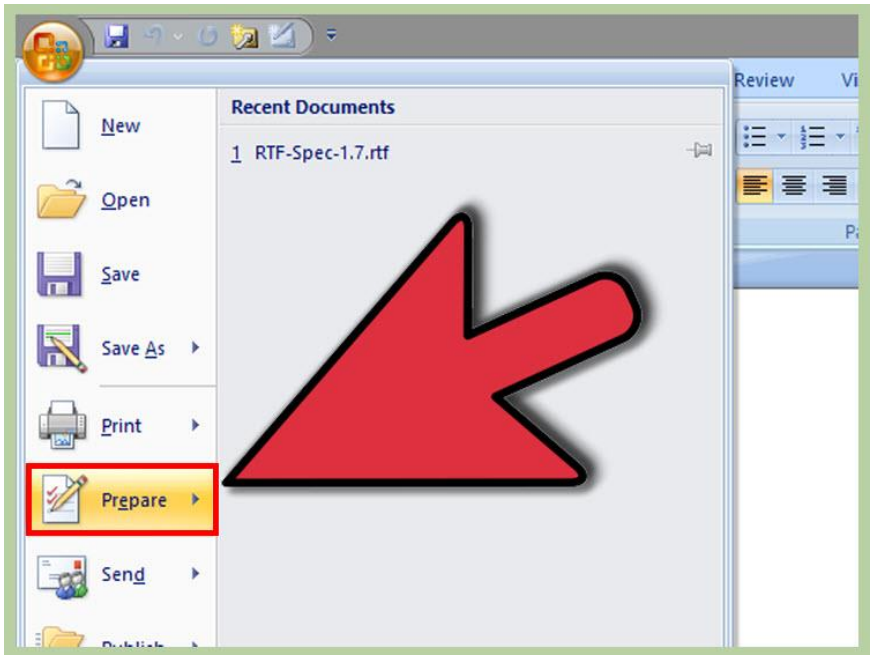
- In order for the password to take effect, you must save the file.



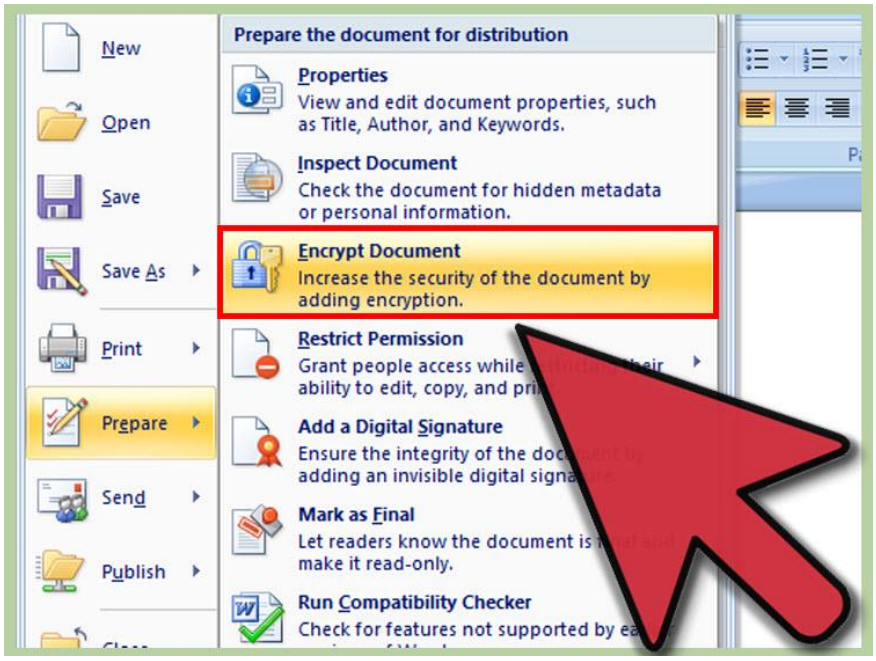
4. **Remove your password.** If you want to remove your password, open the document and click the File menu again. Click Protect Document and select "Encrypt with Password". There will be a password in the box, delete it and press OK.



Method -2 Word 2007

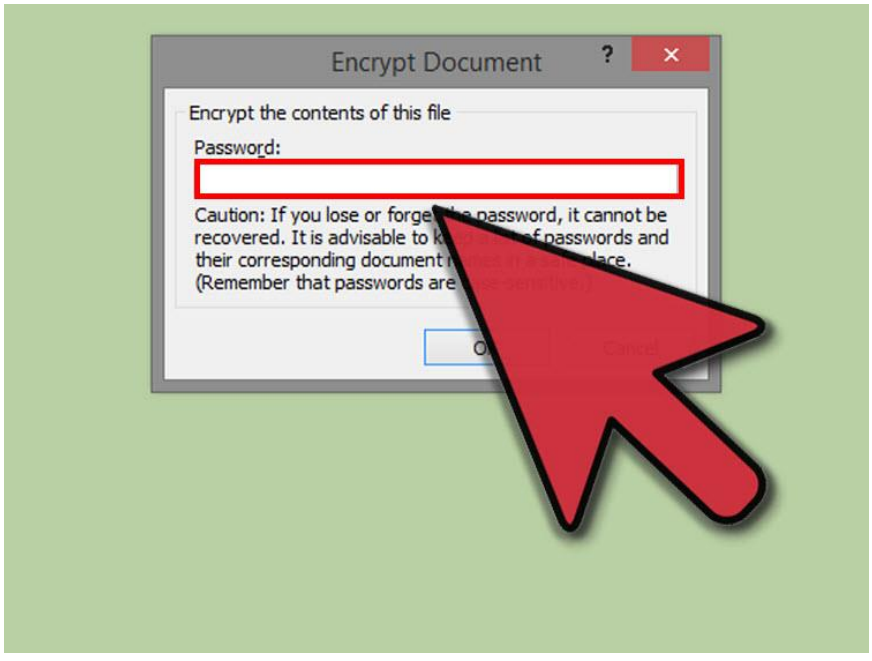


1. **Move your mouse over Prepare. This option is located between Print and Send. A new menu will appear.**



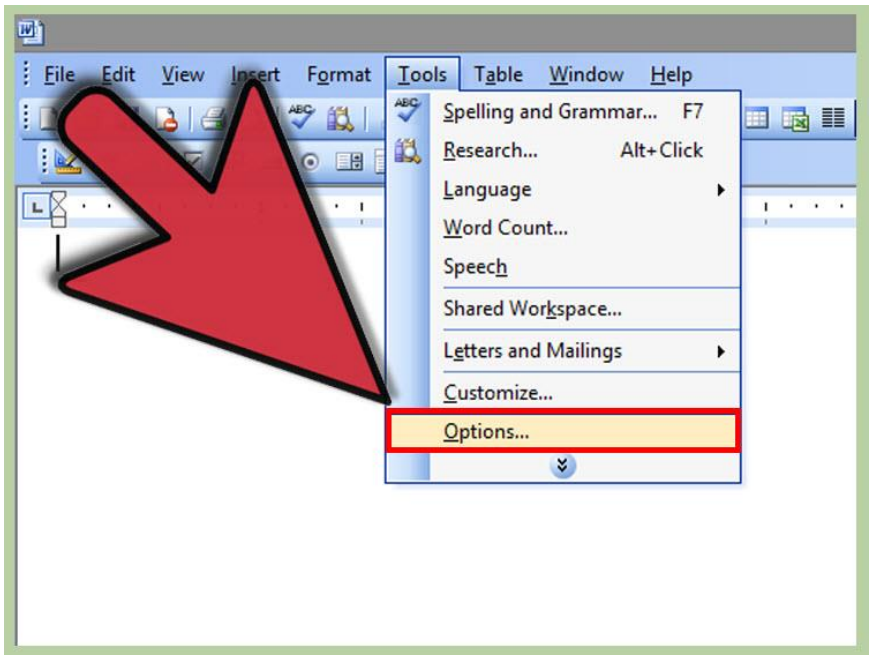
2. **Click "Encrypt Document".** A small box will appear where you can enter the password that you would like. You will be asked to enter the password twice to confirm it. You will not be able to retrieve this password if you forget it, so write it down in a safe location.

- In order for the password to take effect, you must save the file.

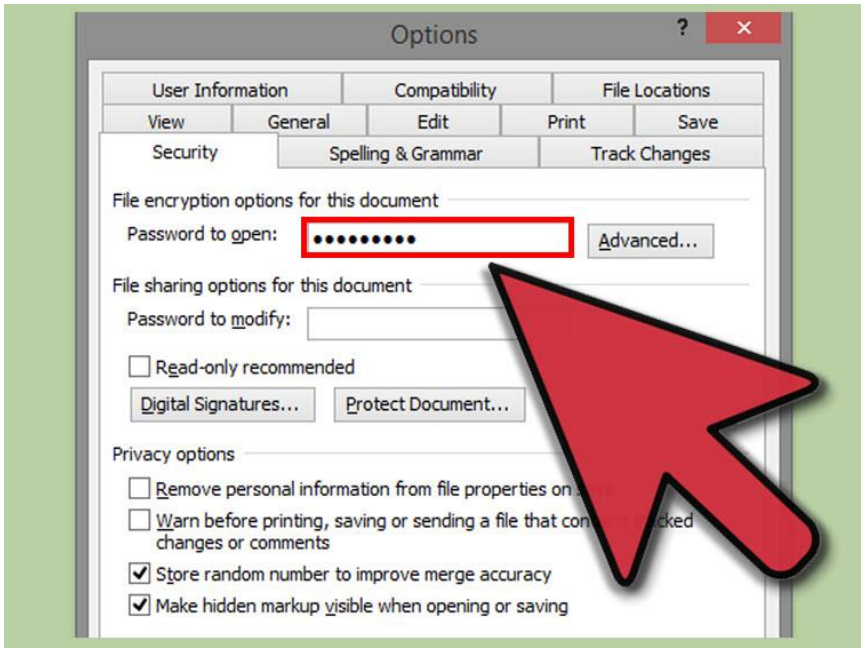


3. **Remove your password.** If you want to remove your password, open the document and click the Microsoft Office Button again. Hover over Prepare and select "Encrypt Document". There will be a password in the box, delete it and press OK.

Method 3 Word 2003

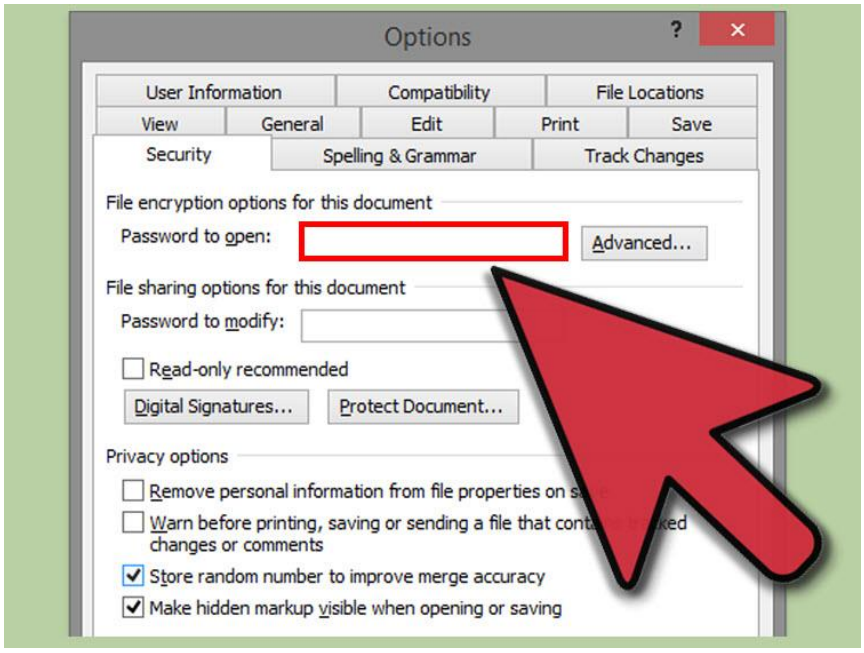


1. **Click the Tools menu.** Click Options and a new window will open. Click on the Security tab.



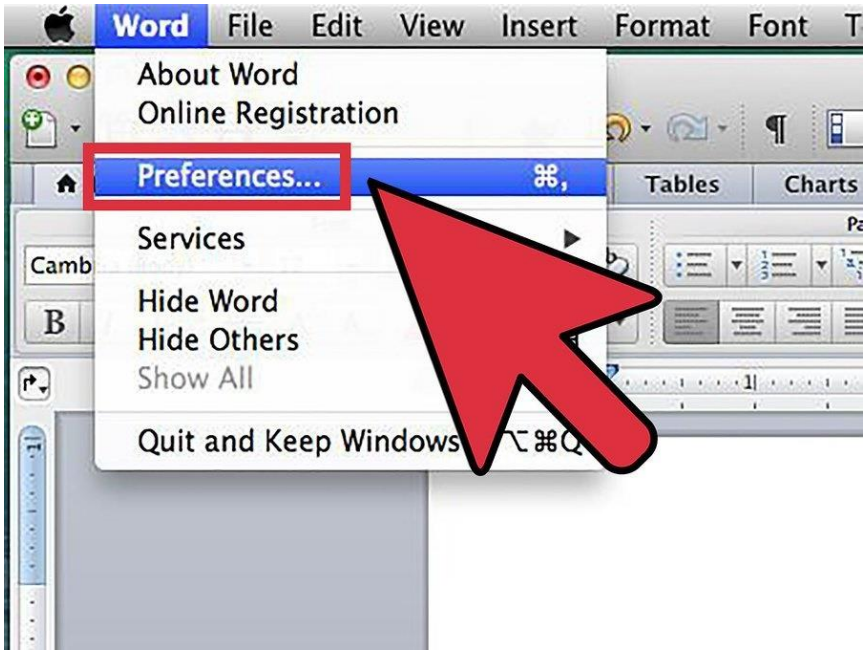
2. **Create a password**. In the Security tab, enter your new password in the "Password to open" field. Press OK to save the password. You will not be able to retrieve this password if you forget it, so write it down in a safe location.

You will be asked to confirm the password after pressing OK.
In order for the password to take effect, you must save the file.

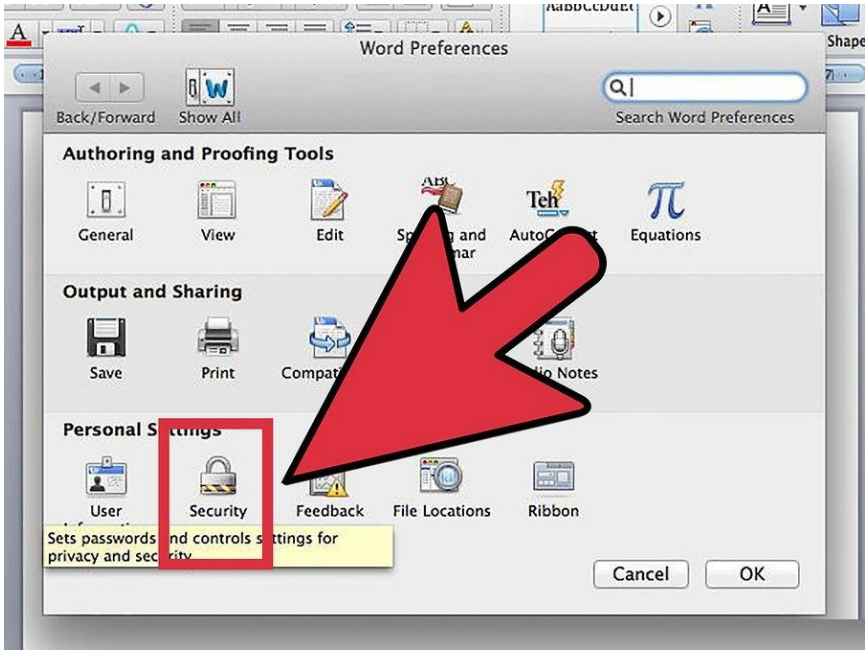


3. **Remove your password.** If you want to remove your password, open the document and click the Tools menu again. Select Options and then click the Security tab. There will be a password in the box, delete it and press OK.

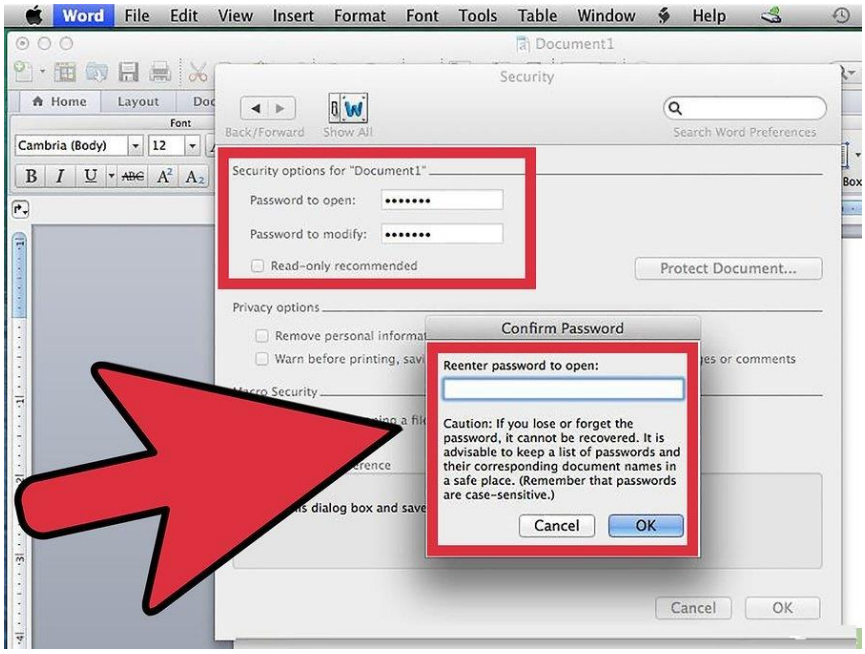
Method 4 Word 2008/2011 (Mac)



1. **Click the Word menu.** This is located in the top-left corner, between the Apple menu and the File menu. Select Preferences.



2. **Click Security.** This can be found under the Personal Settings section. This will open the Security window.



3. **Create your password**. In the "Password to open" field, type in your password and then click OK. You will be asked to reenter your password to confirm it. You will not be able to retrieve this password if you forget it, so write it down in a safe location.

- In order for the password to take effect, you must save the file.

4. Remove your password. If you want to remove your password, open the document and click the Word menu again. Select Preferences and then click Security. There will be a password in the box, delete it and press OK.

EXPERIMENT-3

Aim: To study the steps to remove Passwords from Microsoft Word 2007.

3.0 Learning Objective

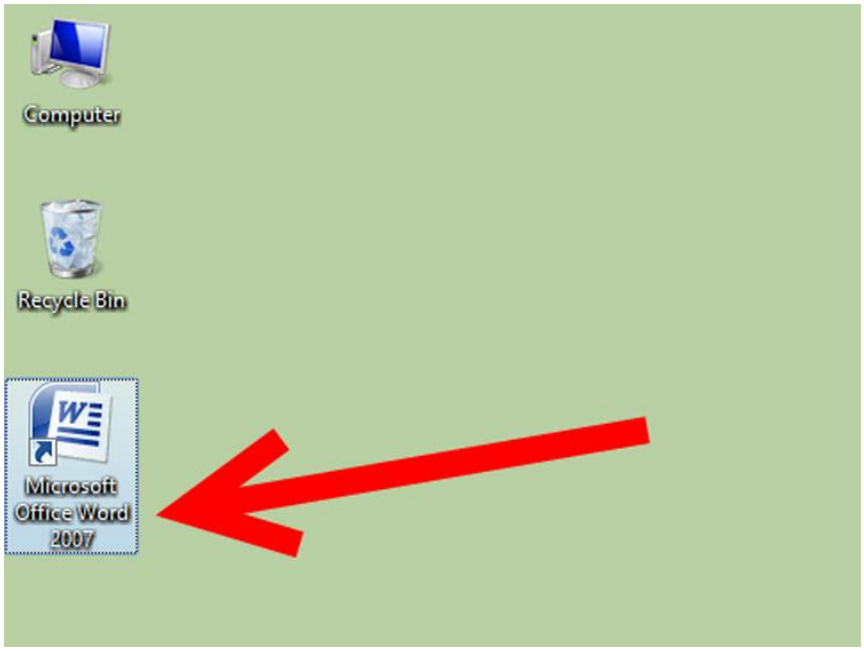
At the end of the session you will be able to be familiar with

- To understand the steps of operation how to remove password from Microsoft Word 2007.

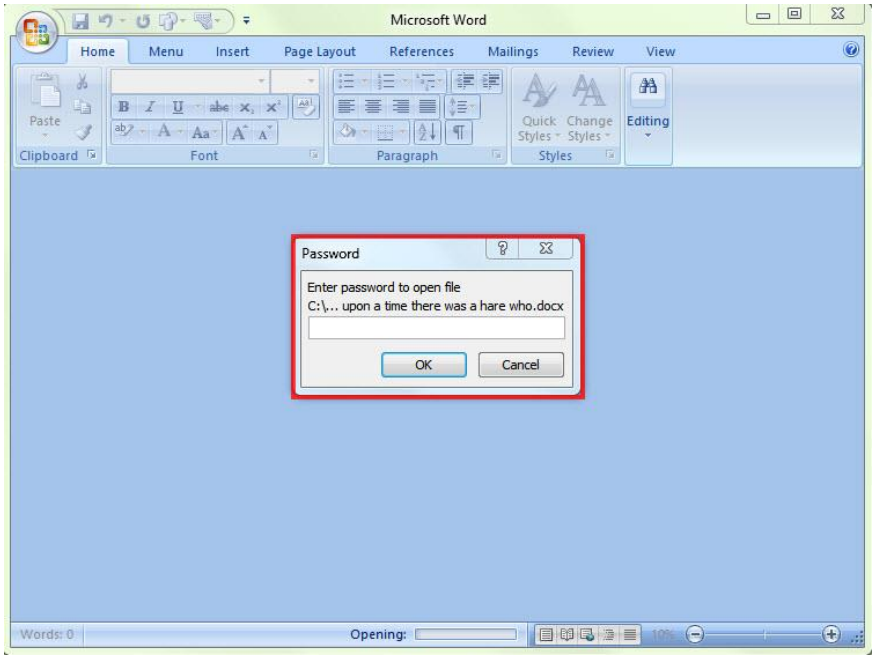
3.1 Introduction

Microsoft Word 2007 can be useful for personal and business applications. You can create letters, flyers, mailing labels, greeting cards and documents of numerous types quickly and easily. Word 2007 also allows you to create passwords for opening and for editing your documents. There are occasions where you may need to remove those passwords, however, and that can be challenging if you don't know how. See Step 1 below for more information on how to remove passwords from Microsoft Word 2007 without destroying the text of the document in question.

Step 1

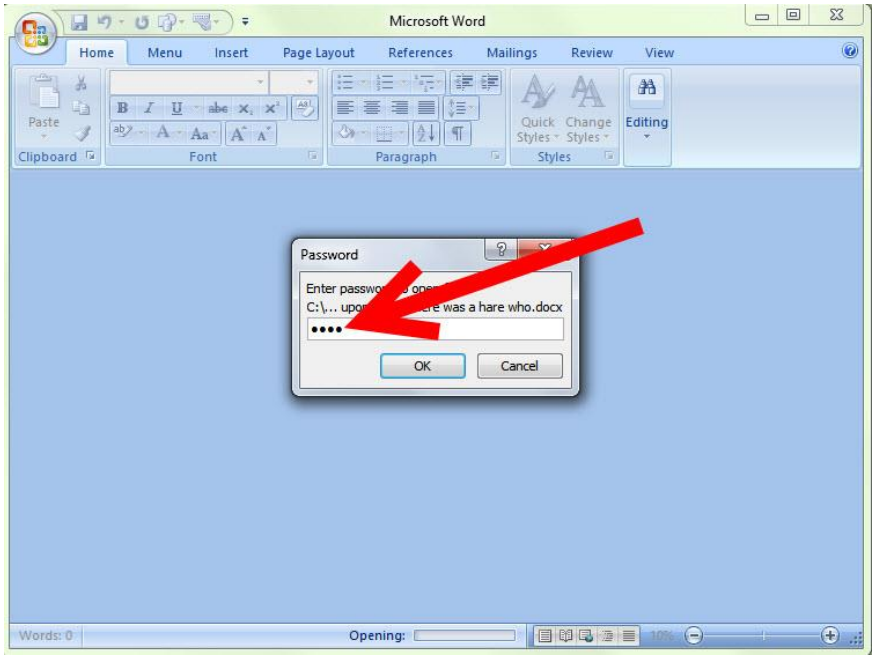


Step 2



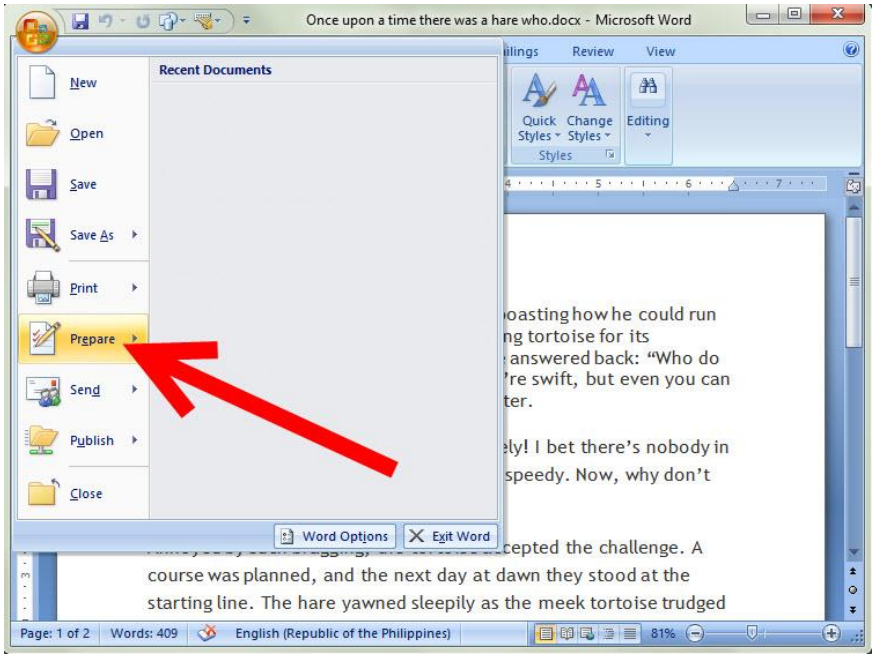
Attempt to open the document that has password protection.

Step 3

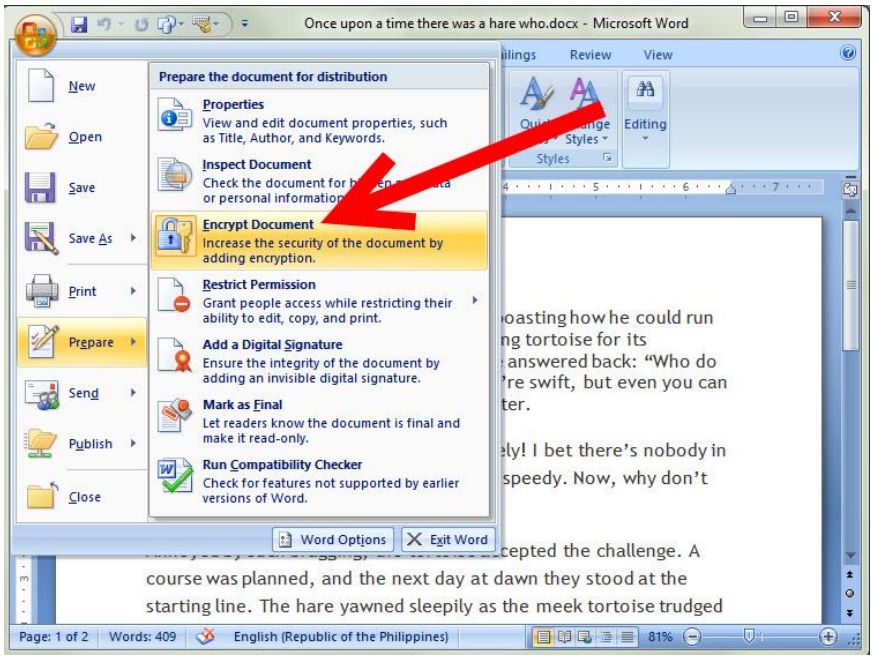


Enter the password to open the document if prompted.

You may need to recreate the file if you have forgotten your password.

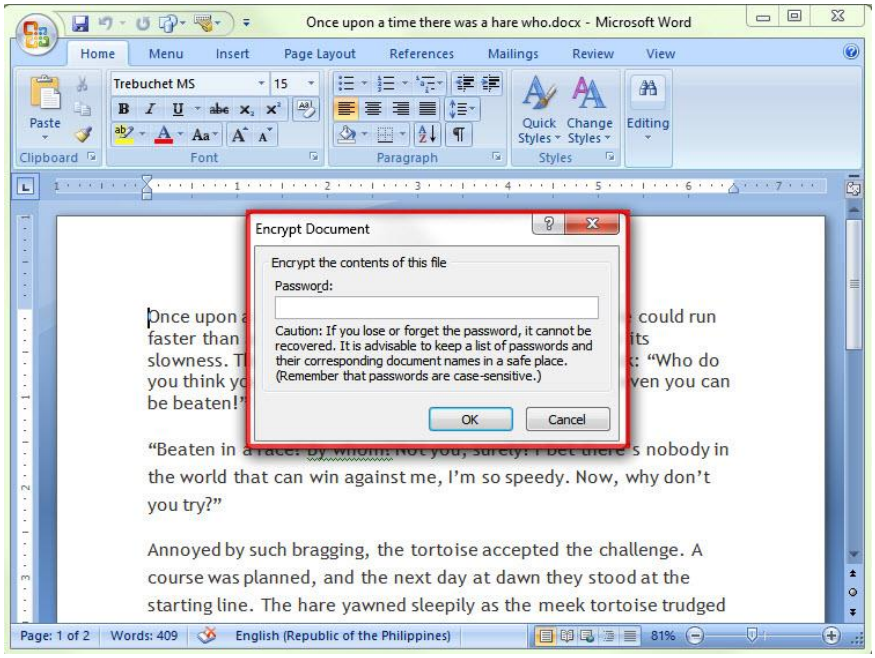


Step 4 Click the Office button in the upper left corner of the window and mouse over the "Prepare" option.

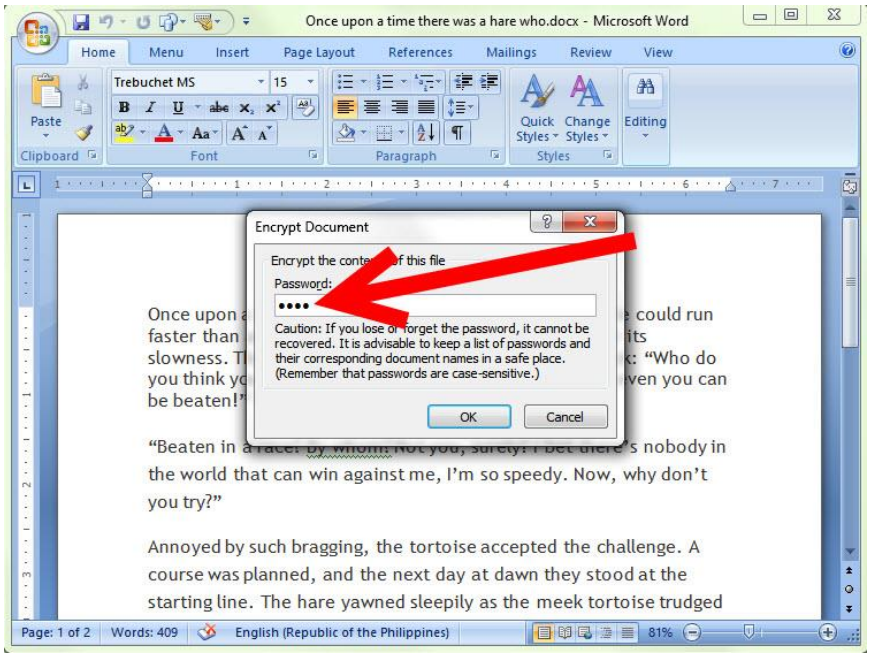


Step 5 Select "Encrypt document" from the slide-out menu.

- An encrypted document cannot be opened without supplying the password.

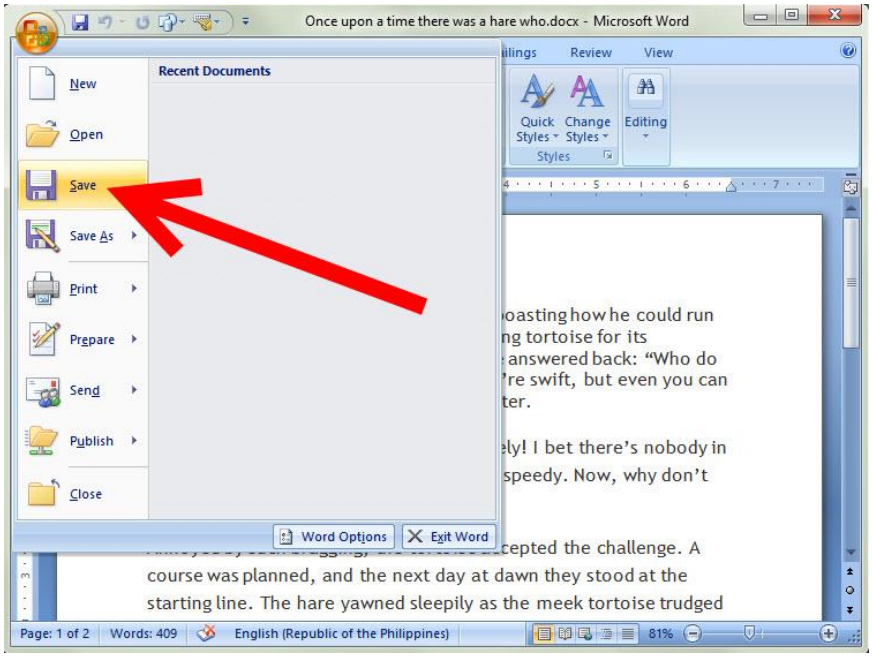


A password protection window will pop up with asterisks where the password was entered.



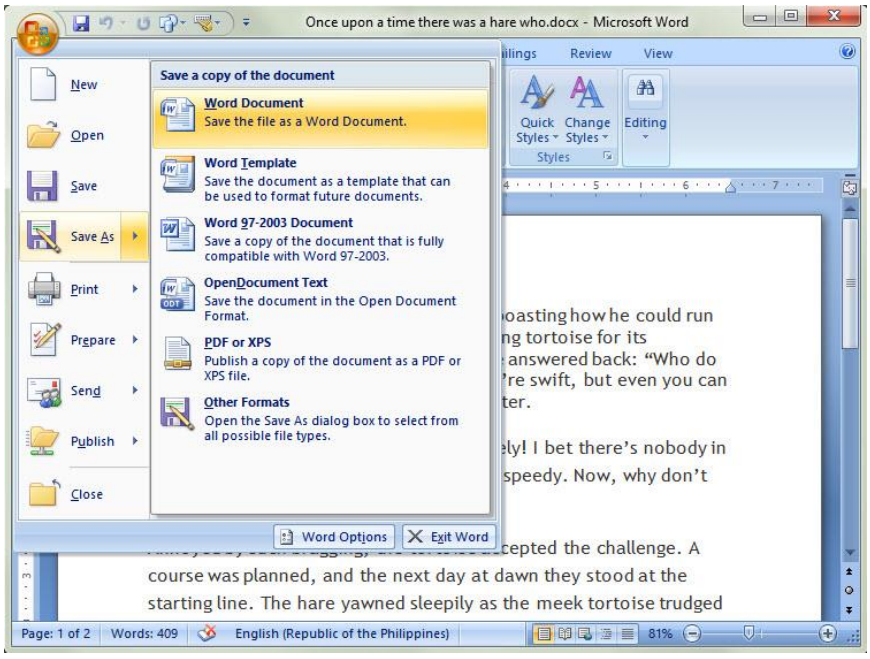
Step 6 Clear the password field and then click "OK."

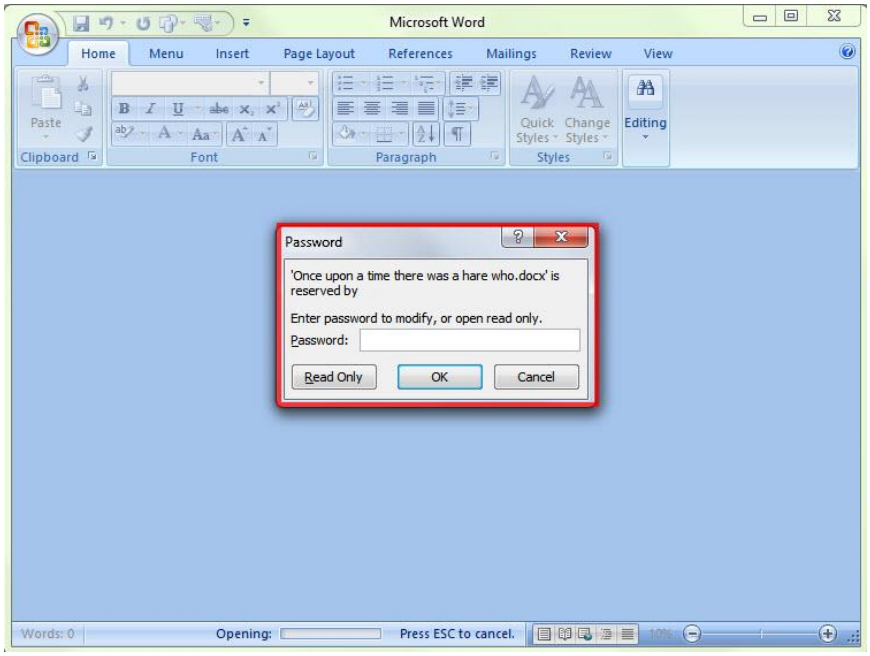
This will remove the encryption.



Step 7 Save the document.

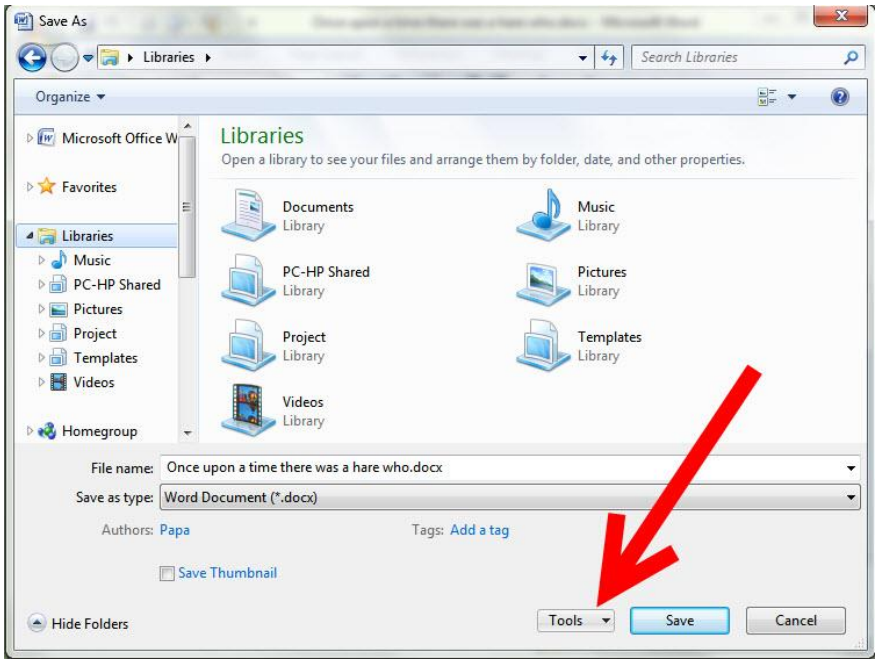
- If you want to keep the original document with password protection, choose "Save As" and enter a new name for your document.



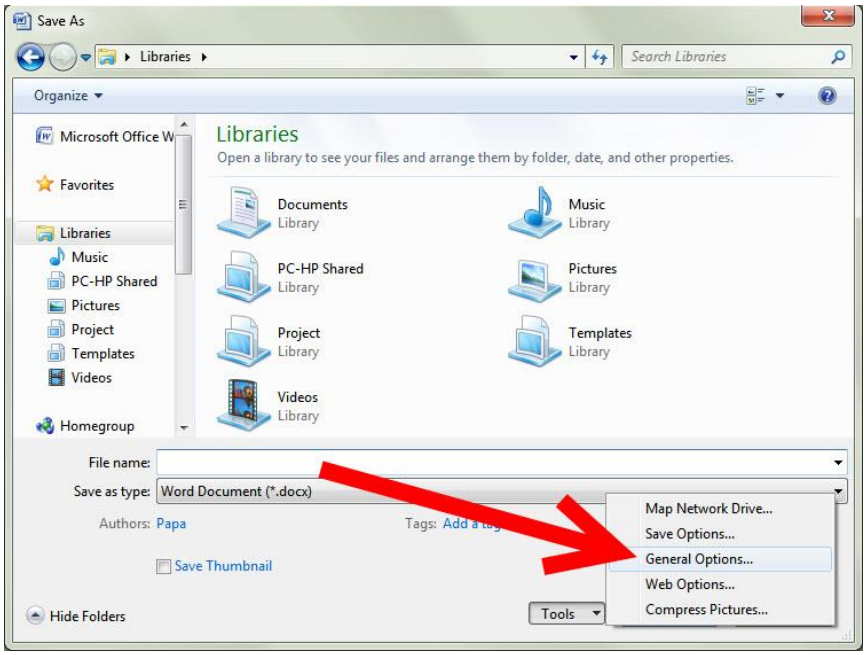


Step 8 Remove the password required to edit the document.

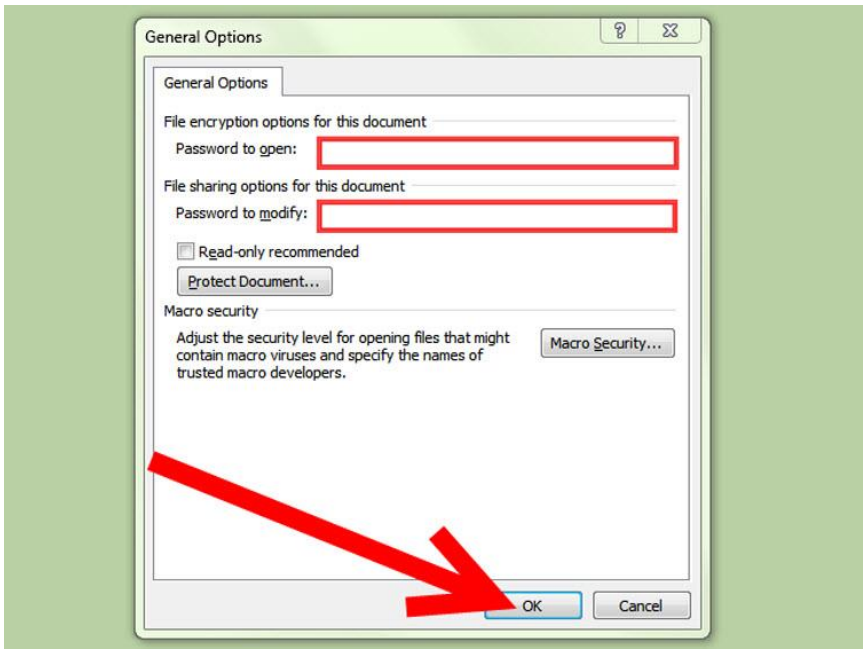
- Password protection against editing a document only prevents users from saving the document with the same name and overwriting the original text.
- Click the "Tools" link from the save window and then select the "Save As" menu, which is at the bottom of the document.

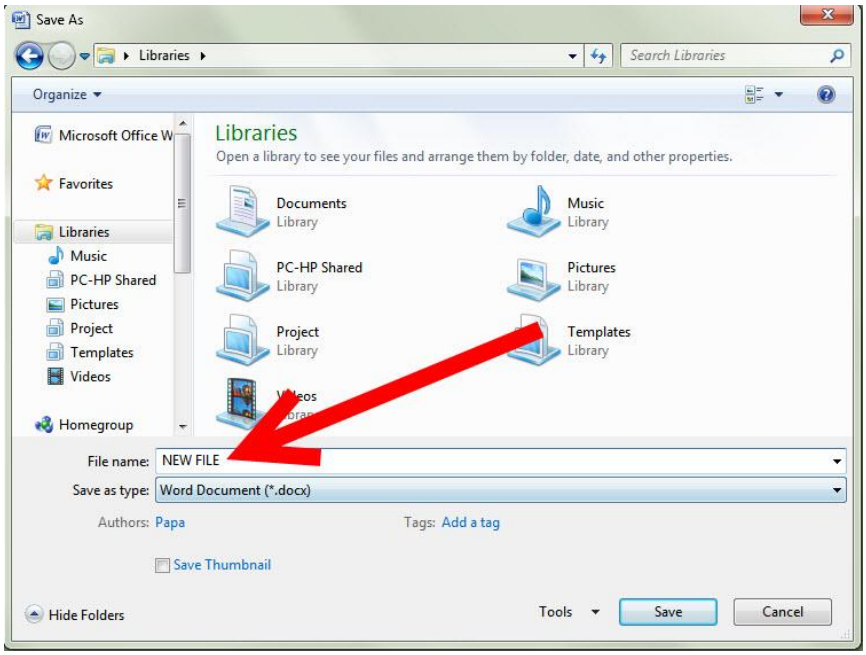


- Choose "General Options" from the menu.



- Clear the passwords from all fields here and then click the "OK" button to close the window.





Step 9 Enter a new file name if you want to preserve the original document with modified password protection and then click the "Save" button.

EXPERIMENT-4

Aim: To study various methods of protecting and securing databases.

4.0 Learning Objective

After going through this unit, you will be able to:

- Be familiar with any database environment like MySQL or Oracle etc.
- Know different techniques of protecting a database.
- Note the security majors to protect the database.

4.1 Introduction

You don't have to go far to find out how important database security is. For instance, Target is still reeling from their systems being hacked, exposing the credit card information of many of their customers. It's the kind of harm that requires a lot of time, money, and resources for damage control, as well as the aftermath of breaking the trust in the company and diverting resources toward making sure it doesn't happen again.

Ensuring the security of your company's information is important, and even some of the biggest businesses can expose themselves to hackers exploiting security flaws. The information in your company's databases are important, so it stands to reason that database security is too.

Here are five things you can do to keep your company and customer information safe and secure.

4.2 Have secure passwords.

The most sophisticated systems on Earth can't protect against a bad password. There are the typical culprits — 12345, ABCDE, anything else on the most guessed password list — but hackers have increasingly sophisticated tools at their disposal that makes many other passwords increasingly vulnerable. Now, it's not just making your password "password" that you have to worry about. It can be words in-and-of themselves. Programs exist that guess passwords that might be words in the dictionary or commonly used phrases, so those are out.

You can try to make a combination of letters, numbers and symbols to throw off would-be hackers. You can check your password here to see how long it

would take hackers to guess it. Business Bee has also rated some password management tools that may be able to help you.

One other suggestion is to set rules that make employees change passwords on a revolving basis. If a password isn't changed after 90 days, lock out that account pending administrator approval to make sure that an old password isn't a hacker's way in.

4.3 Encrypt your database.

Just as important as the passwords is the encryption of your database. Encryption means converting your data to a format such that, were it to be intercepted, would seem like a string of letters and numbers with no tangible meaning. But to the database program, it all easily converts to the data you want. But it ties back into passwords. A Yahoo! hack in 2012 exposed more than 400,000 passwords in plain text to the web at large. This meant open access to emails and passwords, and the need for a whole lot of users who put their faith in Yahoo! to change their passwords. Here, too, you don't want to be the company at the other end of that controversy. Make sure that your database is encrypted with up-to-date encryption software.

4.4 Don't show people the backdoor?

It is a simple way to protect your database. Leave it out of sight. This means keeping it hidden from search engine results through the robots.txt file, and also not linking to it directly. While you want employees to have access to database information, you may not want to put the log-in directly on the site. If you have an online database, do yourself a favour and keep it on a need-to-know basis. After all, the first step toward hacking a database is finding it in the first place.

4.5 Segment your database.

A wide open database is a wide open vulnerability. You'll want to segment your data to make sure that not just anyone sees everything. In many systems, various roles can be created within the database.

For instance, you might want to have users, super users, administrators, and super administrators. Users can access or input basic information, but not alter information beyond what they've put in, whereas a superuser has computer permissions that allow wider access to data without being able to change everything. An administrator can work above all of these users, altering the structure of the database or having access to more sensitive information, while a super administrator can run the whole operation. For the upper tiers, you'll want to keep the number of people with those

clearances low, such as managers or department heads. This ensure that, should a password be exposed on the site, it's not devastating if it's only someone with access to basic information on the site.

4.6. Monitor and audit your database.

One way to prevent database breaches is to keep an eye on the database itself. Monitoring access and behaviors of database users can help you ensure that no odd behaviors are exhibited that might imply a leak. Checking unfamiliar IP addresses can ensure that no one has an employee password who shouldn't. Think of it like when you get a call from the bank asking you to confirm a transaction. Your address is in New York, but your card is being used in Calgary. It's a red flag to bank security, and the same thing should be a red flag to your business.

In addition, regular audits of your database help find inactive accounts, helping eliminate problems that might arise with someone obtaining old employee information. Perform regular audits, and your company can tighten up security before problems arise.

4.7 Database security categories

The configuration categories shown in Figure below are based on best practices obtained from field experience, customer validation, and the study of secure deployments. The rationale behind the categories is as follows:

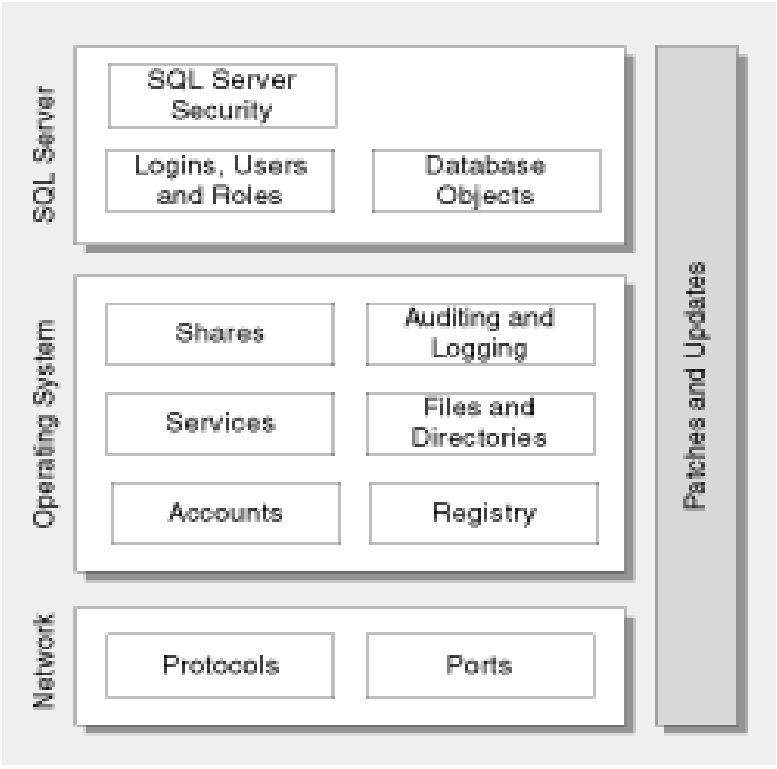


Fig- Categories of Database Security

- **Patches and Updates**

  Many security threats exist because of vulnerabilities in operating systems, services, and applications that are widely published and well known. When new vulnerabilities are discovered, attack code is frequently posted on Internet bulletin boards within hours of the first successful attack. Patching and updating your server's software is the first step toward securing your database server. There may be cases where vulnerability exists and no patch is available. In these cases, be aware of the details of the vulnerability to assess the risk of attack and take measures accordingly.

- **Services**

  Services are prime vulnerability points for attackers who can exploit the privileges and capabilities of the service to access the server and potentially other computers. Some services are designed to run with privileged accounts. If these services are compromised, the attacker can perform privileged operations. By default, database servers generally do not need all services enabled. By disabling unnecessary and unused services, you quickly and easily reduce the attack surface area.

- **Protocols**

  Limit the range of protocols that client computers can use to connect to the database server and make sure you can secure those protocols.

- **Accounts**

  Restrict the number of Windows accounts accessible from the database server to the necessary set of service and user accounts. Use least privileged accounts with strong passwords in all cases. A least privileged account used to run SQL Server limits the capabilities of an attacker who compromises SQL Server and manages to execute operating system commands.

- **Files and Directories**

  Use NTFS file system permissions to protect program, database, and log files from unauthorized access. When you use access control lists (ACLs) in conjunction with Windows auditing, you can detect when suspicious or unauthorized activity occurs.

Shares

Remove all unnecessary file shares, including the default administration shares if they are not required. Secure any remaining shares with restricted NTFS permissions. Although shares may not be directly exposed to the Internet, a defense in depth strategy with limited and secured shares reduces risk if a server is compromised.

- **Ports**

  Unused ports are closed at the firewall, but it is required that servers behind the firewall also block or restrict ports based on their usage. For a dedicated SQL Server, block all ports except for the necessary SQL Server port and the ports required for authentication.

- **Registry**

  SQL Server maintains a number of security-related settings, including the configured authentication mode in the registry. Restrict and control access to the registry to prevent the unauthorized update of configuration settings, for example, to loosen security on the database server.

- **Auditing and Logging**

  Auditing is a vital aid in identifying intruders, attacks in progress, and to diagnose attack footprints. Configure a minimum level of auditing for the database server using a combination of Windows and SQL Server auditing features.

- **SQL Server Security**

  A number of SQL Server security settings can be controlled through Enterprise Manager. These include the authentication mode, auditing level, and the accounts used to run the SQL Server service. For improved security, you should use Windows authentication. You should also enable SQL Server logon auditing and ensure that the SQL Server service runs using a least privileged account.

- **SQL Server Logins, Users, and Roles**

  SQL Server 2000 manages access control using logins, databases, users, and roles. Users (and applications) are granted access to SQL Server by way of a SQL server login. The login is associated with a database user and the database user is placed in one or more roles. The permissions granted to the role determine the tables the login

can access and the types of operations the login can perform. This approach is used to create least privileged database accounts that have the minimum set of permissions necessary to allow them to perform their legitimate functionality.

- **SQL Server Database Objects**

  The ability to access SQL Server database objects, such as built-in stored procedures, extended stored procedures and **cmdExec** jobs, should be reviewed. Also, any sample databases should be deleted.

EXPERIMENT-5

Aim: To study "How to make strong passwords" and "passwords cracking techniques".

5.0 Learning Objective

After going through this unit, you will be able to:

- Generate secure passwords
- Apply password manager to generate secure password
- Point out various features of different password managers

5.1 How to Generate Secure Password

5.1.1 Guideline for setting secure Password

Choosing the right password is something that many people find difficult, there are so many things that require passwords these days that remembering them all can be a real problem. Perhaps because of this a lot of people choose their passwords very badly. The simple tips below are intended to assist you in choosing a good password.

Basics

- Use at least eight characters, the more characters the better really, but most people will find anything more than about 15 characters difficult to remember.
- Use a random mixture of characters, upper and lower case, numbers, punctuation, spaces and symbols.
- Don't use a word found in a dictionary, English or foreign.
- Never use the same password twice.

Things to avoid

- Don't just add a single digit or symbol before or after a word. e.g. "apple1"
- Don't double up a single word. e.g. "appleapple"
- Don't simply reverse a word. e.g. "elppa"
- Don't just remove the vowels. e.g. "ppl"
- Key sequences that can easily be repeated. e.g. "qwerty","asdf" etc.
- Don't just garble letters, e.g. converting **e** to **3**, **L** or **i** to **1**, **o** to **0**. as in "z3r0-10v3"

Tips

- Choose a password that you can remember so that you don't need to keep looking it up, this reduces the chance of somebody discovering where you have written it down.
- Choose a password that you can type quickly, this reduces the chance of somebody discovering your password by looking over your shoulder.

Bad Passwords

- Don't use passwords based on personal information such as: name, nickname, birthdate, wife's name, pet's name, friends name, home town, phone number, social security number, car registration number, address etc. This includes using just part of your name, or part of your birthdate.
- Don't use passwords based on things located near you. Passwords such as "computer", "monitor", "keyboard", "telephone", "printer", etc. are useless.
- Don't ever be tempted to use one of those oh so common passwords that are easy to remember but offer no security at all. e.g. "password", "letmein".
- Never use a password based on your username, account name, computer name or email address.

Choosing a password

- Use good password generator software.
- Use the first letter of each word from a line of a song or poem.
- Alternate between one consonant and one or two vowels to produce nonsense words. eg. "taupouti".
- Choose two short words and concatenate them together with a punctuation or symbol character between the words. eg. "seat%tree"

Changing your password

- You should change your password regularly, I suggest once a month is reasonable for most purposes.
- You should also change your password whenever you suspect that somebody knows it, or even that they may guess it, perhaps they stood behind you while you typed it in.
- Remember, don't re-use a password.

Protecting your password

- Never store your password on your computer except in an encrypted form. Note that the password cache that comes with windows (.pwl files) is NOT secure, so whenever windows prompts you to "Save password" don't.
- Don't tell **anyone** your password, not even your system administrator
- Never send your password via email or other unsecured channel
- Yes, write your password down but don't leave the paper lying around, lock the paper away somewhere, preferably off-site and definitely under lock and key.
- Be very careful when entering your password with somebody else in the same room.

Remembering your password

Remembering passwords is always difficult and because of this many people are tempted to write them down on bits of paper. As mentioned above this is a very bad idea. So what can you do?

- Use a secure password manager, see the downloads page for a list of a few that won't cost you anything.
- Use a text file encrypted with a strong encryption utility.
- Choose passwords that you find easier to remember.

Bad Examples

- "fred8" - Based on the user's name, also too short.
- "christine" - The name of the users girlfriend, easy to guess
- "kciredref" - The users name backwords
- "indescribable" - Listed in a dictionary
- "iNdesCribaBle" - Just adding random capitalisation doesn't make it safe.
- "gandalf" - Listed in word lists
- "zeolite" - Listed in a geological dictionary
- "qwertyuiop" - Listed in word lists
- "merde!" - Listed in a foreign language dictionary

Good Examples

None of these good examples are actually good passwords, that's because they've been published here and everybody knows them now, always choose your own password don't just use somebody elses.

- "mItWdOtW4Me" - **M**onday **i**s **t**he **w**orst **d**ay **o**f **t**he **w**eek **f**or **me**.

5.2 Password cracking techniques

There are a number of techniques that can be used to crack passwords. We will describe the most commonly used ones below;

Dictionary attack– This method involves the use of a wordlist to compare against user passwords.

Brute force attack– This method is similar to the dictionary attack. Brute force attacks use algorithms that combine alpha-numeric characters and symbols to come up with passwords for the attack. For example, a password of the value “password” can also be tried as p@$$word using the brute force attack.

Rainbow table attack– This method uses pre-computed hashes. Let’s assume that we have database which stores passwords as md5 hashes. We can create another database that has md5 hashes of commonly used passwords. We can then compare the password hash we have against the stored hashes in the database. If a match is found then we have the password.

Guess– As the name suggests, this method involves guessing. Passwords such as QWERTY, password, admin etc. are commonly used or set as default passwords. If they have not been changed or if the user is careless when selecting passwords, then they can be easily compromised.

Spidering– Most organizations use passwords that contain company information. This information can be found on company websites, social media such as facebook, twitter etc. Spidering gathers information from these sources to come up with word lists. The word list is then used to perform dictionary and brute force attacks.

Spidering sample dictionary attack wordlist

1976 <founder birth year>
smith jones <founder name>
acme <company name/initials>
built|to|last <words in company vision/mission>
golfing|chess|soccer <founders hobbies

EXPERIMENT-6

Aim: To study the steps to hack a strong password**.**

6.0 Learning Objective

At the end of the session you will be able to

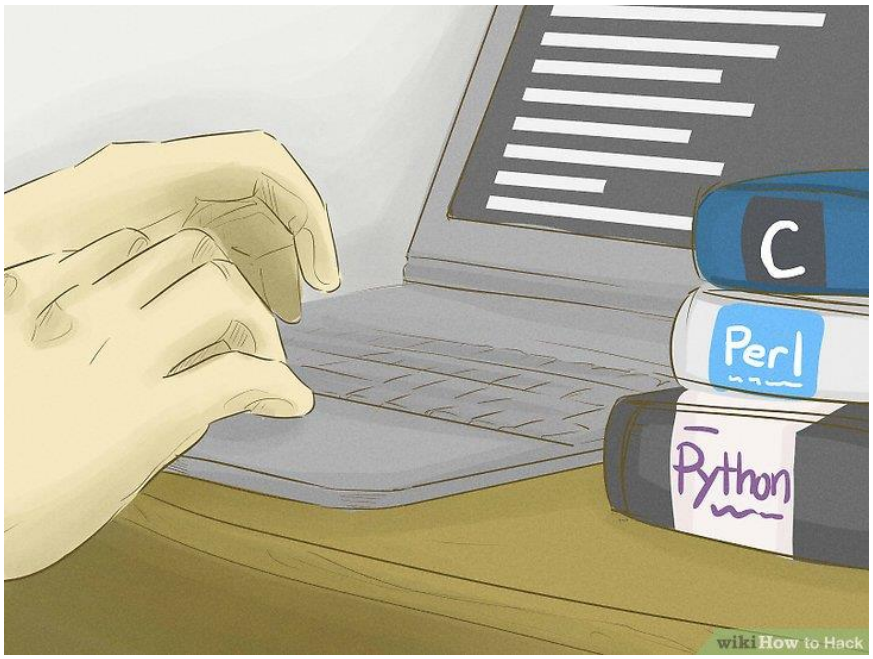
- Know how to hack a simple or a strong password.
- Know the different types of hacking process and type of applications.

6.1 Introduction

Primarily, hacking was used in the "good old days" for leaking information about systems and IT in general. In recent years, thanks to a few villain actors, hacking has taken on dark connotations. Conversely, many corporations employ hackers to test the strengths and weaknesses of their own systems. These hackers know when to stop, and the positive trust they build earns them a large salary.

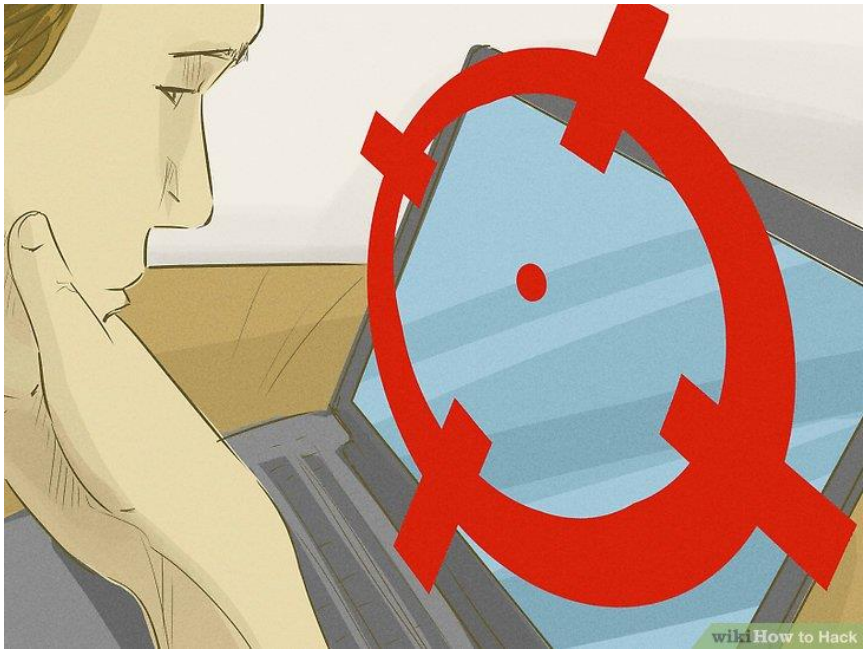
If you're ready to dive in and learn the art, this article will share a few tips to help you get started!

Before You Hack



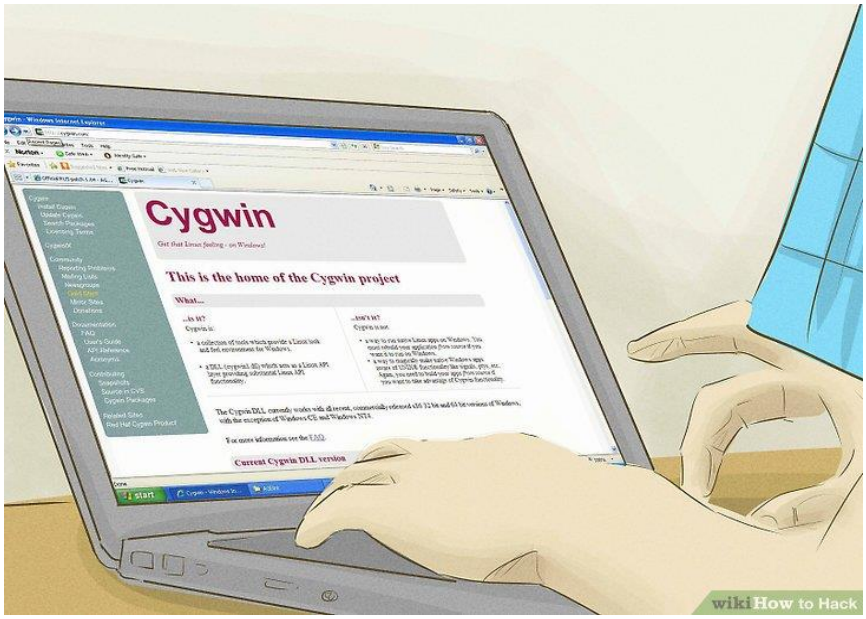
1 Learn a programming language. You shouldn't limit yourself to any particular language, but there are a few guidelines.

- C is the language that UNIX was built with. It (along with assembly language) teaches something that's very important in hacking: how memory works.
- Python or Ruby are high-level, powerful scripting languages that can be used to automate various tasks.
- Perl is a reasonable choice in this field as well, while PHP is worth learning because the majority of web applications use PHP.
- Bash scripting is a must. That is how to easily manipulate Unix/Linux systems—writing scripts, which will do most of the job for you.
- Assembly language is a must-know. It is the basic language that your processor understands, and there are multiple variations of it. You can't truly exploit a program if you don't know assembly.



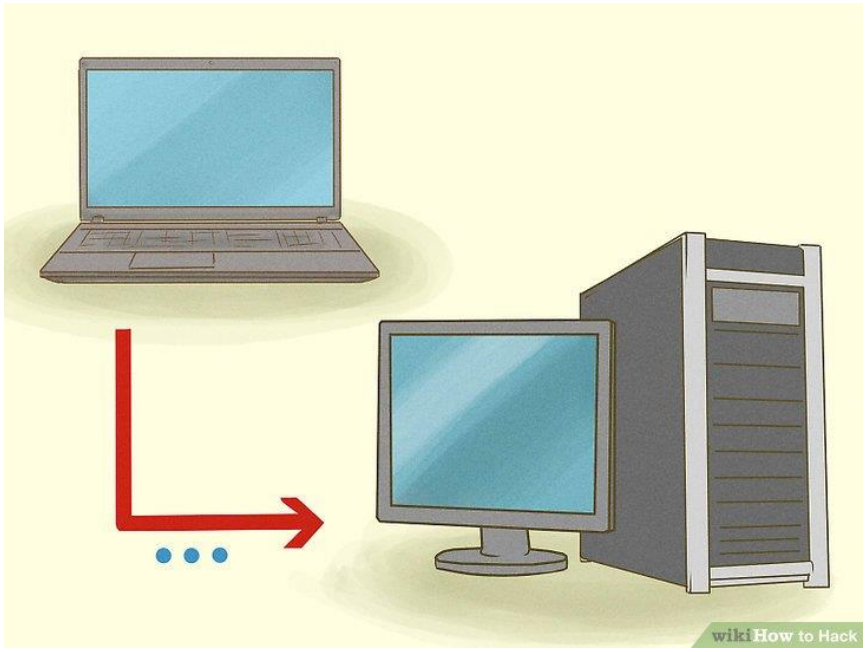
2. **Know your target.** The process of gathering information about your target is known as *enumeration*. The more you know in advance, the fewer surprises you'll have.

Hacking

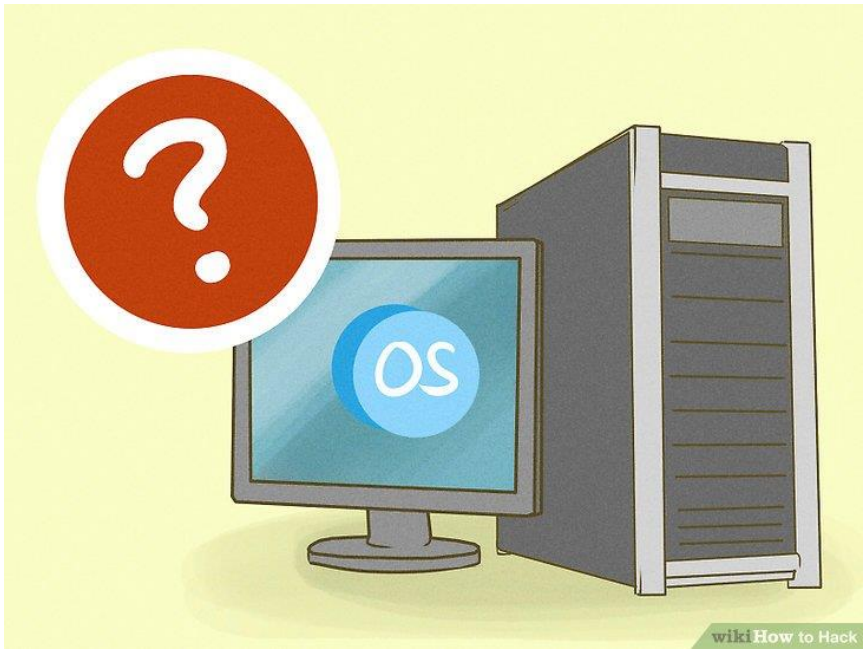


1. **Use a *nix terminal for commands.** Cygwin will help emulate a *nix for Windows users. Nmap in particular uses WinPCap to run on Windows and does not require Cygwin. However, Nmap works poorly on Windows systems due to a lack of raw sockets. You should also consider using Linux or BSD, which are both more flexible. Most Linux distributions come with many useful tools pre-installed.

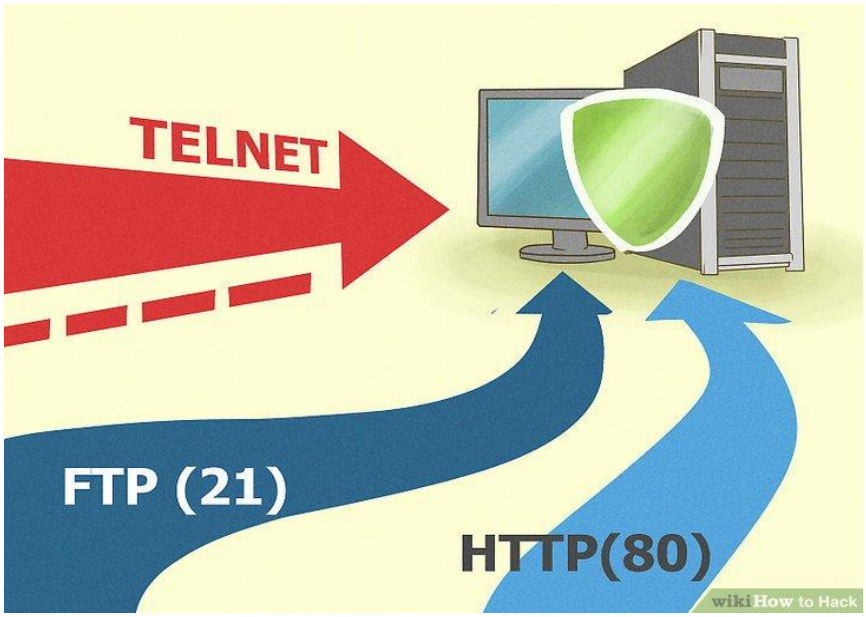
2. **Secure your machine first.** Make sure you've fully understood all common techniques to protect yourself. Start with the basics — but make sure you have authorization to attack your target: attack your own network, ask for written permission, or set up your own laboratory with virtual machines. Attacking a system, no matter its content, is illegal and WILL get you in trouble.



3. **Test the target.** Can you reach the remote system? While you can use the ping utility (which is included in most operating systems) to see if the target is active, you cannot always trust the results — it relies on the ICMP protocol, which can be easily shut off by paranoid system administrators.



4. **Determine the operating system (OS).** Run a scan of the ports, and try pOf, or nmap to run a port scan. This will show you the ports that are open on the machine, the OS, and can even tell you what type of firewall or router they are using so you can plan a course of action. You can activate OS detection in nmap by using the -O switch.



5. **Find a path or open port in the system.** Common ports such as FTP (21) and HTTP (80) are often well protected, and possibly only vulnerable to exploits yet to be discovered.

- Try other TCP and UDP ports that may have been forgotten, such as Telnet and various UDP ports left open for LAN gaming.
- An open port 22 is usually evidence of an SSH (secure shell) service running on the target, which can sometimes be brute forced.

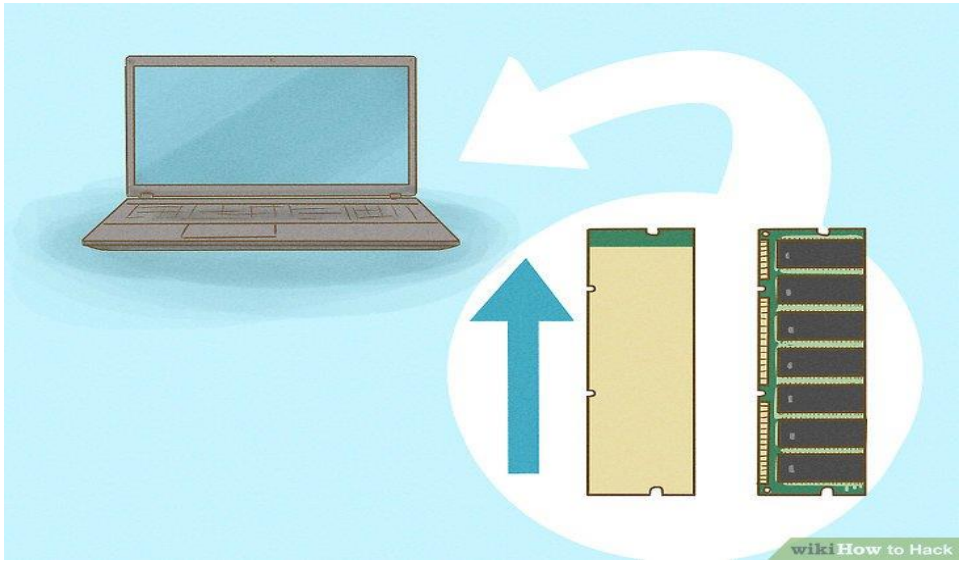
6. **Crack the password or authentication process.** There are several methods for cracking a password, including brute force. Using brute force on a password is an effort to try every possible password contained within a pre-defined dictionary of brute force software

- Users are often discouraged from using weak passwords, so brute force may take a lot of time. However, there have been major improvements in brute-force techniques.
- Most hashing algorithms are weak, and you can significantly improve the cracking speed by exploiting these weaknesses (like you can cut the MD5 algorithm in 1/4, which will give huge speed boost).
- Newer techniques use the graphics card as another processor — and it's thousands of times faster.
- You may try using Rainbow Tables for the fastest password cracking. Notice that password cracking is a good technique only if you already have the hash of password.
- Trying every possible password while logging to remote machine is not a good idea, as it's easily detected by intrusion detection systems, pollutes system logs, and may take years to complete.
- You can also get a rooted tablet, install a TCP scan, and get a signal upload it to the secure site. Then the IP address will open causing the password to appear on your proxy.
- It's often much easier to find another way into a system than cracking the password.

7. Get *super-user* privileges. Try to get root privileges if targeting a *nix machine, or administrator privileges if taking on Windows systems.

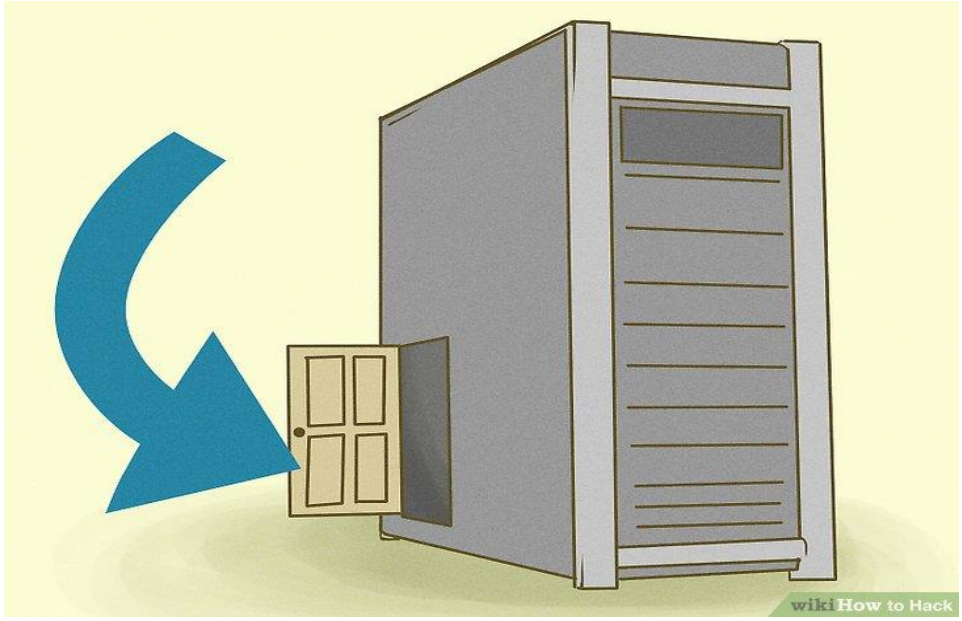
- Most information that will be of vital interest is protected and you need a certain level of authentication to get it. To see all the files on a computer you need super-user privileges - a user account that is given the same privileges as the "root" user in Linux and BSD operating systems.
- For routers this is the "admin" account by default (unless it has been changed); for Windows, this is the Administrator account.

- Gaining access to a connection doesn't mean you can access everything. Only a super-user, the administrator account, or the root account can do this.

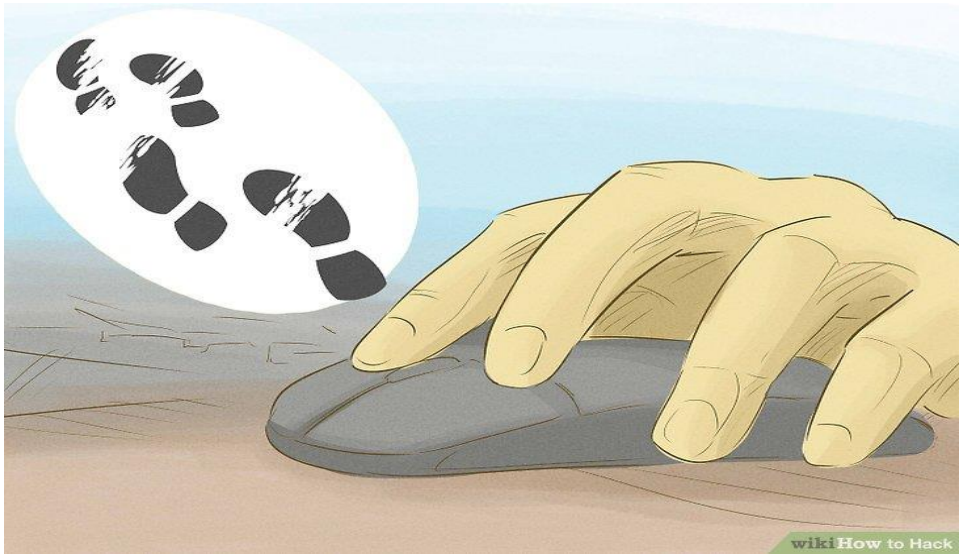


8. **Use various tricks.** Often, to gain super-user status you have to use tactics such as creating a *buffer overflow*, which causes the memory to dump and that allows you to inject a code or perform a task at a higher level than you're normally authorized.

- In Unix-like systems this will happen if the bugged software has setuid bit set, so the program will be executed as a different user (super-user for example).
- Only by writing or finding an insecure program that you can execute on their machine will allow you to do this.



9. **Create a backdoor.** Once you have gained full control over a machine, it's a good idea to make sure you can come back again. This can be done by *backdooring* an important system service, such as the SSH server. However, your backdoor may be removed during the next system upgrade. A really experienced hacker would backdoor the compiler itself, so every compiled software would be a potential way to come back.



10. **Cover your tracks.** Don't let the administrator know that the system is compromised. Don't change the website (if any), and don't create more files than you really need. Do not create any additional users. Act as quickly as possible. If you patched a server like SSHD, make sure it has your secret password hard-coded. If someone tries to login with this password, the server should let them in, but shouldn't contain any crucial information.

References:

1. http://www.wikihow.com
2. https://www.wikipedia.org